УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Аца С. Алексић

# СТАТИСТИЧКИ МОДЕЛ АУТОМАТИЗОВАНОГ УПРАВЉАЊА ДИГИТАЛНИМ СЕРТИФИКАТИМА

докторска дисертација

Београд, 2012.

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Aca S. Aleksić

# STATISTICS MODEL OF AUTOMATED MANAGEMENT OF DIGITAL CERTIFICATES

Doctoral Dissertation

Belgrade, 2012

Ментор:

**Др Зоран Радојичић,**
ванредни професор Факултета организационих наука у Београду

Чланови комисије:

**др Братислав Петровић,**
редовни професор Факултета организациних наука у Београду

**др Драган Вукумировић,**
редовни професор Факултета организациних наука у Београду

**др Душан Старчевић,**
редовни професор Факултета организациних наука у Београду

**др Вељко Милутиновић,**
редовни професор Електротехничког факултета у Београду

Датум одбране: _____

Датум промоције: _____

# *Статистички модел аутоматизованог управљања дигиталним сертификатима*

*Апстракт:* У оквиру ове докторске дисертације, под развојем дигиталних сертификата подразумева се увођење концепта инфраструкутре јавних кључева PKI (*PKI - Public Key Infrustructure*) система, које обједињује мноштво елемената и појава из домена рачунарске статистике, информационо – комуникационих технологија и електронског пословања.

Стратешка важност примене концепта дигиталних сертификата и његова недовољна развијеност у електронском пословању Републике Србије,указује на потребу постављања теориске подршке његовог ефикасног развоја и примене.У том смислу,предмет истраживања ове дисертације представља унапређење развоја и увођења дигиталних сертификата, који су усмерени на изградњу одређене инфраструктуре јавних кључева - PKI система, који треба да буде дизајниран тако да буде ефикасан и флексибилан у циљу лаког решавања различитих PKI захтева.

Изградња информационог система базира се на статистичкој анализи ефикасности примене PKI система и дигиталних сертификата. Основни циљеви су да, на основу статистичких метода и анализе доступних реалних података из процеса PKI система, је могуће препознати латентне параметре система, чија би адекватна идентификација и примена квалитативно допринела побољшању процеса управљања дигиталним сертификатима PKI система у електронском пословању и извршити аутоматизацију кључних процеса управљања дигиталним сертификатима одабраног PKI система, путем статистичких метода, са циљем да се обједине у одговарајући статистички модел.

Експерментални део докторске дисертације односи се на апликациони модел, који представља примену дигиталних сертификата, где су дефинисне активности које имају стратешку улогу у унапређењу електронског пословања, одређивању степена значаја активности и мерења ефекта његове примене. На оваквом апликативно модулу уз примену статистчких анализа дошли смо до циљне архитектуре PKI система, који је дао најбоље резулате у практичној примени савременим пословним окружењима.

За равој дигиталних сертификата пресудне су информације, јер пружају податке на основу којих корисници електронских сервиса,доносе ефикасније и ефективније одлуке и самим тим повећавају степен задовољства живота.

*Кључне речи*: дигитални сертификат, дигитални потпис, криптографија, информационо-комуникационе технологије, електронски документ, електронско пословање, статистичка контрола процеса.

*Научна област:* Информациони системи

*Ужа научна област:* Рачунарска статистика

*Statistical model of automated management of digital certificates*

*Abstract:* In this dissertation, the development of digital certification involves the introduction of the concept of PKI (*Public Key Infrastructure*) system, which incorporates many elements and phenomena in the field of computational statistics, information - communication technologies and electronic commerce.

The strategic importance of applying the concept of digital certificates and its underdevelopment in electronic commerce of Serbia, points to the need of setting Theoretical support for its efficient development and implementation. In this sense, the subject of this dissertation is to improve the development and deployment of digital certificates, which are focused on building specific Public Key Infrastructure - PKI system, which should be designed to be efficient and flexible solution to light of different PKI requirements.

Construction of an information system based on statistical analysis of the effectiveness of PKI and digital certificates. The analysis is to define the business needs of PKI in accordance with the development of electronic services, using modern methods for static evaluation. The main objectives are that, based on statistical methods and analysis of real data available from the process of PKI, it is possible to identify latent system parameters, which would be adequate identification and application of quality management processes contribute to the improvement of PKI digital certificates in electronic commerce and make the automation of key management processes PKI digital certificates of the selected system, using statistical methods, in order to integrate the appropriate statistical model.

The experimental part of a doctoral dissertation relates to the application model, which is the use of digital certificates, which are defined activities that have a strategic role in promoting e-business, determining the degree of importance of activities and measuring its effectiveness. In this module, using applicative statistical analysis we came to the target architecture PKI system, which gave the best results in the practical application of modern business environments.

For the development of digital certificates is critical information because they provide information on which users of electronic services, making more efficient and effective decisions and therefore increase the level of satisfaction with life.

*Key words:* digital certificates, digital signatures, cryptography, information and communication technology, electronic documents, electronic commerce, statistical process control.

*Academic Expertise:* Information Systems

*Special Topics:* Computational Statistics

# САДРЖАЈ

**СПИСАК СЛИКА**

**СПИСАК ТАБЕЛА**

**СПИСАК ГРАФИКОНА**

# 1. УВОД

## 1.1. Опис проблема

Миграција рачунарских окружења ка дистрибуираним, мрежним решењима радикално је променила начин на који компаније реализују пословање. Електронска трговина (e-commerce) и електронско пословање (e-business) постали су стварност и компаније могу сада пословати користећи електронску размену пословних докумената на глобалном нивоу без посебних тешкоћа. Многе организације су унапредили своје рачунарске мреже и целу комуникациону инфраструктуру у циљу искоришћења свих предности нових система, остварујући бенефиције на основу ниске цене Интернета и његових карактеристика глобалности. [Otuteye E.,2002.]

Поред предности, електронска трговина, као и свако решење базирано на отвореним рачунарским мрежама и електронским документима, доноси и нове опасности по интегритет пословног процеса. Овај елеменат има негативан утицај на ширење електронског пословања, јер сва корист која се оствари применом електронске размене може бити елиминисана уколико се не обезбеди адекватна заштита пословног процеса. Ова констатација се посебно односи на критичне апликације као што су финансије, процеси уговарања, пословне тајне, планирање и развој и сл. Стога је стални предмет научног истраживања, развој нових безбедносних система који су намењени да елиминишу наведене ризике и пруже квалитетнију заштиту од оне која је својствена пословању преко папира.

У системима са традиционалном организацијом, мере безбедности су се базирале на ограничавању неауторизованог приступа информацијама и заштићеним деловима система. Међутим, овај модел није погодан за дистрибуирано окружење као што је Интернет – који има основну карактеристику да омогућује отворену и што доступнију комуникацију уз примену заштите свих стандардних интернет пословних апликација. [Brian Komar, 2004]

Безбедност корпорацијских података је од изузетног значаја за сваки пословни систем. Информације, интелектуална својина, документација, садржај, мреже, подаци о запосленима и корисницима се могу сматрати делом кључних добара дате корпорације. Сваки од ових елемената треба да буде брижљиво чуван у циљу обезбеђења да пословне тајне једне организације остану поверљиве, што пружа додатне компаративне предности на тржишту.

Криптографски механизми представљају најраспрострањенији начин за остваривање безбедности у отвореним системима и мрежама. У последње време је дефинисан широк дијапазон нових система за заштиту Интернет система, и у

већини се користе криптографски механизми заштите. Ове технологије се примењују за различите системе електронске размене као што су заштићено слање порука, заштићени e-mail сервис, системи електронског плаћања, заштита софтверских апликација и мрежних комуникација.

### 1.2. Осврт на релевантне библиографске изворе и остварене резултате који су у вези с предметом истраживања

Последњих година вршена су интезивна истраживања из области која је заснована на анализи дигиталних сертификата и његовим специфичном појавном облику, везаном за реализацију инфраструктуре система са јавним кључевима PKI система (*PKI – Public Key Infrastructure*). PKI систем је информациони систем за заштиту података и мрежних ресурса који се базира на технологији јавних криптографских кључева и принципима асиметричне криптографије.

Кључни елемената сваког PKI система, је сертификационо тело CA (*CA – Certification_Authority*) које има задатак да издаје дигиталне сертификате, како интерним службеницима, тако и спољашњим корисницима система, што ће омогућило брже увођење електронског пословања у компанијама у складу са Законом о електронском пословању и електронском потпису, као и у складу са европском и светском законском регулативом у овој области.

Да би се ефикасно управљало сертификатима, потребно је мерити (пратити) употребу сертификата, а пре свега дигиталних, ради постизања већег степена заштите система којим управља сертификационо тело. Мерење као сам процес представља проблем, посебно у реалним условима када се суочавамо са разним утицајима који ометају квалитетно мерење. Процес креирања квалитетне мере и учење из добијених резултата, представља основни и суштински циљ самог процеса.[Радојичић З., 2001].Током целог живота човек непрестано врши мерења које се одвијају у његовој средини, са мање или више успеха, па управо из тих разлога можемо претпоставити следеће ставове: [Zigon, J.,1995;Zigon, J., 1998;Zigon, J.,1999.]

- "Не можеш управљати појавама које не можеш измерити"
- "Не можеш унапредити стање ако га не можеш измерити"
- "Успех захтева јасан циљ, циљ који је мерљив"
- "Захтев за успешним решењем захтева успостављање метрике"

Статистичко мерење базира се на самој природи статистике. Статистика као наука бави се истраживањима масовних појава. Процес статистичког мерења обухвата методе снимања (прикупљања) и обраде посматраних појава. Као

резултат њихове примене добијамо бројчане информације о посматраним појавама. Да би се понашање једне масовне појаве у целини снимило, потребно је обухватити њене манифестације и посматрати све случајеве на које се она испољава како би се квантитативном анализом уоченог варијабилитета утврдиле њене основне карактеристике. [Радојичић З., 2007.]

Проблеми који се јављају приликом статичког мерења представљају врло комплексну област. За успешно и ефикасно мерење потребно је из популације са одређеним карактеристиком изабрати одговарајући узорак, који ће моћи ефикасно да репрезентује популацију која се посматра. На основу резултата извршених мерења врши се статистичко закључивање.

Изградња статистичког модела за управљање и аутоматизацију употребе дигиталних сертификата је кључни корак ка успостављању контроле над системом дигиталних сертификата.

Развој Интернет технологија, Web сервиса и система сигурности и заштите, као и све шира примена дигиталних документа, обезбедили су подршку све напреднијим начинима и могућностима електронског пословања. У новије време, дистрибуирани системи и системи који се ослањају на интернет чине основу пословања све већег броја предузећа и организација. Све чешће се примењују веома комплексни портали и интегрисани дистрибуирани системи пословања. Осим тога, системска подршка у савременим оперативним системима и различитим системима базе података, трансакциони сервери и системи олакшава и убрзава развој електронског пословања. [Плесконић Д, Мацек Н, Ђорђевић Б, Царић М., 2007.]

Претње по безбедности података, односно информација које се на основу њих добијају, јесу бројне и морају бити идентификоване пре него што се приступи пројектовању система заштите. Све претње са собом носе ризик који мора бити измерен и којим се мора управљати да би се одржао на адекватном нивоу, јер је његово потпуно уклањање у стално променљивим условима пословања немогуће. На претње по сигурност одговара се различитим мерама заштите, у зависности од природе саме претње. [Костић М., 2006.]

Примена квалитативних система за заштиту у системима електронске трговине и електронског пословања нуди нове видове пословних апликација и ефикаснију реализацију пословања. Међународни односи снабдевача и корисника су сада лако остварив, а безбедносни механизми омогућавају елементе поверења који су неопходни да заштите све фазе у трговини и комуникацијама. Правна регулатива у вези електронског потписа је донета, тако да су избегнуте евентуалне правне дилеме и проблеми, и има основни циљ да обезбеди услове које треба да испуне пословни субјекти, да би се електронски потпис у електронском пословању правно изједначио са својеручним потписом у стандардном пословању.[Закон о електронском потпису, Службени гласници Републике Србије, 2004.]

Научна подршка - примени дигиталних сертификата у сервисима електронске трговине и електронског пословања није довољно обрађена. Стратешка важност овог концепта указује на потребу сталне доградње теоријске подршке која је потребна за његов ефикасан развој и примену. У том смислу је и представљен предмет истраживања ове дисертације, базиран је на развијању подршке у облику изградње статистичког модела аутоматизације управљања PKI система у пракси и његовог специфичног облика, везаног за електронска пословања окружења.

У докторској дисертацији размотрене су: активности и системи које је потребно применити и развити, како би се дигитални сертификати приближили корисницима услуга, повећањем ефикасности, ефективности и квалитета рада и функционисања. Да би се постигли наведени резултати статистика заузима једно од кључних места у систему тј. она представља "науку и уметност развоја и примене метода прикупљања, укрштања и интерпретације квантитативних података у смислу да се варљивост закључака и оцењивања може проценити помоћу индуктивног закључивања базираног на математичкој вероватноћи". [Anderson R.L., Bancroft T.A., 1952.]

Развој PKI система огледа се:у развоју нових апликативних услуга са заштитом, усмерених на потребе корисника, у подизању нивоа свести циљаних група, и повећања задовољства корисника.

Инфраструктура система са јавним кључевима (*PKI – Public Key Infrastructure*) омогућује амбијент за поуздану примену електронског пословања и он се најчешће базира на комбинованој примени асиметричних и симетричних шифарских система. PKI инфраструктура се састоји од више компонената, апликација, и докумената за рад, који дефинишу начин реализације четири основне криптографске функције у електронском пословању:[Gardiner B.,2003.]

- заштита тајности – реализује се симетричним криптографским системима,
- аутентичност - примена асиметричних шифарских система и специјализованих протокола,
- интегритет - примена асиметричних шифарских система кроз технике дигиталног потписа и дигиталних цертификата,
- непорецивост трансакција – примена асиметричних шифарских система(дигитални потпис). [McCullagh A., Caelli W.,2000]

Док се функције заштите тајности и интегритета могу реализовати и применом традиционалних симетричних техника, функције аутентичности и непорецивости трансакција захтевају примену софистицираних система – PKI система. Најбоље карактеристике показују системи у којима су реализоване све поменуте четири функције. PKI системи обезбеђују поуздан метод за реализацију

функција провере аутентичности и непорицања трансакција који је базиран на прецизно утврђеној политици рада. PKI системи су брзо постали кључна карика свих система електронске трговине и корпорацијске безбедности и сигурно ће доминирати у безбедносном системима будућности. [Adams C., Lloyd S., 2003.]

Услед сложености и стратешке важности PKI у електронском пословању, предмет докторске дисертацује представља сложен и мултидициплинаран задатак. Он задире у области примене принципа моделовања, савремених статистичких метода и информационо комуникационих технологија, с намером да се исте обједине у анализи и сагледавању оптерећеност система који користе дигиталне сертификате, као и управљање истим.

Област криптографије јавним кључем високо је стандардизована. Развој примене дигиталних сертификата незамењив је без PCI DSS (*PCI DSS -Payment card industry data security Standard*) инфраструктуру и без развоја CA инфраструктуре и протокола размене кључева. *[Public Key Infrastructure: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings]*.

То омогућује да се данас користећи PCI DSS инфраструктуру развијате скалабилно и динамично окружење које ће бити адаптивно апликативним потребама у циљном пословном амбијенту савременог пословања.[John R. V., 2004.]

Основа за разматрање проблема развоја и унапређења PKI инфраструктуре налазе се у актуелним стандардизованим техникама криптографије са јавним кључем, те њеним предностима и ограничењима у пословном окружењу.[Schneier B., 1996.]

Статистичке методе индуктивног и дедуктивног закључивања, омогућавају научну обраду статистичких података и доношење закључака на бази истих. Ова два метода омогућавају да се дају одговори на постављена питања, тј. да се на основу измерених резултата, донесе закључак и о ономе што није измерено. [Вуковић Н., 2000.]

Услед сложености и стратешке важности доношења одлука у систему електронског пословања, посебно у домену размене информација путем Web сервиса, сва истраживања рађена су на постављању теоријске поставке и детаљног описа процеса који одређују проблеме управљања PKI системима у организацијама пословних корпорација, нарочито у специфичним околностима када је тренутна доступност конкретних садржаја изузетно битна. Зато је, истраживање базирано на утврђивању и дефинисању чињеница, на основу статистичких мерења, које су показале неоспорно повећање перформанси PKI система применом квалитетног управљања дигиталним сертификатима у електронском пословању.

Почетна истраживања у докторској дисертацији, базирана су на анализи проблема управљања садржајем у процесима PKI система, применом постојећих информационо – комуникационих технологија. Коришћење предности савремених информационо-комуникационих достигнућа и Web сервиса као комуникационог механизма у области управљања садржајем у пословним процесима, без предрасуда везаних за њихову безбедност, постала је интересна оријентација сваке организације, а посебно у компанијама, које желе да повећају ефикасност својих функционалних процеса и при томе значајно побољшају правовремено и исправно одлучивање, успешно и ефикасно извођење свих операција.

### 1.3. Циљ докторске дисертације

Циљ докторске дисертације је унапређење развоја и увођења дигиталних сертификата, који су усмерени на изградњу одређеног PKI система, који треба да буде дизајниран тако да буде ефикасан и флексибилан у циљу лаког решавања различитих PKI захтева. У ова обележја су укључени:

- Вишеструки системи за регистрацију и доставу сертификата и кључева – потребно је да дати PKI систем подржава различите механизме регистрације и доставе PKI параметара, укључујући: е-маил сервис, web комуникацију, личну доставу, VPN и друго.
- Подршка различитим безбедносним модулима: HSM (*HSM - Hardware Security Module*) као и малим хардверским модулима (токенима) и смарт картицама за ефикасно генерисање дигиталног потписа, [Gisela M., 2002.]
- Подршка примени различитих криптографских алгоритама, како јавних, тако и приватних алгоритама дефинисаних од стране специјализованих дизајнера или самих корисника система,
- Вишеструки системи публикације издатих и повучених сертификата који укључују различите екстерне сервисе (LDAP i X.500), као и публикацију на хард диск у циљу олакшавања интерне публикације, [Boeyen S., Howes T., Richard P.,1999.]
- Подршка различитим методама провере валидности (повучености) дигиталних сертификата, као што су CRL (*CRL-Certificate Revocation List*), CRL дистрибуционе тачке и OCSP (*OCSP - Online Certificate Status Protocol*), DOSCP (*Distributed OCSP*),
- Подршка комплексним PKI хијерархијама – PKI систем мора подржати хијерархију сертификационих тела (Root CA и структура Intermediate CA било које дубине), вишеструка регистрациона тела (RA), вишеструке

операторе RA, и мора подржати процедуру међу-сертификације са другим CA,

- Подршка вишеструким кључевима и сертификатима по кориснику – политика рада PKI система, и самог Сертификационог тела (CA), треба да предвиди коришћење вишеструких кључева и сертификата по кориснику, а да се коришћење ових кључева тако конфигурише да се одвојени кључеви користе за дигитално потписивање и за шифровање (у оквиру дигиталне енвелопе),
- Систем треба да подржи флексибилни ауторизациони процес – сваки захтев за издавањем сертификата може бити ауторизован од стране једне или више овлашћених особа, што треба дефинисати у политици рада CA. Додатно, систем треба да омогући да се захтеви за издавање сертификата процесирају и аутоматски, без потребе за применом специфичне процедуре ауторизације, и
- Отвореност система у циљу евентуалних захтева за интероперабилношћу, PKI систем мора задовољавати особину да се базира на отвореним стандардима, од којих је најважнији X.509v3 стандард за формат дигиталног сертификата као и каснији стандарди за конкретну примену и Интернет пословном амбијенту.[RFC 3280.,2002; RFC 3447.,2003; RFC 3739.,2004.]

Циљ рада је изградња модела који се базира на статистичкој анализи ефикасности примене PKI система и дигиталних сертификата. Анализа представља дефинисање потребе пословања PKI у складу са развојем електронских услуга, применом савремених статичких метода ради мерења постигнутих резултата.

Савремена схватања статистике су она схватања која статистичке методе интерпретирају као моделе где спадају математичко-статистички модели података, њихова веза и структура тј. статистика је моделирање података. Са таквог становишта долази се до концептуализације "статистичких услова" и стварних података где се статистика третира као аналитички модел за обраду података.

Приступ истраживања, базиран на постављању апликативног модела примене активности дигиталних сертификата. Апликативни модел је дефинисао активности које имају стратешку улогу у унапређењу електронских пословања, одређивању степена значаја активности и мерењу ефеката њихове примене. На овако постављеном моделу уз примену статистичке анализе дошло до циљне архитектуре PKI система која даје најбоље резултате у практичној примени у савременим пословним окружењима.

### 1.4. Полазне хипотезе

За рачунарство дигиталних сертификата, пресудне су информације, јер пружају податке на основу којих корисници електронских сервиса, доносе ефикасније и ефективније одлуке, и самим тим повећавају степен задовољства живота.

Дигитални сертификати треба да учине своје пословање ближе корисницима електронских сервиса, да утичу на модернизацију и побољшање квалитета услуга, на побољшање ефикасности, транспаретности и ефективности рада.

Основна хипотеза овог истраживања је да на основу статистичких метода и анализа доступних реалних података из процеса PKI система могуће је препознати латентне параметре система, чија би адекватна идентификација и примена квалитативно допринела побољшању процеса управљања дигиталним сертификатима PKI система у електронском пословању. Другим речима, могуће је извршити аутоматизацију кључних процеса управљања дигиталним сертификатима одабраног PKI система, путем статистичких метода, са циљем да се обједине у одговарајући статистички модел.

Остале хипотезе овог истраживања:

1. Подршка различитим политикама рада PKI система

PKI систем мора омогућити подршку за примену различитих безбедносних политика крајњег корисника. Ове политике утичу на формат и екстензије које се користе у дигиталним сертификатима и које се конфигуришу применом алата едитора безбедносне политике (*security policy editor*). Политике могу такође да садрже информације о пословној регистрацији које се не појављују у самом сертификату али су сакупљене и безбедно сачуване за време регистрационог процеса.

2. Безбедност система

С обзиром да CA представља централни део PKI система са најважнијим циљем да успостави тачку поверења читавог система, основни захтев који се поставља пред читавим системом је највиша безбедност самог CA. Наиме, ако је CA компромитовано (ако је тајни кључ асиметричног шифарског система CA компромитован) било интерним или екстерним нападом, и читав PKI систем је компромитован. Из тих разлога, CA и читав PKI систем је потребно заштитити на највишем нивоу.

3. Скалабилност

Комерцијално доступни PKI системи су скалабилно дизајнирани тако да се крећу од малих конфигурација које раде на једном PC рачунару на коме су реализоване апликације CA, RA и неопходне базе података до великих

инсталација система. У великим инсталацијама система, постоје вишеструка RA са више оператора, организована као подређени чиниоци вишеструком хијерархијском систему CA, који су под јурисдикцијом једног "Root CA" система.

Као друга веома значајна особина, PKI систем мора подржати евентуално проширивање система додавањем одређених модула без потребе заустављања рада система. Другим речима, ако се дата организација проширује, или ако се захтеви за PKI технологијом повећавају, све се то може решити додавањем одговарајућих специфичних PKI модула.

Предности система увођења дигиталних сертификата огледају се у следећем:

- брзо и ефикасно деловање у циљу аутоматизованог прикупљања података, праћења и приказ ситуације, одлучивања, правовремене реализација одлуке и доношења практичних решења,
- повећање управљачких и безбедносних перформанси PKI апликација које користе софтверске и хардверске криптографске механизме, што редукује трошкове и повећава ниво контроле,
- могућност коришћења дигиталних сертификата од стране великог броја корисника истовремено, применом Web сервиса.

### 1.5. Научне методе истраживања

У току рада на дисертацији коришћења су сазнања из стручне литературе (домаће и стране књиге и часописи), веб сајтова и веб претраживача доступних на Интернету, као и информационе комуникационе технологије у области електронског пословања.

У овом истраживању су примењене:

- Методе емпиријског истраживања
- Метод посматрања
- Статистичке методе
- Компаративне методе
- Мерење

Методе логичког објашњења:

- Методе анализе и синтезе
- Индуктивно и дедуктивно закључивање.

### 1.6. Резултати докторске дисертације

Истраживањем, предмета докторске дисертације, започето је испитивањем релевантне литературе и остварених резултата у домену дигиталних сертификата који се односи на примену PKI система у електронском пословању. Након теоријског, спроведено је емпириско истрживање ради утврђивање степена развоја и примене електронских сертификата.

Научни значај се огледа у систематизацији сазнања до којих се дошло анализом електронског пословања применом дигиталних сертификата, као и могућности формулисања и спровођења активности ради унапређења електронских сервиса. Потреба за применом дигиталних сертификата се огледа у интензивном развоју све већем електронских услуга у електронском пословању и потреби да се тај процес заштити од спољашњих злоупотреба.

Пошто у домаћој литератури још увек ова област није у довољној мери заступљена , зато је детаљно обрађена и систематизована теориска и практична примена дигиталних сертификата у PKI системима, што посебно чини стручни допринос овог рада.Експериментални део докторске дисертације односи се на имплементацију предложеног система, које укључује следеће главне активности: анализу пословних процеса и имплементацију апликативног решења. Имплементација PKI система са дигиталним сертификатима довела је до побољшања квалитета и заштите електронских сервиса, а тиме и до низа технолошких, функционалних дугорочних економских предности, као што су безбедно управљање документима и записима у електронском пословању.

Од изузетне важности је примена статистичке мултиварицоне метдологије на прецизним, мерљивм, нумеричким критеријумима за оцењивање и *мерење постигнутих резултата*. На прктичним примерима студије случаја приказани су резултати почетног стања и резултати након имплементације.

Спроведена методологија статистичке стратегије управљања дигиталним сертификатима, представља разумевање процеса статистичког закључивања у изградњи, анализирању и интерпретирању употребе, са становишта аутоматизације PKI система.

### 1.7. Структура рада

Ова докторска дисертација се састоји од девет поглавља, списка референци и прилога, укључујући већи број илустрација и табела на укупно 216 страна.

Други поглавље разматра општи аспект функционисања инфраструктуре јавних кључева - PKI ( *PKI - Public Key Infrustructure*) који је комплексан систем, који се састоји од: Криптографских технологија, протокола, стандарда, политика, процедура, сервиса и апликација. PKI систем представља основу за примену решења заштите електронских података, којим се обезбеђује тајност података, аутентитификација, интегритет, и непорицивост. Основни концепт на коме се заснива PKI систем је асиметрична криптографија или криптографија јавних криптографских кључева (Public Key Cryptography).

У трећем делу дисертације су најважније компоненте PKI система: сертификационо тело – CA (*CA- Certification Authority*), регистрационо тело - RA (*RA- Registration Authority*), јавни именик (*PublicDirectory*) и корисничке апликације. Сертификационо тело извршава следеће послове: Издавање, обнављање, суспендовање и опозивање дигиталних сертификата (*digital certificate*) конфигурисање различитих врста, животног циклуса и других параметра цертификата, објављивање опозваних сертификата – CRL( *CRL-(Certificate Revocation List*), узајамна сертификација са другим сертификационим телима и друго. Регистрационо тело представља спону између корисника који постављају захтеве за издавањем сертификата и сертификационог тела. Послови регистрационог тела су: прихватање захтева корисника за издавањем сертификата, проверавање идентитета корисника и прикупљање потребних података и посредовање захтева корисника за издавањем сертификата ка сертификационом телу. Јавни именик је локација на којој се чувају дигитални сертификати, тј јавни криптографски кључеви за шифровање и верификовање потписаних докумената. Посредством јавних именика PKI систем обезбеђује дистрибуцију сертификата корисницима. Корисничке апликације омогућавају корисницима да употребом дигиталних сертификата врше шифровање/дешифровање докумената и потписивање/версификовање потписаних докумената.

У четвртом делу дисертације описане су активности симетричне и асиметричне криптографије и образложено коришћење криптографских кључева приликом шифровања/дешифровања докумената и приликом потписивања/версификовања потписаних докумената. Осим тога представљени су различити начини за размену јавних криптографских кључева по дигиталних сертификата. Наиме у оквиру сертификата се налазе јавни криптографски кључеви, тако да се разменом сертификата размењују јавни криптографски кључеви. Зато је најбољи начин за успешну реализацију PKI система, иницирање пилот – пројекта, који ће брзо, релативно, јефтино и аргументовано да покаже предности и евентуалне недостатке у постојећој пракси.

У петом делу приказане су статистичке методе у функцији изградње статистичког модела ради спровођења процеса аутоматизације управљања. На основу методе статистичког закључивања, индуктивног и дедуктивног, модел

омогућава научну обраду статистичких података и доношење закључака на бази таквих података. Статистички модел омогућава да се дају одговори на деловање система, тј. да се на основу измерених резултата, донесе закључак и о ономе што није измерено, те спроведе понашање система у правцу заштите од неауторизованог приступа. Ради изналажења одговарајућих анализа, ради изградње модела, коришћене су методе експлораторне анализе, методе мултиваријационе анализе и дата мининг-а. Правилна примена модела је хеуристичко питање, као што је важан избор теорија, хипотеза, метода индикатора и других елемената научног истраживања. С тога статистичка анализа третира се као моделирање података тј. њихових латентних својстава и односа.

Добра теоријска основа изведена је из формалних аксиома јер само у том случају представља потпун дедуктивни систем, а својства која предвиђа могу се израчунати. То је правило свих формалних система и оно не подразумева да је теоријски модел тачан. Тачност таквих модела проверава се било кроз анализу унутрашње усаглашености, било кроз анализу усаглашености са реалним светом. За анализу усаглашености са реалним светом постављене су емпиријске хипотезе које се проверавају помоћу података – где се статистика намеће као инструмент.

Статистичка контрола процеса је метода за прикупљање и анализу података у циљу решавања практичних проблема контроле квалитета. Статистичка контрола процеса своди се на графичко приказивање узорака у облику контролних тачака на контролној карти, са границама које су претходно одређене.

Шест Сигма је организован и систематичан метод, за стратешко унапређење пословних процеса (као и развој нових производа и услуга), који се конципира на статистичким методама и константно смањује број дефектних производа/услуга. Програми континуалног побољшавања као што је Шест Сигма (Сих Сигма) се најчешће имплементирају на два нивоа – кроз пројекат и кроз организацију. Суштина Шест Сигма пројеката је смањивање варијансе процеса. Конкретно, Шест Сигма тежи редукцији и контроли варијансе процеса у тој мери да иако излаз варира до ±6σ, он је у потпуности повинован доњој и горњој граници спецификације. Шест Сигма програми успостављају иницијативу за континуално побољшање перформанси организационих система – раст ефикасности и модификовање процеса у складу за жељама наших клијената.

Дискриминациона анализа једана је од често коришћених алата у статистици. Она се заснива на креирању модела који омогућује да се одреди модел који нам за вредности интервалних променљивих (задатих атрибута неке појаве) одреди припадност групи. Да би се добио добар модел, који је представљен дискриминационом функцијом, потребно је да улазни подаци садрже поред вредности атрибута и припадност групи.

Са техничке стране основни циљ дискриминационе анализе је формирање линеарних комбинација независних променљивих којима ће се дискримнација

између унапред дефинисаних група тако извршити да грешка погрешне класификације опсервација буде минимизирана, или другачије речено, да се максимизира релативан однос варијанси између и унутар група. Линарном комбинацијом независних променљивих за сваког испитаника или објекат одредимо број, дискриминациони скор, који се затим трансформише у апостериорну вероватноћу да испитаник или објекат потиче из једне од група.

У шестом делу дисертације представљено и описано је, емпиријско истраживање о примени дигиталних сертификата. Основу истраживања чини апликативни модел презентован програм који омогућује упоредни преглед резултата добијених применом класичног и новог приступа дискриминационој анализи.

У седмом делу докторске дисертације у студији примера, извршена је анализа, излазних резултата који су добијени применом технике SOFT COMPUTING–а, који пружају бољи увид у посматрану појаву, јер у анализи су укључене и логичке комбинације атрибута, а не само атрибути, као што то чини класичан приступ.

На крају је дат закључак рада са одговором на питања у вези са постављеним циљем и хипотезама. Дата је систематизација и преглед научних доприноса који су проистекли из рада на докторској дисертацији, скуп отворених проблема и могућности за даљи рад у области докторске дисертације.

Литература садржи релевантну литературу која је коришћена приликом израде докторске дисертације.

Докторска дисертација детаљно приказује досадашња истраживања и сазнања из области дигиталних сертификата. Описани су елементи који чине инфраструктуру ситема јавних кључева. Реализовано је апликативно решење које представља примере примене дигиталних сертификата за реализацију електронских сервиса у електронском пословању.

# 2. СИСТЕМИ СА ЈАВНИМ КЉУЧЕВИМА

Инфраструктура система са јавним кључевима (*PKI – Public Key Infrastructure*) ствара услове за поуздану примену елекронског пословања. Он се најчешће базира на комбинованој примени асиметричних и симетричних шифарских система. PKI инфраструктура се састоји од више компонената, апликација и докумената који дефинишу начин реализације четири основне криптографске функције у електронском пословању:[ Gardiner B., 2003.]

- заштита тајности – реализује се симетричним криптографским системима,
- аутентичност – асиметрични шифарски системи,
- интегритет - асиметрични шифарски системи, и
- непорецивост трансакција - асиметрични шифарски системи.

Док се функције заштите тајности и интегритета могу реализовати и применом традиционалних симетричних техника, функције аутентичности и непорецивости трансакција захтевају примену софистицираних система – PKI система. Најбоље карактеристике показују системи у којима су реализоване поменуте четири функције. PKI системи обезбеђују поуздан метод за реализацију функција провере аутентичности и непорицања трансакција који је базиран на прецизно утврђеној политици рада. PKI системи су брзо постали кључна карика свих система електронске трговине и корпорацијске безбедности и, и као такви, сигурно ће доминирати у безбедносним системима будућности. [Adams C., Lloyd S., 2003.]

Основни функционални захтеви које треба да испуни одређени PKI систем су следећи: подршка различитим политикама рада PKI система, безбедност, скалабилност, флексибилност, једноставно коришћење, и отвореност система. [Marković M., 2009.]

## 2.1. Подршка различитим политикама рада PKI система

PKI систем мора омогућити подршку за примену различитих безбедносних политика крајњег корисника. Наиме, ова функционалност омогућује адаптацију система на промене законске, пословне и других политика рада које утичу на реализацију PKI система. С обзиром да PKI системи представљају инфраструиктуру у којој су, поред техничких аспеката, веома битни и значајни и легални и процедурално-организациони аспекти, могућност адаптације система на промене политике функционисања представља кључни захтев.

### 2.2. Безбедност

С обзиром да CA представља централни део PKI система са најважнијим циљем да успостави тачку поверења читавог система, основни захтев који се поставља пред читавим системом је највиша безбедност самог CA. Наиме, ако је CA компромитовано (ако је тајни кључ асиметричног шифарског система CA компромитован) било интерним или екстерним нападом, и читав PKI систем је компромитован. Из тих разлога, CA и читав PKI систем је потребно заштитити на највишем нивоу.

### 2.3. Скалабилност

Комерцијално доступни PKI системи су скалабилно дизајнирани тако да се крећу од малих конфигурација које раде на једном PC рачунару на коме су реализоване апликације CA,RA и неопходне базе података до великих инсталација система. У великим инсталацијама система постоје вишеструка RA са више оператора, организована као подређени чиниоци вишеструком хијерархијском систему CA, који су под јурисдикцијом једног "*Root CA*" система.

Друга веома значајна особина, PKI система да је он мора подржати евентуално проширивање система додавањем одређених модула, без потребе заустављања рада система. Другим речима, ако се дата организација шири, или ако се захтеви за PKI технологијом повећавају, све то се може решити додавањем одговарајућих специфичних PKI модула.

### 2.4. Флексибилност

Одређени PKI систем треба да је дизајниран тако да буде екстремно флексибилан у циљу лаког решавања различитих PKI захтева. У ова обележја су укључени:

- вишеструки системи за регистрацију и доставу сертификата и кључева – потребно је да дати PKI систем подржава различите механизме регистрације и доставе PKI параметара, укључујући: e-mail сервис, web комуникацију, личну доставу, VPN и друго,
- додршка различитим безбедносним модулима, малим хардверским модулима (токенима) и smart картицама,

- подршка примени различитих криптографских алгоритама, како јавних, тако и приватних алгоритама дефинисаних од стране дизајнера или самих корисника система,
- вишеструки системи публикације издатих и повучених сертификата који укључују различите екстерне директоријумске сервисе (*LDAP и X.500*), као и публикацију на хард диск у циљу олакшавања процеса публикације,
- подршка различитим методама провере валидности (повучености) дигиталних цертификата, као што су CRL (*Certificate Revocation List*), CRL дистрибуционе тачке и OCSP (*Online Certificate Status Protocol*),
- подршка комплексним PKI хијерархијама – PKI систем мора подржати хијерархију сертификационих тела (било које дубине), вишеструка регистрациона тела (RA), вишеструке операторе RA, и мора подржати процедуру међу-сертификације са другим CA,
- подршка вишеструким кључевима и сертификатима по кориснику – политика рада PKI система, и самог сертификационог тела (CA), треба да предвиди коришћење вишеструких кључева и сертификата по кориснику, а да се коришћење ових кључева тако конфигурише да се одвојени кључеви користе за дигитално потписивање и за шифровање (у оквиру дигиталне енвелопе),
- систем треба да подржи флексибилни ауторизациони процес – сваки захтев за издавањем сертификата може бити ауторизован од стране једне или више овлашћених особа, што треба дефинисати у политици рада CA. Додатно, систем треба да омогући да се захтеви за издавање сертификата процесирају и аутоматски, без потребе за применом специфичне процедуре ауторизације.

### 2.5. Једноставно коришћење

У сваком PKI систему најважнији субјекти су:[Ross R.,Stoneburner G.,2004.]

- администратор безбедности PKI система који успоставља и мониторише рад читавог PKI система,
- администратор CA,
- оператори RA који сакупљају регистрационе информације и могу да ауторизују процес цертификације и повлачења сертификата,

- крајњи корисници који подносе захтев за издавањем сертификата.

PKI систем треба да буде дизајниран тако да за све горе поменуте категорије корисника систем буде веома једноставан за коришћење, и да корисници једини имају приступ функцијама које су им омогућене за коришћење. Ово минимизује процес обуке неопходан за сваки тип корисника и редукује могуће проблеме које они могу имати у циљу коришћења система.

### 2.6. Отвореност система

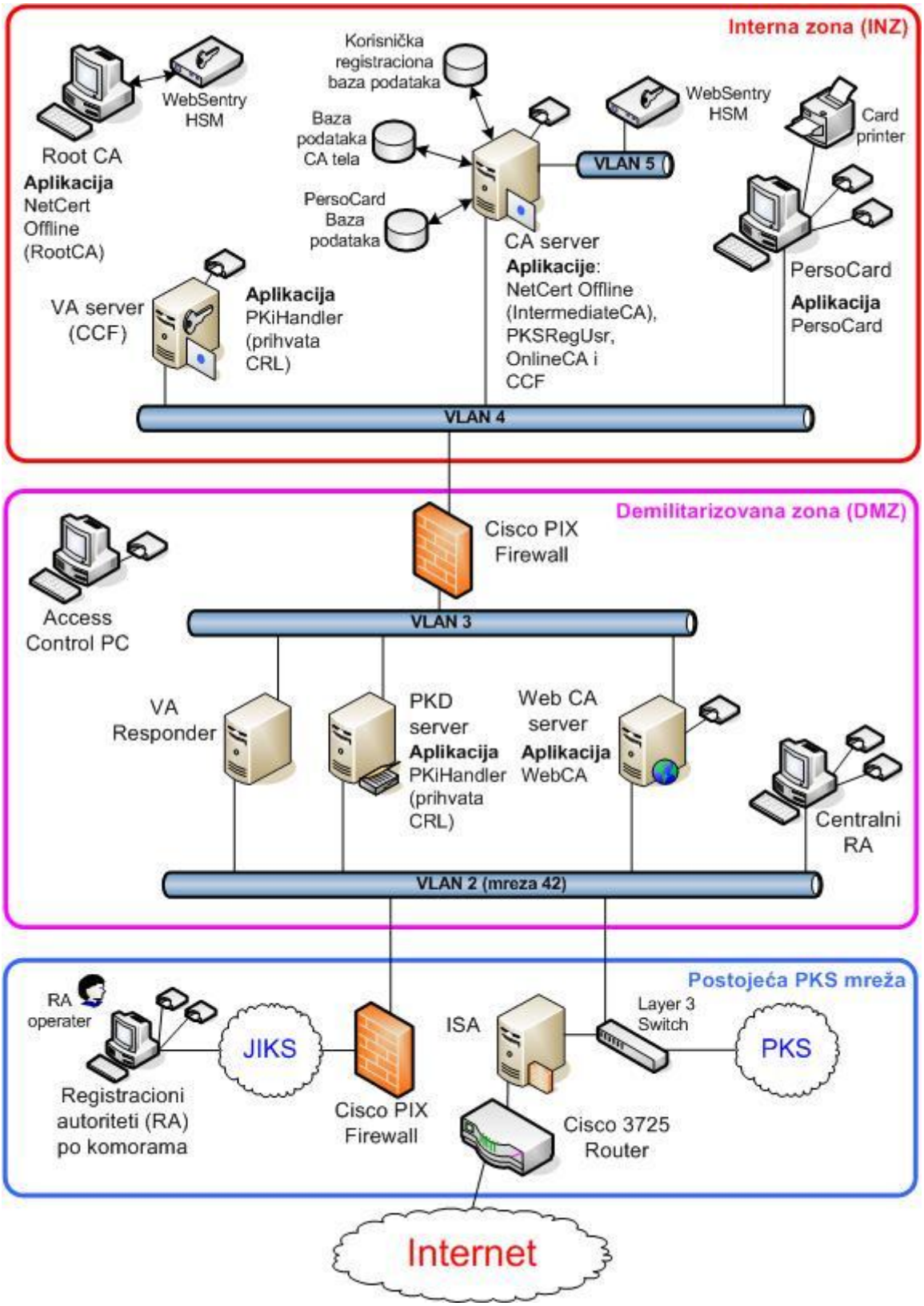
У циљу евентуалних захтева за интероперабилношћу, PKI систем мора задовољавати особину да се базира на отвореним стандардима, од којих је најважнији X.509v3 стандард за формат дигиталног сертификата.

# 3. КОМПОНЕНТЕ PKI СИСТЕМА

Инфраструктура система са јавним кључевима (*PKI систем)* представља комбинацију хардверских и софтверских производа, политика и процедура.[ Kuhn D.R., Hu V. C., Polk W. T.,2001.] PKI системи омогућују основно безбедносно окружење које се захтева у системима лектронског пословања (*e-business*), у коме корисници, који се не познају или су дистрибуирани по свету и налазе се на великим удаљеностима, могу комуницирати безбедно кроз мрежу поверења. Детаљна инфраструктура PKI система приказана је на слици 3.1.[Sertifikaciono Telo, Integrisanog Komorskog Sistema Srbije, 2004.]

PKI системи се базирају на дигиталним идентитетима (*digital IDs*) познатим под називом *дигитални сертификати,* који играју улогу својеврсних "дигиталних пасоша" или "дигиталних личних карата", и који повезују име власника датог сертификата са његовим јавним кључем асиметричног криптографског система, као што је на пример RSA алгоритам. PKI систем се базира на политици заштите информационог система у коме се примењује. Политика заштите успоставља и дефинише основне правце и стратегију развоја безбедности информационог система дате организације, и прописује процедуре и принципе коришћења криптографских механизама у систему .[Privredna Komora Srbije, Politika Sertifikacije, Kvalifikovani Elektronski Sertifikati, 2009. ]

Типично, безбедносна политика прописује на који се начин управља кључевима и осталим неопходним информацијама у систему, и прописује неопходне нивое контроле који одговарају нивоима ризика. PKI систем се састоји од следећих основних компонената: [Marković M., 2004.]




**Слика 3.1**:Инфраструктура PKI ситема [Привредна Комора Србије 2009.]

- Основни документ рада PKI система - Политика сертификације **(***CP – Certificate Policy***)** – утврђује основне принципе рада сертификационог тела и осталих компонената PKI система.
- *CPS – Certificate Practice Statement* – представља документ који практично описује рад Сертификационог тела (*CA – Certification Authority*) и неопходан је у случају комерцијалног CA. CPS представља детаљан документ који садржи операционе процедуре за реализацију принципа који су наведени у политици сертификације, и представља практичну подршку систему. Типично, CPS укључује дефиниције како је CA формирано и начин рада, како се генеришу дигитални сертификати, како се повлаче, како ће кључеви бити генерисани, регистровани и сертификовани, где ће се чувати и како ће бити расположиви корисницима.
- *Сертификационо тело (CA)* – је најважнија компонента и основа поверења датог PKI система чији је задатак да управља дигиталним сертификатима у њиховом читавом животном циклусу. Основни задаци CA су да:
  - генерише дигиталне сертификате повезивањем идентификационе података одређеног корисника у систему са његовим јавним кључем асиметричног криптографског система, и све то потврђује својим дигиталним потписом свих података у сертификату,
  - управља роком важности издатих дигиталних сертификата,
  - обезбеђује функцију повлачења издатих дигиталних сертификата у случајевима када за то постоје услови, и у том смислу, публикује листе повучених сертификата (*CRL – Certificate Revocation List*).

У поступку формирања PKI система, организација може да реализује сопствено CA, или да користи услуге CA сервиса, реализованог од неке треће стране од поверења.

- *Регистрационо тело (RA)* – обезбеђује интерфејс између корисника и CA. RA прихвата захтеве и проверава аутентичност корисника и прослеђује стандардни захтев за издавање дигиталног сертификата. Квалитет процедуре провере идентитета корисника одређује ниво поверења који се уграђује у сертификат.
- *Системи за дистрибуцију сертификата* – Генерисани дигитални сертификати се могу дистрибуирати на различите начине, у зависности од структуре читавог PKI система, као на пример директно корисницима или преко директоријумског сервера. Директоријумски сервер може већ постојати у датом информационом систему саме организације, или може бити испоручен као део читавог PKI решења.

- *PKI апликације* – читав PKI систем се креира да подржи рад већег броја апликација, као што су: [Rosing M., 1998.]
  - заштита WEB трансакција,
  - заштита е-маил сервиса,
  - VPN – виртуелне приватне мреже,
  - безбедно управљање електронском документацијом, и
  - контрола радног времена и приступа одређеним просторијама, ...

### 3.1. Модули PKI система

У циљу задовољења неопходних захтева који се постављају пред систем заштите, PKI систем и CA морају бити модуларно реализовани. Сви модули комуницирају међусобно, коришћењем базе података, или заштићених (*PKIX*) TCP/IP конекција[Marković M., 2004.]. Основни модули PKI система су:

- *Сертификационо тело (CA)* – дигитално потписује дигиталне сертификате и публикује сертификате и листе повучених сертификата,
- *Оператор Сертификационог тела (CAO)* – CAO је безбедносни администратор читавог PKI .
- *Регистрационо тело (RA)* – рутира информације, сертификате и захтеве за издавањем сертификата кроз хијерархију датог PKI система,
- *Оператор RA (RAO)* – има задатак да потврди или одбије удаљене и лично поднете захтеве за издавањем сертификата,
- *Архивни сервер* – ово је опциони модул који се користи за евентуално чување корисничких парова кључева за шифровање дигиталном енвелопом,

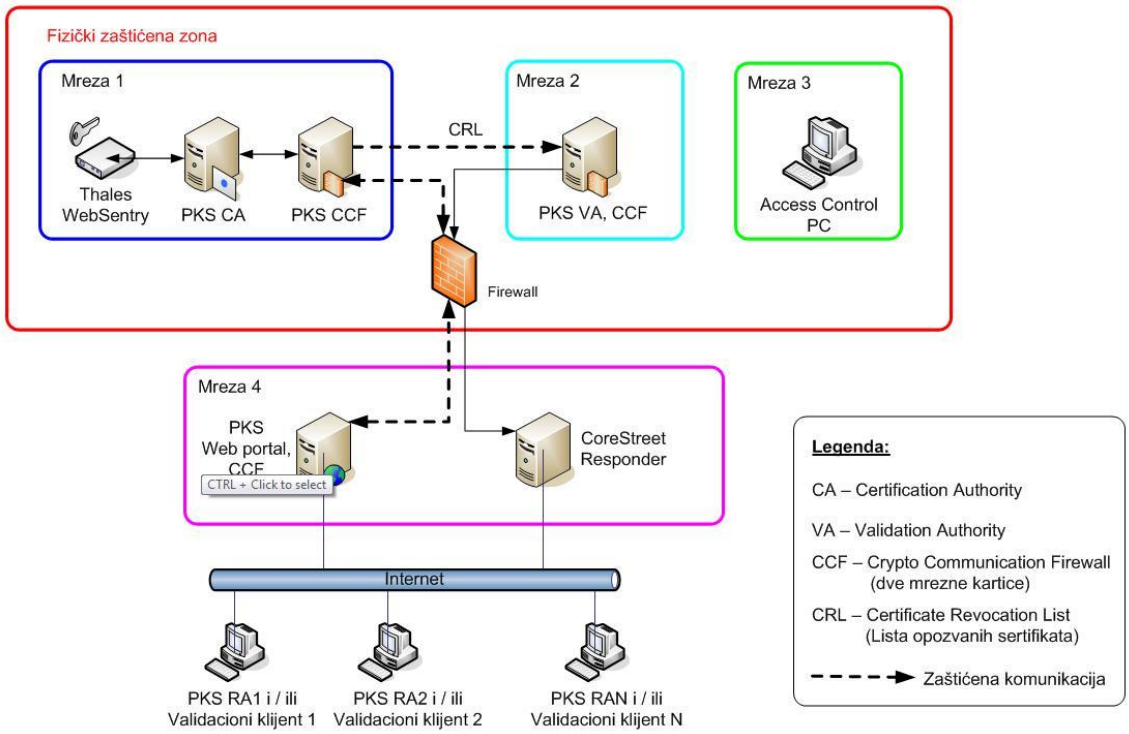
### 3.2. Сертификационо тело (CA)

Сертификационо тело или Сертификациони ауторитет (CA) представља језгро читавог PKI система. Читаво поверење садржано у PKI инфраструктури зависи од дигиталног потписа CA.CA функционише на бази сопствене флексибилне политике рада, и контролисано је од стране CAO.

Сертификационо тело представља софтверско-хардверску апликацију која, као улазни параметар, узима јавни кључ асиметричног криптографског система,

смешта га у оквир дигиталног сертификата и, заједно са осталим подацима, дигитално потписује у циљу гаранције да дати јавни кључ припада дефинисаном кориснику (власнику датог дигиталног сертификата.Функционалност CA детаљно је приказана на слици 3.2.

За разлику од самопотписаних сертификата (као што су дигитални сертификати Root Цертификационих тела), дигитални сертификати потписани од стране CA и који се издају корисницима имплицирају да је CA, као "трећа страна од поверења" (*Trusted Third Party*), проверила да дати јавни кључ припада дефинисаном кориснику и да својим потписом сертификује да је то истинито. У најкраћем, идеја се састоји у томе да одређено овлашћено екстерно тело (CA) преузме личне податке одређеног корисника и његов јавни кључ, форматира те податке на стандардни начин, у облику дигиталног сертификата, кога затим дигитално потпише. Дигитални сертификат, на основу дигиталног потписа CA, представља поуздану везу идентитета одређеног корисника и његовог јавног кључа. Наиме, име власника сертификата, јавни кључ и додатне информације као што су: датум издавања и рок важности, име CA које је издало сертификат, итд. форматирају се у облику дигиталног сертификата у стандардном формату (X.509v3 стандард) тако да га стандардни програми за претраживање (*browser)* и криптографски софтверски системи могу процесирати. ). [Marković M., 2009.]




**Слика 3.2**:Функционалност CA [Привредна Комора Србије 2009.]

### *3.2.1. Функционалност CA*

Функционалност CA се огледа у следећем:

- CA прихвата потврђене захтеве за генерисањем и повлачењем сертификата од регистрационих тела (RA) и CAO и испоручује дигиталне сертификате и потврдне поруке,
- ако је тако предвиђено утврђеном политиком рада, CA такође доставља крајњим корисницима пар кључева за шифровање који су означени да се архивирају у бази кључева, о потписује сертификате подређених CA, као и других CA у случају унакрсне сертификације (*cross-certification*),
- публиковање CRL (*Certificate Revocation List*) – CA дигитално потписује све информације објављене у форми CRL,
- дигитално потписивање порука – све поруке које се шаљу од стране CA су дигитално потписане,
- верификација порука – CA верификује све поруке које добије у циљу провере аутентичности и заштите интегритета,
- шифровање података – све поруке које се размењују преко CA су шифроване у PKCS#7 формату,
- архивирање података – сви релевантни подаци и log фајлови се архивирају у бази података CA. Све архиниране информације су дигитално потписане од стране CA. Сваки улазак у базу поседује одговарајући јединствени процесни број,
- публикација сертификата и других неопходних параметара – CA опционо публикује сертификате и CRL на LDAP или X.500 директоријуме. CA подржава и публикацију поменутих параметара на хард диску, као један механизам публикације сертификата који се може лако кастомизовати,
- опционо – CA може бити одговорно за публикацију CRL и на OCSP *(Online Certification Status*) серверу, [Cooper D. A.,1999;Cooper M.,2005; Cooper D. A., 2005.]
- генерисање асиметричног пара кључева – CA генерише свој сопствени пар кључева за асиметрични криптографски алгоритам (то је за CA) и за CAO, и
- провера јединственог имена *Dname* и јавних кључева – CA може опционо да проверава да ли сви издати дигитални сертификати имају јединствено *Dname* и јавни кључ.

### *3.2.2. Обележја CA*

Обележја CA су:

- CA треба да подржи различите хардверске елементе, као што су: smart картице за крајње кориснике, хардверски безбедносни модули (*HSM – Hardware Security Module*) и други токени,
- CA треба да подржи могућност коришћења DAP и LDAP механизама,
- CA обезбеђује вишеструко генерисање парова асиметричног кључа. Опционо, CA може имати индивидуални пар кључева за сваку од функција: дигитално потписивање сертификата, дигитално потписивање CRL, шифровање података, шифровање кључа,
- CA подржава променљиво време публиковања CRL, и
- CA треба да подржи OCSP сервисе.

CA треба да подржи читаву палету симетричних и асиметричних кључева. Што се тиче асиметричних криптографских техника, CA би требало да подржава следеће алгоритме: RSA, DSA i ECDSA.

## 3.3. Оператор цертификационог тела (CAO)

Модул оператора сертификационог тела (CAO) представља модул за администрацију, надзор и безбедност CA и PKI система у целини који се базира на датом CA. CAO контролише све администраторске функције у систему и додељује одговарајуће привилегије осталим модулима и подсистемима.[Marković M., 2009.]

### *3.3.1.Функционалност CAO*

- CAO прослеђује потврђене захтеве за издавањем сертификата директно CA. Захтеви за повлачењем сертификата се смештају у CA базу података,
- креирање политике рада CA – CAO је одговоран за креирање и одржавање политике издавања сертификата. CAO такође одржава политике и процедуре рада CA и свих RA,

- ажурирање нових верзија политике рада CA и целог PKI система – CAO динамички доставља нове верзије политике и процедура рада до индивидуалних оператора регистрационих тела (RAO) у циљу обезбеђења да се сви дигитални сертификати увек издају у условима ажурних верзија политике датог PKI система,
- повлачење сертификата – сваки сертификат може бити повучен од стране CAO,
- развој PKI система – CAO може додати нове модуле или апликације у PKI систем и дати им одговарајуће привилегије,
- генерисање кључева – CAO је одговоран за генерисање одговарајућих кључева (симетричних и асиметричних) за кориснике,
- дигитално потписивање порука – све поруке које се шаљу од стране CAO су дигитално потписане,
- верификација потписаних порука – све поруке које CAO прима пролазе проверу (верификацију) дигиталног потписа у циљу провере аутентичности потписника и интегритета садржаја поруке,
- шифровање података – све поруке које се размењују преко CAO модула су шифроване у PKCS#7 формату, и
- архивирање података – сви подаци и log фајлови се архивирају у бази података CA. Све информације које се архивирају се дигитално потписују од стране CAO. Сваки улазни слог има свој јединствени процесни број (*tracking number*).

### *3.3.2. Обележја CAO*

Обележја CAO су:

- CAO треба да подржи различите хардверске елементе, као што су: smart картице за крајње кориснике, хардверски безбедносни модули (*HSM – Hardware Security Module*) и други токени,
- поседује графички интерфејс, једноставан за коришћење,
- процесира цертификате и CRL, и
- сваки CAO може имати различите нивое привилегија.

## 3.4. Регистрационо тело (RA)

Регистрационо тело (RA) игра улогу рутера између оператора регистрационог тела (RAO) и CA. RA може имати своју сопствену политику рада, која се одржава локално или од стране CAO[Marković M., 2004.].

### *3.4.1. Функционалност RA*

Функционалнос RA огледа се у следећем:

- RA прослеђује потврђене захтеве за издавањем или повлачењем сертификата, добијене од RAO, до CA. RA добија сертификате и потврдне поруке од стране CA и доставља их до RAO,
- RA прослеђује захтеве за издавањем или повлачењем сертификата до RAO и доставља сертификате и информационе поруке назад,
- дигитално потписивање порука – све поруке послате од стране RA су дигитално потписане,
- верификација порука – све дигитално потписане поруке које RA добија се процесирају у смислу верификације дигиталног потписа у циљу провере аутентичности потписника и интегритета садржаја поруке,
- шифровање података – све поруке које се размењују преко RA су шифроване у PKCS#7 формату, и
- архивирање података – сви подаци и log фајлови се архивирају у бази података RA. Све архиване информације су дигитално потписане од стране RA. Сваки улазни слог има јединствени процесни број.

### *3.4.2. Обележја RA*

Обележја RA су:

- RA треба да подржи различите хардверске елементе, као што су: smart картице за крајње кориснике, хардверски безбедносни модули (*HSM – Hardware Security Module)* и други токени, и
- Опција аутоматског потврђивања – у случају да је то политиком рада предвиђено, RA може бити подешено тако да аутоматски потврђује (дигитално потписује) све удаљене захтеве који стижу без потребе за интервенцијом RAO.

### 3.5. Оператор регистрационог тела (RAO)

Оператор регистрационог тела (RAO) има функцију да потврђује (дигитално потписује) захтеве за издавањем или повлачењем сертификата који ће даље бити процесирани од стране CA. Међутим, у случају да политика рада CA то предвиђа и дозвољава, RAO може реализовати и функцију генерисања кључева за крајњег корисника, као и да у изузетним случајевима издаје дигиталне сертификате крајњим корисницима.[Marković M., 2004.]

#### *3.5.1. Функционалност RAO*

- RAO прима захтеве за издавањем сертификата преко RA, или их креира директно у личном контакту са крајњим корисником (*face-to-face manner*,
- RAO је одговоран за потврђивање или одбијање захтева за издавањем сертификата од крајњег корисника који су добијени у личном контакту или електронском комуникацијом (ова функција зависи од утврђене политике рада PKI система),
- RAO шаље потврђене захтеве за издавањем или повлачењем сертификата до RA,
- RAO може генерисати кључеве (асиметрични пар кључева) за крајњег корисника у софтверу или на криптографском хардверу (*HSM*), уколико је то политиком рада предвиђено,
- дигитално потписивање порука – све поруке послате од стране RAO су дигитално потписане,
- верификација порука – све дигитално потписане поруке које RAO добија се процесирају у смислу верификације дигиталног потписа у циљу провере аутентичности потписника и интегритета садржаја поруке, и
- шифровање података – све поруке које се размењују преко RAO модула су шифроване у PKCS#7 формату.

Архивирање података – сви подаци и log фајлови се архивирају у бази података RA. Све архиване информације су дигитално потписане од стране RAO. Сваки улазни слог има јединствени процесни број.[Housley R., 2002;Adams C., Farrell S., Kause T., Mononen T.,2005; Adams C., Lloyd S., 2003.]

### *3.5.2. Обележја RAO*

Обележја RAO су:

- RAO треба да подржи различите хардверске елементе, као што су: smart картице, хардверски безбедносни модули (*HSM – Hardware Security Module*) и други токени, и
- поседује графички интерфејс једноставан за коришћење.

## 3.6. Сервер за архивирање кључева

PKI систем треба да буде способан да се опорави у смислу пуне функционалности у случају системских или комуникационих оштећења која се могу десити у коришћењу.[ Souppaya M.,Harris A.,McLarnon M.,Selimis N.,2002;Stallings W.,2005.] Дакле, потребно је да систем има реализовану стратегију опоравка и неометаног даљег рада у случају оштећења проузрокованог вишом силом.[NSA.,2000.] Углавном, два основна критична елемента PKI система:тајни кључеви и база података. Уколико се реализује поуздана *back-up* функција ових елемената, читав PKI систем ће бити способан да се комплетно опорави и да се врати у претходно стање[Marković M., 2004.]. Интерна база података PKI система (база података CA и RA) користи се углавном:

- за чување свих захтева за издавање сертификата, издатих сертификата и CRL,
- као база за размену порука између CA и RA,
- за чување log фајлова у читавом систему и свих активности које су реализоване од стране оператора,
- за чување детаља о регистрационим политикама, и
- за чување регистрационих информација које нису укључене у сертификате (као на пример атрибути дефинисани од стране самих корисника, скениране фортографије, биометрички подаци, итд.

Безбедност читавог система је ојачана тако што је сваки унос у базу, или поступак читања, дигитално потписан уз помоћ тајног кључа одређеног процеса или оператора који је дату трансакцију урадио. Поред тога, сваки захтев за издавање сертификата поседује придружени идентификациони број трансакције, који се користи током процесирања датог захтева у датом PKI систему.[Tracy M., Jansen W., McLarnon M., 2002.].

Коришћење поступка дигиталне енвелопе значи да шифровану информацију може прочитати само корисник коме је та информација намењена. Свака организација која своју безбедност базира на PKI систему жели да буде способна и да може накнадно, у изузетним случајевима, да дешифрује неке податке. У том смислу, не сме се допустити да тајни асиметрични кључеви, којима се једино могу дешифровати симетрични кључеви, којима су шифроване одређене поруке изгубе, јер су тада изгубљене и те шифроване поруке. Овај захтев повлачи за собом следеће:

- важним подацима фирме, који су шифровани и намењени неком службенику, не може се приступити уколико дати службеник у том тренутку није присутан,
- подаци се не могу дешифровати ако је тајни кључ изгубљен или оштећен,
- подаци се не могу дешифровати ако је лозинка заборављена, и
- крајњи корисници могу бити онда демотивисани (или у страху) да шифрују важне податке плашећи се да ти подаци касније неће моћи бити дешифровани.

Наведени проблеми се могу разрешити ако би се копије тајних кључева чувале на безбедном месту. То би омогућило опоравак шифрованих података у сваком тренутку. Међутим, то би такође омогућило вероватноћу проневере дигиталних потписа од стране злонамерне особе која има приступ бази тајних кључева.То је неприхватљиво са становишта постизања функције непорецивости у систему.

Ови проблеми се на задовољавајући начин могу решити тако што се у систему омогући корисницима да имају више парова асиметричних кључева, а последично и више сертификата (по један сертификат на сваки пар кључева). Један пар кључева треба да буде за шифровање, а други за дигитално потписивање. Најприхватљивија шема је да пар кључева за дигитално потписивање генерише сам корисник, по могућству на криптографском хардверу (smart картици) који обезбеђује функцију непорецивости, а да пар кључева за шифровање генерише CA за датог корисника и да му их доставља. У том случају, CA може чувати копију тајног кључа за шифровање на серверу за архивирање података, што омогућује потпун опоравак шифрованих података (уколико на пример корисник изгуби smart картицу), без утицаја на функцију непорецивости датог корисника.[Housley R., 2002; Adams C., Lloyd S., 2002;Adams C., Lloyd S., 2003.]

Сервер за архивирање кључева има функцију да безбедно ускладишти тајне кључеве асиметричног криптографског система крајњих корисника који се примењују у оквиру поступка дигиталне енвелопе.[Tracy M., Jansen W., McLarnon M., 2002.] Ова функција омогућује каснији опоравак датих кључева, као и

евентуалног дешифровања шифрованих порука (поступком дигиталне енвелопе), у случајевима губитка или оштећења кључева, или у случајевима када одређени ауторитет налаже дешифровање порука (у судским или арбитражним процесима, итд.). Кључеви се чувају на серверу за архивирање кључева једино у случају да је то изричито предвиђено политиком рада PKI система.

### *3.6.1. Функционалност сервера за архивирање кључева*

- Сервер за архивирање кључева шифрује тајни кључ кога треба ускладиштити применом одређеног симетричног алгоритма са одговарајућим DEK (*Data Encipherement Key*) кључем, јединственим за сваки тајни кључ који се архивира. Тако шифровани тајни кључ се смешта у посебну базу података (AC база података).
- DEK кључ се такође шифрује посебним симетричним алгоритмом и посебним кључем и такође се смешта у базу података .
- Дигитално потписивање порука – све поруке послате од стране архив сервера су дигитално потписане.
- Верификација порука – све дигитално потписане поруке које архив сервер добија се процесирају у смислу верификације дигиталног потписа у циљу провере аутентичности потписника и интегритета садржаја поруке.
- Архивирање података – сви подаци и log фајлови се архивирају у AC бази података. Све архивиране информације су дигитално потписане од стране AC. Сваки улазни слог има јединствени процесни број.

### *3.6.2. Обележја Архив сервера*

- поседује графички интерфејс једноставан за коришћење са интерфејсом који се може прилагодити корисниковим потребама, и
- архив сервер треба да подржи различите хардверске елементе, као што су: smart картице, хардверски безбедносни модули (*HSM – Hardware Security Module*) и други токени.

### 3.7. Дигитални сертификати

Дигитални сертификати представљају елемент којим се утврђује веза између идентитета субјекта и његовог јавног кључа за примену асиметричног криптографског алгоритма. Располагање јавним кључем потписника је услов за поуздану верификацију дигиталног потписа. Наиме, страна која врши верификацију мора бити сигурна да дати јавни кључ представља криптографски пар са тајним кључем којим је порука дигитално потписана. Јавни и тајни кључ асиметричног криптографског алгоритма су две велике бројне величине, и немају детерминистичку везу са идентитетом било ког правног или физичког лица.[Housley R., 2002;Adams C., Lloyd S., 2003;Adams C., Farrell S., Kause T., Mononen T.,2005.] Дигитални сертификати механизми за поуздано придруживање датог пара бројева идентитету неког субјекта, тако да се та веза не може фалсификовати. На тај начин дигитални сертификати представљају електронске еквиваленте некој врсти "дигиталне личне карте" или "дигиталног пасоша". [Marković M., 2004.]

Да би се добио дигитални сертификат, мора се прво формирати захтев за добијање сертификата (*Certificate Request*), који се доставља одређеном Сертификационом ауторитету (CA) у циљу издавања дигиталног сертификата. Овај захтев садржи све податке о кориснику који ће се појавити и у дигиталном сертификату. Захтев за сертификат је дигитално потписан у циљу гаранције његовог интегритета. Сертификациони ауторитет проверава аутентичност добијеног захтева коришћењем јавног кључа који је у њему садржан. Постоје два коришћена типа захтева за издавање дигиталног сертификата, познати као PKCS#10 и RFC 2511. PKCS#10 формат је далеко једноставнији. PKCS#10 тип захтева за издавањем сертификата састоји се од следећа 4 поља:

- број верзије формата захтева (од 1 до 3),
- назив власника дигиталног сертификата (*DistinguishedName - Dname*),
- јавни кључ власника дигиталног сертификата, и
- атрибути.

Поље атрибута садржи оне елементе за које постоји потреба да се нађу у дигиталном сертификату, као што је број телефона, број факса, e-mail адреса, највиша вредност финансијске трансакције у случају банкарских сертификата и друге карактеристике. У овом пољу се може наћи све оно што не потпада под поље *Dname* а представља јединствени стринг који идентификује власника сертификата. Поред тога, Dname представља пут кроз X.500 директоријум, тако да се једино може састојати из следећих поља[Housley R., 2002; Adams C., Farrell S., Kause T., Mononen T.,2005]:

- двословни низ који означава државу,

- регион,
- електронска адреса,
- фирма,
- одељење у фирми, и
- име власника сертификата.

Имајући на располагању дигитални сертификат одређеног субјекта, могуће је извршити верификацију дигиталног потписа порука које је тај субјект потписао. Уколико је верификација успешна, верификатор је сигуран у интегритет поруке, у аутентичност њеног потписника и у немогућност накнадног порицања датог потписника за издавање дате поруке. У оквиру система заштите савремених рачунарских мрежа, дигитални сертификати се, између осталог, могу примењивати за верификацију дигиталног потписа, контролу приступа субјеката криптозаштићеним апликацијама и у процедурама аутентикације. Садржај дигиталног сертификата, у складу са стандардом X.509, је приказан је на слици 3.3:

| |
|---|
| Верзија формата сертификата (*v3*) |
| Серијски број сертификата |
| Идентификатор алгоритма којим се врши дигитални потпис |
| Назив Сертификационог тела које је издало сертификат |
| Рок важности сертификата |
| Власник сертификата |
| Јавни кључ |
| Одређени специфични подаци који се односе на услове коришћења сертификата |
| **ДИГИТАЛНИ ПОТПИС СЕРТИФИКАТА ТАЈНИМ КЉУЧЕМ СЕРТИФИКАЦИОНОГ ТЕЛА** |

**Слика3.3:** Садржај дигиталног сертификата[Marković M., 2009.]

### *3.7.1. ITU X.509 v3 сертификат-структура*

Према овом стандарду дигитални сертификат се састоји од три дела.[ Housley R., 2002.] Први део чине подаци значајни за сам сертификат представљени промењливом *tbsCertificate,* други део представља идентификатор алгоритма за потписивање представљен промењливом *signatureAlgorithm* и на крају сам потпис представљен промењливом *signature.* Промењлива *tbsCertificate* је структурног типа и садржи следећа поља:

- верзија (*Version*) – представња ознаку структуре дигиталног сертификата која је специфицирана у стандарду X.509 при чему су валидне верзије 1, 2 и 3,
- церијски број (*Serial Number*) – редни број издатог сертификата. Начин додељивања серијских бројева мора бити јединствен тј. име издавача сертификата и редни број сертификата јединствено одређују сертификат. Серијски број сертификата је вредност коју додељује серификациони ауторитет у тренутку креирања дигиталног сертификата,
- идентификатор алгоритма дигиталног потписа (*Signature Algorithm*) - ознака асиметричног криптографског алгоритма (RSA, DSA) и кориштене *hash* функције (MD5, SHA1) који су примењени у процесу генерисања дигиталног потписа сертификационог тела,
- назив издавача дигиталног сертификата (*Issuer*) - структура која идентификује сертификационо тело (сертификациони ауторитет, CA) које је генерисало дати сертификат и састоји се из следећих елемената:
  - име издавача сертификата (c*ommonName*),
  - оделење у организацији (*organizationalUnitName*),
  - организација (*organization*),
  - место (*localityName*),
  - елекронска адреса (*emailAddress*),
  - регион или република у оквиру државе (*stateOrProvinceName*), и
  - ознака државе (*countryName*).
- валидност – специфицира се период унутар којег се сертификат сматра важећим уколико није опозван. Рок важности сертификата представља временске оквире валидности дигиталног сертификата. У процесу верификације прихвата се само сертификат коме није истекао рок важности. Наведено поље се састоји од два елемента:
  - почетак важности сертификата (Valid From), и
  - крај важности сертификата (Valid To).
- власник сертификата (Subject) – идентификатор (име) власника сертификата коме се придружује јавни кључ који садржи сертификат. Назив власника дигиталног сертификата је структура која идентификује власника дигиталног сертификата и састоји се од следећих компоненти:
  - име власника сертификата,
  - оделење у организацији,
  - организација,

- место,
- елекронска (e-mail) адреса ,
- регион или република у оквиру државе,
- ознака државе.

- јавни кључ (Public Key) – јавни кључ власника сертификата и идентификатор алгоритма за који је намењен. Информација о јавном кључу власника садржи нумеричку репрезентацију јавног кључа и идентификатор асиметричног алгоритма (RSA, DSA) са којим се дати кључ примењује,
- поље додатних информација (Extension) – садржи скуп поља (екстензије) која, по потреби, могу носити још неке информације осим ових основних. Неке од ових додатних информација могу поседовати атрибут CRITICAL или NONCRITICAL. Уколико апликација која користи сертификат пронађе информацију означену са CRITICAL и не препозна је, мора сертификат одбацити као неисправан, и
- дигитални потпис (Digital Signature) сертификата од стране CA.

Поље додатних информација може садржати информације помоћу којих се идентификује јавни кључ којим се сертификат проверава, уколико издавач има више парова јавних и тајних кључева. Такође дато поље може да садржи информације о намени јавног кључа који власник сертификата поседује, опис услова под којима је сертификат креиран и за што се може користити, алтернативна имена издавача и власника сертификата.

Према досадашњим искуствима оваква структура сертификата испуњава захтеве савремених криптографких система заштите. Сходно томе, већина (ако не и сви) савремених система заштите, који укључују инфраструктуру система са јавним кључевима (*PKI системе*), базира се на примени X.509 дигиталних сертификата. Дати сертификати се још називају PKI дигитални сертификати.

### *3.7.2. Екстензије у сертификату*

Екстензије у сертификату су уведене када је дефинисан X.509v3 стандард за формат сертификата. У претходним верзијама (*v1*, *v2*) уколико било која информација, која није из домена *Dname*, треба да се унесе у сертификат, она је уписивана као део Dname структуре. Употреба екстензија чини савремене сертификате изузетно флексибилним, тиме што се повећава могућност увођења и подршке нових PKI апликација. Дакле, екстензије се могу користити у циљу придруживања нових атрибута кориснику у односу на оне информације које се могу унети у *Dname* структуру. Екстензије могу бити такође коришћене за

креирање хијерархије дигиталних сертификата. Такође, постоји неколико предефинисаних и међународно препознатих екстензија. Поред тога, могу се такође реализовати нове екстензије за приватне потребе коришћењем генеричких екстензија. Поља за екстензије у сертификату могу бити коришћена да се обезбеде идентификационе информације, ауторизациони подаци и поља контроле приступа. Укратко, екстензија сертификата може бити коришћена да садржи информације за које корисник сматра да могу бити корисне у процесу анализе дигиталних сертификату.[Marković M., 2004.]

Све екстензије у сертификату могу бити означене као критичне (*critical*) или некритичне *(noncritical*). Ако је екстензија означена као некритична, то значи да ће, ако нека PKI апликација не препозна дату екстензију, она бити игнорисана и да ће се дати сертификат даље процесирати. Екстензију треба означити као критичну ако се жели да се осигура да ограничење на коришћење датог сертификата, које се уводи поменутом екстензијом, неће моћи да се пренебрегне било којом апликацијом. Неке екстензије морају бити обавезно проглашене критичним у складу са стандардом X509v3. Међутим, за већину екстензија се препоручује да буду некритичне.

Потребно је, такође, пажљиво процењивати потребу за додавањем сваке екстензије, јер оне доприносе увећању самог сертификата. Такође, што више екстензија се дода то је већа вероватноћа да ће у будућности неке информације из екстензија бити невалидне, и да ће се због тога морати повући сертификат. У том смислу, препорука је да се у сертификат додају само суштински важне екстензије и да се не повећава непотребно величина сертификата додавањем непотребних информација.

Екстензије су карактеристичне за верзију V3 дигиталних серификата. У пољу екстензија се налазе додатне информације везане за власника и издавача сертификата. Стандардне екстензије у сертификату су:[Housley R., 2002;Adams C., Lloyd S., 2003.]

- Идентификатор кључа ауторитета (*Authority Key Identifier*),
- Идентификатор кључа субјекта (*Subject Key Identifier*),
- Употреба кључа (*Key Usage*),
- Период коришћења приватног кључа (*Private Key Usage Period*),
- Политике сертификације (*Certificate Policies*),
- Мапирање политике (*Policy Mappings*),
- Алтернативно име субјекта (*Subject Alternative Name*),
- Алтернативно име издавача цертификата (*Issuer Alternative Name*),
- Директоријумски атрибути субјекта (*Subject Directory Attributes*),
- Основна ограничења (*Basic Constraints*),

- Ограничења везана за име субјекта (*Name Constraints),*
- Ограничења везана за примењену политику (*Policy Constraints*),
- Проширено коришћење кључа (*Extended Key Usage*),
- Дистрибутивне тачке за листу повучених сертификата (*CRL (Certificate Revocation List) Distribution Points*)).

Наведене екстензије у сертификату су предложене од стране PKIX радне групе (*Internet X.509 Public Key Infrastructure Certificate and CRL profile, RFC2459).*

#### *3.7.2.1. Идентификатор кључа ауторитета*

Када сертификациони ауторитет има више различитих тајних асиметричних кључева намењених за издавање дигиталних сертификата различитим групама корисника, идентификатор кључа ауторитета омогућава идентификацију јавног кључа CA који одговара приватном кључу коришћеном за дигитално потписивање сертификата. Поменута идентификација може бити базирана било на идентификатору кључа (идентификатор кључа субјекта у екстензији сертификата), или на имену CA и серијском броју.

Усклађен CA сертификат је сертификат који укључује екстензију основних ограничења а вредност CA у тој екстензији је "*true"*. У циљу олакшаног формирања везе сертификата, поље *keyIdentifier* у екстензији *authorityKeyIdentifier* мора бити укључено у свим усклађеним CA сертификатима. Уколико се ради о самопотписаном CA сертификату, идентификатор кључа ауторитета може бити изостављен зато што су у том случају идентификатори кључева субјекта и ауторитета идентични.

Вредност поља *keyIdentifier* се изводи из јавног кључа који се користи у процесу верификације дигиталног потписа сертификата или применом метода која генерише јединствене вредности. Ако се користи екстензија идентификатор кључа ауторитета она треба да буде означена као *некритична*.

#### *3.7.2.2. Идентификатор кључа субјекта*

Идентификатор кључа субјекта је намењен за идентификацију сертификата који садрже одређен јавни кључ. У циљу олакшаног формирања везе сертификата, ова екстензија се мора појавити у свим усклађеним CA сертификатима.

Вредност идентификатора кључа субјекта мора бити смештена у поље идентификатора кључа у екстензији идентификатор кључа ауторитета. За CA цертификате, идентификатор кључа субјекта треба да буде изведен из јавног кључа, или применом метода који генерише јединствене вредности. Уобичајене методе за генерисање идентификатора кључа из јавног кључа су:

- *keyIdentifier* – сачињен од 160-битне SHA-1 hash вредности израчунате над вредношћу *BIT STRING* поља *subjectPublicKey* (искључујући таг, дужину и број неискоришћених бита), и
- *keyIdentifier* – сачињен од 4-битног поља вредности 0100 праћених са последњих 60 бита (најмање значајних) SHA-1 hash вредности израчунате у односу на *BIT STRING* вредност поља *subjectPublicKey.*

Уобичајени метод за генерисање јединствених вредности је монотоно увећавање секвенце целобројних вредности. У случају да је крајњи корисник добио више сертификата, нарочито од више CA, идентификатор кључа субјекта омогућује брзу идентификацију скупа сертификата који садрже одређени јавни кључ. Ова екстензија треба да буде укључена у све сертификате крајњих корисника са циљем да се омогући апликацијама да идентификују одговарајуће сертификате.

За сертификате крајњих корисника, идентификатори кључа субјекта требају бити изведени из јавног кључа, коришћењем једног од два већ поменута уобичајена метода. Ако се користи екстензија идентификатор кључа субјекта она треба да буде означена као *некритична екстензија*.

*3.7.2.3. Коришћење кључа*

Екстензија под именом коришћење кључа (*Key Usage*), дефинише сврху кључа који се садржи у сертификату (јавни кључ), као и њему одговарајућег приватног кључа (тајни или приватни кључ). Могуће је дефинисати следеће примене кључа:

- креирање дигиталног потписа порука (d*igitalSignature* вредност) означава да се тај пар кључева користи за реализацију дигиталног потписа,
- слична примена је и непорецивост (*nonRepudiation),*
- шифровање и дешифровање симетричног кључа (*keyEncipherment*) које се примењује у процесу креирања дигиталне енвелопе,
- шифровање и дешифровање порука (*dataEncipherment),* и
- креирање дигиталног потписа сертификата (*certificateSigning).*

Ако се користи екстензија коришћење кључа она треба да буде означена као *критична екстензија*.

*3.7.2.4. Период коришћења приватног кључа*

Ова екстензија омогућава CA да специфицира период важности приватног кључа субјекта, који, према овој екстензији, може бити и различит у односу на

период важности сертификата. Ова екстензија је намењена за коришћење у односу на кључ за дигитално потписивање и састоји се од две опционе компоненте: *notBefore и notAfter*.

Међутим, PKIX радна група се изјаснила против коришћења ове екстензије и CA који поштују X.509 стандардни профил не смеју да генеришу сертификате са критичном екстензијом у смислу периода коришћења приватног кључа.

#### *3.7.2.5. Политике сертификације*

Ова екстензија садржи секвенцу од једног или више параметара одређених политика, који означавају политику под којом је дати сертификат издат, као и сврхе за које се дати сертификат може користити.[Chokhani S., Ford W., 1999.] У циљу успостављања интероперабилности, предложено је да ови параметри морају садржати само идентификаторе објеката (*Object Identifier, OID*). Када је недовољна примена само идентификатора објеката, предлаже се употреба опционих квалификатора. Ова спецификација дефинише два типа квалификатора који се користе од стране оних који израђују политику сертификације и Сертификационих тела. Типови квалификатора су *CPS Pointer* и *User Notice* квалификатори. Квалификатор *CPS Pointer* садржи показивач на *Certificate Practice Statement (CPS*) које публикује CA. Квалификатор *User Notice* је намењен за приказивање страни у комуникацији када се користи сертификат.

Апликације које имају специфичне захтеве у односу на политику сертификације треба да имају листу политика које прихватају и пореде их са идентификаторима објеката политике у сертификатима који процесирају.

X.509 стандард омогућава да ова екстензија буде или критична или некритична. Ако је дефинисана као критична, систем за валидацију сертификата мора имати могућност да једнозначно интерпретира ову екстензију (укључујући опциони квалификатор), или мора да одбаци дати сертификат.

#### *3.7.2.6. Мапирање политике*

Ова екстензија се користи само у CA сертификатима.[ Choudhury S., Bhatnager K., Haque W., 2002.] У њој се приказују један или више парова идентификатора објеката (OID). Сваки пар укључује *issuerDomainPolicy* и *subjectDomainPolicy.*паривање означава да CA које издаје дигиталне сертификате примењује њену *issuerDomainPolicy* еквивалентну *subject DomainPolicy* од CA које је издало дигитални сертификат датом субјекту.

Корисници CA које издаје сертификате могу прихватити *issuerDomainPolicy* за одређене апликације. Мапирање политика говори корисницима CA које издаје сертификате које политике, придружене CA датог

субјекта, су упоредиве са политикама које они прихватају. Важно је истаћи да CA и апликације могу да подрже ову екстензију, која мора бити *некритична*.

#### *3.7.2.7. Алтернативно име субјекта*

Ова екстензија омогућава додатним идентитетима да буду повезани са субјектом сертификата. Дефинисане опције укључују следеће:

- Интернет e-mail адресу,
- IP адресу,
- DNS име, и
- URI – *Uniform Resource Identifier*.

Остале опције постоје, укључујући комплетну локалну дефиницију опција. Увек када вишеструка имена, или вишеструке форме једног имена, требају бити укључене у сертификат, екстензија алтернативног имена субјекта треба да се користи. С обзиром да је алтернативно име субјекта такође прикључено јавном кључу, CA мора верификовати све делове екстензија.

Ако је једини идентитет субјекта у сертификату представљен у форми алтернативног имена, као што је e-mail адреса, тада се мора осигурати да је *Dnam*e субјекта празна секвенца и да је *subjectAltName* екстензија присутна и означена као критична. Могуће је ограничити алтернативна имена субјекта на исти начин као и *Dname* субјекта коришћењем екстензије ограничења имена.

#### *3.7.2.8. Алтернативно име издаваоца*

Као и у случају алтернативног имена субјекта, ова екстензија се може користити у циљу придруживања Интернет идентификационих карактеристика CA. Алтернативно, име издаваоца треба да буде приказано на исти начин као и алтернативно име субјекта и ова екстензија се не сме означити као критична.

#### *3.7.2.9. Директоријумски атрибути субјекта*

X.509 стандард и PKIX радна група не препознају ову екстензију као суштински део профила, али се може искористити у локалним окружењима. Ако се ова екстензија користи, не треба бити означена као критична.

#### *3.7.2.10. Основна ограничења*

Ова екстензија идентификује да ли је субјект сертификата CA, као и дужину сертификационог пута (*Certification Path*) кроз дато CA. Преко наведене екстензије се специфицира да ли власник датог сертификата може да генерише

дигиталне сертификате за остале кориснике (*Subject Type=CA*) или не (*Subject Type=End Entity*).

Поље *pathLenConstrain*t има значење само ако је вредност CA у овој екстензији постављено на "*true*".У том случају, ово поље даје максималан број CA сртификата који могу пратити овај сертификат у оквиру сертификационог пута.Вредност нула означава да само сертификати крајњих корисника могу бити у датом сертификационом путу. Када ово поље не постоји, не постоји ни ограничење на дозвољену дужину сертификационог пута. Ова екстензија не треба да се појављује у сертификатима крајњих корисника а у случајевима када се користи, мора да буде критична екстензија у свим CA сертификатима.

### *3.7.2.11. Ограничења имена*

Ова екстензија се може једино користити у CA сертификату. Ова екстензија означава простор имена у који треба да се сместе сва имена у накнадним сертификатима у датом сертификационом путу. Ограничења се могу применити на право или алтернативно име субјекта. Ограничења се примењују само када је дата форма имена присутна. Ако нема имена тог типа у сертификату, сертификат је прихватљив. Ограничења се дефинишу у облику дозвољених и искључених подграна имена. Било које име које спада у ограничење дефинисано у искљученој подграни, поље *excludedSubtrees*, није валидно без обзира на информације које стоје у пољу *permittedSubtrees*. За URI, ограничење се примењује на host део имена.

Ако се користи ова екстензија она треба да буде означена као *критична*.

### *3.7.2.12. Ограничења политике*

Ова екстензија се може користити у сертификатима који су издати одређеним CA. Ова екстензија ограничава валидацију сертификационог пута на два начина.[Choudhury S., Bhatnager K., Haque W., 2002 ] Екстензија може бити коришћена да спречи мапирање политика или у циљу захтева да сваки сертификат у путу садржи прихватљив идентификатор политике.

Ако је поље *inhibitPolicyMapping* присутно, његова вредност означава број додатних сертификата који се могу појавити у сертификационом путу пре него што је спречено мапирање политика. На пример, вредност један означава да се процедура мапирања политике може процесирати у сертификатима издатим од стране субјекта датог сертификата, али не и у додатним сертификатима у сертификационом путу.

Ако је поље *requiredExplicitPolicy* присутно, накнадно издати сертификати ће укључивати прихватљив идентификатор политике. Вредност овог поља означава број додатних сертификата који могу да се појаве у сертификационом

путу пре него што се захтева експлицитна политика. Идентификатор прихватљиве политике је идентификатор политике која се захтева од стране корисника сертификационог пута или идентификатор политике која је означена као еквивалентна кроз процедуру мапирања политика.

Усклађена CA не смеју да издају сертификате када је ограничење политике *null* секвенца. То значи да најмање једно од два поља (*inhibitPolicyMapping* или *requiredExplicitPolicy*) мора да биде присутно. Уколико се користи ова екстензија, она може бити означена као критична или некритична.

*3.7.2.13. Проширено коришћење кључа*

Ова екстензија означава једну или више намена за које се сертификовани јавни кључ може користити, заједно са, или уместо, основе сврхе која је означена у екстензији коришћења кључа. Дата екстензија дефинише додатну намену пара кључева асиметричног алгоритма специфицираног у дигиталном сертификату. Могуће је дефинисати следећа проширења примене кључа: [Housley R., 2002;Adams C., Lloyd S., 2003.]

- дигитално потписивање извршног програма (*CodeSigning),*
- дигитално потписивање порука које се преносе посредством електронске поште (*Secure Email*),
- аутентикација сервера приликом креирања криптографског тунела са клијентским рачунаром (*Server Authentication*), и
- аутентикација клијента приликом креирања криптографског тунела са серверским рачунаром (*Client Authentication*).

Ако се ова екстензија користи, она може бити означена као критична или некритична. Ако је екстензија означена као критична, тада се сертификат може користити само за једну од наведених сврха.

Ако је екстензија означена као некритична, тада она означава намењену сврху или сврхе примене кључа и може бити коришћена за проналажење коректног кључа/ сертификата корисника који има вишеструке кључеве/сертификате, и у том случају, се може користити само као саветодавно поље.

Ако сертификат садржи критично поље коришћења кључа и критично поље проширеног коришћења кључа, тада оба поља морају да се процесирају независно и сертификат може бити коришћен само у сврхе које су конзистентне са оба поља. Ако нема такве сврхе, сертификат се не може користити.

*3.7.2.14. CRL дистрибутивне тачке*

Ова екстензија означава како се могу добити информације о CRL. Ова екстензија је подржана од стране CA и апликација.Ако се ова екстензија користи, она треба да буде означена као *некритична*.[Housley R., 2002 ]

### *3.7.3. Најчешће коришћене екстензије*

У претходном погављу је приказана структура дигиталног сертификата. Дат је опис свих поља у структури дигиталног сертификата при чему су детаљније обрађени додатни атрибути–екстензије. Екстензије су карактеристичне за верзију v3 дигиталних серификата. У пољу екстензија се налазе додатне информације везане за власника и издавача сертификата. Најчешће екстензије присутне у верзији v3 дигиталних серификата су:[Housley R., 2002;Adams C., Lloyd S., 2003.]

- основна ограничења (*Basic Constraints*). Преко наведене екстензије се специфицира да ли власник датог сертификата може да генерише дигиталне сертификате за остале кориснике (*Subject Type=CA*) или не (*Subject Type=End Entity),*
- спецификација примене кључа (*Key Usage*). Дата екстензија одређује намену кључа асиметричног алгоритма специфицираног у дигиталном серификату. Могуће је дефинисати следеће примене кључа:
  - креирање дигиталног потписа порука (*Digital Signature*),
  - дешифровање порука чиме се може остварити функција непорецивости (*Non-Repudiation*),
  - шифровање симетричног кључа (*KeyEncipherment*) које се примењује у процесу креирања сесијског кључа или дигиталне енвелопе,
  - шифровање порука (D*ataEncipherment*),
  - креирање дигиталног потписа сертификата (*Certificate Signing*).
- додатна спецификација примене кључа (*Enhanced Key Usage*). Дата екстензија дефинише додатну намену кључа асиметричног алгоритма специфицираног у дигиталном серификату. Могуће је дефинисати следећа проширења примене кључа:
  - дигитално потписивање извршног програма (*CodeSigning),*
  - дигитално потписивање порука које се преносе посредством електронске поште (*Secure Email*),
  - аутентикација сервера приликом креирања криптографског тунела са клијентским рачунаром (*Server Authentication*),

- аутентикација клијента приликом креирања криптографског тунела са серверским рачунаром (*Client Authentication*),

- политика примене дигиталног сертификата (*Certificate Policy*). Дата екстензија поближе дефинише политику и начин примене датог дигиталног серификата. Свака политика примене сертификата је представљена са:
  - ознаком дате политике (*Policy Qualified Id),*
  - вредношћу која описује начин примене сертификата у складу са специфицираном политиком (*Qualified*) .

### 3.8. Методе регистрације корисника

CA може било да добије јавни кључ од самог корисника и да га сертификује, или да генерише за сваког корисника пар јавног и тајног кључа асиметричног криптографског система, и дистрибуира заједно тајни кључ и PKI дигитални сертификат. Из разлога сигурности, сматра се бољом праксом ако корисник сам генерише пар асиметричних јавних кључева (јавни и тајни кључ), а затим да захтев за издавањем сертификата који садржи његов јавни кључ достави CA на сертификацију. Овај метод обезбеђује да се тајни кључ увек чува на једној локацији – код корисника. Међутим, поменути разлози сигурности се могу оправдати само са становишта корисника. Са становишта PKI система (CA), сигурније је да само CA буде надлежно за генерисање парова асиметричних кључева јер се једино на тај начин може контролисати и одржати јединствен квалитет изгенерисаних кључева и јединственост процедуре безбедног чувања изгенерисаних кључева. У том случају, тајни кључеви се дистрибуирају на безбедним медијумима, као што су smart картице или USB smart токени. [Марковић М., 2009.]

Да би се добио дигитални сертификат, мора се прво формирати захтев за добијање сертификата – *Certificate request,* и да га доставите одређеном CA у циљу издавања дигиталног сертификата. [Prodanović R., Petrović M.,2006; Prodanović R.,2007.] Овај захтев садржи све личне информације које ће се појавити и у вашем дигиталном сертификату.Формирани захтев за добијање сертификата-*Certificate request* је дигитално потписан (самопотписан) у циљу гаранције његовог интегритета. CA проверава аутентичност добијеног захтева коришћењем јавног кључа који се у њему садржи. Постоје два коришћена типа захтева за издавање дигиталног сертификата, познати као PKCS#10 и RFC 2511. PKCS#10 формат је далеко једноставнији.

PKCS#10 тип захтева за издавањем сертификата састоји се од следећа 4 поља:

- број верзије формата захтева (од 1 до 3),
- назив власника дигиталног сертификата (означеног као *Dname*),
- јавни кључ власника дигиталног сертификата, и
- атрибути.

Поље атрибута садржи све оне елементе који се морају наћи у дигиталном сертификату, као што је број телефона, број факса, e-mail адреса, највиша вредност финансијске трансакције у случају банкарских сертификата и многе друге карактеристике. У овом пољу се може уградити све оно што не потпада под поље *Dname*, које у ствари представља јединствени стринг који идентификује власника сертификата. Поред тога, *Dname* представља пут кроз X.500 директоријум, тако да се једино може састојати из следећих поља:

- двословни код који означава државу,
- регион,
- адресу,
- фирму,
- одељење у фирми, и
- име власника сертификата.

Постоје генерално два могућа начина генерисања пара јавног и тајног кључа и креирање дигиталног сертификата на бази јавног кључа:

- CA генерише пар јавног и тајног кључа, формира дигитални сертификат и доставља тајни кључ и сертификат власнику, и
- генерисање пара јавног и тајног кључа локално од стране самог власника сертификата коришћењем хардверских или софтверских механизама. Затим се изврши креирање захтева за издавањем сертификата који садржи јавни кључ власника који се шаље ка CA.

У оквиру датог PKI система, политика рада по којој се издају сертификати од стране CA одређује ниво поверења које ће стране у комуникацији имати у датом сертификату. И то је такође публиковано у оквиру CP и CPS. Тако су дефинисане политике по којима се издају сертификати са различитим нивоима поузданости и, у складу са тим, дефинишу се различите методе регистрације које морају бити примењене у вези лица која захтевају сертификате. У ствари, процес регистрације подразумева прикупљање и одговарајућу проверу различитих података од крајњих корисника, директно у личном контакту или у индиректном удаљеном захтеву преко гејтвеја (на пример web претраживачког програма).

У смислу процеса регистрације, политика цертификације PKI система детаљно дефинише следеће:

- како треба применити процес регистрације,
- које информације о лицима је потребно проверити или записати,
- број парова асиметричних кључева (и самим тим број различитих сертификата) које треба генерисати за датог корисника (типично се различити парови кључева генеришу за дигитално потписивање и за дигиталну шифровање (енвелопу),
- где ће се и на ком медијуму генерисати кључеви; кључеви могу бити генерисани од стране самих корисника, од стране RAO или од стране CA, и могу бити сачувани на хард диску, дискети, мини CD медијуму, smart картици или неком другом токену.
- формат сертификата који треба да се генеришу, и
- додатне пословне информације које треба да буду прикупљене за време процеса регистрације.

### *3.8.1. Регистрација у личном контакту*

За одређене PKI системе, директне регистрационе процедуре на бази личног контакта представљају једини безбедни начин за коректну аутентификацију крајњих корисника и дистрибуцију и генерисање кључева и сертификата.

У Intranet окружењу, организација може да примени политику рада према којој корисници морају лично да контактирају особу надлежну за послове безбедности у циљу преузимања токена или smart картице са њиховим кључевима и сертификатима. Ова регистрација захтева да корисник покаже *ID* картицу запослених, личну карту, возачку дозволу, пасош или неки други метод идентификације.

У Internet окружењу, организације са јавним пословницама, као што су банке, поште, итд., могу захтевати од корисника да лично дођу у дату пословницу и дају своје личне податке.[Марковић М., 2009.]

Регистрација личним контактом се одвија тако што службеник који користи апликацију RAO модула унесе личне информације корисника и потврди захтев за издавање сертификата (својим дигиталним потписом). Кључеви се могу генерисати од стране саме RAO апликације и сачувани на диску у заштићеном облику путем лозинке изабране од стране корисника, или корисник може да генерише сопствене кључеве, а да достави само захтев за издавање сертификата до RAO модула.

Одређене RA апликације могу користити и одређене терминалне уређаје за аквизицију биометричких података, као што је фотографија, отисак прста, глас, параметри зенице ока, итд., и да те нетекстуалне податке такође чува у одговарајућем облику у бази података.

Када се изгенерише дигитални сертификат за датог корисника, тај сертификат може бити сачуван на дискети, мини CD медијуму, хард диску, smart картици или на неком другом токену.

Процес издавања дигиталног сертификата на бази личног доласка власника у RA уобичајено се састоји из следећих корака:

- будући власник дигиталног сертификата доставља RAO своје податке лично,
- RAO формира захтев за издавање сертификата на бази добијених података,
- RAO шаље креирани захтев до базе, означава га као процесирани и дигитално га потписује,
- RA узима процесирани захтев из базе, верификује га, дигитално потписује и шаље га као заштићену стандардизовану поруку путем TCP/IP конекције до CA.
- CA верификује добијени захтев. Уколико је захтев валидан, CA издаје и потписује дигитални сертификат у X.509 стандардном формату за дати захтев и смешта га у базу података,
- CA публикује сертификате на X.500/LDAP директоријум. CA такође периодично публикује листу повучених сертификата (CRL – *Certificate Revocation List*) и листу повучених ауторитета (*ARL – Authority Revocation List).* Све листе које се издају морају бити дигитално потписане. ARL се реферише на сертификате самих PKI компонената (само CA, CAO, RA, RAO, итд.), док се CRL односи на власнике дигиталних сертификата у оквиру датог PKI система,
- CA шаље издати сертификат до RA преко TCP/IP. Дигитални сертификат се садржи у заштићеној (дигитално потписаној и шифрованој) стандардизованој поруци,
- RA верификује дату поруку, дигитално је потписује и придружује је бази података,
- RAO преузима издати сертификат из базе, верификује га и чува га у захтеваном формату (PKCS#7, PKCS#12, или други, и
- RAO обезбеђује достављање дигиталног сертификата власнику који га је тражио.

### *3.8.2. Удаљена регистрација*

У многим случајевима, захтева се метода регистрације, која се не ослања на регистрацију личним контактом. Најчешће, ова методасе примењују када је корисник удаљен од RA. У том случају, омогућује се регистрација путем слања захтева за издавање сертификата коришћењем *Internet* претраживачких програма и *WEB* комуникације, e-mail сервиса или *VPN* конекција.[Oppliger, R., 1998;Oppliger, R., 2000;Oppliger R.,2003.] Међутим, најчешће се у ове сврхе користи метода регистрације коришћењем *WEB* комуникације. У тим случајевима, корисник свој захтев доставља до базе RA преко web комуникације. Коришћењем RAO модула се дати захтев даље процесира на исти начин као и у случају регистрације путем личног контакта. Алтернативно, ако политика рада то дозвољава, могуће је да RA буде конфигурисано тако да се добијени захтеви аутоматски прослеђују до CA, без потврђивања од стране RAO. Процес удаљене цертификације уобичајено укључује следеће кораке: [Марковић М., 2009.]

- будући власник дигиталног сертификата доставља захтев за издавање сертификата - *Certificate service request* (*CSR - обично у PKCS#10 формату*) до web сервера CA (*WEB cajm CA*) преко TCP/IP мреже,
- WEB сервер CA шаље добијени захтев преко TCP/IP мреже до RA где се добијени захтев дигитално потписује и смешта у базу података PA. За ову сврху, постоји одговарајуће RA на локацији CA,
- оператор RA (RAO) преузима добијени захтев из базе података и процесира га,
- RAO затим враћа процесирани захтев назад у базу при чему га претходно дигитално потписује и означава као процесираног,
- RA узима процесирани захтев из базе, дигитално га потписује и шаље га као заштићену стандардизовану поруку преко TCP/IP конекције до CA,
- CA верификује добијени захтев. Уколико је захтев валидан, CA издаје и потписује дигитални сертификат у X.509 стандардном формату и смешта га у базу података,
- CA публикује сертификате на X.500/LDAP директоријум. CA такође периодично публикује листу повучених сертификата (CRL – *Certificate Revocation List*) и листу повучених ауторитета (ARL – *Authority Revocation List*).[Myers M., Adams C., Solo D., Kemp D., 1999.] Све листе које се издају морају бити дигитално потписане. ARL се реферише на сертификате самих PKI компонената (само CA, CAO, RA, RAO, итд.), док се CRL односи на власнике дигиталних сертификата у оквиру датог PKI система,

- CA шаље издати сертификат до RA преко TCP/IP. Дигитални сертификат се садржи у заштићеној стандардизованој поруци,
- RA верификује дату поруку, дигитално је потписује и придружује је бази података,
- RA узима дигитални сертификат из своје базе података и шаље га до web сервера преко TCP/IP мреже, и
- *Web* сервер омогућује приступ дигиталном сертификату од стране власника који га је захтевао. У зависности од конфигурације, дигитални сертификат се чува на одређеном директоријуму на хард диску а URL адреса се шаље електронском поштом власнику.

### 3.9. Системи за дистрибуцију сертификата

Дистрибуција сертификата је једна од основних функција које дати PKI систем треба да реализује на флексибилан начин. Постоје три различита типа дистрибуције сертификата:

- достављање издатих сертификата до крајњег корисника,
- публиковање CA цертификата, и
- публиковање издатих и повучених сертификата крајњих корисника на одговарајући начин (путем одговарајућих директоријума) у циљу да буду доступни свим другим крајњим корисницима.

Све ово треба да буде реализовано тако да буде у служби крајњег корисника и да користи организациону инфраструктуру.

Сертификати за крајње кориснике морају бити испоручени лицу које је поднело захтев на начин и у формату који одговара његовим потребама.На пример, сертификати који су захтевани личним контактом могу бити издати било у софтверу било на криптографском хардверу, као на пример *smart* картици. Сертификати издати на основу удаљених захтева углавном су дистрибуирани на исти начин као што су захтеви и стигли, на пример WEB комуникацијом.

Сертификат самог CA мора бити јаван и расположив колико год је то могуће. Сваки корисник у систему мора бити способан да поседује сертификат CA пре него што почне да користи сервисе датог PKI система. Сертификат CA је неопходан да би се верификовао дигитални потпис сертификата свих учесника у систему – тј. да би се проверила аутентичност везе између идентитета одређеног учесника у систему и његовог јавног кључа асиметричног криптографског система. Сертификат CA, као и остали издати сертификати у систему, могу бити испоручивани у различитим форматима, као и публиковани на X.500 или LDAP

директоријуму. Следећа листа формата за запис сертификата треба да буде подржана у систему: PEM; DER, PKCS#7 и PKCS#10.

Коришћење директоријума може значајно побољшати функционалност система. Наиме, у циљу шифровања поруке и њеног слања у облику дигиталне енвелопе, неопходно је поседовати сертификат намењеног примаоца. Такође, у циљу верификације дигиталног потписа неке поруке, потребно је имати сертификат потписника и могућност да се изврши валидација датог сертификата (да ли је у важећем року и да ли није повучен). Због ових разлога, обично се сертификати и CRL смештају на директоријум који је расположив свим овлашћеним учесницима у систему.

Сертификати и CRL могу бити публиковани и на WEB сајту CA, расположиви преко OCSP сервиса, или дистрибуирани e-mail сервисом до свих учесника у систему, у зависности од утврђене политике рада CA.[Myers M., Adams C., Solo D., Kemp D., 1999.]

### 3.10. Повлачење сертификата

За време животног века сертификата (обично је то период од једне до пет година) могуће је да се стекну разлози да се дати сертификат прогласи неважећим и да се датом кориснику не дозволи приступ систему. У том смислу, повлачење сертификата се односи на праксу проглашавања неважећим јавног кључа датог корисника, чиме се аутоматски и његов тајни кључ проглашава неважећим и датом кориснику се тако онемогућава дигитално потписивање порука. Међутим, од суштинске је важности да информација о повучености датог сертификата буде што је могуће пре јавно објављена и доступна свим учесницима у систему (директоријум, *WEB* сајт или *OCSP* сервис). Функција повлачења сертификата је у одговорности CAO, RAO, као и самих крајњих корисника.

Обележја PKI система која подржавају сервис повлачења сертификата укључују:[Housley R., 2002; Adams C., Lloyd S., 2003:]

- креирање листе повучених сертификата (*CRL*) верзије 2,
- креирање интерфејса за повлачење сертификата у оквиру CAO и RAO,
- омогућавање, ако је то у складу са политиком рада CA, да се захтеви за повлачењем сертификата достављају и од стране самих крајњих корисника,
- публиковање CRL на директоријум и коришћење OCSP сервиса, [Myers M., 1999.]

- коришћење дистрибутивних тачака за сертификате (*CDP – Certificate Distribution Points)* које омогућавају дељење CRL на мање делове и стога њихово брже претраживање,
- коришћење функције суспензије сертификата, уместо повлачења јер се суспендован сертификат може поново учинити валидним касније док се једном повучени сертификат не може учинити поново валидним него се мора издати нови сертификат,
- записивање разлога за повлачење сертификата што је омогућено коришћењем CRL верзија 2,
- периодично публиковање CRL или њено ажурирање са сваком новом променом у смислу додавања повучених сертификата. Време и учестаност ажурирања CRL је прописано у политици рада CA,
- записивање времена повлачења сертификата што је омогућено коришћењем CRL верзија 2, и
- опционо укључивање лозинки у политику издавања сертификата које омогућавају крајњим корисницима да повуку њихове сопствене сертификате.

Листа повучених сертификата (*CRL – Certificate Revocation List*) омогућује клијентима и серверима, као и другим ентитетима који комуницирају у датом PKI систему, проверу валидности дигиталних сертификата друге стране у комуникацији.

CRL је бинарна датотека која садржи следеће информације:

- листу повучених сертификата са разлогом њиховог повлачења,
- назив издаваоца CRL,
- време када је CRL издато, и
- време када ће следећа верзија CRL бити публикована.

Важно је истаћи да у случају када CA које издаје сертификате истовремено публикује и CRL, тада је CRL дигитално потписана од стране CA, чиме се омогућује свим корисницима да буду сигурни у информације које CRL садржи.

Приступ CRL се врши када је потребно користити јавни кључ из PKI сертификата одређеног корисника коме треба послати шифровану поруку или треба верификовати дигитални потпис примљене поруке од стране тог корисника. Било која од поменутих активности треба да садржи следеће кораке:

- проверити валидност дигиталног сертификата датог корисника,
- узети серијски број сертификата,

- приступити (учитати) CRL (обично се то ради download-овањем са X.500 директоријума коришћењем LDAP претраге и LDAP одговора или узимањем из локално сачуване CRL),
- проверити дигитални потпис CRL, време њеног публиковања и време када ће следећа верзија бити публикована,
- проверити да ли се дати сертификат налази у CRL (на бази серијског броја),
- алармирати датог корисника ако је сертификат повучен, и
- извршити жељену криптографску апликацију уколико се сертификат не налази у CRL или ако намењени корисник, након аларма, предузме активности да његов сертификат не буде више у CRL.

Уобичајено, CA је одговорно за непорецивост трансакција, обезбеђујући audit log датотеке и чувајући све публиковане верзије CRL. Алтернативно, корисничка апликација може реализовати механизме којима се обезбеђује непорецивост трансакција. Међутим, у том случају, за сваку извршену трансакцију, мора се чувати сама порука као и CRL које је коришћено у тренутку када је верификован дигитални потпис поруке (или је порука шифрована јавним кључем корисника). Једино сте тада у могућности да докажете да сте користили јавни кључ намењеног корисника за верификацију или шифровање у тренутку када његов дигитални сертификат није био повучен.[Марковић М., 2004.]

Предности CRL су:

- CRL је широко подржана технологија у оквиру PKI индустрије,
- CRL може бити дистрибуирано до крајњих корисника на различите начине, укључујући push и pull методу,
- CRL може бити архивирано да обезбеди непорецивост за претходно извршене трансакције,
- CA издаје и PKI сертификате и CRL, и
- многе PKI апликације могу добити CRL са X.500 директоријума коришћењем DAP/LDAP протокола.

Препозната су следећа ограничења употребеCRL:[ Housley R., 2002.]

- Корисник мора имати текућу верзију CRL у тренутку верификације дигиталног потписа или шифровања података. Пошто је CRL датотека, корисникова апликација мора обезбедити нову верзију CRL, ако је копија на његовом локалном систему застарела. У великом PKI окружењу, корисник може имати потребу да обезбеђује CRL веома често, а само CRL може бити веома велико. Стога, све то може значајно успорити рад неке PKI апликације због неопходности да се увек

обезбеђује последња верзија CRL са веома заузетог директоријумског сервера (или неке друге CRL дистрибуционе тачке),

- CRL се креира и публикује периодично, при чему је тај период одређен политиком рада CA (CPS – *Certificate Practice Statement*). У систему је потребно веома студиозно евалуирати колико често треба креирати и публиковати CRL у оквиру датог PKI система. Пречесто публиковање CRL може загушити читаву инфраструктуру, док недовољно често публиковање може резултовати у потенцијалној могућности да се неки сертификати користе иако су већ повучени, и
- CA периодично креира CRL датотеку на бази примљених захтева за повлачењем издатих дигиталних сертификата. По креирању, CRL укључује информације од када је CRL валидна, до када је валидна и када ће се креирати нова верзија CRL која ће заменити претходну верзију. Као што је раније речено, CA дигитално потписује CRL тако да крајњи корисници могу бити сигурни у интегритет и аутентичност информација у оквиру CRL.

Када истекне важност дигиталних сертификата, њихов статус у вези повучености се више не приказује у оквиру CRL. Ова мера помаже да се минимизује величина CRL за време рада датог CA а и сматра се да статус повучености нема значаја за сертификат коме је истекла важност.

Поред процедуре повлачења сертификата, постоји и још једно специјално стање које се назива суспензија сертификата. За разлику од једном повученог сертификата, суспендован сертификат има карактеристику да поново може бити валидан. CA обично суспендује сертификате када постоји било каква сумња да је тајни кључ корисника компромитован или изгубљен. То такође може бити веома корисно стање сертификата у случајевима када је крајњи корисник сигуран да једно време неће користити свој тајни кључ. Суспендујући свој сертификат, крајњи корисник у ствари онемогућује коришћење свог тајног кључа све док CA не учини дати сертификат поново валидним. Услови под којима се врши суспензија, престанак суспензије или повлачење сертификата дефинисано је у CPS датог CA. Серијски број суспендованог сертификата је укључен у CRL уз наведену карактеристику повлачења: “суспендован”. Ако је сертификат поново валидан, његов серијски број се брише из наредне публиковане верзије CRL.

Профил CRL који одговара стандарду X.509v2 (RFC 3280) дефинише основни скуп информација које се очекују да буду садржане у свакој CRL.[Housley R., 2002.] Поменути профил такође дефинише локације у оквиру CRL за често коришћене атрибуте, као и заједничке репрезентације тих атрибута.

Према поменутом стандарду, профил назван *certificateList* садржи следећа поља:

- *tbsCertList*, које садржи следеће податке:
  - *version* – када се користе екстензије, како је специфицирано стандардом X.509 v2 профилом, ово поље мора постојати и мора специфицирати верзију 2,
  - *signature* – садржи идентификатор алгоритма којим се дигитално потписује CRL,
  - *issuer* – представља издаваоца CRL (најчешће је то CA које издаје дигиталне сертификате),
  - *thisUpdate* – указује на датум публиковања дате CRL,
  - *nextUpdate* – указује на датум када ће следећа верзија CRL бити публикована. Нова верзија може бити публикована и пре наведеног датума, али никако касније од тога.
  - *RevokedCertificates* – дигитални сертификати повучени од стране CA су јединствено идентификовани њиховим серијским бројем. Време повлачења и друге CRL екстензије су такође дефинисане.
  - *CRLextensions* – поље које може бити коришћено само ако се ради о верзији 2 и садржи додатне атрибуте који могу бити од користи, као што су: редни број CRL, дистрибуциону тачку, итд.
- *signatureAlgorithm* – садржи идентификатор алгоритма који CA користи за дигитално потписивање поља *tbsCertList* и мора садржати исти алгоритам као и претходно наведено поље *signature*.
- *signatureValue* – садржи дигитални потпис поља *tbsCertList* кодован по стандарду *ASN.1 DER.*

CA је одговорно за одговарајућу дистрибуцију и расположивост CRL за окружење које опслужује. Најчешће је то постигнуто излагањем CRL на X.500 директоријумском серверу, као типичном сервису подржаном од стране CA. Након тога је у одговорности крајњег корисника, или његове софтверске апликације, да преузима CRL из X.500 директоријума. Постоје и алтернативни начини дистрибуције CRL, као што је слање CRL свим корисницима путем електронске поште *(push* метод) или објављивање CRL на одговарајућем *WEB* сајту CA са кога корисници могу преузети (d*ownload*-овати) CRL датотеку (*pull* метод као што је и преузимање CRL са X.500 директоријумског сервера). Поменуте две алтернативе су мање присутне у PKI окружењу из разлога погодности X.500 приступа и широке распрострањености примене LDAP комуникационог протокола коришћеног за интеракцију са X.500 директоријумом.[Housley R., Hoffman P.,1999; Boeyen S., Howes T., Richard P., 1999.]

DAP (*Directory Access Protocol*) је један од четири протокола дефинисаних у оквиру X.500 стандарда у циљу подршке отвореним и стандардизованим директоријумским сервисима. Директоријум, у X.500 стандардном смислу, представља специјалну форму базе података која је дизајнирана да буде посебно погодна за коришћење на Internet-у и другим дистрибуираним системима.

X.500 стандард дефинише две основне компоненте директоријума:

- Директоријумски системски агент (DSA) – за управљање информацијама у оквиру директоријума, и
- Директоријумски кориснички агент (DUA) – корисничка апликација која омогућује кориснички приступ директоријумским сервисима.

DAP дефинише протокол комуникације између DUA и DSA који омогућује успоставу конекције између клијентске апликације и директоријума, преузимање информације из директоријума и ажурирање информација унутар директоријума.[Burr W.E., 1988.]

LDAP (*Lightweight Directory Access Protocol*) поједностављује приступ директоријумским сервисима који су моделовани на бази X.500 стандарда. [ Tuttle S., Ehlenberger A.,2004.] LDAP има сличне функције као и DAP али ради директно на TCP/IP протоколу. [Bruce Schneier,1996; Johner H., Fujiwara S., Yeung A. S., 2000.]

### 3.11. Стандарди који се односе на функционисање PKI система

Стандарди који се односе на функционисање PKI система неопходни су за дефинисање:

- процедуре регистрације субјеката,
- формата цертификата,
- формата листа опозваних цертификата,
- формата порука при регистрацији (захтеви и одобрења издавања цертификата),
- формата дигиталних цертификата,
- аутентикационих протокола.
- најважније тело задужено за интероперабилност PKI стандарда је PKI радна група IETF (Internet Engineering Task Force) организације, позната

и као PKIX група. PKIX спецификација се базира на две групе стандарда :

- ITU-T X.509 стандарди
- PKCS стандарди дефинисани од стране RSA Data Security. [Adams C., Farrell S., Kause T., Mononen T., 2005.]

Општеприхваћени и највише коришћен стандард који подржава PKI системе је ITU-T X.509 чија основна сврха је у дефинисању стандардног формата дигиталних сертификата. Верзија 3 овог стандарда која је тренутно важећа, усвојена је 1996. године. Међутим, овај стандард није намењен за дефинисање комплетних функција PKI система.

Стандардом X509 дефинисана је структура, поступак добијања и начин представљања цертификата. Структура цертификата описује се коришћењем ASN.1 метода за описивање апстрактних типова. У наставку ће бити наведене његове основне карактеристике и структура цертификата која је у складу са овом нотацијом. Софтверски систем за производњу дигиталних сертификата користи ASN.1 нотацију за опис структуре сертификата. [Adams C., Farrell S., Kause T., Mononen T., 2005.]

### *3.11.1. Abstract sintax notation one - ASN.1*

Open System Interconnections (OSI) је стандард којим су дефинисана правила за међусобно повезивање рачунарских система и то од основног, физичког нивоа, до апликативног нивоа. Да би стандард био независтан од имплементационих карактеристика појединачних система објекти се описују на апстрактан начин, кроз податке које садрже, сервисе које пружају и комуникационе интерфејсе према спољашњој средини. Систем који се примењује у *OSI Abstract Syntax Notation On*e је метод за описивање апстрактних типова података и начин за кодирање вредности неког типа дефинисаног овом методом. Према овом стандарду тип је дефинисан скупом својих вредности и постоје четири основна облика типова:[Adams C., Farrell S., Kause T., Mononen T., 2005.]

1. прости типови, представљају скупове основних вредности,
2. структурни типови који се састоје од компоненти,
3. везани типови, они се изводе из других типова, и
4. остали типови.

Типови и њихове вредности могу се именовати и та се имена могу користити у дефинисању других типова и вредности. Оператор додељивања се означава са ::=. Сваки *ASN.1* тип (осим *CHOICE* и *ANY*) одређен је припадношћу класи и једним ненегативним бројем. Постоје четири класе:

- универзална, за типове чије је значење исто независно од апликације,
- апликативна, за типове код којих је значење дефинисано унутар апликације,
- приватне за типове чије значење је везано за локално окружење, и
- контексно-зависна за типове чије је значење специфично у оквиру структурних типова.

Два типа се сматрају једнаким ако и само ако припадају истој класи и имају исти број. Овим механизмом се може описати сваки апстрактни тип података.

Следеће питање адресирано овим стандардом је начин представљања вредности апстрактно дефинисаног типа. То питање се разрешава формулисањем основних правила за кодирање, *Basic Encoding Rules (BER),* којима се свака *ASN.1* вредност представља као низ бајтова. Овај, основни начин кодирања, није једнозначан тј. иста вредност се може кодирати на више различитих начина. Начини кодирања су следећи: [Марковић М., 2009.]

1. примитивни - са унапред познатом дужином податка,
2. конструктивни - са унапред познатом дужином податка,
3. конструктивни - са непознатом дужином податка.
4. код вредности неког типа састоји се од најмање прва три блока, од следећа четири:
5. идентификациони део - којим се једнозначно одређује тип податка (класа и број), метод кодирања (примитивни или коструктивни),
6. спецификација дужине податка - којом се код података са одређеном дужином специфицира број бајтова за регистровање податка или, ако дужина није унапред позната, садржи код којим се та ситуација идентификује,
7. садржај - низ бајтова којим се репрезентује вредност, и
8. ознака за крај податка - уколико није унапред познате дужине.

Напоменули смо раније да *BER* кодирање није једнозначно што може изазивати проблеме у ситуацијама када је једнозначност захтевана особина. Због тога је формулисан низ ограничења на правила *BER* кодирања тако да се постигне једнозначност у кодирању вредности неког *ASN.1* типа. Тај рестриктивни скуп правила се означава са *DER* (*Distinguished Encoding Rules*). Грубо говорећи, једнозначност се постиже захтевајући да код вредности буде минималан у погледу дужине (броја бајтова). Дакле, овим системом смо у могућности да опишемо и представимо вредност произвољног апстрактног типа.

### *3.11.2. ITU X.509 v3 сертификат-структура*

Према овом стандарду сертификат се састоји од три дела. Први део чине подаци значајни за сам цертификат представљени променљивом *tbsCertificate,* други део представља идентификатор алгоритма за потписивање представљен променљивом s*ignatureAlgorithm* и на крају сам потпис представљен променљивом signature.

Променљива *tbsCertificate* је структурног типа и садржи следећа поља:[Housley R., 2002; Adams C., Lloyd S., 2003.]

- верзија – означава верзију стандарда која је примењена при генерисању сертификата,
- серијски број – редни број издатог сертификата. Начин додељивања бројева мора бити јединствен тј. име издавача сертификата и редни број цертификата јединствено одређују сертификат,
- потпис – садржи идентификатор алгоритма којим издавач сертификата врши потпис цертификата,
- валидност – специфицира се период унутар којег се сертификат сматра важећим ако није опозван,
- власник сертификата – идентификатор (име) власника сертификата коме се придружује јавни кључ који садржи цертификат,
- јавни кључ – јавни кључ власника сертификата и идентификатор алгоритма за који је намењен,
- јединствени идентификатори – поље које омогућава поновну употребу имена присутних у сертификату,
- поље додатних информација – садржи скуп поља која по потреби могу носити још неке информације осим ових основних. Неке од ових додатних информација могу носити атрибут *CRITICA*L или *NONCRITICAL*. Уколико апликација која барата цертификатом наиђе на информацију означену са *CRITICAL* и не распозна је, мора сертификат одбацити као неисправан.

Поље додатних информација може садржати информације помоћу којих се идентификује јавни кључ којим се сертификат проверава, уколико издавач има више парова јавних и тајних кључева. Затим информације о намени јавног кључа који сертификат садржи, опис услова под којима је цертификат добијен и под којим се и зашта може користити, алтернативна имена издавача и власника сертификата.

Према досадашњим искуствима оваква структура сертификата испуњава све захтеве које је пракса поставила.

### *3.12.3. ITU X.509 v2 листа опозваних сертификата*

Према овом стандарду листа опозваних сертификата се састоји од три дела. Први део чини листа опозваних сертификата представљена променљивом *tbsCertList,* други део представља идентификатор алгоритма за потписивање листе опозваних сертификата представљен променљивом *signatureAlgorithm* и на крају сам потпис представљен променљивом *signature.* Променљива *tbsCertList* је структурног типа и садржи следећа поља:[Housley R., 2002; Adams C., Lloyd S., 2003.]

- верзија – означава верзију стандарда која је примењена при генерисању листе опозваних сертификата,
- потпис – садржи идентификатор алгоритма којим издавач листе опозваних сертификата врши потпис листе опозваних сертификата,
- име издавача листе – идентификује издавача листе,
- датум издавања текуће листе опозваних сертификата,
- датум следећег ажурирања листе опозваних сертификата,
- списак опозваних сертификата, и
- поље додатних информација.

Списак опозваних сертификата се састоји од низа редних бројева сертификата који заједно са идентификатором издавача сертификата на јединствен начин одређују опозвани сертификат.

### *3.12.4. ITU X.509 v2 листа опозваних сертификата - формирање*

Издавач сертификата региструје и формира захтеве за опозив сертификата сходно својој политици, формира нову листу опозваних сертификата. Затим се као и код генерисања цертификата од *BER* кода коришћењем договорених алгоритама формира отисак и потпис листе опозваних сертификата.[ Housley R., 2002, ;Adams C., Lloyd S., 2003.]

У циљу додатне стандардизационе подршке *X.509* стандарду, произвођачи, корисници и комитети за стандарде су се углавном окренули коришћењу de facto PKI стандарда, дефинисаних у PKCS (*Public Key Cryptographic Standards*).[Dworkin M.,2001.]

PKCS представља серију стандарда који покривају функције PKI система у областима регистрације, обнављања издатих дигиталних сертификата и дистрибуције листа опозваних сертификата. За интероперабилност PKI система,

најважнија су следећа четири PKCS стандарда: [Adams C., Lloyd S., 2002;Adams C. , Lloyd S., 2003.]

- PKCS#1 стандард за опис реализације процедура дигиталног потписивања и дигиталне енвелопе на бази RSA асиметричног криптографског алгоритма,
- PKCS#7 стандард за синтаксу криптографских порука (*Cryptographic Message Syntax Standard*),
- PKCS#10 стандард за синтаксу захтева за издавање дигиталног цертификата *(Certificate Request Syntax Standard),* и
- PKCS#12 стандард за синтаксу размене личних информација (*Personal Information Exchange Syntax Standard*).

### 3.13. Типови CA и могући начини реализације

Постоји неколико типова CA, од којих су четири типа најзначајнија[Marković M., 2004.]:

- појединачна CA одређених предузећа (*corporate CA*),
- CA затворених група корисника,
- CA вертикалних индустрија (финансијски системи, медицина, телеком, ...),
- јавна CA (домаћа – интернационална).

Што се тиче начина реализације CA, постоје генерално три начина:

- коришћење услуга постојећег CA (*outsourced CA*),
- изградња сопственог CA у оквиру дате организације на бази иностране CA технологије (*insourced CA*), и
- изградња сопственог CA у оквиру дате организације на бази домаће CA технологије (*insourced CA*).

Прва варијанта представља најповољније решење за компанију која жели да имплементира PKI технологију искључиво у својој организацији (за своје запослене и сараднике) а не жели да инвестира превише у решење CA. У том смислу, одређене организације које представљају јавна међународна CA (као што су *GlobalSign и VeriSign*) нуде outsourced CA решење у коме они практично издају дигиталне сертификате корисницима дате организације, која у том случају игра улогу PA. [Burr W.E., 1988.]

Међутим, уколико организација претендује да има одређене економске користи од јавне продаје дигиталних сертификата заинтересованим корисницима из њиховог домена, тада су прикладније друге две варијанте реализације CA. То решење је онда значајно скупље од прво поменутог решења outsourced CA. Од две наведене insourced варијанте, варијанта која подразумева страну CA технологију је сигурно скупља него варијанта са домаћом технологијом. Са друге стране, реализација CA са домаћом технологијом омогућује адаптивност и скалабилност решења у складу са дефинисаном политиком корисника. [Kumar I., 1997;Burr W.E.,1998.]

### 3.14. Подршка политици рада PKI система

Било које безбедносне мере које се примењују у оквиру неке рачунарске мреже, које између осталог могу да укључују мрежне баријере (*firewall*), ID картице или контролу приступа до PKI инфраструктуре захтевају постојање свеобухватне безбедносне политике (политика заштите) рада дате мреже. Ова политика дефинише процедуре које омогућују приступ корпорацијским ресурсима или информацијама, и које онемогућују неауторизованим корисницима приступ тим ресурсима. Ова безбедносна политика укључује поставку и детаљну дефиницију функција које треба да реализују сви елементи PKI инфраструктуре датог система. У тој безбедносној политици, посебно место треба да заузимају специфичне процедуре, профили и ограничења везана за сертификате и захтеве за издавање сертификата. Овај део безбедносне политике се назива политика сертификације. [Chokhani S., Ford W., 1999.]

Управљање политиком рада одређеног PKI система врши Сертификационо тело. У том смислу, све PKI апликације које користе софтверске и хардверске криптографске механизме се централистички управљају, што редукује трошкове и повећава ниво контроле. [ISO/IEC 9594-8/ITU-T 1997.;Mell P., Bergeron T., Henning D.,2005;Moses T.,2003.]

Политика сертификације, тј. политика по којој се издају сертификати у датом PKI систему, треба да пропише све процедуре које се односе на коришћење и издавање сертификата. Ова политика укључује следеће:

- под којим условима се издају сертификати,
- које информације треба да буду укључене у сертификат,
- за коју сврху се користи дати сертификат, и
- шта се дешава када истекне важност сертификата (када сертификат дође до краја свог животног века).

Генерисање политике сертификације је веома велики и сложен посао који треба да буде недељиви део корпорацијске безбедносне политике. Могући поступак генерисања политике сертификације би се могао поделити на четири главна дела:

- одлучивање који све елементи јединственог имена (distinguished name – Dname) који јединствено идентификују корисника треба да се појаве у свим сертификатима који су издати у складу са политиком сертификације (неки елементи могу бити опциони),
- одређивање које екстензије ће се појавити у сертификатима издатим у складу са овом политиком,
- одлучивање које додатне регистрационе информације треба да буду прикупљане у циљу издавања сертификата. Ове информације се не публикују у сертификату, и
- одређивање додатних операционих ограничења која треба да буду спроведена у вези издавања и коришћења сертификата.

### 3.15. Управљање радом PKI система

Једна од основних обележја политике сертификације треба да буде у могућности управљања радом читавог PKI система.На веома високом нивоу, политике сертификације се деле на оне које се односе на прикупљање захтева за издавањем сертификата у личном контаку и на оне које добијају захтеве удаљеним путем (нпр. путем *WEB* комуникације) .[Марковић М., 2009.]

- **Прихватљива величина кључа** – задатак овог дела политике сертификације је да обезбеди да дужина кључева који се генеришу у оквиру CA и дужина кључева које користе елементи PKI система (CAO, CA, RAO, RA) за дигитално потписивање не буду краћи од оних који се захтевају у безбедносној политици датог система.
- **Прихватљиви асиметрични криптографски алгоритми** – и у овом случају политика сертификације треба да обезбеди да се листа прихватљивих (од стране политике безбедности) асиметричних алгоритама користи за дигитално потписивање и дигиталну енвелопу. Ова листа типично садржи следеће алгоритме RSA, DSA и ECDSA.
- **Прихватљиви hash алгоритми** – идентично као у претходне две тачке, политика сертификације треба да дефинише прихватљиву листу hash алгоритама. Најчешће се користе MD5 и SHA-1 алгоритми.

- **Извор генерисања кључева** – ово операционо ограничење се углавном односи на политику сертификације у вези регистрације личним контактом, и конкретно се односи на то како треба да се генерише асиметрични пар кључева за датог корисника.[Merkle, R.C. and Hellman, H.E.,1981.] Могуће опције су: генерисање кључева коришћењем функција из PKCS#11 стандардног интерфејса на smart картици или токену, локално генерисање кључева у оквиру RAO модула у софтверу и учитавање захтева за издавањем сертификата у PKCS#10 формату из одговарајуће датотеке, токена или smart картице.
- **Период валидности сертификата** – овај период се дефинише конкретно у оквиру CPS документа. Минимално овај период може бити један дан а максимално до краја истека важности сертификата самог CA.
- **Замена сертификата** – када сертификат дође до краја свог животног века, политика сертификације треба да прецизно дефинише поступак којим се врши издавање новог сертификата као и процедуре (ручне или аутоматске) обавештавања корисника и саме процедуре замене.
- **Архивирање тајног кључа** – у складу са безбедносном политиком, за одређене асиметричне парове кључева предвиђа се архивирање тајног кључа за каснији опоравак шифрованих порука у случају потребе.
- **Лозинка за потребе повлачења сертификата** – нормално се сертификати повлаче на основу захтева од CAO или RAO модула који има функцију издавања сертификата. Међутим, могуће је дозволити крајњем кориснику могућност да пошаље захтев за повлачење свог сертификата путем WEB комуникације али уз коришћење лозинке која је дефинисана током процедуре регистрације датог корисника.

### 3.16. Безбедносни аспекти PKI система

С обзиром да је CA срце читавог PKI система, основни захтев безбедности који се поставља пред PKI систем је потпуна безбедност самог CA. Ако је CA систем компромитован интерним или екстерним нападом, и читав PKI систем је компромитован. Конкретно, CA систем мора да реализује следеће: [Марковић М., 2009.]

- потпуну безбедност тајних кључева CA,
- да спречи нападе спољашњих злонамерних корисника,

- да обезбеди редудантност система и обезбеђење оперативности у случају било какве хаварије, и
- да обезбеди персоналну идентификацију свих активности које се спроводе од стране CAO и RAO.

Дакле, систем безбедности CA треба да осигура потпуну безбедност тајних кључева, интегритет података и константну расположивост система.[CERT/CC Statistics 1988-2006;CERT, Securing Network Servers.,2000.] Ове перформансе система се остварују применом smart картица за контролу приступа важним ресурсима система, за дигитално потписивање и заштиту тајности порука, као и применом хардверских безбедносних модула (HSM) за остваривање безбедносно најкритичнијих апликација у систему (генерисање тајног кључа CA и дигитално потписивање цертификата (издавање цертификата)). У том смислу, тајни кључеви CA и RA система, као и њихових оператора, треба да су заштићени криптографским механизмима највишег нивоа. Сви важни подаци коришћени од стране CA и RA се чувају у базама података, што олакшава примену редудантних механизама у циљу спречавања губитка података. Све интеракције и размене података између елемената PKI система се дигитално потписују и шифрују у поступку дигиталне енвелопе што осигурава немогућност приступа датој комуникацији од стране злонамерних корисника.[Chen L. and Pederson T.P.,1995.] Обележја која би требало да су подржана од стране конкретног CA система:

- CA систем треба да подржи коришћење хардверског безбедносног модула (HSM) за генерисање тајног кључа самог CA, за безбедно складиштење података и за дигитално потписивање сертификата,
- систем треба да подржи коришћење smart картица за безбедно чување података, контролу приступа и генерисање/дистрибуцију кључева и сертификата на свим кључним тачкама датог PKI система,
- коришћење стандардних порука (у стандардном формату) дигитално потписане и шифроване (дигитална енвелопа) за сву комуникацију између појединих елемената и модула PKI система,
- сваки приступ базама података треба да има јединствени процесни број,
- CA систем треба да има могућност да безбедно архивира корисничке парове асиметричних кључева за шифровање у процедури дигиталне енвелопе у циљу омогућења њиховог накнадног опоравка у случају да је потребно дешифровати податке који су шифровани помоћу ових кључева, и
- Потребно је да дати PKI систем прође одређену званичну сертификацију од стране овлашћених лабораторија за ту сврху у смислу способности за реализацију активности за које је дати систем намењен.

Као што је већ речено, безбедност PKI система је одређена безбедношћу пре свега тајног кључа CA, али и свих осталих тајних кључева који се користе у систему. Овај ниво безбедности се може остварити само уз коришћење одговарајућег криптографског хардвера како на страни корисника система, тако и на страни самих кључних елемената у систему. У том смислу, потребно је користити smart картице, као криптографски хардвер прилагођен коришћењу за крајње кориснике и за оператере у оквиру PKI система, и хардверске криптографске модуле (HSM), неопходне за коришћење у серверским апликацијама и у самом CA систему. У системима у којима се захтева највиши ниво безбедности, HSM модули се предвиђају за коришћење и на нивоу RAO и CAO оператора. У циљу обезбеђења функције непорецивости у систему, потребно је да крајњи корисници свој асиметрични пар кључева генеришу и чувају на криптографском хардверу (smart картици). Другим речима, фундаментални захтев и сврха криптографског хардвера је да осигура да тајни кључ никад не напусти хардверски модул, у ком случају би евентуално могао бити компромитован.

### *3.16.1. Општа обележја HSM*

- Генерисање кључева на HSM – генерисање пара кључева асиметричног криптографског алгоритма, као и захтеваног броја симетричних кључева (опционо), реализује се унутар HSM, [Marković,M., Đorđević, G., Unkašević, T., 2003.]
- Безбедно чување криптографских параметара – кључеви и остали криптографски параметри се безбедно чувају (у шифрованом облику) на HSM модулу,
- Безбедни back-up криптографског материјала – кључеви и други криптографски параметри се могу безбедно сачувати (back-up-овати) на smart картицама или другим HSM модулима,
- HSM мора реализовати функцију детекције покушаја злонамерног приступа модулу (*tamperproof)* – модул треба да обезбеди детекцију злонамерног приступа и уништење безбедносног материјала на модулу ако је детектован приступ,
- Модул мора бити способан да реализује криптографске функције – ово је једна од основних намена HSM и ови модули су оптимизовани за реализацију функција генерисања кључева, као и реализацију симетричних и асиметричних криптографских алгоритама много ефикасније него у софтверу или на smart картицама, и
- Безбедно коришћење *PIN* броја – модул се активира уношењем *PIN* броја.

### *3.16.2. Општа обележја smart картица*

- генерисање кључева на *smart* картици – генерисање пара кључева асиметричног криптографског алгоритма, као и захтеваног броја симетричних кључева (опционо), реализује се унутар *smart* картице,[Gisela Meister, 2002.]
  - безбедно чување криптографских параметара – кључеви и се безбедно чувају у заштићеном делу меморије smart картице,
  - Smart картице су саме по себи *tamperproof* модули,
  - *Smart* картица је способна да реализује криптографске функције на самој картици али спорије него на *HSM* модулима, и
  - безбедно коришћење *PIN* броја – приступ функцијама *smart* картице је омогућен уношењем коректног *PIN* броја.

# 4. КРИПТОГРАФСКИ АСПЕКТИ ЗАШТИТЕ РАЧУНАРСКИХ МРЕЖА

## 4.1. Криптографија

Потреба за споразумевањем међу људима стара је безмало колико и само људско друштво. Многи облици споразумевања постојали су и пре појаве писма.У настојању да омогуће бржу и лакшу размену информација, људи су непрекидно усавршавали облике споразумевања. Први сукоби међу народима условили су појаву прикривања садржаја информација ради чувања њихове тајности. Наиме, развојом друштва је и до сукобљавања интереса, што је условило појаву неповерења, а тиме и потребу сакривања намера супростављених страна.Тако се појавила шифра као средство заштите тајности. Шта су заправо шифре - те увек добро чуване тајне о којима се мало говори и пише, а ипак понешто зна? Када се ово каже, мисли се на људе који су посвећени у тајне шифре, али и на оне који се труде да у њима поникну. Тако шифра сама за себе представља тајну. Она је намењена да сачува туђе тајне, те се зато каже да је шифра унапред договорени поступак којим се нека информација трансофрмише у неразумљив облик за свакога који га не познаје.

Шифра је стара, вероватно, колико и само писмо.Првобитна писма састојала су се из низа цртежа који су имали симболичка значења.Свако писмо може се сматрати шифром у том смислу што коришћени знаци немају значење сами по себи, већ изражавају одређену мисао тек пошто се протумаче по унапред утврђеним и договореним правилима између онога ко пише и онога ко чита. За сваког ко не познаје знаке неког језика-све-што је на том језику написано представља тајну. Та се тајна може открити тек када се савлада писмо тог језика.

Научна област која се бави истраживањем поступака заштите тајности информација на начин да се било која информација може трансформисати у облик који ће бити неразумљив за свакога коме није намењена назива се **КРИПТОГРАФИЈА** (крипто–тајна, логија–наука). Криптологија је мултидисциплинарна научна област јер у себи садржи математику, статистику, лингвистику, електронику и друге научнотехничке дисциплине и области људске делатности.Њен развитак је највећем делом везан за математику и њој сродне области, јер се користи њиховим методама у проналажењу и анализирању нових шифара.

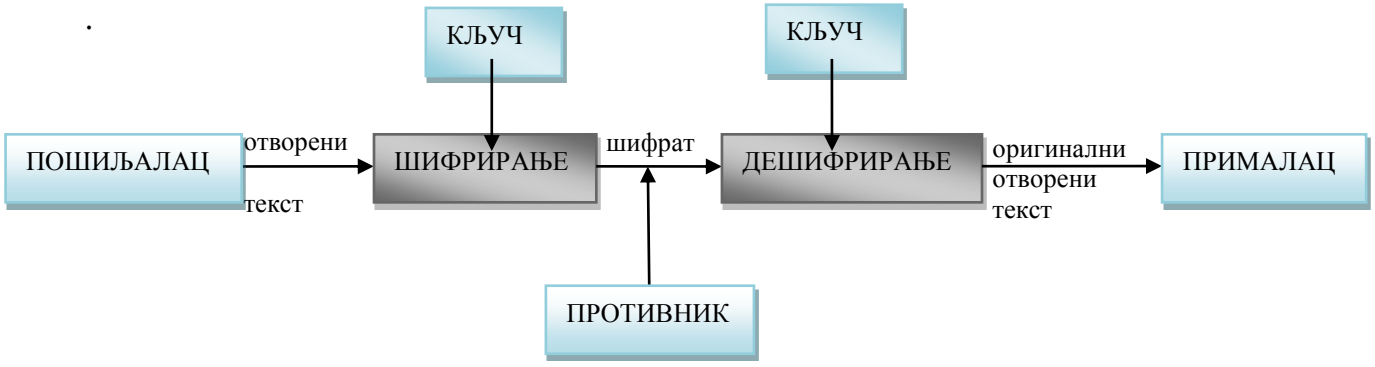
Криптологија се развија у два правца, и сагасно томе, дели се на две подобласти. Једна од њих бави се проналажењем и проучавањем метода за“разбијање“ шифара и назива се **криптоанализа.** [Chabaud F.,1995.] У преносу

информација срећу се различите врста порука:писани текст, говор, слика, итд вака од ових врста има специфичну заштиту, тако да се у оквиру криптографије разликујемо криптографију – која се бави истраживањем и проучавањем метода жаштите писаног текста, риптофонију – која се бави жаштитом говора, криптовизију – која се бави заштитом слике, тд.

Сваки напсани логичан текст (исто важи и за говор, слику, или рачунарске податке) зове се **отворени текст (ОТ).** Поступак његовог трансформисања помоћу шифре зове се **шифровање**, а обрнуто, добијање отвореног текста из шифрованог – **дешифровање.** Тако добијени шифровани текст зове се **шифрат (СТ).** Када се не познаје шифра, тада се шифрат зове **криптограм.** Зато се, поред појма *дешифровање*, уводи појам *декриптирање*, као поступак којим се до отвореног текста поруке долази и без познавање шифере, односно трансформације којом се отворени текст преведан у шифрат.[Schneier B., 1996.]

Трансформисање (шифровирање) отвореног текста у шифровани одређеним трансформацијама (шифрама) може се вршити коришћењем операција премештања или замењивања слова и конбинацијама ових двеју операција.То су једино могуће операције шифровања.У зависности од тога шта се узима за елеменат отвореног текста могу се у шифратима уочавати одређене карактеристике које се преко уведених трансформација преносе из отвореног у шифровани текст. На слици 4.1. шематски је приказан целокупан процес криптовања тј. шифрирања, односно декриптовања тј. дешифровања поруке, тачније отвореног текста.

.




**Слика 4.1**: Шифрирање и дешифрирање поруке

Једна могућа шема постизања тајности може да буде ова:ентитети А и Б размењују кључ пар **(e, d)**. У неком следећем тренутку, ако А жели да пошаље поруку **m** ентитету Б, потебно је да израчуна $\boldsymbol{c = E_{e(m)}}$ и да резултат (шифровану поруку, односно шифрант) пошаље Б.По пријему **c**, рачуна $\boldsymbol{D_d(c) = m}$ регенеришући на тај начин оргиналну поруку m. Ее означава трансформацију шифровања, а $\boldsymbol{D_d}$ трансформацију дешифровања, при чему је потребно да **d** тј. $\boldsymbol{D_d}$ буде тајно.

Зашто нису једноставно одабране функције за шифровање и одговарајућа функција за дешифровање? Разлог је далекосежан:у том случају, откривање пара који омогућава шифровање/дешифровање услови би редизајнирање читаве шеме шифровања, док је у случају употребе кључева довољно променити пар **(e, d)**. Тајност поруке заснива се искључиво на тајности кључа:ниједан озбиљан алгоритам за криптографију не заснива тајност поруке на тајности или недоступности алгоритма. Шта више, сви алгоритми за криптографију који се употребљавају јавно су и лако доступни.[ Schneier B., 1996.]

Према поступку налажења пара**(e, d)** разликујемо *симетрично* и *асиметрично* шифровање.Ако је знањем **e** једноставно одредити **d,** тада је цео пар **(e , d )** мора бити тајан и реч је о симетричном алгоритму, тј.о криптографији тајних кључева.Уколико знајући само **e** немамо практичног начина да одредимо **d**, реч је о асиметричном алгоритму, тј о.криптографији јавних кључева. У овом случају само трба обезбедти тајност **d**.Стога ће у наредном излагању ће бити детаљније објашњено о криптографским алгоритмима. Криптографски алгоритми који се примењују у системима заштите Интернет/Интранет рачунарских мрежа деле се у две велике групе:

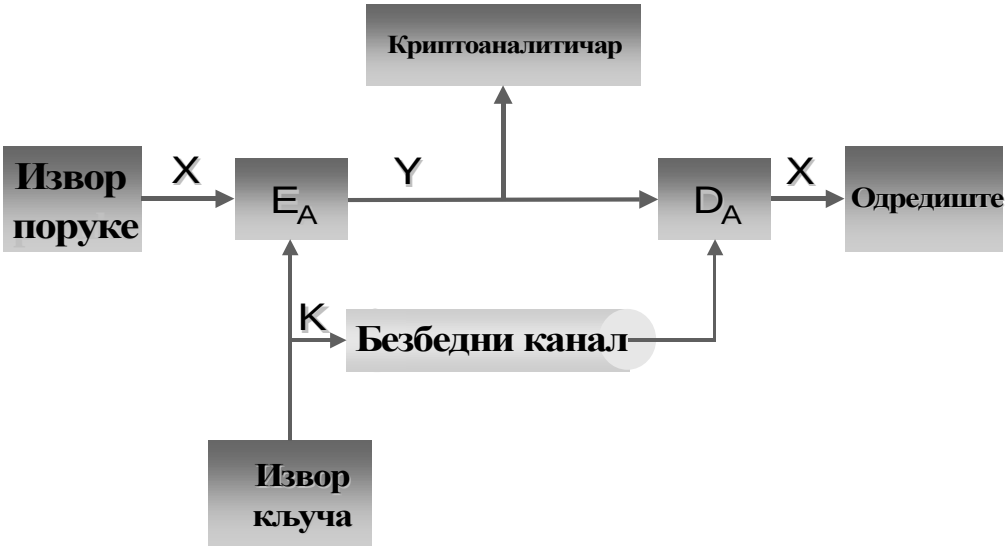
- симетрични криптографски алгоритми, и
- асиметрични криптографски алгоритми.

Подела је изведена на основу поседовања информација неопходних за шифровање и дешифровање.

### 4.2. Симетрични криптографски алгоритми

Групу симетричних криптографских алгоритама представљају алгоритми код којих је кључ за шифровање идентичан кључу за дешифровање, слика 4.2. Алгоритми из ове групе се такође називају и алгоритми са тајним кључем јер је тајност кључа који се користи и за шифровање и за дешифровање есенцијална за безбедност порука у систему. Ови системи представљају основу традиционалне криптолошке теорије и развијају се већ веома дуги низ година. С обзиром да заштита информација тежишну примену има у пословима везаним за државне структуре (војска, полиција и дипломатија), ови системи су били искључиво тајни системи, наменски дефинисани и реализовани од стране надлежних државних институција. Са порастом интензитета и примене електронских облика комуникација јавила се потреба за дефинисањем јавних симетричних криптографских алгоритама, па је последњих десетак година дефинисано више јавних симетричних криптографских алгоритама за примену у апликацијама у којима за то постоји потреба.[Марковић М., 2009.]

Ови алгоритми се углавном користе у апликацијама везаним за системе пословних и финансијских комуникација. Имајући у виду експлозивни развој пословних и финансијских система у последње време, јавни симетрични криптографски алгоритми су постали доминантни у погледу коришћења. Међутим, ниједан од њих није усвојен као генерални стандард већ поменути системи углавном користе одговарајуће листе могућих криптографских алгоритама. На тај начин, као параметар комуникације, бира се и идентификатор симетричног шифарског алгоритма који ће се користити при датој трансакцији.




**Слика 4.2:** Симетрични криптографски системи

Иако је комерцијална употреба симетричних криптографских алгоритама по масовности далеко превазишла употребу у тајном сектору (везаном за државне структуре), главни теоријски резултати се и даље дешавају у области тајне криптологије и тајних система. Велика већина држава има специјализоване организације које се баве дизајнирањем и анализом разних врста шифарских система (нпр. NSA у САД). Степени достигнућа у тој области најчешће нису јавно познати и налазе се у сфери претпоставки.

Постоје две основне врсте симетричних шифарских система:

- блок шифарски системи, и
- секвенцијални шифарски системи (*stream cipher*).

### *4.2.1. Блок шифарски системи*

Блок шифарски системи процесирају блокове нешифрованог сигнала - отвореног текста (ОТ) и шифрованог сигнала – шифрата (СТ), обично у блоковима чија је величина 64 бита или више. Секвенцијални шифарски системи

процесирају низове бита, бајтова или речи (16 или 32 бита) ОТ и СТ. Ако се у току процеса шифровања једне поруке неким блок шифарским системом више пута појављује исти блок отвореног текста (ОТ) резултат ће бити увек исти блок шифрата (СТ), што није случај код секвенцијалних шифарских система. Код секвенцијалних шифарских система вероватноћа да исти низ бита, бајтова или речи ОТ при сваком појављивању у једној поруци производи исти шифрат тежи нули уколико су низ за шифровање и отворени текст независни. Блок шифарски системи се веома много користе у системима пословних и финансијских трансакција, али су њихове безбедносне особине доста слабије од секвенцијалних шифарских система.[McNab C., 2004.] И поред тога дефинисан је велики број јавних алгоритама базираних на блок шифарским системима, као што су DES, 3-DES, RC2, IDEA, и многи други који су нашли веома широку примену у савременим информационим системима. У 2001. години, NIST организација у САД је усвојила нови стандард AES (*Advanced Encryption Standard*).

#### *4.2.1.1. AES Алгоритам*

AES.Као што је већ речено, у току 2001. године, NIST организација у САД *(National Institute of Standards and Technology)* је објавила стандард за симетричне криптографске алгоритме AES (*Advanced Encryption Standard*), који треба да замени претходни стандард DES (*Data Encryption Standard*). Након дуге селекционе процедуре, за AES алгоритам изабран је Rijndael алгоритам кога су реализовали Белгијски истраживачи: *Joan Daemen* и *Vincent Rijmen. Rijndael* представља блок шифарски алгоритам који подржава променљиву дужину блока информације (128, 192 и 256 бита), као и променљиву дужину кључа (128, 192 и 256 бита). Наиме, поруке шифроване DES алгоритмом су се, због недостатака у самом алгоритму (безбедоносни недостаци у супституционим s-табелама), мале дужине кључа (56-бита) и повећане процесне моћи рачунара, могле дешифровати за само пар часова. Након селекционе процедуре, за реализацију AES стандарда изабран је *Rijndael* алгоритам кога су реализовали белгијски матечатичари: *Joan Daemen и Vincent Rijmen. Rijndael* је блок шифарски алгоритам који подржава променљиву дужину блока отвореног текста (128, 192 и 256 бита) као и променљиву дужину кључа (128, 192 и 256 бита). Ријндаел алгоритам је у односу на конкуретске алгоритме (*MARS, RC6, Serpent, Twofish*) био бржи и захтевао је мање оперативне меморије у процесу шифровања и дешифровања порука. *Rijndael* алгоритам са 128-битном дужином кључа је бржи за око 2.5 пута у односу на 3-DES алгоритам. AES алгоритам реализује операције шифровања и дешифровања блока података у променљивом броју циклуса. Број циклуса зависи од величине кључа и износи 10/12/14 за величину кључа 128/192/256 бита, респективно. Пре почетка шифровања или дешифровања врши се експанзија кључа.

#### 4.2.1.1.1. Реализација шифровања у AES алгоритму

У реализацији шифарске трансформације блока података отвореног текста се извршавају четири различита типа функција које се примењују над елементима матрице међурезултата димензија 4×4 бајта:

- нелинеарна замена бајтова помоћу супституционе табеле (функција ByteSub),
- промена места бајтова унутар истог реда (функција ShiftRow),
- трансформација бајтова унутар исте колоне (функција MixColumns),
- сабирање по модулу два са одговарајућем делом кључа (функција AddRoundKey).

У последњем циклусу шифровања се не обавља трансформација бајтова унутар исте колоне (функција MixColumns).

У Ријндаел алгоритму све операције сабирања и множења се врше над елементима коначног поља (поред коначних поља од p-елемената (p-прост број) постоје и коначна поља од $q=p^m$ елемената, где је m природан број; наведена коначна поља се називају и поља Галоа (Galois Field) у ознаци $GF(p^M)$, у част француског математичара Галоа (E. Galois)) од 256 елемената (у ознаци $GF(2^8)$ ):

- при сабирању бајтова примењују се битска операција сабирања по модулу два,
- резултат множења две вредности је производ по модулу вредности неразложивог полинома (полином p(x) n-тог степена је несводљив ако није дељив ни са једним полиномом степена m где је $0 < m < n$).

$$c(x)=a(x)*b(x) \bmod m(x)$$

где је вредност неразложивог полинома:

$$m(x)=x^8+x^4+x^3+x+1$$

Сваки елемент коначног поља, a(x), има једнозначну инверзну вредност, $a_{inv}(x)$, која задовољава услов:

$$a(x)*a_{inv}(x) \bmod m(x)=1$$

Да би се убрзао процес множења у скупу од 256 елемената коначног поља формирају се логаритамска и антилогаритамска табела. Вредност сваког елемента коначног поља п може да се представи у облику степена простог броја. У Rijndael алгоритму за креирање логаритамске и антилогаритамске табеле користи се прост број {03}. У логаритамској табели за сваки елеменат коначног поља x постоји одговарајућа вредност L која задовољава услов $\{x\}=\{03\}^L$. У антилогаритамској табели за сваки елеменат коначног поља x постоји одговарајућа вредност E која задовољава услов $\{E\}=\{03\}^x$. У процесу множења два елемента коначног поља a и

b, помоћу логаритамске табеле се одреде коефицијенти α и β такви да је a={03}$^{\alpha}$ и b= {03}$^{\beta}$. Множењем вредности a и b добија се вредност a·b= {03}$^{\alpha+\beta}$. Тражени производ се добија када се из антилогаритамске табеле из улаза x=α + β одреди вредност E = a·b. Логаритамска и антилогаритамска табела се такође могу користити за проналажење инверзног елемента. Наиме, из логаритамске табеле се за дати елеменат a, одреди вредност α, таква да задовољава услов a= {03}$^{\alpha}$. Инверзна вредност E=$a^{-1}$, дате величине, се добија када се из антилогаритамске табеле из улаза x=255-α , прочита вредност E.

У процесу шифровања се реализују следеће функције:

1. Функција ByteSub врши нелинеарну трансформацију бајта улазне поруке помоћу супституционе s-табеле (ткз. S-box табеле). При креирању супституционе s-табеле, вредност улаза x (x=0…255) се добија у два корака:

- одређивање инверзне вредности улазне величине $x_{inv} = x^{-1}$ помоћу логаритамске и антилогаритамске табеле, према претходно описаном механизму.
- вредност датог улаза супституционе c-табеле се добија одређивањем вредности сваког бита i унутар бајта ($0 \le i < 8$):

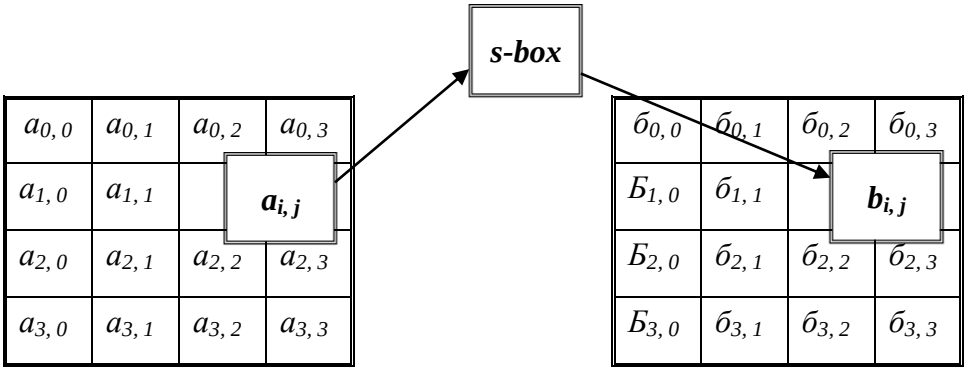
$$x_i'^{-1} = x_i^{-1} \oplus x_{(i+4)\ mod 8}^{-1} \oplus x_{(i+5)\ mod 8}^{-1} \oplus x_{(i+6)\ mod 8}^{-1} \oplus x_{(i+7)\ mod 8}^{-1} \oplus c_i ,$$

где је: c={$63_x$},

Наведени поступак се може приказати и у матричном облику:

$$\begin{bmatrix} x_7'^{-1} \\ x_6'^{-1} \\ x_5'^{-1} \\ x_4'^{-1} \\ x_3'^{-1} \\ x_2'^{-1} \\ x_1'^{-1} \\ x_0'^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7^{-1} \\ x_6^{-1} \\ x_5^{-1} \\ x_4^{-1} \\ x_3^{-1} \\ x_2^{-1} \\ x_1^{-1} \\ x_0^{-1} \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Након креирања s-табеле врши се нелинеарна трансформација улазне поруке, слика aes.1., која је уписана у матрици димензија 4×4 бајта, тако што се сваки бајт улазне поруке замени са вредношћу из одговарајућег улаза из s-табеле.

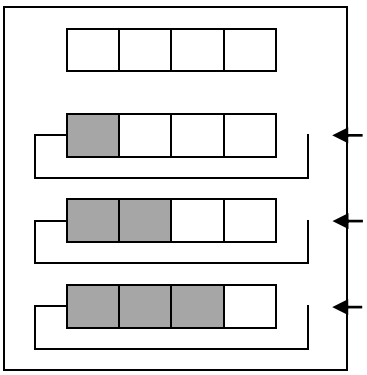



**Слика 4.3:** Графички приказ нелинеарне трансформације поруке помоћу s-табеле

2. Функција ShiftRows обавља операцију над елементима у редовима матрице података добијене након нелинеарне трансформације помоћу s-табеле. Правило по коме се врши промена места бајта унутар истог реда матрице је приказано следећим изразом:

$$d_{p,\,c} = b_{p,\,[c+x\,(p,\,Nc)]\bmod Nc}$$

где је за AES усвојена варијанта Rijndael алгоритма : $N_c=4$, $0 < p < 4$ и $x(p, N_c)=x(p)$. Ротација бајтова унутар истог реда матрице међурезултата је приказана на слици 4.4.



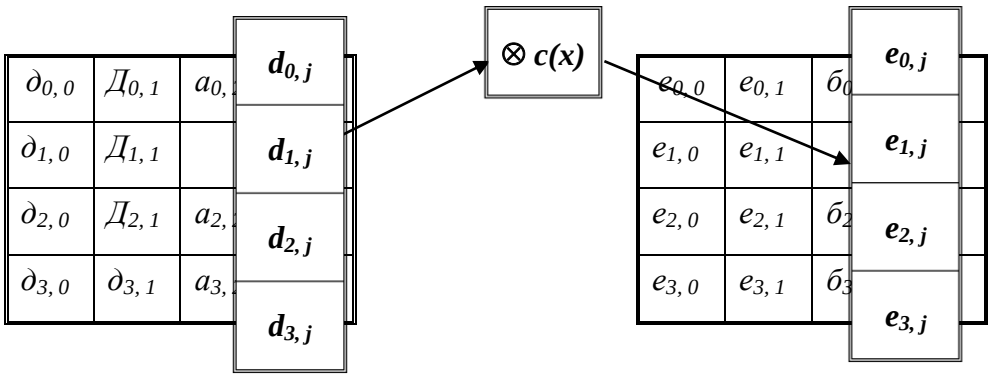
**Слика 4.4:** Графички приказ промене места бајтова у реду матрице међурезултата

3. Функција MixColumns врши трансформацију елемената колоне матрице међурезултата након реализације функције ShiftRows. Елементи колоне матрице се посматрају као коефицијенти полинома, при чему сваки коефицијент представља елеменат коначног поља $GF(2^8)$. Затим се, тако добијени полиноми, множе са константним полиномом $н(x)='03'x^3 + '01'x^2 + '01'x + '02'$ по модулу $x^4 +1$. Наведено модуларно множење се може приказати и у матричном облику:

$$\begin{bmatrix} e_{3,c} \\ e_{2,c} \\ e_{1,c} \\ e_{0,c} \end{bmatrix} = \begin{bmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 02 & 03 \end{bmatrix} . \begin{bmatrix} d_{3,c} \\ d_{2,c} \\ d_{1,c} \\ d_{0,c} \end{bmatrix}$$

где је: 0≤c<4.

Начин на који се врши трансформација колона матрице је приказана на слици 4.5




**Слика 4.5:** Графички приказ промене места бајтова у колонама матрице међурезултата

4. Функција AddRoundKey врши операцију екслузивне дисјункције над елемената матрице, добијене након извршења функције MixColumn, и матрицом одговарајућег дела експандованог кључа, слика 4.6.Оптимизација реализације шифровања у AESалгоритмуТранформација колоне улазне матрице кроз један цео циклус шифровања се може математички приказати следећим низом израза:

$$\begin{bmatrix} e_{0,0} & e_{0,1} & e_{0,2} & e_{0,3} \\ e_{1,0} & e_{1,1} & e_{1,2} & e_{1,3} \\ e_{2,0} & e_{2,1} & e_{2,2} & e_{2,3} \\ e_{3,0} & e_{3,1} & e_{3,2} & e_{3,3} \end{bmatrix} \oplus \begin{bmatrix} к_{0,0} & к_{0,1} & к_{0,2} & к_{0,3} \\ к_{1,0} & к_{1,1} & к_{1,2} & к_{1,3} \\ к_{2,0} & к_{2,1} & к_{2,2} & к_{2,3} \\ к_{3,0} & к_{3,1} & к_{3,2} & к_{3,3} \end{bmatrix} = \begin{bmatrix} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} \\ p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,0} & p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,0} & p_{3,1} & p_{3,2} & p_{3,3} \end{bmatrix}$$

**Слика4.6:** Графички приказ функције AddRoundKey

$$\begin{bmatrix} r_{0,j} \\ r_{1,j} \\ r_{2,j} \\ r_{3,j} \end{bmatrix} = \begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$ (функција AddRoundKey)

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix}$$ (функција MixColumns)

$$\begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j-1} \\ b_{2,j-2} \\ b_{3,j-3} \end{bmatrix}$$ (функција ShiftRows)

$$\begin{bmatrix} b_{0,j} \\ b_{1,j-1} \\ b_{2,j-2} \\ b_{3,j-3} \end{bmatrix} = \begin{bmatrix} s[a_{0,j}] \\ s[a_{1,j-1}] \\ s[a_{2,j-2}] \\ s[a_{3,j-3}] \end{bmatrix}$$ (функција ByteSub)

Сумарно се добија следећи израз који описује процес трансформације j-те колоне $(0 \le j < 4)$ улазног података у једном циклусу шифровања.

$$\begin{bmatrix} r_{0,j} \\ r_{1,j} \\ r_{2,j} \\ r_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s[a_{0,j}] \\ s[a_{1,j-1}] \\ s[a_{2,j-2}] \\ s[a_{3,j-3}] \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Множење матрица може се приказати и следећим изразом:

$$\begin{bmatrix} r_{0,j} \\ r_{1,j} \\ r_{2,j} \\ r_{3,j} \end{bmatrix} = s[a_{0,j}] \cdot \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \oplus s[a_{1,j-1}] \cdot \begin{bmatrix} 03 \\ 02 \\ 01 \\ 01 \end{bmatrix} \oplus s[a_{2,j-2}] \cdot \begin{bmatrix} 01 \\ 03 \\ 02 \\ 01 \end{bmatrix} \oplus s[a_{3,j-3}] \cdot \begin{bmatrix} 01 \\ 01 \\ 03 \\ 02 \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Чинилац множења $c[a_{i,j}]$ се добија одређивањем вредности улаза $a_{i,j}$ супституционе с-табеле. Да би се убрзао процес множења могу се креирати 4 табеле:

$$T_0[a]=\begin{bmatrix} s[a]\cdot 2 \\ s[a] \\ s[a] \\ s[a]\cdot 3 \end{bmatrix} \qquad T_1[a]=\begin{bmatrix} s[a]\cdot 3 \\ s[a]\cdot 2 \\ s[a] \\ s[a] \end{bmatrix} \qquad T_2[a]=\begin{bmatrix} s[a] \\ s[a]\cdot 2 \\ s[a]\cdot 3 \\ s[a] \end{bmatrix} \qquad T_2[a]=\begin{bmatrix} s[a] \\ s[a] \\ s[a]\cdot 3 \\ s[a]\cdot 2 \end{bmatrix}$$

Свака од четири табеле садржи 256 четворобајтних речи, тако да је укупан меморијски простор потребан за њихово складиштење 4КБ. Применом датих табела, трансформација j-те колоне улазног податка у једном циклусу шифровања се може представити изразом:

$$r_j = T_0\left[a_{0,j}\right] \oplus \ T_1\left[a_{1,j=1}\right] \oplus \ T_2\left[a_{2,j-2}\right] \oplus \ T_3\left[a_{3,j-3}\right] \oplus \ k_j$$

Дефинишимо функцију RowByte(W) која врши ротацију сваког бајта улазне речи за једно место удесно $W=b_3b_2b_1b_0$ ($b_i$ , i-ти бајт речи), тако да је излазна реч облика $W=b_2b_1b_0b_3$.

Веза између табела $T_0$, $T_1$, $T_2$ и $T_3$ се може приказати следећом релацијом:

$$T_i[a] = RotByte\left(T_{i-1}[a]\right)$$

Трансформација j-те колоне матрице улазног податка у једном циклусу шифровања се може представити следећим изразом:

$$r_j = k_j \oplus T_0\left[a_{0,j}\right] \oplus RotByte\left(T_0\left[a_{1,j-1}\right] \oplus RotByte\left(T_0\left[a_{2,j-2}\right] \oplus RotByte\left(T_0\left[a_{3,j-3}\right]\right)\right)\right)$$

Применом ове формуле уместо четири табеле са укупно 1024 четворобајтних речи (4КВ) потребно је креирати једну табелу од 256 речи (1КВ), али циклус шифровања траје незнатно дуже, за три додатне операције ротације бајта унутар речи (функција RotByte).

#### 4.2.1.1.2. Реализација дешифровања у AES алгоритму

Процес дешифровања поруке је сличан процесу шифровања. У процесу дешифровања се примењују четири различита типа функција над елементима матрице међурезултата димензија 4×4 бајта:

- нелинеарна замена бајтова помоћу инверзне супституционе табеле (функција InvByteSub),
- промена места бајтова унутар истог реда (функција InvShiftRow),
- трансформација бајтова унутар исте колоне (функција InvMixColumns),
- сабирање по модулу два са одговарајућим делом кључа (функција AddRoundKey).

У последњем циклусу дешифровања се не обавља трансформација бајтова унутар исте колоне (функција InvMixColumns).

У процесу дешифровања се реализују следеће функције:

1. Нелинеарна трансформација улазне матрице димензија 4×4 бајта се врши помоћу инверзне супституционе s-табеле. У процесу креирања инверзне супституционе s-табеле вредност за сваки од улаза x (x=0..255) се одређује у два корака:

- трансформација вредности улазног бајта x се реализује одређивањем вредности сваког бита и унутар бајта ($0 \le i < 8$):

$$x'_i = x_{(i+2)\ mod 8} \oplus x_{(i+5)\ mod 8} \oplus x_{(i+7)\ mod 8} \oplus d_i$$

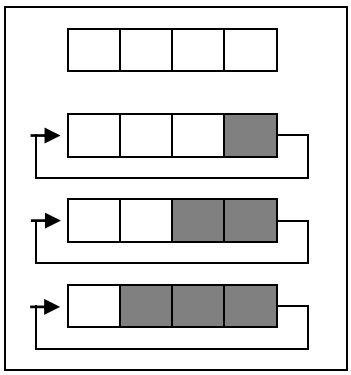
  где је: $d=\{05_x\}$,

- вредност улаза x у инверзној супституционој табели се добија као резултат инверзне трансформације претходно добијене вредности $b=(x')^{-1}$.

2. Функција InvShiftRows обавља операције над елементима у редовима матрице међурезултата, добијеном након претходно описане трансформације. Правило по коме се врши промена месту бајта унутар истог реда матрице се може приказати следећим изразом:

$$d_{p,\,[c+x\,(p,\,Nc)]\ mod\ Nc}\ b_{p,\,c}$$

где је за AES усвојена варијанта Rijndael алгоритма : $N_c=4$, $0 < p < 4$ и $x(p, N_c)=x(p)$. Ротација бајтова унутар истог реда матрице међурезултата је приказана на слици 4.7.



**Слика 4.7:** Графички приказ промене места бајтова у реду матрице међурезултата

3. Функција InvMixColumns врши трансформацију елемената колоне матрице добијене након извршења функције InvShiftRows. Елементи колоне матрице се посматрају као коефицијенти полинома, при чему сваки коефицијент представља елемената коначног поља $GF(2^8)$. Затим се, тако добијени полиноми, множе са

константним полиномом п(x)='0B'$x^3$ + '0D'$x^2$ + '09'x + '0E' по модулу $x^4$ +1. Наведено модуларно множење се може приказати у матричном облику:

$$\begin{bmatrix} e_{3,c} \\ e_{2,c} \\ e_{1,c} \\ e_{0,c} \end{bmatrix} = \begin{bmatrix} 0E & 09 & 0D & 0B \\ 0B & 0E & 09 & 0D \\ 0D & 0B & 0E & 09 \\ 09 & 0D & 0B & 0E \end{bmatrix} . \begin{bmatrix} d_{3,c} \\ d_{2,c} \\ d_{1,c} \\ d_{0,c} \end{bmatrix}$$

где је: 0≤c<4.

4. Функција AddRoundKey врши сабирање по модулу два елемента матрице, добијена након извршења функције InvMixColumns, са одговарајућим делом кључа за дешифровање:

$$\begin{bmatrix} r_{3,c} \\ r_{2,c} \\ r_{1,c} \\ r_{0,c} \end{bmatrix} = \begin{bmatrix} e_{3,c} \\ e_{2,c} \\ e_{1,c} \\ e_{0,c} \end{bmatrix} \oplus \begin{bmatrix} k_{3,c} \\ k_{2,c} \\ k_{1,c} \\ k_{0,c} \end{bmatrix}$$

#### *4.2.1.2. Криптографски модови блок шифарских алгоритама*

Криптографски мод представља начин употребе базичног шифарског алгоритма и најчешће је комбинација неке врсте повратне петље и одређених једноставних операција. Операције које се примењују над алгоритмом су углавном једноставне јер је безбедност одређена базичним шифарским алгоритмом а не криптографским модом. Блок шифарски системи се примењују у различитим криптографским модовима, као што су *ECB (Electronic CodeBook mode), CBC (Cipher Block Chaining), CFB (Cipher FeedBack)* и *OFB (Output FeedBack*). [Dworkin M.,2001.]

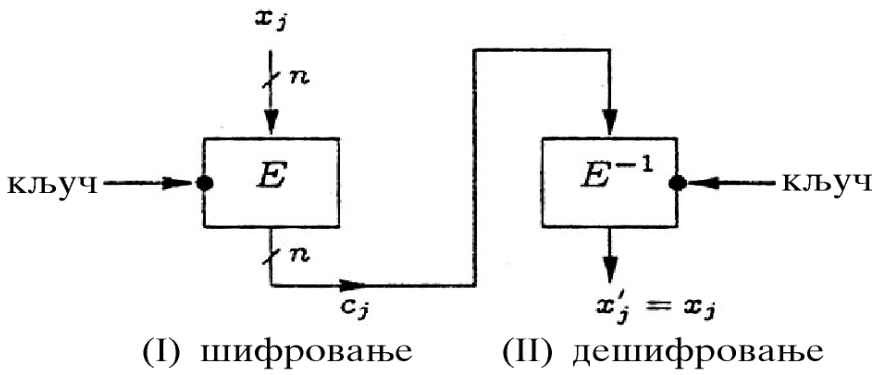
##### 4.2.1.2.1. Мод електронске кодне књиге (ECB – Electronic CodeBook).

ECB мод представља најприроднији и најлакши начин примене блок шифарских система - блок OT се шифрује у блок CT, слика4.8. Сваки OT блок се шифрује независно. Са криптолошке стране, ECB мод је најпроблематичнији.[Daeman J., 1995.]

Наиме, ако криптоаналитичар поседује парове OT и CT за неколико порука, могуће је да током конверзације две стране формира праву кодну књигу, скуп одговарајућих парова CT и OT, и без познавања кључа. У већини реалних ситуација: фрагменти порука теже понављању, различите поруке имају заједничке делове, одређени рачунарски генерисане поруке (као e-mail) имају регуларну структуру, поруке могу бити веома редундантне и имати веома дуге низове нула и паузе. Ови проблеми су најистакнутији на почетку и на крају поруке, где се у

добро дефинисаним заглављима и футнотама могу налазити информације о пошиљаоцу, примаоцу, датуму, итд.

Формирање репрезентативне кодне књиге не само да омогућава трећој страни приступ информацијама већ јој додатно омогућава да може модификовати и понављати шифроване поруке (тзв. *block replay* проблем) без познавања кључа и алгоритма, у случају да има могућност пресретања шифрованих порука између две стране.[Campbell C.M., 1978.] Ови проблеми су иницирали успостављање зависности између суседних блокова шифрата кроз дефинисање нових криптографских модова блок шифарских система.

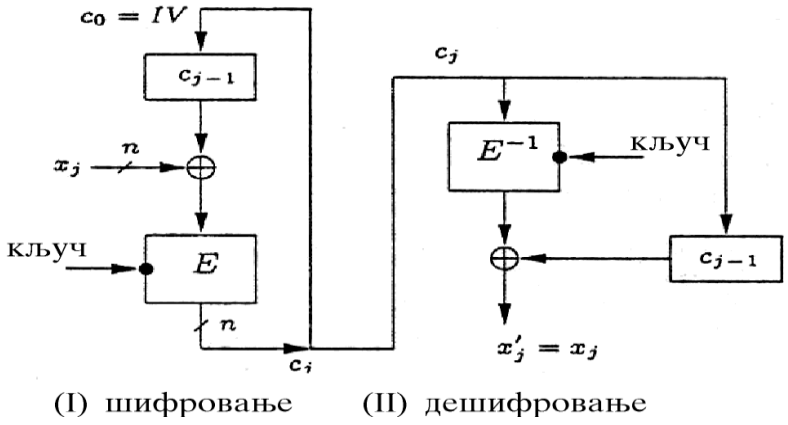



**Слика 4.8**: Графички приказ рада у ECB моду

4.2.1.2.2. Мод уланчавања блокова (CBC – Cipher Block Chaining)

Механизам уланчавања повезује блокове шифрата тако што се резултат шифровања претходних блокова користи при шифровању текућег блока. Другим речима, сваки блок се користи за модификацију шифровања следећег блока тако да сваки блок CT зависи не само од текућег блока OT већ и од свих претходних блокова OT. Начини на које се то може остварити су разноврсни.

У *CBC* моду, слика 4.9 тај утицај се реализује тако што се извршава операција "ексклузивно или" (*XOR*) између OT и непосредно претходног блока CT, а затим се тако добијени блок података шифрује. Прецизније:




**Slika 4.9:** Графички приказ рада у *CBC* моду

1. у повратни регистар се смести иницијална вредност,
2. блок отвореног текста и садржај повратног регистра се спрегну операцијом ексклузивне дисјункције и тако добијени блок се трансформише шифарском трансформацијом E чиме се формира блок шифрата C, и
3. у повратни регистар се смести C и процес се понавља од корака 2 све док има блокова за шифровање.

На тај начин, резултат шифровања сваког блока зависи од свих претходних блокова. Процес дешифровања следи директно и одвија се на следећи начин:

1. у повратни регистар се смести иницијална вредност.
2. блок шифрата C дешифрује се применом трансформације $E^{-1}$, тако добијени блок текста и садржај повратног регистра се спрегну операцијом ексклузивне дисјункције и тако се добије блок отвореног текста.
3. у повратни регистар се смести C и процес се понавља од корака 2 све док има блокова за дешифровање.
4. математички, процес шифровања и дешифровања може се приказати на следећи начин, релацијама, респективно:

$$CT_i = E_k(OT_i \oplus CT_{i-1})$$

$$OT_i = CT_{i-1} \oplus D_k(CT_i)$$

*CBC* мод проузрокује да се идентични блокови OT шифрују у различите CT блокове само ако су неки претходни блокови различити. Две комплетно идентичне поруке ће се ипак шифровати у исте CT.[Savage J.E., 1967.]

Овај проблем се може решити тако што се за први блок података узима нека случајна величина. Овај блок случајних података се назива иницијализациони вектор (ИВ). Када прималац дешифрује овај блок, он просто смешта ИВ у повратни регистар. Текуће време система (timestamp) често

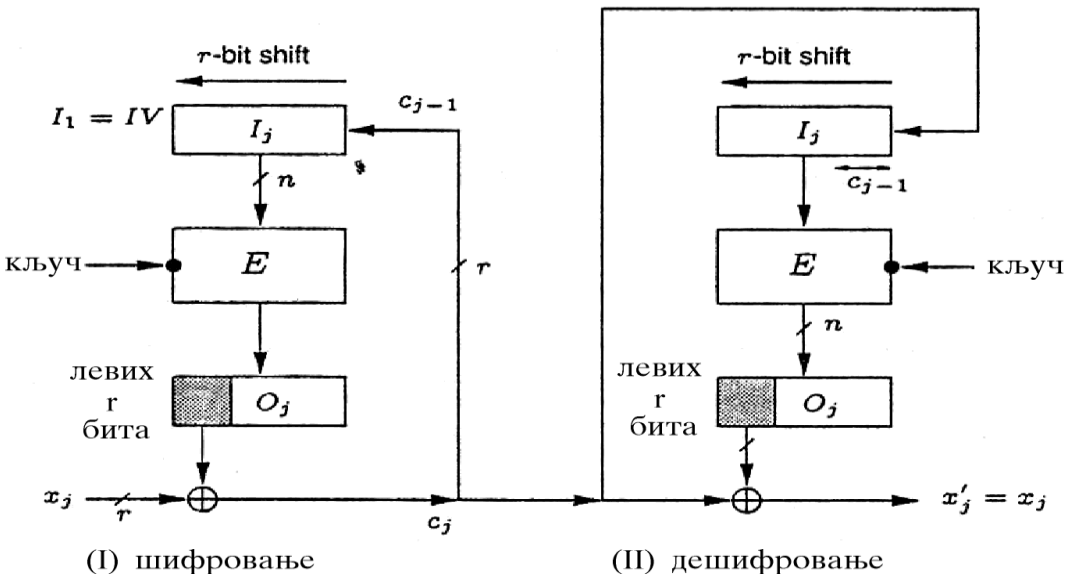
представља добро решење за ИВ. Применом ИВ, идентичне поруке се шифрују у различите СТ. Применом ИВ, елиминисана је могућност примене block replay методе. Штавише, ИВ не мора да буде тајни податак и може се пренети отворено, заједно са СТ, уз употребу неког од механизама заштите интегритета.[Guannela G., 1946.]

Међутим, можда не тако очигледно као у *ECB* моду, и *у CBC* моду постоје одређени безбедносни проблеми који се могу манифестовати као одређена могућност да криптоаналитичар додаје одређене блокове на крајеве порука које се размењују и у чињеници да веома дуге поруке и даље нису имуне на појављивање одређених идентичних облика иако се врши процес уланчавања.[ Daeman J., Govaerts R., 1994; Daeman J., 1995.]

4.2.1.2.3 Мод повратног шифровања (CFB - Cipher-Feedback Mode)

У неким апликацијама се јавља потреба да се делови отвореног текста шифрују и преносе у у јединицама величине r бита (r < n –величина блока), што у *CBC* моду није могуће. Овим модом се превазилази основни проблем *CBC* мода - да шифровање и пренос података не могу почети све док се не прими комплетан блок података. У *CFB* моду, подаци се шифрују у мањим јединицама од актуелне величине блока и овај мод се означава као r-битни *CFB* мод, где је r мање или једнако од величине блока основног блок шифарског система.[Preneel B., Nuttin M., Rijmen V., and Buelens J., 1994.]

Процес шифровања се одвија на следећи начин, слика 4.10:




**Слика 4.10:** Графички приказ рада у *CFB* моду

1. Отворени текст се подели у блокове величине r бита, формира се иницијални вектор величине n бита и смести у повратни регистар. Одабере се К, кључ за шифарску трансформацију.
2. Формира се излазни блок, О, тако што се изврши шифарска трансформација кључем К текућег садржаја повратног регистра.
3. Блок шифрата се формира тако што се операција ексклузивне дисјункције изврши над текућим блоком отвореног текста и r бита најмање тежине блока О.
4. Садржај повратног регистра се помера за r бита у лево и на место r бита најмање тежине се смешта формирани блок шифрата.

Кораци 2-4 се понављају све док има блокова отвореног текста. Дешифровање се одвија на сличан начин.

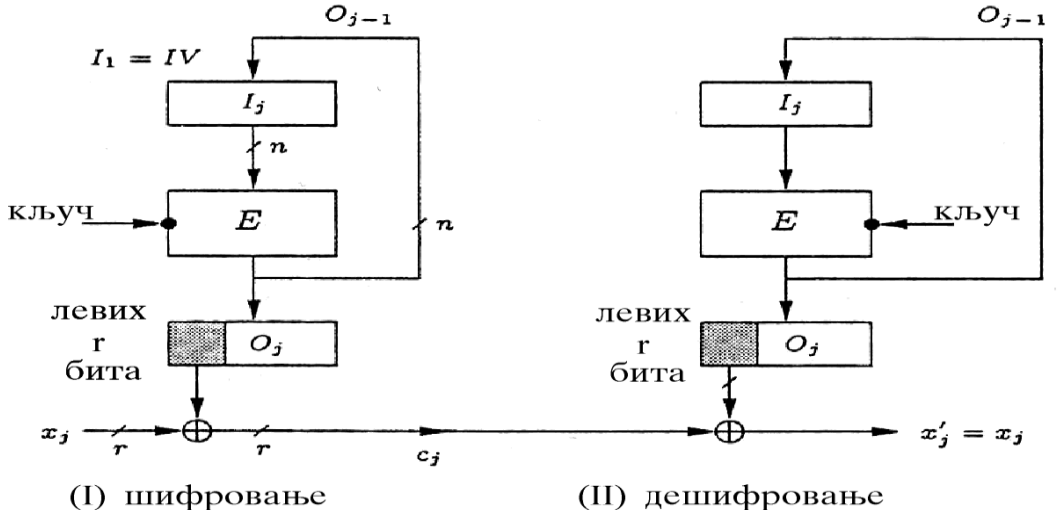
1. Формира се иницијални вектор величине n бита и смести у повратни регистар. Одабере се К, кључ за шифарску трансформацију.
2. Формира се излазни блок, О, тако што се иврши шифарска трансформација кључем К текућег садржаја повратног регистра.
3. Блок отвореног текста се формира тако што се операција ексклузивне дисјункције изврши над текућим блоком шифрата и r бита најмање тежине блока О.
4. Садржај повратног регистра се помера за r бита улево и на место r бита најмање тежине се смешта текући блок шифрата.

Иницијализациони вектор има исту улогу као и у CBC моду, да спречи појављивање истих шифрата у случају истих порука шифрованих једнаким кључевима. Из описа начина трансформације јасно је да је за исправно дешифровање неопходно да је претходних $\left\lceil \frac{n}{k} \right\rceil$ блокова шифрата исправно дешифровано.

С обзиром да се и у процесу шифровања и у процесу дешифровања користи иста шифарска трансформација, то алгоритам којим се формира блок О не може бити из класе алгоритама са јавним кључем.

#### 4.2.1.2.4 Излазни повратни мод (OFB – Output Feedback Mode)

Овај мод рада представља спој добрих особина *ECB* и *CFB* модова рада, спречава пропагацију грешке и има побољшане безбедносне карактеристике. *OFB* мод рада такође омогућава пренос података у јединицама мањим од величине блока. [Campbell C.M., 1978.] Трансформација отвореног текста се одвија на следећи начин, слика 4.11:




**Слика 4.11:** Графички приказ рада у *OFB* моду

1. отворени текст се подели у блокове величине r бита, формира се иницијални вектор величине n бита и смести у повратни регистар. Одабере се К, кључ за шифарску трансформацију.
2. формира се излазни блок, О, тако што се изврши шифарска трансформација кључем К текућег садржаја повратног регистра .
3. блок шифрата се формира тако што се операција ексклузивне дисјункције изврши над текућим блоком отвореног текста и r бита најмање тежине блока О.
4. блок О постаје садржај повратног регистра.

Кораци 2-4 се понављају све док има блокова отвореног текста. Дешифровање се одвија на сличан начин:

1. формира се иницијални вектор величине n бита и смести у повратни регистар. Одабере се К, кључ за шифарску трансформацију.
2. формира се излазни блок, О, тако што се иврши шифарска трансформација кључем К текућег садржаја повратног регистра.
3. блок отвореног текста се формира тако што се операција ексклузивне дисјункције изврши над текућим блоком шифрата и r бита најмање тежине блока О.и
4. садржај повратног регистра замени се формираним блоком О.

Кораци 2-4 се извршавају све док има блокова за дешифровање.

Претходно изложени опис је према стандарду *ISO 10116*. Постоје такође и друге варијације на ову тему (нпр. FIPS-81), .[FIPS PUB., 1981.] али се ова изложена верзија сматра, за сада, најбезбеднијом.[FIPS 180-1., 1995.]

Поред тога што се радом у овом моду онемогућава пропагација грешке, добра особина овог мода рада је и то што се већи део израчунавања може извршити off-line, након чега се врши само *XOR*-овање излаза алгоритма и јединица ОТ.[Davies D.W. and Parkin G.I.P., 1982; Davies D.W. and Parkin G.I.P., 1983.]

Детаљна *анализа OFB* мода рада је показала да овај мод рада треба користити само у случају да је r једнако дужини блока n. Другим речима, 64-битне блок шифарске алгоритме треба користити у 64-битном *OFB* моду.

### *4.2.2. Избор одговарајућег мода рада блок шифарског система*

Један од четири базична мода рада – *ECB, CBC, OFB* или *CFB* погодан је за скоро сваку апликацију. Који ће се мод користити зависи од корисникових специфичних захтева.[FIPS PUB 81,1981; FIPS 186-1,2000;FIPS PUB 180-2, 2002. ] Ако су једноставност и брзина најбитнији, E*CB* мод је прави избор, као најлакши и најбржи мод за коришћење блок шифарских система. Међутим, *ECB* мод је најслабији са безбедносне тачке гледишта, и не препоручује се за шифровање порука. Са друге стране, *ECB* мод је веома добар за шифровање кратких случајних података, као што су на пример кључеви, јер се при томе не исказују препознате слабости *ECB* мода.

За шифровање нормалног ОТ треба користити *CBC, CFB* или *OFB* мод. *CBC* је генерално најбољи мод за шифровање датотека. Такође, ако је апликација софтверски базирана, CBC је скоро увек најбоље решење. Са друге стране, *CFB* мод (специјално 8-битни CFB мод) је генерално мод који треба бирати за шифровање низова карактера у којима се сваки карактер третира индивидуално, као на пример у вези између терминала и host рачунара. *OFB* мод рада се најчешће користи у синхроним системима високих брзина где се не толерише пропагација грешака.

### *4.2.3. Секвенцијални шифарски системи*

Секвенцијални шифарски системи представљају веома важну класу шифарских алгоритама. Они трансформишу појединачне карактере (најчешће бите и бајтове отвореног текста) користећи трансформацију која поред кључа зависи на одређени начин и од временског тренутка у којем се примењује, за разлику од блоковских шифарских система који трансформишу блокове отвореног текста непроменљивом трансформацијом током шифровања целе поруке. Као и обично, у пракси, ова подела није тако ригидна, постоје трансформације које се могу по својим особинама сврстати и у једне и у друге.

Тако на пример *CFB* и *OFB* модови блоковских шифарских система имају неке карактеристике секвенцијалних шифарских система. Са друге стране секвенцијални шифарски системи се могу сматрати блоковским код којих је дужина блока један карактер (бит, бајт или машинска реч (word) дужине 16, 24 или 32 бита).

Генерално говорећи секвенцијални шифарски систем састоји се од генератора низа кључа (keystream генератор) који генерише низ јединица кључа $к_1$, $к_2$, …, $к_i$, … и функције f која се примењује на низ јединица ОТ: $п_1$, $п_2$, …, $п_i$, производећи низ јединица СТ: $c_1$, $c_2$, …, $c_i$, на бази следеће релације:[Kumar, I., 1997.]

$$c_i = f(k_i, p_i)$$

На другом крају комуникације, применом инверзне функције на парове јединица шифрата и јединица кључа добијају се јединице послатог ОТ. Наиме:

$$p_i = f^{-1}(k_i, c_i)$$

јер је функција f тако одабрана да је

$$p_i = f^{-1}(k_i, f(k_i, p_i))$$

Због једноставности обраде за f се најчешће користи ексклузивна дисјункција (XOR операција). Безбедност низовног шифарског система примарно је одређена криптолошким квалитетом генератора низа кључа.

#### *4.2.3.1 Класификација секвенцијалних шифарских система*

Класификација секвенцијалних шифарских система се може вршити по различитим критеријумима, по начину на који се генерише низ кључа, по типу примењеног алгоритма (са јавним или тајним кључем), итд. Основна је подела по начину на који се генерише низ кључа. У том смислу постоје системи са случајним и псеудо-случајним низом.

**Системи са случајним низом** – код ових система низ кључа се генерише на случајан начин, тако што се јединице кључа генеришу независно и случајно. Ако се, према претходним ознакама за функцију f, узме ексклузивна дисјункција, тада се добија такозвани "*one time pad*" систем за који се може теоријски доказати да је апсолутно сигуран, тј. да шифрат не носи никакву информацију о отвореном тексту. Са друге стране, тај систем је и оптималан у смислу да користи најкраћи кључ којим се постиже апсолутна сигурност. Наиме, Шенон је у својим радовима показао да је неопходан услов за апсолутну безбедност да ентропија кључа буде већа или једнака од ентропије поруке. Како је код овог система ентропија кључа једнака дужини поруке, чија ентропија не може бити већа од њене дужине, то следи да је ово збиља оптималан систем у наведеном смислу.Недостатак овог система је што оба учесника комуникације морају имати исти низ кључа који мора бити тајан, што понекад производи, непремостиве, проблеме у управљању

кључевима, јер треба обезбедити и доставити странама у комуникацији велике количине кључева како би могле несметано да комуницирају.

**Системи са псеудослучајним низом** – код ових система се, на основу иницијалне вредности и договореног алгоритма, генерише низ јединица кључа. Поседовањем идентичне иницијалне вредности, обе стране у комуникацији су у стању да продукују исти низ јединица кључа и да остваре безбедну комуникацију. Како је генерисање јединица кључа детерминистичко, низ кључа је у потпуности дефинисан са:

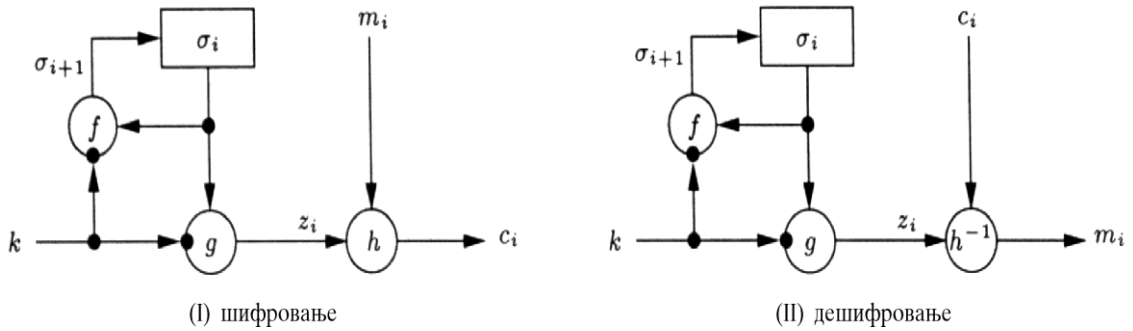
- почетним унутрашњим стањем – иницијална вредност којом се дефинише почетно стање генератора кључа,
- функцијом наредног стања – која на бази претходног унутрашњег стања генерише ново унутрашње стање, и
- излазном функцијом – која на основу унутрашњег стања генерише излазну јединицу кључа.

Последица чињенице да је низ кључа детерминистички је да је он нужно периодичан. Иако су ово на изглед чињенице које ове системе значајно дезавуишу, ствари не стоје тако лоше, јер се и ти проблеми могу успешно превазићи. Наиме, безбедност ових система директно зависи од величине иницијалних података и квалитета договореног алгоритма. Добро дизајнирани алгоритми овог типа пружају заштиту која је по квалитету врло близу апсолутно безбедним системима.

Секвенцијални шифарски системи са псеудослучајним низом се деле у две велике групе:

1. синхрони секвенцијални шифарски системи, и
2. самосинхронишући секвенцијални шифарски системи.

**Синхрони секвенцијални шифарски системи** су они системи код којих се низ кључа генерише независно од отвореног текста и шифрата, слика 4.12



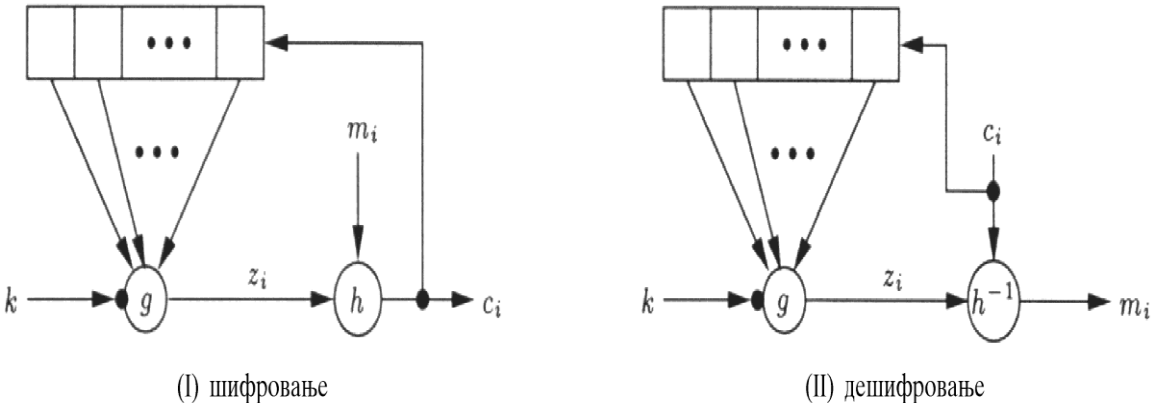

**Слика 4.12**: Графички приказ рада синхроних секвенцијалних шифарских система

Процес шифровања се може описати следећим скупом једначина

$$\sigma_{i+1} = f(\sigma_i, k)$$
$$z_i = g(\sigma_i, k)$$
$$c_i = h(z_i, m_i)$$

Где се почетно стање, $\sigma_0$, одређује на основу иницијалне вредности k, f је функција следећег стања, g је функција која продукује низ кључа $z_i$ а h излазна функција која од отвореног текста $m_i$ и низа кључа $z_i$ формира шифрат $c_i$. Код ових система низ кључа се генерише независно од низа јединица поруке. На обе стране у комуникацији се истовремено генеришу низови кључа. Учесници у комуникацији су у стању да размењују поруке све дотле док су алгоритми за генерисање низа кључа синхронизовани међу собом. Уколико се деси губитак или уметање једног или више јединица током преноса СТ, дешифровање ће бити некоректно. У случају таквог догађаја, генератори низа кључа на предајној и пријемној страни морају се ресинхронизовати, пре него што наставе комуникацију. Са друге стране, у овим ситемима се не пропагира грешка и сваки погрешан бит у преносу остаће и у дешифрованом облику погрешан, али та грешка неће утицати ни на претходне ни на будуће бите за пренос. Претходно наведена особина може послужити активном противнику као основа за различите врсте покушаја компромитовања оваквог система.

**Самосинхронишући асинхрони системи** су они системи код којих је низ кључа добија у функцији иицијалне вредности, договореног алгоритма и извесног константног броја претходних јединица шифрата, слика 4.13.Процес шифровања се описује следећим скупом једначина




(I) шифровање (II) дешифровање

**Слика 4.13**: Графички приказ рада самосинхронишућих система са псеудо-случајним низом

$$\sigma_i = (c_{i-t}, c_{i-t-1,\ldots,} c_{i-1})$$
$$z_i = g(\sigma_i, k)$$
$$c_i = h(z_i, m_i)$$

Где је $\sigma_0 = (c_{-t}, \ldots, c_{-1})$ иницијално стање, почетно стање одређује се на основу иницијалне вредности k, f је функција следећег стања, g је функција која продукује низ кључа $z_i$ а h излазна функција која од отвореног текста $m_i$ и низа кључа $z_i$ формира шифрат $c_i$.

Код ових система могуће је остварити самосинхронизацију зато што дешифровање зависи само од фиксног броја претходних јединица шифрата, тако да је могуће синхронизацију поново успоставити враћањем на одређени број добро примљених знакова шифрата.

Код ових система пропагација грешке је такође ограничена на фиксиран број узастопних јединица.После тога се преостале јединице шифрата могу исправно дешифровати. Секвенцијални шифарски системи имају велику улогу у заштити масовних података јер обезбеђују квалитетну заштиту и при реализацији обезбеђују велику брзину обраде.

Теорија анализе и синтезе секвенцијалних шифарских система са псеудослучајним низом је веома развијена и углавном једна подстиче другу на развој.

#### *4.2.3.1 Компаративна анализа блок и секвенцијалних шифарских система*

Иако су блок и секвенцијални шифарски системи веома различити, блок системи се могу имплементирати као секвенцијални системи и обрнуто. Разлике се највише исказују у имплементацији ових система. Наиме, секвенцијални шифарски системи који шифрују и дешифрују сваку јединицу ОТ нису превише погодни за софтверске имплементације. Они су погодни за шифровање и дешифровање података у реалном времену, посебно ако су реализовани у хардверу. С друге стране, блок шифарски системи су лакши за имплементацију у софтверу јер често избегавају временски захтевне битске манипулације и раде над подацима у рачунарски подељеним блоковима. Постоје неки специфични моменти где шифровање јединица ОТ може бити од интереса и у рачунарским системима, као на пример шифровање везе између тастатуре и процесора, али и у том случају блок који се шифрује треба да буде најмање ширине магистрале података.[Rescorla E., 2001.]

У савременом развоју криптологије сведоци смо све интензивнијег коришћења и блок и секвенцијалних шифарских система. Савремене апликације финансијских и пословних трансакција су проузроковале експлозиван раст примена поменутих шифарских система и то: DEA, 3-DES, RC2, RC4, RC5, IDEA, AES, итд. као блок шифарских система, и RC6, и других, као секвенцијалних шифарских система.[Matsui M.,1994.] У савременим софтверским и хардверским производима за заштиту финансијских, пословних и државних рачунарских мрежа углавном се подржава читав скуп највише коришћених блок и секвенцијалних

алгоритама (*de facto* стандардних алгоритама).[Rivest R. L., 1977; Contini S., Rivest R., 1998; Rivest R.L., Robshaw M.J.B., Sidney R., Yin Y.L., 1998.]

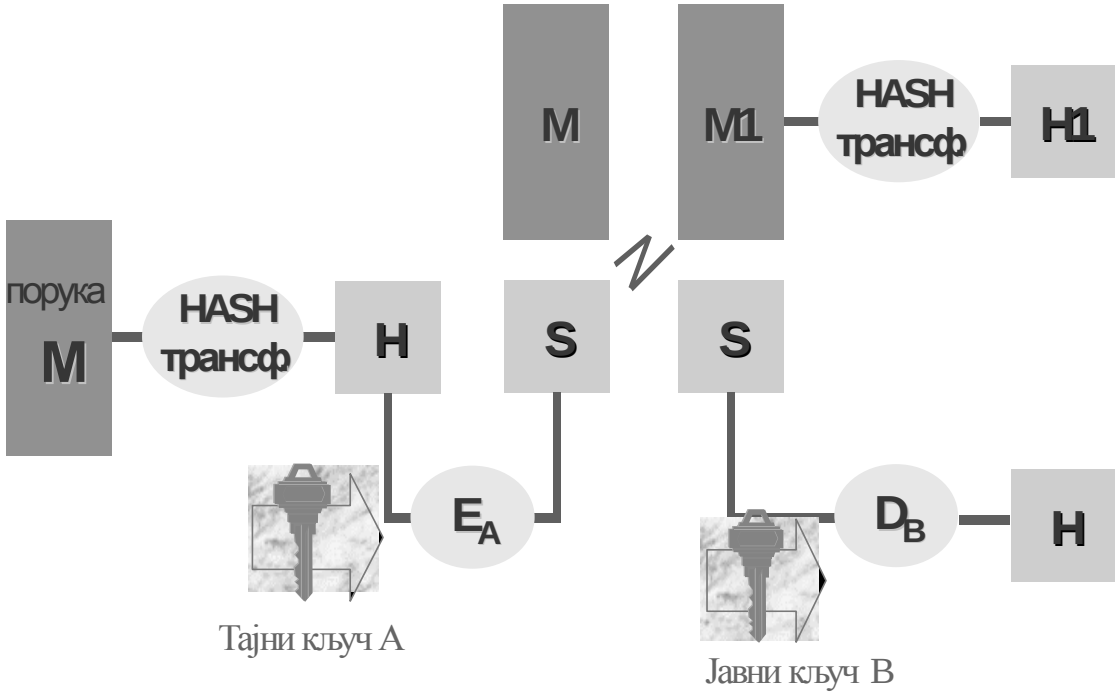
### 4.3. Асиметрични криптографски алгоритми

Асиметрични криптографски алгоритми представљају једно од највећих достигнућа криптологије друге половине XX века. Откривени су у процесу решавања проблема везаних за заштиту тајности и дистрибуцију кључева који је често био актуелан у применама симетричних криптографскх алгоритама. Наиме, у асиметричним шифарским системима се користе различити кључеви за шифровање и дешифровање, тзв. јавни и тајни кључ, тако да кључ за шифровање може имати свако а само поседник кључа за дешифровање може дешифровати поруку. Међутим, висока рачунарска захтевност ових алгоритама утиче на перформансе система у којима се примењују, тако да се не препоручује примена за заштиту тајности информација у системима са великим протоком информација. Наравно ово не искључује аутоматски ове алгоритме, јер начин на који је, уз коришћење оваквих алгоритама, могуће остварити функције интегритета, аутентичности и непорицања има несумњиву предност над традиционалним техникама.У литератури је описано више алгоритама са јавним кључем, али са становишта квалитета, отпорности на разне врсте напада, ефикасност и лакоћу имплементације, и распрострањеност, нису сви подједнако добри.У том смислу се као природни избор намеће RSA алгоритам који више од двадесет година одолева свим теоријским и технолошким нападима. Опис и начин употребе овог алгоритма прописани су у стандарду PKCS#1 верзија 2.RSA алгоритам је први пут публикован 1978. године. Назив је добио по првим словима презимена аутора алгоритма (*R.L.Rivest, A.Shamir, L.Adleman*).Поред RSA алгоритма могуће је користити и друга два алгоритма, DSA (Digital Signature Algorithm) и ECDSA (*Elliptic Curve DSA*), која спадају у стандард дигиталног потписа (*NIST стандард DSS (Digital Signature Standard*)). [Rosing M.,1998.]

PKCS#1.PKCS#1 стандард описује методе шифровања података коришћењем RSA асиметричног алгоритма и најчешће се користи за конструкцију дигиталног коверта и дигиталног потписа.[Marković, M., Djorđević, G., Unkašević, T., 2002;Marković, M., Djorđević, G., Unkašević, T., 2003.] У случају дигиталног коверта, садржај поруке се прво шифрује одређеним симетричним алгоритмом (као што су DES, 3-DES, RC2, RC4, RC5, RC6, IDEA, AES, или неки наменски приватни алгоритми).[Menezes A., Oorschot van P. C., Vanstone S. A., 1997; Rivest R.L., Robshaw M.J.B., Sidney R., Yin Y.L., 1998;Robshaw M.J.B.,2001.] Затим се тајни кључ примењеног симетричног алгоритма који је употребљен за шифровање дате поруке шифрује RSA алгоритмом употребом јавног кључа корисника коме је

дата порука намењена (*RSA public key* операција). Тако шифрован садржај поруке и тајни кључ којим је та порука шифрована заједно представљају дигитални коверат.

У случају дигиталног потписа, слика 4.14, садржај који треба да се потпише, порука M, прво се редукује у отисак поруке (*message digest*), H, применом неког од метода за креирање отиска поруке, *message-digest* алгоритма (као што су на пример MD5 или SHA-1 алгоритми), а затим се добијени отисак поруке шифрује применом, на пример, RSA алгоритма користећи тајни кључ потписника поруке (*RSA private key операција*), кључ A. Шифровани отисак поруке представља дигитални потпис дате поруке, S, и постаје њен придружени део. Када оваква порука стигне до примаоца којем је намењена извршава се поступак верификације дигиталног потписа. Овај поступак се састоји од дешифровања отиска добијене поруке применом RSA алгоритма уз употребу јавног кључа пошиљаоца поруке, кључ B. По дешифровању дигиталног потписа прималац поруке изврши исти *message digest* поступак над добијеном поруком, M1. Ако је добијени отисак поруке, H1, идентичан са дешифрованом вредношћу отиска, верификација је успела, у противном верификација је негативна. Уколико је верификација успела, прималац поруке је сигуран у следеће: [Марковић М., 2009.]




**Слика 4.14**: Процедура дигиталног потписа и верификације

- аутентичност пошиљаоца – јер је успешно дешифровао отисак поруке применом RSA алгоритма са јавним кључем датог пошиљаоца,

- интегритет послате поруке – ако су израчунати и дешифровани отисци дате поруке идентични закључује се да порука на преносном путу није мењана, и
- немогућност да пошиљалац накнадно порекне да је ту поруку послао јер је његов дигитални потпис успешно верификован.

Да би дати прималац био у могућности да прима поруке од датог пошиљаоца и спроведе процес верификације дигиталног потписа, мора имати могућност приступа јавном кључу пошиљаоца. Приступ и дистрибуција јавних кључева се могу организовати на различите начине а најчешће се реализују у процесу утврђивања идентитета путем размене дигиталних сертификата.

Поред безбедносних механизама, PKCS#1 стандардом се дефинише и унутрашња структура валидних порука, чиме се омогућава додатни механизам верификације исправности порука. Наиме, свака порука која има нарушену структуру се сматра неисправном и одбацује се. Треба посебно нагласити да је тренутно актуелан и важећи PKCS#1 стандард верзије 2 и да су њиме значајно измењене препоруке дате у PKCS#1 стандарду верзије 1.5, које се односе на формат блока података који подлеже операцијама шифровања и потписивања. Разлог за овакве драстичне промене лежи у чињеници да према верзији 1.5 при формирању блока за шифровање постоји низ бита на почетку блока који је увек исти. То се може искористити да се без познавања тајних информација, само уз познавање шифрата, дође до отвореног текста.Треба нагласити да овим није компромитована безбедност самог RSA алгоритма већ је, грубо говорећи, начин његове употребе био такав да је под одређеним условима долазило до отицања информација. У верзији 2 овог стандарда блок података, који се шифрује претходно, кодира се OAEP (*Optimal Assymetric Encryption Padding*) методом, која има добре безбедносне карактеристике тако да чак ни два идентична блока података после кодирања овим методом не дају исти резултат. Тиме су избегнуте слабости детектоване у верзији 1.5.

### *4.3.1. RSA алгоритам*

RSA алгоритам је први пут публикован 1978. године. Назив је добио по првим словима презимена аутора алгоритма (R.L.Rivest, A.Shamir, L.Adleman). [R.L.Rivest, A.Shamir, L.Adleman.,1979.] Теоријска основа алгоритма за реализацију шифровања и дешифровања порука приказана је у следећим теоремама.[Stinson D., 1996.]

Теорема 1: Линеарна конгруенција

$$ax \equiv b(\mathrm{mod}\, m)$$

има решење ако и само ако је NZD(a, m)|b (NZD-највећи заједнички делилац), и у том случају, ако је $x_0$ једно решење конгруенције, онда је опште решење

$$x \equiv x_0 \left( \bmod \frac{m}{d} \right)$$

где је $d = NZD(a, m)$.

Последица 1а: Ако су бројеви a и m релативно прости, тј. $NZD(a, m) = 1$, онда линеарна конгруенција $ax \equiv b(\bmod m)$ има тачно једно неконгруентно решење по модулу m.

Теорема 2: (Кинеска теорема о остацима) Ако су $n_1, n_2, \ldots, n_k$ по паровима релативно прости цели бројеви, тада систем конгруенција:

$$x \equiv a_1 (\bmod n_1)$$
$$x \equiv a_2 (\bmod n_2)$$
$$\vdots$$
$$x \equiv a_k (\bmod n_k)$$

има јединствено решење по модулу $n = n_1 \cdot n_2 \cdots n_k$.

Теорема 3: (Ојлерова теорема (L.Euler)) Ако су a и n узајамно прости бројеви, онда је:

$$a^{\varphi(n)} \equiv 1 (\bmod n)$$

где је са $\varphi(n)$ означен број природних бројева, не већих од n, узајамно простих са n.

Последица 3а: (Фермаова теорема (P. Fermat)) Ако је p прост број и NZD(a, p)=1, онда је

$$a^{p-1} \equiv 1 (\bmod p).$$

Последица 3б: Ако је n производ простих позитивних бројева p, q (n=p·q) и NZD(a, n)=1, онда је

$$a^{(p-1)(q-1)} \equiv 1 (\bmod n).$$

Теорема 4: Нека је производ n=p·q природан број где су p и q прости позитивни бројеви. Нека је e природан број такав да је $1 < e < (p-1) \cdot (q-1)$ и нека су бројеви e и производ $(p-1) \cdot (q-1)$ релативно просте величине. Тада постоји природан број d такав да је:

$$d \equiv e^{-1} \bmod((p-1) \cdot (q-1))$$

и за сваки природан број a, 0 ≤ a < n важи:

$$a^{e\cdot d} \equiv a \left(\text{mod } n\right)$$

Доказ:

Како су бројеви e и производ бројева $(p-1)\cdot(q-1)$ релативно просте величине тада се може, на основу теореме 2, закључити да постоји природан број d такав да је испуњено:

$$e\cdot d \equiv 1 \bmod \left((p-1)\cdot(q-1)\right)$$

Дати производ се може представити на следећи начин:

$$e\cdot d = 1 + A\cdot(p-1)\cdot(q-1)$$

где је A природан број.

Може се доказати да за произвољан број a важи $a^{e\cdot d} \equiv a\left(\text{mod } n\right)$.

Нека су a и n релативно прости бројеви (NZD(a, n)=1), тада је према Ојлеровој теореми :

$$\begin{aligned} a^{e\cdot d} &\equiv a^{1+A\cdot(p-1)\cdot(q-1)} \left(\text{mod } n\right) \\ &\equiv a\cdot(a^{(p-1)\cdot(q-1)})^{A} \left(\text{mod } n\right) \\ &\equiv a\cdot 1^{A} \left(\text{mod } n\right) \\ &\equiv a \left(\text{mod } n\right) \end{aligned}$$

Нека је NZD(a, n)>1 и 0 ≤ a < n. Тада је, с обзиром на облик броја n, NZD(a, n)=p или је NZD(a, n)=q. Ако се претпостави да је NZD(a, n)=p, тада је, према Фермаовој теореми:

$$a^{e\cdot d} \equiv a \ \bmod(p) = 0 \ \bmod(p)$$

$$\begin{aligned} a^{e\cdot d} &\equiv a^{1+A\cdot(p-1)\cdot(q-1)} \bmod(q) \\ a^{e\cdot d} &\equiv a\cdot(a^{(q-1)})^{A\cdot(p-1)} \bmod(q) \\ a^{e\cdot d} &\equiv a\cdot 1^{A\cdot(p-1))} \bmod(q) \\ a^{e\cdot d} &\equiv a \bmod(q) \end{aligned}$$

Како су p и q прости бројеви, према кинеској теореми о остацима, систем конгруенција:

$$a^{e\cdot d} \equiv X \bmod(p)$$

$$a^{e\cdot d} \equiv X \bmod(q)$$

има јединствено решење X које је мање од n=p·q. Према претходном a је једно такво решење па према томе и једино. На исти начин се поступа у случају да је NZD(a, n)=q. Према претходно наведеном, показује се да је у било ком случају задовољено $a^{e\cdot d} \equiv a\left(\text{mod}(n)\right)$.

Алгоритам за трансформацију порука базиран на наведеној теореми одвија се на следећи начин.

Нека је M порука коју је потребно трансформисати.

- Први корак у реализацији алгоритма је одабир простих позитивних бројева p, q и одређивање вредности њиховог производа n=p·q.
- У следећем кораку бира се природан број e, $1 < e < (p-1)\cdot(q-1)$ такав да је $NZD(e,(p-1)\cdot(q-1)) = 1$.
- Након одабира вредности за e се израчунава број d такав да је $d \equiv e^{-1} \bmod((p-1)\cdot(q-1))$.

Процес трансформације порука одвија се на следећи начин. Ако се са M означи нумерички еквивалент поруке M и напише у облику $M=M_1M_2 \ldots M_к$ где је $0 \le M_i < n$, i=1, 2, … , к; тада се за свако $M_i$, i=1, 2, … , к израчуна:

$$C_i = M_i^{\,e} \bmod(n)$$

Порука $C=C_1C_2 \ldots C_к$ представља трансформисани облик поруке M и у датом облику се порука M преноси примаоцу комуникационим каналима. Прималац реконструише поруку тако што знајући вредности d, p и q израчунава:

$$C_i^{\,d} = M_i \bmod(n)$$

и уланчавањем формира оригиналну поруку $M=M_1M_2 \ldots M_к$. Коректност наведеног начина трансформације и реконструкције порука директна је последица теореме 4. Уређени пар (e, n) је јавни кључ а уређена тројка (d, p, q) је тајни кључ RSA алгоритма. По безбедносној класификацији претходни алгоритам спада у класу рачунски безбедних система. Сигурност овог алгоритма базира се на непознавању ефикасног алгоритма за факторизацију природних бројева и директно зависи од величине броја n (која се може изражавати бројем цифара у декадном или бинарном запису).

### 4.4. Hash функције

Такозване једнокорачне hash или message digest функције H(M) извршавају се над поруком M произвољне дужине, производећи hash вредност h=H(M) фиксне дужине m. Hash функције треба да задовоље следеће карактеристике:

- за дату поруку M, треба да је релативно једноставно изгенерисати h,
- за дато h, треба да је изузетно тешко израчунати M тако да је H(M)=h, и

- за дато M, треба да је изузетно тешко наћи другу поруку M’ такву да је испуњено H(M)=H(M’).

Алгоритам MD5 задовољава горе наведене карактеристике и представља један од најчешће коришћених hash алгоритама.[Schneier B., 1991; Rivest R.L., 1992.] Поред тога, овај алгоритам је специфициран за коришћење у оквиру стандарда PKCS#1. Алгоритам MD5 продукује 128-битну hash вредност. Поред овог алгоритма, као што је већ речено, могућа је опција коришћења SHA-1 hash алгоритма који продукује 160-битну hash вредност.[Eastlake D., Jones P., 2001.] MD5. MD5 је алгоритам који процесира улазну поруку у блоковима од 512 бита, подељеним у 16 подблокова дужине 32 бита. Наиме, прво се порука проширује на тај начин да се добије порука која је по дужини тачно 64 бита краћа од одговарајућег мултипла од 512 бита. Проширивање је врло једноставно, прво се на крај поруке дода један бит јединице, праћен захтеваним бројем нула. Затим се 64-битна репрезентација дужине поруке прикључи резултату. Ова два корака служе у циљу формирања поруке чија је дужина тачно мултипл од 512 бита, што се захтева у алгоритму, обезбеђујући при томе да различите поруке неће изгледати исто након поменутог проширивања. Излаз алгоритма представља скуп од 4 32-битна блока, спојена тако да једнозначно формирају 128-битну hash вредност. Алгоритам се састоји од следећих корака:[Daeman J., 1995.]

- порука се обради тако да је њена дужина тачно мултипл од 512 бита,
- иницијализују се 4 32-битне променљиве (тзв. променљиве уланчавања):

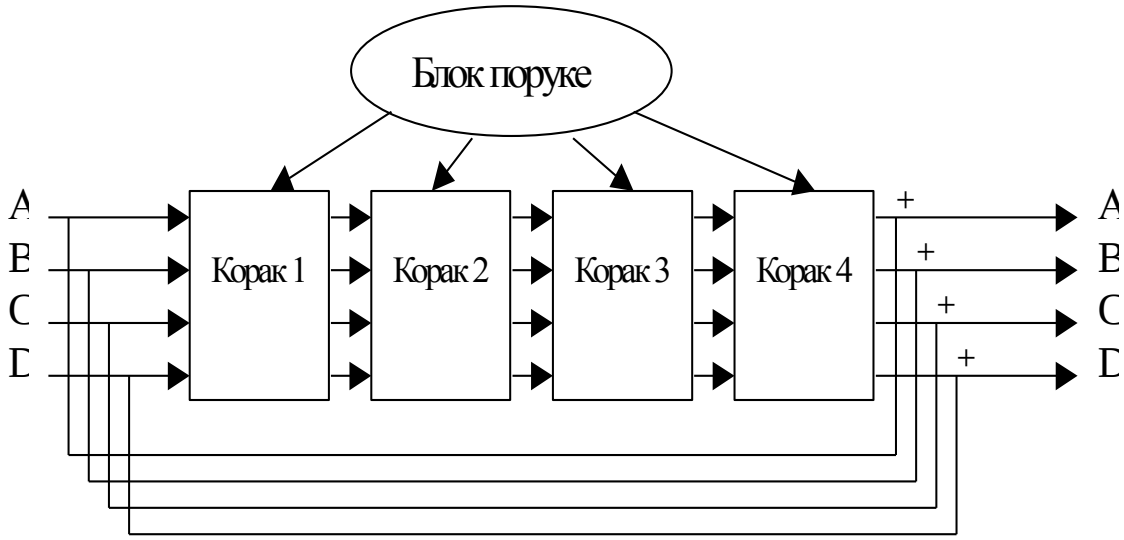
A=0x01234567

B=0x89abcdef

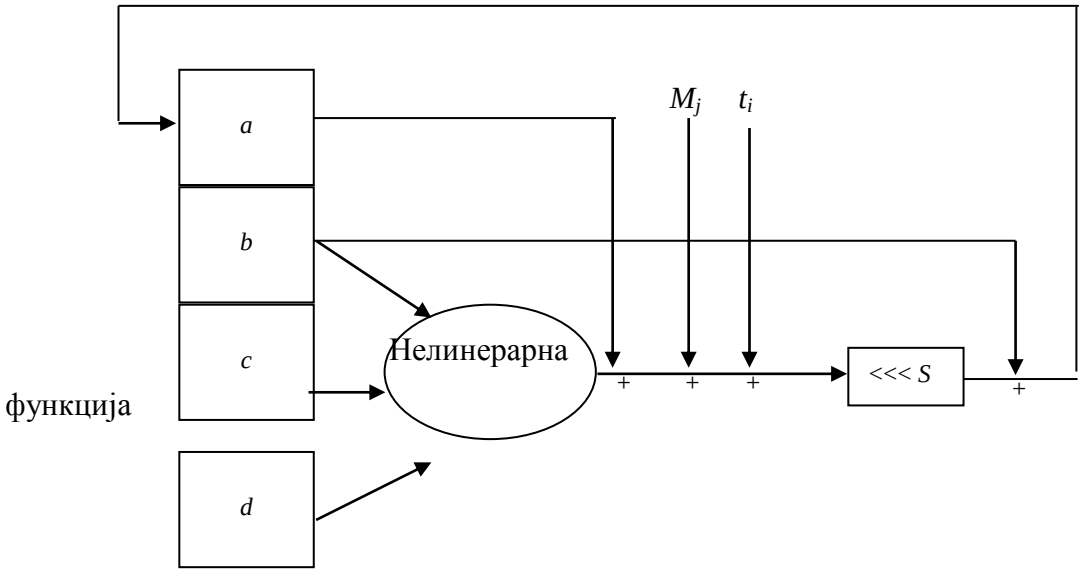
C=0xfedcba98

D=0x76543210

- затим почиње главна петља алгоритма која се извршава за све блокове дужине 512 бита дате поруке. Четири иницијалне променљиве се копирају у променљиве a, b, b и d. Главна петља се састоји од 4 фазе које су веома сличне. Свака фаза користи различиту операцију 16 пута, која се састоји од примене одређене нелинеарне функције над три од четири променљиве a, b, c или d. Затим се тако добијени резултат додаје четвртој променљивој, подблоку поруке и једној константи. Добијени резултат се ротира улево променљиви број бита и додаје се једној од четири променљиве a, b, c или d. На крају, резултат замењује једну од променљивих a, b, c или d. Видети слике 4.15 и 4.16




**Слика 4.15:** Главна петља MD5 алгоритма




**Слика 4.16:** Једна операција MD5 алгоритма

Постоје четири нелинеарне функције, по једна се користи у свакој операцији:

$$F(X, Y, Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge (\neg Z))$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee (\neg Z))$$

где наведени функцијски знаци представљају ($\oplus$ - XOR функција, $\wedge$ - AND функција, $\vee$ - OR функција, и $\neg$ - NOT функција).

Ако $M_j$ представља j-ти подблок поруке, j=0, …, 15, a <<< s представља функцију циркуларног шифтовања за s бита, тада се поменуте четири операције могу представити на следећи начин:

FF(a, b, c, d, $M_j$, s, $t_i$) означава: a = b + ((a + F(b, c, d) + $M_j$ + $t_i$) <<< s)

GG(a, b, c, d, $M_j$, s, $t_i$) означава: a = b + ((a + G(b, c, d) + $M_j$ + $t_i$) <<< s)

HH(a, b, c, d, $M_j$, s, $t_i$) означава: a = b + ((a + H(b, c, d) + $M_j$ + $t_i$) <<< s)

II(a, b, c, d, $M_j$, s, $t_i$) означава: a = b + ((a + I(b, c, d) + $M_j$ + $t_i$) <<< s)

Након претходно описаног поступка, a, b, c и d се додају на A, B, C и D, респективно, и алгоритам наставља са наредним блоком података. Крајњи резултат се формира конкатенацијом од добијених A, B, C и D.

### 4.5. Примена криптографских алгоритама у информационим системима

У претходном тексту било је речи о криптографским техникама које се могу користити при дизајнирању и реализацији система за заштиту информација. Криптографске технике које се користе смо сврстали у две групе:симетричне и асиметричне криптографске системе. Са становишта безбедносних услуга јасно је да се, уз мање или веће проблеме при реализацији у сваком од ових система, може реализовати већина основних безбедносних сервиса.

У обе врсте система неоспорно се може постићи поверљивост података. Чињеница је да симетрични системи на бази случајног и псеудослучајног низа пружају виши ниво безбедности од система са јавним кључем при истим дужинама кључева. Такође, системи са јавним кључем су знатно спорији од симетричних система и неопходни су им кључеви знатно веће дужине. С друге стране, код симетричних система у случају интензивног саобраћаја јавља се проблем дистрибуције кључева.

Што се тиче утврђивања аутентичности и идентитета субјекта у комуникацији, то се изузетно квалитетно реализује у системима са јавним кључем коришћењем технике дигиталног потписа, уз употребу дигиталних цертификата.У системима са тајним кључем такође се могу реализовати системи за аутентификацију.Најпознатији је Kerberos, али са становишта логике самог процеса аутентификације ту постоји једна непремостива тешкоћа. Наиме у таквим системима увек постоји трећа страна од поверења која активно учествује у процесу аутентификације, и као таква представља потенцијални извор опасности.

Што се тиче заштите интегритета података у оба система се поменути сервис релативно лако реализује, а као критеријум се узима успешно дешифровање (структура и садржај поруке).

Код реализације сервиса непорицања код симетричних система се јавља проблем постојања активне треће стране од поверења која у спорним ситуацијама врши арбитражу. Предност асиметричних система у овом случају је у томе што је субјект сам у стању да пружи доказе учешћа другог ентитета у трансакцији, уколико су остали безбедносни механизми система адекватни (пасивна трећа страна од поверења).

Из претходног излагања природно проистичу закључци о концепцији система заштите у ИТС пословних ситема. Најједноставније и најлогичније је формирати систем који користи добре стране и једних и других криптографских алгоритама, поготову што су они по својим добрим особинама комплементарни.

Према томе, најефикаснији приступ у конципирању система заштите ИТС пословних система је формирање хибридног система, који користи добре особине и једних и других система, па тако за утврђивање аутентичности, заштите интегритета и обезбеђење непорицања треба користити асиметричне системе а за заштиту тајности података симетричне криптографске алгоритме.[ Pfleeger, C.P., Pfleeger, S.L., 2002.]

Од алгоритама са јавним кључем природан избор би био RSA алгоритам због своје робусности и чињенице да се исти алгоритам користи и за шифровање и за потписивање порука. Распрострањеност овог алгоритма у применама учинила га је важећим *de facto* стандардом у тој класи.

Од јавних симетричних алгоритама ни један не може добити препоруку *a priori*, из простог разлога јер се сви поменути алгоритми користе за заштиту тзв. осетљивих информација, тј. оних које по свом садржају не представљају тајну информацију већ обезбеђују приватност. У случају безбедносно класификованих информација за заштиту тајности неопходно је обезбедити алгоритме адекватне степену тајности информације која се штити. За криптографску заштиту података који ће се размењивати у оквиру ИТС пословних система не може се дати препорука за коришћење јавних алгоритама са малим дужинама кључева, као што су RC4 (40), DES (40), DES (56), као ни за алгоритма за које је познато да имају криптографске слабости (RC2, RC4, DES, 3-DES). У том смислу, од јавних алгоритама препоручује се примена AES алгортима са кључевима дужине веће од 128 бита (препорука је да се користе најмање 256 бита), или примена верификованих посебно креираних криптографских алгоритама.

# 5. МУЛТИВАРИЈАЦИОНЕ СТАТИСТИЧКЕ МЕТОДЕ

## 5.1. Увод у мултиваријациону анализу

Израз мултивариациона нализа се користи да се опише анализа података који су мултиваријациони, у смислу да су многобројне обсервације измерене на великом броју промењивх.Типично анкетирање поставља од 30 до 100 питања сваком исипитанику.При описивању финаансиског стања компаније на пример , инвеститор може пожелети да испита 5-10 мерила рада конпаније.Обично су одговори на нека од ових мерила повезани међусобно.Изазов представља разјашљавања компликованих међуодноса различитих мерила над истим опсервацијама.Представљање ових резултата је оно што чини мултиваријациону анализу као надградњу истраживача.Често резултати који се добијају, не могу се постићи без коришћења мултиваријационе анализе. [Радојичић З., 2007.]

Мултиваријациона статистика обезбеђује могућност анализе комплексних низова података, тамо где има много независних и зависних промењивих које су корелисане једна са другом на различитим нивоима повезивања.Постојање софтвера који има могућност да обради комплексност великих мултиваријационих низова података, доводи до повећања и популаризације употребе мултиваријационе статистике.Тренутно научна методологија убрзано тражи комплексне релације између промењивих у покушају да обезбеди комплетније обухватније студије и моделе, те стога и ова докторска дисертација покушава да проникне у дубину тих релација.

Да би се дошло до низа резултата мултиваријационе анализе потребно је корисити процес који ће нам то омогућити, а то је итеративног и стохастичког карактера.За анлизу коју захтева мултиваријациону статистику, одговарајући низ података се морају формирати од вредности који одговарају броју промењивих у односу на број субјеката.Такође, одговарајући низови података могу бити организовани као матрице података, корелационе матрице, матрица варијанси-коваријанси, матрица суме квадрата и матрица унакрсних производа (cross product) или као низ резидуалав. [Tabachnick i Fidell, 1989.]

У процесу научног објашњења природе неког феномена полазну основу анализе сачињавају подаци који се односе на један или више скупова објеката.Ови објекти у анализи могу бити појединци, људске заједнице, различити предмети, а такође природни феномени или оне појаве које су производ активне делатности човека.Често нисмо у прилици да комплексну природу објекта сагледамо у потпуности.Међутим, на располагању нам стоји могућност обухвата тазличитих карактеристика, једне, по својој природи, вишедимензионе појаве. Те карактеристике, однсно обележја представљају предмет нашег мерења.Њих ћемо

једноставно звати промењиве.Покушај да се испита природа објекта истовременим мерењем већег броја промењивих на свакој јединици посматрања из једног или више скупова објекта назива се мултиваријациону анализу. [Радојичић З., 2007.]

## 5.2. Статистичка контрола процеса

### *5.2.1. Процес мерења*

Испитивање (истраживање) представља методологију објективног или субјективног утврђивања особина испитиваног објекта, односно својства испитиване појаве. Сагласно томе, испитивање се заснива на процесу мерења одговарајућих величина које одређују објекат, односно посматрану појаву. [Радојичић., 2001.]

Процес мерења у истраживањима може се посматрати кроз неколико фаза: дефиниција мерења, резултат мерења, принцип мерења, поступак мерења, мерна величина, мерни објекат или мерна појава, мерни инструмент, мерна инсталација и тачност мерења. [Радојичић З., 2007.]

Мерење као процес представља проблем, посебно у реалним условима када се суочавамо са разним утицајима који ометају квалитетно мерење. Процес креирања квалитетне мере за било коју врсту појаве (проблема) и учење из добијених резултата, са циљем имплементирања добијене мере као мере интензитета (нивоа активности) посматране појаве, представља основни и суштински циљ самог процеса. [Радојичић З., 2001.]

### *5.2.2. Контролне карте*

Приликом дефинисања контролних карата, најпре је потребно одредити границе случајног варијабилитета, односно стабилности процеса. Тако одређене границе случајног варијабилитета служе као мерило прихватљивог квалитета. Контролне карте су специфична врста тестова, прилагођених потребама контроле одређеног процеса.

У статистички стабилном процесу су присутне само случајне варијације, које доводе до флуктуације индивидуалних вредности унутар граница случајног варијабилитета (природне толеранције процеса).

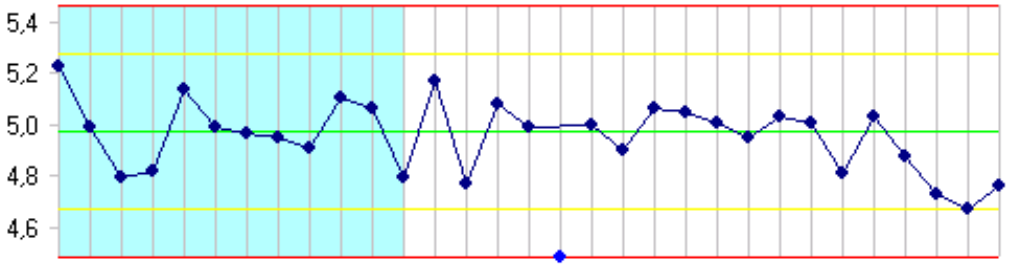
Према врстама карактеристика квалитета, контролне карте се деле на:

- контролне карте за нумеричке/мерљиве карактеристике квалитета и
- контролне карте за атрибутивне/описне карактеристике квалитета.

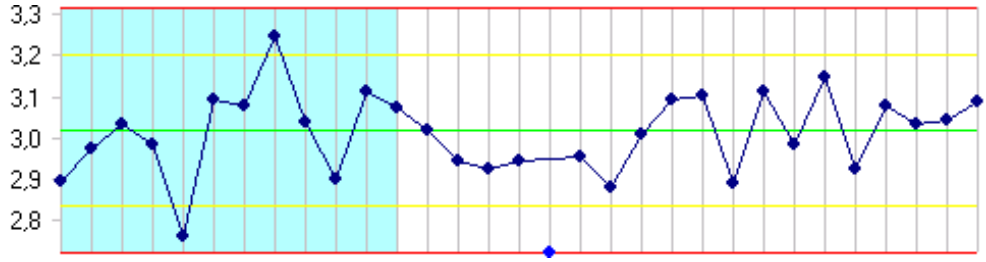
Нумеричке карактеристике квалитета су таква својства која се оцењују бројним вредностима, као, на пример: температура, притисак, дужина, густина, снага итд. Обично се при томе користи одговарајућа мерно-контролна и испитна опрема.

Атрибутивне карактеристике квалитета су својства која се оцењују описно, па се каже да је нешто добро или лоше, да одговара или не, да иде или не иде итд. Визуелна контрола квалитета је типично атрибутивно оцењивање.

Суштина одређивања стабилности контроле процеса помоћу контролних карата је у томе што се на основу индивидуалних вредности контролисане карактеристике пружања услуга извучених по временским секвенцама током одвијања процеса одмах сазна да ли је процес „под контролом“. Примери случаја када је процес „под контролом“ и „ван контроле“ приказани су на сл. 5.1и 5.2.




Слика 5.1. Процес је „под контролом“

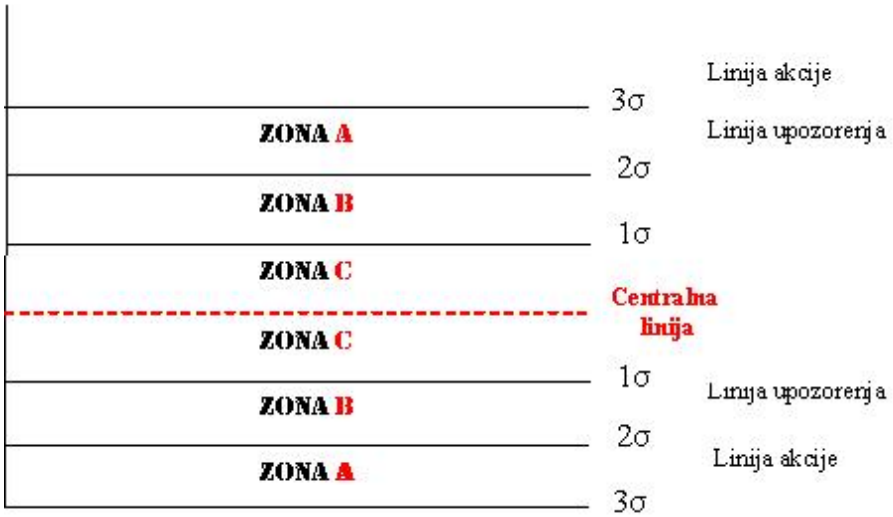



Слика 5.2. Процес је „ван контроле“

При употреби контролних карти користе се контролне границе као мера варијације процеса. То су линије акције и линије упозорења. Оне могу бити горње и доње. Горња линија акције се налази на удаљености од +3σ, а доња на удаљености од -3σ од централне линије. Горња линија упозорења се налази на удаљености од +2σ, а доња на удаљености од -2σ од централне линије. Простор између контролних граница се даље може поделити у три зоне. Те зоне, назване А, Б и Ц, полазе од централне линије и користе се у анализи и тумачењу контролних карти (слика 5.3).

Линије акције $X \pm 3\ \sigma_e$

Линије упозорења $X \pm 2\ \sigma_e$




Слика 5.3. Границе контролних карата [Oakland J., 2008.]

### *5.2.3. Методологија статистичке контроле процеса*

Основни циљ савремене контроле квалитета јесте превенција грешке, која се остварује квалитетним управљањем процесима. Статистичка контрола процеса -SPC(статистицал процесс цонтрол – SPC) је метода за прикупљање и анализу података у циљу решавања практичних проблема контроле квалитета.

Квантитативно мерење карактеристика квалитета је основ за примену SPC. Идеја је да се прикупи довољно узорака, односно података о процесу како би се стекла знања о процесу који се прати. То значи сагледати када процес функционише добро, његове границе, јер сваки процес варира, без обзира на то како добру контролу има. Поменуте варијације процеса представљају кумулативну грешку сваке његове компоненте. Те грешке, односно варијације су природа сваке компоненте процеса и на њих се може утицати само одговарајућим променама у датом процесу. [http://www.indicators.scot.nhs.uk]

Нормално варирање процеса се објашњава ефектом уобичајених узрока. Процес је „под контролом“ ако су варијације параметара квалитета производа у границама природне флуктуације процеса. Ако је процес под контролом, онда он функционише оптимално и никакво подешавање није потребно.

Треба нагласити да „под контролом” не значи да производ или услуга задовољава захтеве купца. То само значи да је процес конзистентан, можда конзистентно лош. На пример, може се догодити да су неке контролне тачке изван граница спецификације али унутар статистичких контролних граница, што значи

да је процес „под контролом“ али да није способан да задовољи захтеве спецификације. У том случају постоје две могућности – побољшање процеса или промена спецификације производа. Важно је запамтити да спецификација производа дефинише оно што се мисли да човеку треба (човек чини), а статистичке контролне границе показују шта процес може урадити конзистентно.

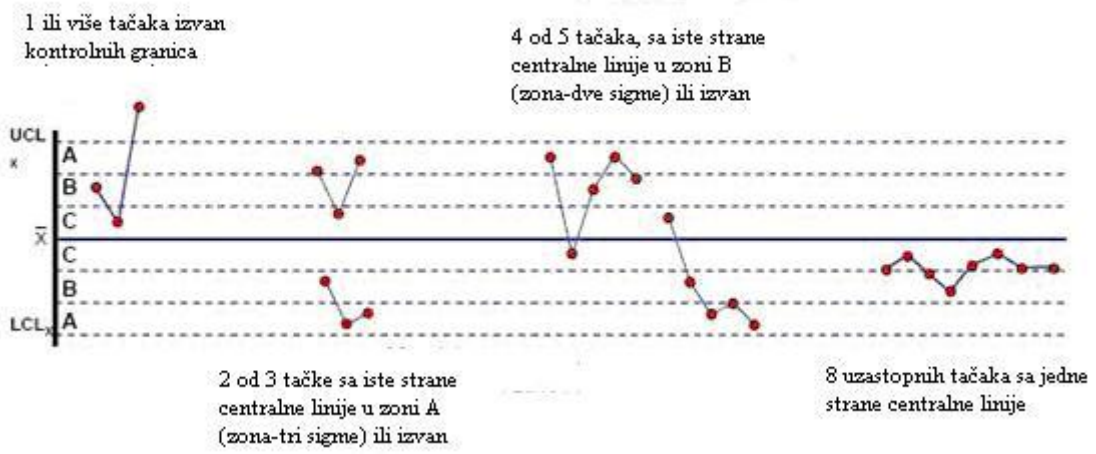
Велики број узрока варијација процеса је могуће лако идентификовати и елиминисати. У SPC терминологији, природне границе варирања процеса се називају статистичке контролне границе и оне су утврђене на основу мерења у дужем временском периоду.

Узорак у SPC терминологији значи скуп од једног или више мерења и служи за израчунавање тачке на контролној карти. Група је било који комплетан сет узорака који се користе за конструисање контролне карте. Ако се користе вишеструка мерења као узорак, онда се такав сет података назива подгрупа.

Будућа статистичка контрола процеса своди се на графичко приказивање узорака у облику контролних тачака на контролној карти, са границама које су дефинисане претходним поступком. Уколико је процес „под контролом”, појавиће се потпуно случајан распоред контролних тачака на контролној карти. Корисник ће у том случају користити контролну карту да би утврдио перформансе процеса. Када контролне тачке формирају тренд или необичан циклус, или су изван контролних граница, биће регистровани алармом. [Čisar, 2010.]

За процес се каже да је „ван контроле“ уколико се јави једно од следећих правила (графикон 5.1и 5.2):

- једна или више тачака изван контролних граница;
- 2 од 3 тачке са исте стране централне линије у зони А (зона-три сигме) или изван;
- 4 од 5 тачака, са исте стране централне линије у зони Б (зона-две сигме) или изван;
- 8 узастопних тачака са једне стране централне линије;
- 6 узастопних тачака монотоно растућих или монотоно опадајућих;
- 14 тачака у низу циклују горе-доле;
- 15 тачака у низу у зони Ц (зона-једне сигме), изнад и испод централне линије;
- 8 тачака са обе стране линије али не у зони Ц.




Графикон 5.1. Правила када је процес изван контроле – 1[Oakland J., 2008.]


Графикон 5.2. Правила када је процес изван контроле – 2 [Oakland J., 2008.]

### 5.3. Шест сигма методологија

Организације дефинишемо као "циљно оријентисане административне јединице које трансформишу улазе у излазе".[Aldrich, H. E., 2000.] Управо због тога, организација може бити компанија или стратешка пословна јединица унутар компаније.[Drucker, P.F., 1993.] Организације се врло често труде да искористе програме континуалних побољшања и ови се програми најчешће састоје од великог броја пројеката континуалног побољшавања. Пројекти са циљем побољшања процеса се извршавају коришћењем одговарајућих алата и техника, све са жељом да се унапреде тачно одређени аспекти пословања.

Програми континуалног побољшавања као што је Шест Сигма (Сих Сигма) се најчешће имплементирају на два нивоа – кроз пројекат и кроз организацију.

[Un, C. A., and Cuervo-Cazurra, A., 2004.] Конзистентни и комплементарни напори на оба нивоа су неопходни како би успели у нашем циљу, остваривање континуалног побољшања процеса. [Lok, P., Hung, R. Y., Walsh, P., Wang, P., and Crawford, 2005.] Због свега наведеног, Шест Сигма се може проучавати и са апекта пројекта и са апекта организације.

Суштина Шест Сигма пројеката је смањивање варијансе процеса. Конкретно, Шест Сигма тежи редукцији и контроли варијансе процеса у тој мери да иако излаз варира до ±6σ, он је у потпуности повинован доњој и горњој граници спецификације. [Pande, P. S., Neuman, R. P., and Cavanagh, R. R.., 2000.] Овај стандард се представља као само 3.4 дефекта у милион производа/услуга, што је фантастичан проценат исправности излаза (Слика 5.3.4). Шест Сигма је метрика креирана у компанији Моторола током 80- их година прошлог века. Основни циљ је био побољшање пословних процеса, као и могућност упоређивања перформанси различитих процеса управо помоћу Сигма нивоа.

Иако је на почетку осмишљена као средство за смањивање дефеката, бројне студије показују да се Шест Сигма трансформисала у нешто много више од статистичке контроле процеса. На пример, Панде [Pande, P. S., 2000; Pande, P. S., 2001.] описује Шест Сигма као "...флексибилни систем за постизање пословног успеха. Шест Сигма је јединствена комбинација: размевања захтева клијената, дисциплинованог коришћења података и статистичке анализе." Линдерман [Linderman, K., Schroeder, R. G., Zaheer, S., and Choo, A. S., 2003.] пружа врло сличну дефиницију: "Шест Сигма је организован и систематичан метод, за стратешко унапређење пословних процеса (као и развој нових производа и услуга), који се конципира на статистичким методама и константно смањује број дефектних производа/услуга."

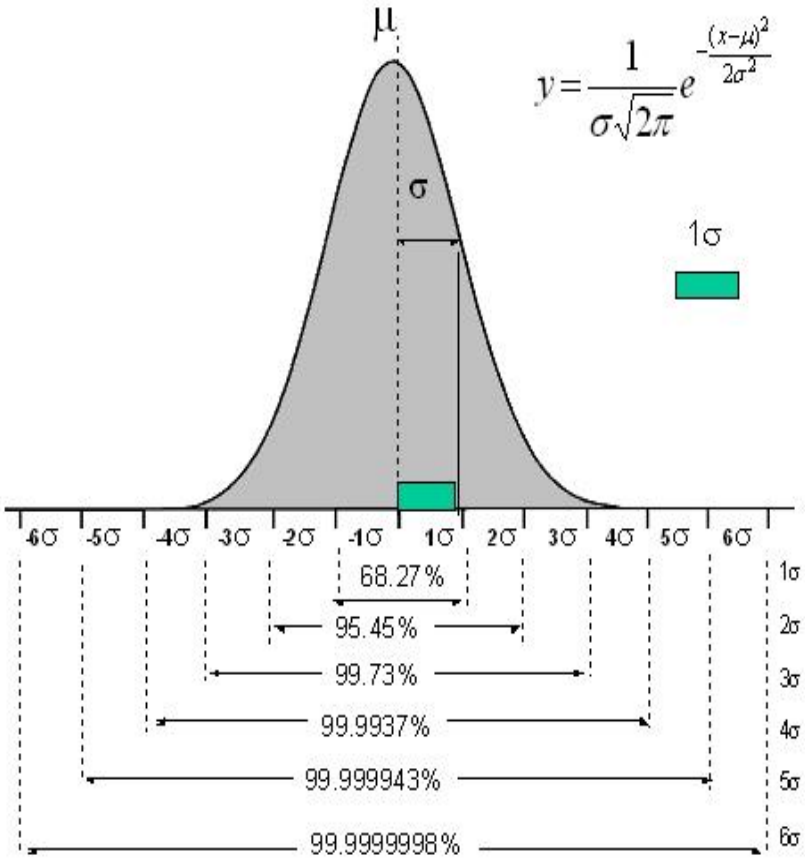
Концепти као што су дефекат и квалитет, су кључни за Шест Сигма методологију. Управо је сврха Шест Сигма пројеката смањивање појављивања дефеката у процесима. Као последица тог приступа долази до повећања квалитета услуга које се пружају клијентима. Управо због свега наведеног се квалитет може посматрати као импликација смањивања дефеката кроз процесе континуалног побољшавања. Шест Сигма пројекти смањују број дефеката у разним процесима, од маркетинга, продаје, преко производње и услуга, све до пост-продајних услуга. Поред тога, тичу се и свих пратећих процеса који служе да омогуће несметано извршавање кључних процеса. Недостатак у било ком аспекту онога што купац очекује од нас се означава као дефекат, док је свако побољшање оно што креира додатну вредност за клијента.

Шест Сигма програми успостављају иницијативу за континуално побољшање перформанси организационих система – раст ефикасности и модификовање процеса у складу за жељама наших клијената. Побољшање процеса се изводи кроз одговарајућу методологију Шест Сигма пројеката, најчешће дефинисану као Define-Measure-Analyze-Imrove-Control(DMAIC ).

Кратак преглед корака у DMAIC оквиру се налази у Табели 5.3.1. [Rasis D., Gitlow H.S., and Popovich E., 2003.]

Табела 5.1. Циљеви сваке од фаза у DMAIC пројектима

| | |
|---|---|
| Дефиниши | □ Одређивање корисничких захтева<br>□ Дефинисање пројектних циљева<br>□ Планирање пројекта и креирање распореда за сваку DMAIC фазу<br>□ Формирање пројектног тима |
| Мери | □ Проучавање процеса и одређивање релевантних метрика<br>□ Оцењивање валидности и поузданости система мерења<br>□ Пројектовање и имплементација новог система мерења, уколико је то неопходно<br>□ Одређивање жељених перформанси за кључне елементе система |
| Анализирај | □ Одређивање варијансе процеса<br>□ Проналажење потенцијалних узрока проблема<br>□ Прикупљање и анализирање података<br>□ Одређивање разлога постојања високе варијансе процеса |
| Поправи | □ Испитати потенцијалне промене у процесима<br>□ Формирати акциони план за имплементацију промена<br>□ Пилот-програм<br>□ Имплементација промена |
| Контрола | □ Обезбеђивање стандардизације предлоџених промена<br>□ Указивање на евентуалне проблеме са прихватањем и имплементацијом предложених промена<br>□ Верификација очекиваних резултата<br>□ Документовати ефекте промена |




Слика 5.4: Шест сигма методологија – проценат исправних (недефектних) производа/услуга

### *5.3.1. Фаза дефинисања(DEFINE)*

Слово D у DMAIC методологији се односи на фазу дефинисања. За било какву иницијативу побољшања процеса, прво морамо да одлучимо шта радимо, зашто то радимо, како то урадити и какве резултате прижељкујемо. Шест Сигма ставља посебан нагласак на активности дефинисања. Послови се заснивају на процесима, производи и услуге се пружају помоћу процеса. Све што урадимо са процесима ће креирати разлику, позитивну или негативну. Централна идеја фазе дефинисања је да пажљиво изаберемо процес који желимо да унапредимо. За почетак, треба прво да дефинишемо шта треба да се промени.Постоје три начина који могу бити изузетно корисни: [Rasis D., Gitlow H.S., and Popovich E., 2003.]

*а) Покварено је - Поправи*

Ово је вероватно најлакши случај. Имамо неку активност која је есенцијална за наш бизнис. Та активност прави велики број проблема, “боде нам очи“ да управо

она мора бити под хитно унапређена.

*б) Потенцијални циљ*

Организација прикупља информације током времена, анализира ове податке и онда користи резултате да би утврдила потенцијалне могућности за побољшање.

*ц) Слушај пажљиво*

Врло су честе наредбе са врха. Топ менаџмент спроводи одређене стратешке акције и одређује које аспекте нашег пословања треба детаљно преиспитати.

Пошто смо дефинисали проблем, спремни смо да започнемо пројекат. Постоје различити приступ овом проблему, али у сваком од њих основне активности у процесу развоја пројекта су идентичне. Један од њих је дефинисање мисије. Наша мисија треба да опише проблем који покушавамо да решимо, циљеве које желимо да постигнемо, као и корист коју ће компанија остварити од успешне имплементације овог пројекта. Све пословне активности захтевају одређени тип спонзорства од стране менаџмента. Такво спонзорство је често имплицитно што често доводи до проблема. Управо зато спонзорство треба учинити експлицитним. У нашем плану пројекта треба тачно да дефинишемо који сектор компаније ће бити наш официјелни спонзор. Одређивањем спонзора у свом плану успостављамо организациону подршку за наш пројекат. У следећим корацима неопходно је креирати шему пројекта, дефинисати тим и ресурсе.

Шема пројекта је изузетно користан алат као што је и организациона шема. Пројекти су као сектори у компанијама, једина разлика што нису перманентни. Постоје због одређених сврха, захтевају одређене улоге. Врше интеракцију са осталим организационим јединицама на специфичне начине. На тај начин наша шема чини пројекат интегралним делом организационе структуре компаније.

Дефинисање пројекта и шема су добре ствари за почетак. Али нећемо много одмаћи од почетка без доброг тима и одговарајућих ресурса. Иако ово делује као нормална ствар, бројни су примери недовољне пажње која се посвећује овом питању. Зато треба одмах у почетним фазама експлицитно дефинисати ко чини тим, који чланови организације ће попунити која места. Након овога следи остваривање одговарајућег нивоа комуникације у тиму.

Готово сигурно есенцијални део програма Шест Сигма се тиче дефеката. Идеја је да дефект повежемо са одговарајућом дефиницијом, како би га одмах препознали. Дефекти моги доћи у много облика. Оно што им је свима заједничко је, (1) то мора бити грешка која прети кључним процесима, (2) то мора бити мерљиво.

Постоје бројне методе које су прилично корисне у фази дефинисања. У нашем раду ћемо објаснити најзаступљенију: Парето charting. Генерално, различити типови дефектности су повезани са различитим кључним излазним варијаблама. Метода Парето charting табеларно представља све дефектности које

креира производни систем. Визуелизацијом велике количине података више не представљају проблем за доносиоца одлуке. Фраза Паретово правило се односи на учестало догађање да се 20% узрока налази у 80% дефеката. У овим случајевима, подсистеми од највећег интереса, који су често уско грло, врло лако бивају препознати помоћу Паретове методе.

### *5.3.2. Фаза мерења (Mesure)*

У организацијама које се базирају на принципима Шест Сигма, мерења су континуалне активности којима се прикупљају преко потребни подаци. Подаци су кључ у одређивању како се заправо ствари одвијају. Као што смо видели у претходним одељцима пројекат Шест Сигма има велики број планова, између осталих план прикупљања података. Овде дефинишемо које процесе и компоненте ћемо мерити. Циљ нам је да креирамо емпиријску слику тренутних перформанси. Потребна су нам барем три корака да би то успели: (1) припрема за мерење (2) мерење (3) чување интегритета прикупљених података. [Rasis D., Gitlow H.S., and Popovich E., 2003.]

Припрема мерења може бити изузетно једноставна ако желимо да измеримо температуру, влажност или ваздушни притисак; барометар постављен на зиду ће обавити посао. Ако меримо ефикасност радника или неку сличну активност, требаће нам много више труда. Када мерење захтева да наш тим уђе у радну околину на начин који може утицати на оно што меримо, неопходно је да припремимо околину за наш долазак. У следећој итерацији морамо да креирамо детаљне мапе процеса. Мапе процеса су репрезентација процеса које детаљно приказују улазе, излазе и токове система. Добра мапа процеса ће нам приказати све специфичности система и помоћи нам да одредимо добар план за прикупљање података. С друге стране, документације су врло често застареле, поготово у системима који се драстично мењају током времена. С обзиром на то, пре почетка било каквог процеса мерења морамо потврдити да су мапе процеса заиста оно што се и дешава у фабричким погонима.

Ако смо све пре овога добро урадили, онда ће сам процес мерења бити изузетно прост. Међутим, и овде постоји неколико ствари са којима треба бити обазрив. Прикупљање података треба вршити из сличних извора, придржавати се временског распореда, користите нова мерења.

У свим Шест Сигма пројектима неопходно је гарантовати интегритет података. Наш тим за мерење треба да осигура да прикупљени подаци остану веродостојни за анализе које предстоје. Такође, постоје и разматрања везана за поверљивост информација. Сви подаци које прикупимо дају нам слику о ефикасности компаније и због тога морају имати статус поверљивих информација.

Бројне су методе које се користе у овој фази DMAIC приступа. Следеће

четири су изузетно распрострањене процедуре: p-charting, u-charting, demerit charting, Xbar& Rcharting.

### *5.3.3. Фаза анализе (Analyze)*

А у DMAIC односи се на анализу, анализирање података који су прикупљени током времена. Ово је само по себи изузетно комплексан део методологије Шест Сигма. Централна идеја је да кроз анализу прикупљених података одредимо корене узрока дефеката или лоших резултата, и да онда успоставимо емпиријску основу за побољшање процеса. Кључно је одредити корен проблема, не само симптоме. Симптоме углавном прилично лако примећујемо и без проблема разрешавамо. [Rasis D., Gitlow H.S., and Popovich E., 2003.]

Фаза анализе укључује успостављање везе узрок-последица између системских улаза и излаза. Више различитих метода користе различите изворе података и генеришу различите визуелне информације за доносиоце одлука. Методе које могу бити релевантне за ову фазу су дизајн експеримената, QFD матрица узрока и последица, мапирање процеса, мапирање тока вредности.

### *5.3.4. Фаза побољшања (Improve)*

После прикупљања и анализе велике количине података, наш Шест Сигма тим ће стећи довољно информација како да побољша процесе и активности у компанији. Фазу анализе можемо посматрати као део Шест Сигма где идентификујете корене проблема. Због тога фазу побољшања можемо посматрати као део где уклањамо те проблеме. Фазу побољшања најчешће чини 6 корака: [Rasis D., Gitlow H.S., and Popovich E., 2003.]

1. Процена,
2. Развој,
3. Селекција,
4. Модификација,
5. Пилот, и
6. Верификација.

Кроз анализу података, наш тим ће поседовати колекцију индикатора побољшања. Ови индикатори показују који процеси имају високу варијансу. Тада на сцену ступа процена наших опција и могућности. Неке опције више обећавају од других, с друге стране неке нису у тој мери реалне. Управо је ту и драж Шест Сигме; кључ је у подацима, али се коначна одлука доноси на основу наше процене. Процену вршимо узимајући у обзир организациону структуру, буџет,

распоред, циљеве које желимо да остваримо.

Постоји неколико начина како да развијемо решења за побољшање процеса. Један је да направимо корелацију са постојећим компонентама процеса. Ако извршимо подешавање елемента процеса који већ постоји у систему, успећемо да побољшамо процесе без много реинжењеринга. Друга могућност је да креирамо нови ток посла са циљем интеграције недостајућих компонената процеса. Ово је случај када подаци показују одсуство одговарајућих елемената који проузрокују значајну варијансу. Трећа могућност је креирање потпуно нових процеса или компоненти.

У фази селекције, Шест Сигма тим се фокусира на доношење одлуке. Неопходно је простудирати све опције које смо предложили, развијали и донети одлуку која опција је најбоља за пројекат.

Након што смо изабрали опцију коју желимо да применимо, побољшавамо процес елиминацијом основног узрока дефекта и унапређујемо га пројектовањем креативних решења. Можемо истраживати иновације и побољшања користећи релевантне технологије. Модификације треба да прате тренд и ограничења презентована у подацима.

Након завршетка свих претходних корака, треба да покренемо процесе кроз праве ситуације, кроз пилот програм. То је корисно из више разлога. Желимо да тестирамо наш предлог у окружењу што сличнијем производњи. Евалуација постигнутих резултата ће нам дати добру слику шта да очекујемо у правом систему. Пошто је пилот завршен и наш тим је сигуран да треба предложити примену, морамо верификовати овај закључак са остатком организације.

### *5.3.5. Фаза контроле (Control)*

Основна сврха контроле је да се организација у потпуности посвети институционализацији ревидираних процеса. Корпоративне навике и рутина су ствари које се тешко мењају. Након представљања неких новитета у раду, компанија има тенденцију да се стално враћа на стари начин рада. То је у потпуности разумљиво. Стари начини су много познатији, лакше их је користити. Али такав начин дефинитивно није формула за успех. [Rasis D., Gitlow H.S., and Popovich E., 2003.]

Изузетно битан аспект је креирање плана са којим желите да координишете имплементацију нових или побољшаних активности. У суштини, план контроле описује шта се имплементира, како ће се то користити и какви материјали су захтевани као подршка. Састоји се од (1) описа процеса који се имплементира. Ако је то нови елемент, опис ће укључивати сврху елемента, кораке новог процеса, примарне и секундарне учеснике, улазе и излазе. Ако је у

питању исправка постојећег елемента, описи су допуна постојеће документације. (2) мапирање нових функционалности у тренутне токове процеса. Процеси и активности су интегрални део система, и као такви утичу један на другога. Тако да ако измените неки део тог система, морате имати у виду како ће реаговати његов претходни или следећи подсистем. (3) идентификација власника процеса. Постоје три категорије, примарни актер који је одговоран да се процес правилно изврши; секундарни актер који нам је неопходан да би пружио улаз у наш процес или користио излазе из нашег процеса, система; менаџҷмент који се ослања на наш процес како би контролисао стандардне активности. (4) опис промене производње. Са увођењем одговарајућих промена у активности, производња ће се променити на неки начин. У сваком случају опис ових промена треба да се налази у плану контроле. Пошто се свака неочекивана новост типично назива девијација и броји као дефект, наш план треба да опише шта ће нове активности имати као свој излаз. (5) локација и приступ помоћном материјалу. То могу бити токови података, упутства за одређене процедуре, форме или било какви алати. У контролном плану треба да идентификујете ове ресурсе и одредите где се налазе. (6) распоред тренинга. Концепт тренинга треба увек да буде у асоцијацији са увођењем неких новина у организацију.То може бити рад у учионици, компујтерско учење, видео тренинг. У сваком случају, процес тренинга треба да буде координисан са онима који ће директно користити новости у раду компаније.

Очигледно, постоји могућност да предложене промене нису иницирале побољшања. У том случају, логично је вратити цео поступак у фазу анализе и/или побољшања са циљем креирања нових предлога. Понекад је неопходно и прекинути пројекат и уверити се да никаква штета није направљена. Укратко, примарни циљ фазе контроле је да пружи јак доказ о достизању циљева који су пред нас стављени. Због тога је неопходно да сва предложена решења буду пажљиво тестирана током пробних периода.

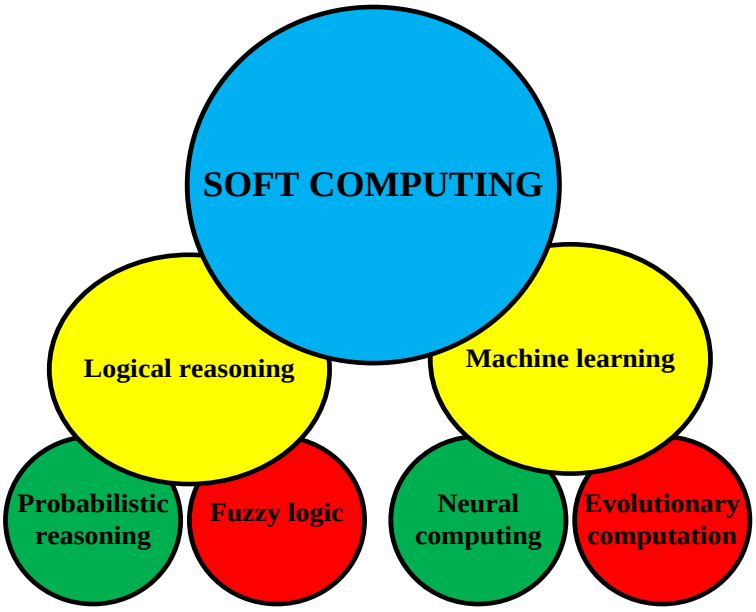
## 5.4. SOFT *COMPUTING* Метода

### *5.4.1. Увод у SOFT COMPUTING методу*

Једна од подручја истраживања у овом раду, је примена *SOFT COMPUTING-а* за анализу података. *SOFT COMPUTING* се разликује од традиционалног (чврстог) рачунања јер је много толерантнији према непрецизности, неизвесности, делимичној истини и апроксимацији. Заправо, модел *SOFT COMPUTING*-а је базиран на раду људског мозга. Главни принципи *SOFT COMPUTING*-а су: толеранције према непрецизности, непредвидљивости,

делимичној истинитости и апроксимацији како би се достигли управљивост система и ниски трошкови решења.

Основне идеје *SOFT COMPUTING*-а су засноване на утицају *Fuzzy Logic (FL), Neural Computing (NC), Evolutionary Computation (EC), Machine Learning (ML)* и *Probabilistic Reasoning (PR).* [Yager R. R., Filev D.,1994.] Ти утицаји чине основне компоненте *SOFT COMPUTING*-а. У последње време користе се и достигнућа из теорије хаоса и теорије учења. *SOFT COMPUTING* је пре свега целина свих наведених области пре него њихова проста мешавина.[Kacprzyk J. .,1994.]Наведене дисциплине уносе различите методологије одерђивања проблема у својим доменима, при чему се допринос *SOFT COMPUTING*-у сваке од њих посматра у светлу међусобног допуњавања. [Radojević D., Petrović B.,1998-2004;Radojevic: D.,2007.]




Слика 5.5. Области *SOFT COMPUTING*-а

Комплементарност дисциплина *(FL), (NC), (EC), (ML)* и *(PR)* има следећу последицу: многи проблеми се могу боље решити комбинацијом наведених дисциплина него појединачном применом сваке од њих. Сарадња наведених дисциплина је у последње време позната под именом "*Neurofuzzy systems*". Овакви системи налазе све већу примену у сфери производа широке потрошње од расхладних уређаја и веш-машина до фотокопир машина и камкордера. Иако мање уочљиви "*Neurofuzzy system*"-у индустријским применама имају још значајнију улогу. Оно што је значајно у обе наведене примене "*Neurofuzzy system*"-а је то да се применом техника *SOFT COMPUTING*-а долази до система који поседују висок *MIQ (Machine Intelligence Quotient).* [Klir G. J.,Yuan Bo., 1995.]

### *5.4.2. Формулација проблема*

Један од често коришћених алата у статистици је дискриминациона анализа. Она се заснива на креирању модела који омогућује да се одреди модел који нам за вредности интервалних променљивих (задатих атрибута неке појаве) одреди припадност групи. Да би се добио добар модел, који је представљен дискриминационом функцијом, потребно је да улазни подаци садрже поред вредности атрибута и припадност групи.

Да би дискриминациона анализа добро радила, потребно је да се испуне следећи предуслови који су везани за улазне податке:

1. групе (кластери, класе) треба да имају бар приближно нормалну расподелу;
2. узорци треба да буду случајни;
3. матрице варијације и коваријације треба да за сваку групу буду исте;и
4. почетни подаци морају да буду тачно квалификовани (подељени у групе).

Основна снага, али како касније можемо видети и слабост класичне дискриминационе анализе, заснива се на томе да се припадност групи одређује преко линеарне комбинације интервалних променљивих (атрибута проблема). Како се мане овог приступа могу избећи, а да алат који користимо и даље остане линеаран, погодан због математичке једноставности и малог броја прорачуна, видећемо пошто размотримо основне претпоставке [0, 1] вредносне логике као природног уопштења логичког закључивања.

Дискриминациона анализа има два основна циља. Први, да утврди да ли постоји статистички значајна разлика у срединама две или више група, а затим да одреди која од променљивих даје највећи допринос утврђеној разлици. Овај циљ анализе називамо дискриминација или раздвајање између група. Други циљ односи се на утврђивање поступка за класификацију опсерваација на основу вредности неколико променљивих у две или више раздвојених унапред дефинисаних група. Овај циљ називамо класификација или алокација опсервација. У конкретном истраживању ова два циља често се међусобно преклапају, па средства анализе која користимо за раздвајање између група истовремено служе и за класификацију опсервација унапред дефинисане групе. У литератури, методе дискриминационе анализе које се односе на први циљ – раздвајање група, излажу се под насловом дескриптивна дискриминациона анализа, док се методе примерене другом циљу – алокацији опсервација, излажу под насловом методе класификације. [Đorđević. M.., 2011.]

Са техничке стране основни циљ дискриминационе анализе је формирање линеарних комбинација независних променљивих којима ће се дискримнација између унапред дефинисаних група тако извршити да грешка погрешне класификације опсервација буде минимизирана, или другачије речено, да се

максимизира релативан однос варијанси између и унутар група. Линарном комбинацијом независних променљивих за сваког испитаника или објекат одредимо број, дискриминациони скор, који се затим трансформише у апостериорну вероватноћу да испитаник или објекат потиче из једне од група.

### 5.5. Дискриминациона анализа

Основну идеју дискриминационе анализе излажемо користећи следећи графички приказ, на коме је илустрован проблем дискриминације између две групе $G_1$ и $G_2$ на основу две независне променљиве $X_1$ и $X_2$.

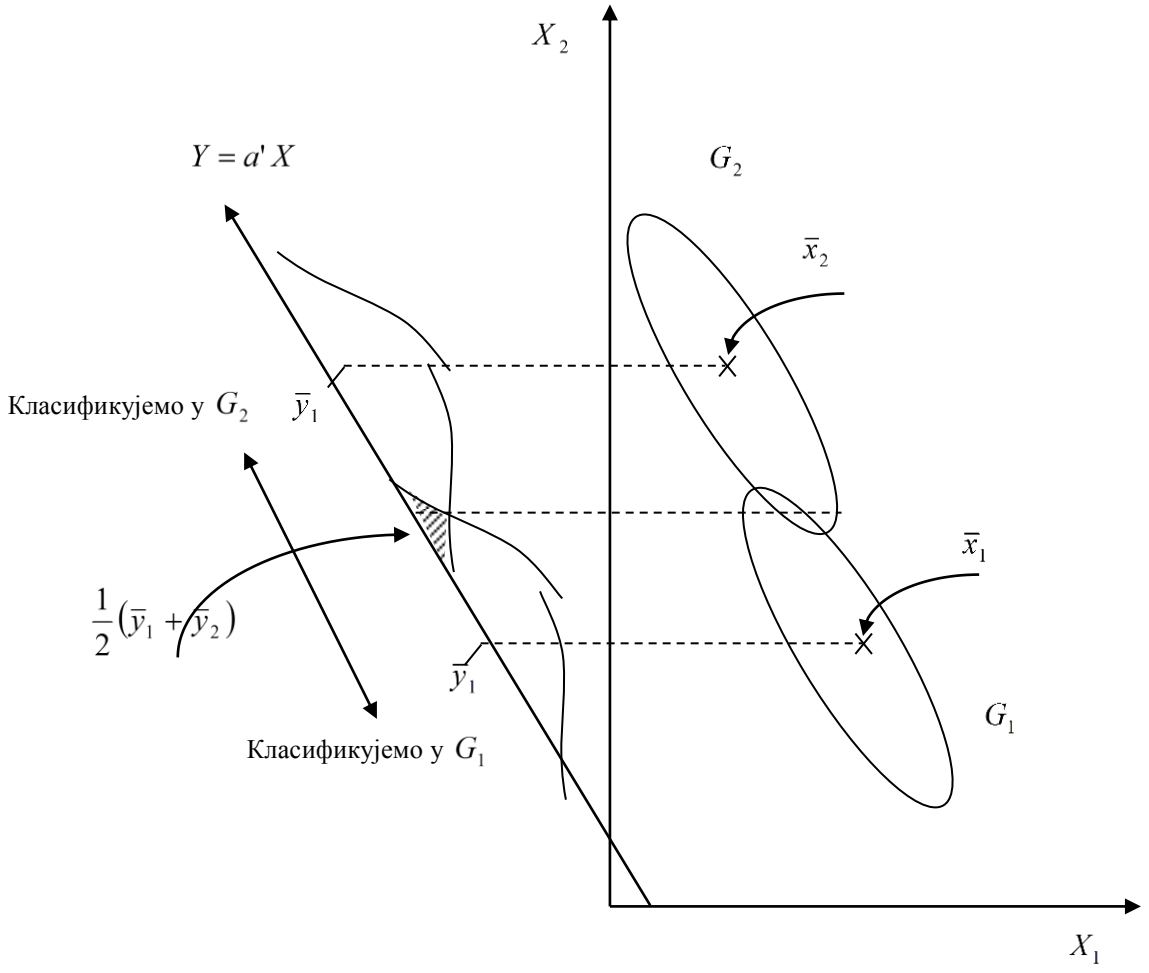



График 5.3. Основна идеја дискриминационе анализе

Елипсама је обухваћено, рецимо 95% опсервација прве и друге групе на односним дијагоналама растурања. Дискриминациони скор за сваког испитаника формира се на основу линеарне комбинације вредности две независне променљиве. Значи да у општем случају имамо *Y=a'X*, где је *Y* дискриминациони скор, *a* је *p*-димензиони вектор дискриминационих коефицијената (коефицијенти линеарне комбинације), а *X* је *p*-димензиони вектор независних промнељивих. Пројекција тачака са дијаграма растурања на *Y* осу генерише једнодимензионе распореде дискриминационих скорова двеју популација $G_1$ и $G_2$. Истовремено су на правим линијама тежишта елипси $\bar{x}_1$ и $\bar{x}_2$ (реализована вредност средине односних група) спојена са њиховим пројекцијама на *Y* осу (тачке $\bar{y}_1$ и $\bar{y}_2$). Средине дискриминационих скорова за ове две групе називамо први односно други центроид. Њиховим поређењем можемо утврдити колико су групе међусобно удаљене. За потребе класификације опсервација унета је и средина центроида, тј. $\frac{1}{2}\left(\bar{y}_1+\bar{y}_2\right)$. Шрафирана површина на крајевима два једнодимензиона распореда добијена њиховим преклапањем биће минимална управо за пројекцију на *Y* осу оне праве линије која пролази кроз две тачке пресека елипси. Шрафирана површина под кривом лево од тачке $\frac{1}{2}\left(\bar{y}_1+\bar{y}_2\right)$ представља вероватноћу погрешне класификације оних испитаника који припадају групи $G_1$, а ми смо их алоцирали у групу $G_2$, а шрафирана површина под кривом десно од тачке $\frac{1}{2}\left(\bar{y}_1+\bar{y}_2\right)$ представља вероватноћу погрешне класификације испитаника игрупе $G_2$ у групи $G_1$.

Као и методе муливаријационе анализе варијансе и муливаријационе регресионе анализе и метода дискриминационе анализе спада у групу метода зависности. Заједничка карактеристика сва три метода јесте да се на основу скупа независних променљивих формирају, предвиђају или описују понашања зависних променљивих. Међутим, за разлику од регресионе анализе, код дискриминационе анализе зависна променљива је фиксна (узима вредност 1 и 0 ако разматрамо проблем дискриминације две групе), а независне променљиве су случајне променљиве нормално распоређене.

Да би се постигао први циљ дискриминационе анализе, што је могуће боље раздвајање група и анализа самог раздвајања, потребно је дефинисати критеријум дискриминације. *Fisher* (1936) је први дефинисао тај критеријум и изложио поступак дискриминације између две и више група.

Поступак раздвајања две групе, по *Fisher*-у, заснивамо на *p*-димензионом случајном вектору *X*. Реализације случајног вектора разликују се међусобно већ према томе да ли потичу из популације $G_1$ или популације $G_2$. Стога сваку од ове две популације описујемо одговарајућом вишедимензионом функцијом густине

$f_1(x)$ и $f_2(x)$ респективно. Да би се смањила димензија разматраног проблема, Fisher је предложио да се p-димензионе опсервације *X* трансформишу (линеарном комбинацијом) у једнодимензиону опсервацију *y* (дискриминациони скор), тако да су вредности *y* из група $G_1$ и $G_2$ међусобно раздвојене што је могуће више. Ако означимо средине дискриминационих скорова прве популације са $\mu_{1\gamma}$, а друге са $\mu_{2\gamma}$, тада Fisher у ствари сугерише да се изаберу коефицијенти линеарне комбинације тако да се максимизира растојање између $\mu_{1\gamma}$ и $\mu_{2\gamma}$ изражено у јединицама стандардне девијације дискриминационих скорова.

Означимо са $\mu_k = E(X|G_k), k = 1,2$, очекивану вредност случајног вектора *X* ако потиче из k-те популације. Предпоставимо да је коваријациона матрица $\Sigma$ иста у обе групе. Тада очекивана вредност линеарне комбинације *Y=a'X*, је $\mu_{1\gamma} = E(X|G_1) = a'\mu_1$, односно $\mu_{2\gamma} = E(X|G_2) = a'\mu_2$, већ према томе да ли се дискриминациони скорови односе на прву или другу групу. Варијанса дискриминационих скорова је $\sigma_\gamma^2 = Var(a'X) = a'\Sigma a$, без обзира о којој је групи реч. Fisher је пошао од количника :

$$\frac{(\mu_{1\gamma} - \mu_{2\gamma})^2}{\sigma_\gamma^2} = \frac{(a'\mu_1 - a'\mu_2)^2}{a'\Sigma a} = \frac{(a'\sigma)^2}{a'\Sigma a}$$ где је $\sigma = \mu_1 - \mu_2$.

Задатак је да се одреди вектор коефицијената линеарне комбинације *a* тако да се максимизира количник $\frac{(a'\sigma)^2}{a'\Sigma a}$. Овај количник назива се *Fisher*-ов дискриминациони критеријум. Показано је (*Wichern* и *Johnson*, 1982) да се максимална вредност *Fisher*-овог дискриминационог критеријума постиже следећим избором коефицијената линеарне комбинације $a = c\Sigma^{-1}(\mu_1 - \mu_2)$, за ма које $c \neq 0$. Ако је $c = 1$ на основу вектора *a* добијамо линеарну комбинацију $Y = a'X = (\mu_1 - \mu_2)'\Sigma^{-1}X$ коју називамо *Fisher*-ова линеарна дискриминациона функција. За овај избор коефицијената линеарне комбинације максимална вредност *Fisher*-овог дискриминационог критеријума је :

$$\max_a \frac{(a'\sigma)^2}{a'\Sigma a} = \sigma'\Sigma^{-1}\sigma = (\mu_1 - \mu_2)'\Sigma^{-1}(\mu_1 - \mu_2)$$

Коефицијенти линеарне кмбинације нису једнозначно одређени јер за ма које $c \neq 0$ било који вектор *ca* максимизираће вредност *Fisher*-овог дискриминациног критеријума. Стога је уобичајно да се проблем оптимизације решава уз ограничење $a'\Sigma a = 1$. Тиме се елиминише утицај јединице мере променљивих на добијене резултате и омогућава њихова лакша интерпретација.

*Fisher*-ову линеарну дискриминациону функцију користимо и за алокацију опсервација у једну од две група. Нека је средишња тачка између средина дискриминационих скорова из прве и друге групе означена са $\mu_\gamma$, где је

$$\mu_\gamma = \frac{1}{2}\left(\mu_{1\gamma} + \mu_{2\gamma}\right) = \frac{1}{2}\left(a'\mu_1 + a'\mu_2\right) = \frac{1}{2}\left(\mu_1 + \mu_2\right)'\Sigma^{-1}\left(\mu_1 + \mu_2\right)$$

и нека за нову опсервацију $x_0$ имамо дискриминациони скор $y_0 = \left(\mu_1 - \mu_2\right)'\Sigma^{-1}x_0$. Може се показати да је

$$E\left(Y_0 \middle| G_1\right) - \mu_\gamma \geq 0 \text{ и } E\left(Y_0 \middle| G_2\right) - \mu_\gamma < 0$$

То значи да је правило класификације нове опсервације:

- Алоцирај $x_0$ у $G_1$ ако је $y_0 = \left(\mu_1 - \mu_2\right)'\Sigma^{-1}x_0 \geq \mu_\gamma$
- Алоцирај $x_0$ у $G_2$ ако је $y_0 = \left(\mu_1 - \mu_2\right)'\Sigma^{-1}x_0 < \mu_\gamma$

Поступак одређивања дискриминационих функција у случају више група започиње одређивањем прве дискриминационе функције тако што се максимизира релативан однос варијација између и унутар група. Затим се одређује друга дискриминациона функција тако да се максимизира однос преосталог дела варијација између и унутар група (преостао након издвајања прве дискриминационе функције) уз додатан услов да дискриминациони скорови одређени на основу прве и друге функције буду некорелисани. Свака наредна дискриминациона функција одређена је уз услов максимизирања односа преосталих варијација између и унутар група (након издвајања предходних дискриминационих функција), уз ограничење да су њени дискриминациони скорови некорелисани са дискриминационим скоровима свих предходно одређених дискриминационих функција, као и напомену да *Y* осе у дискриминационом простору не морају бити међусобно ортогоналне.

Други циљ дискриминационе анализе јесте класификовање или алокација опсервација непознатог порекла у једну од група, односно популација. Већ је показано да *Fisher*-ова линеарна дискриминациона функција може послужити и за алокацију опсервација. Сада желимо да изложимо општи теоријски оквир класификације опсервација.

Наведимо ситуацију у којој дискриминациона анализа може бити од помоћи у доношењу одлуке о алокацији опсервација. Банка је суочена са проблемом да неки од клијената нису у стању да врате кредит на време. Зато је интерес банке да дефинише објективан критеријум на основу кога ће проценити захтев за новим зајмом, да ли ће подносилац захтева бити у стању да врати кредит на време или не. За клијенте који су до тада подносили захтеве постоје подаци о укупном породичном приходу, величини породице, вредности непокретне имовине, старости главе породице и др. као и податак да ли су раније узети

кредити варћени на време или не. На основу ових података одређује се критеријум, помоћу кога ће се сви будући тражиоци сврстати у групу кредитно поузданих, или групу којима је ризично дати кердит. При том алоцирању новог захтева за кредитом банка може погрешити тако што ће кредитно поузданог тражиоца сврстати у групу оних којима не би требало одобрити кредит и обратно, одобрити кредит тражиоцу који неће бити у стању да врати кредит.У оба случаја, погрешна алокација захтева за кредитом, повалчи по банку одређене трошкове, у виду неоствареног прихода у првом случају, односно директиних губитака у другом. Тежња банке је да се број погрешно класификованих захтева по оба основа смањи на најмању могућу меру јер ће тиме минимизирати свој губитак. Према досадашњем искуству у банци је уочено да је број захтева поузданих клијената већи од броја захтева клијената којима је ризично одобрити кредит. [Ђорђевић. М.., 2011.]

Наведени пример илуструје које све елементе анализи проблема алокације треба имати у виду, односно кроз које све етапе у анализи пролазимо да бисмо донели исправну одлуку. У примеру се разликују две међусобно јасно раздвојене групе: кредитно поуздани клијенти ($G_1$) и они којима је ризично дати кредит ($G_2$ ). Означимо са *X* случајан вектор са p променљивих које су мерене код сваког клијента, а са $f_1(x)$ и $f_2(x)$ функције густине вероватноће од *X*, за прву и другу групу респективно. Наш задатак је да простор узорка, односно све могуће реализације случајног вектора *X* поделимо у две обласит $R_1$ и $R_2$ тако да, ако нова опсервација $x_0$ припада области $R_1$, тада одговарајућег клијента алоцирамо у групу $G_1$, а ако припада области $R_2$, тада клијента алоцирамо у групу $G_2$. Очигледно је да клијент може бити класификован само у једну од група па кажемо да су области $R_1$ и $R_2$ међусобно искључиве, а њихова унија прекрива цео простор узорка. Означимо са $p_1$ и $p_2$ априорне вероватноће да случајно изабрани клијент потиче из популације $G_1$ и $G_2$ респективно. Уз нови кредитни захтев који је поднео потенцијални клијент располажемо опсервацијом $x_0$, односно вредностима p променљивих на основу којих доносимо одлуку да ли клијента треба класификовати у област $R_1$ или област $R_2$.

Из теоријске статистике познато је да се тестирање хипотеза може посматрати у оквиру статистичке теорије одлучивања. Неодбацивање или одбацивање нулте хипотезе може бити коректна одлука, али су у процесу одлучивања могуће и грешке, тзв. грешке прве и друге врсте. Вероватноће тих грешака су условне, јер донета одлука је условљена истинитошћу нулте хипотезе. На сличан начин приступамо проблему алокације. Значи да у поступку класификације клијената можемо донети исправну или погрешну одлуку. Клијента исправно класификујемо ако га сврстамо или у групу $G_1$ или у групу $G_2$

, а он заиста потиче из те групе. У друга два случаја кажемо да смо клијента погрешно класификовали.

Први случај, клијент је потекао из групе $G_1$ а ми смо га погрешно сврстали у групу $G_2$. Ову условну вероватноћу означимо са $p(2|1)$

$$p(2|1) = p(X \in R_2 | G_1) = \int_{R_2} f_1(x)dx$$

Други случај, клијент је потекао из групе $G_2$, а ми смо га погрешно сврстали у групу $G_1$. Ову условну вероватноћу означавамо са $p(1|2)$

$$p(1|2) = p(X \in R_1 | G_2) = \int_{R_1} f_2(x)dx$$

Сада можемо одредити вероватноћу да клијент потиче из *j*-те групе и да смо га алоцирали у *i*-ту популацију

$$p(X \in R_i, G_j) = p(X \in R_i, G_j)p(G_j) = p(i|j)p_j \quad i, j = 1,2.$$

Уведимо последњи елемент у анализу, трошкове погрешне алокације. Ако смо исправно класификовали клијента ови трошкови су једнаки нули, а у супротном су у висини $c(i|j)$ када смо клијента из групе $G_j$ погрешно алоцирали у групу $G_i$ при чему је $i \neq j$. Узимајући у обзир могуће исходе класификације клијената, формирамо наредну табелу на којој су приказане све одлуке у погледу класификације клијената, одговарајуће вероватноће и трошкови погрешне класификације.

Табела 5.2. Све одлуке класификације клијента

| | | **Порекло клијента** | |
|---|---|---|---|
| | | **$G_1$** | **$G_2$** |
| **Одлука** | **Класификуј у $G_1$** | **исправна класификација** $p(1\|1)p_1 \;\; c(1\|1) = 0$ | **погрешна класификација** $p(1\|2)p_2 \;\; c(1\|2)$ |
| | **Класификуј у $G_2$** | **погрешна класификација** $p(2\|1)p_1 \;\; c(2\|1)$ | **исправна класификација** $p(2\|2)p_2 \;\; c(2\|2) = 0$ |

Укупна вероватноћа погрешне класификације, у ознаци *E*, једнака је збиру вероватноћа погрешне класификације из предходне табеле.

$$E = p(2|1)p_1 + p(1|2)p_2$$

Ова вероватноћа назива се стопа грешке. Сада се проблем алокације формулише на следећи начин :

- извршити такву поделу простора узорка на области $R_1$ и $R_2$ тако да се минимизира стопа грешке $E$ или еквивалентно да се максимизира вероватноћа исправне алокације

$$1-E = p(1|1)p_1 + p(2|2)p_2$$

- Ако у анализу алокације укључимо и трошкове, тада је очекивани трошак погрешне класификације, у ознаци $C$

$$C = c(2|1)p(2|1)p_1 + c(1|2)p(1|2)p_2,$$

а проблем алокације формулишемо на следећи начин :

- извршити такву поделу простора узорка на обласит $R_1$ и $R_2$ да се минимизира трошак погрешне класификације.

Предпоставимо да нам је вишедимензиона функција густине вероватноће две групе позната, а такође и априорне вероватноће $p_1$ и $p_2$. Задатак је одредити области $R_1$ и $R_2$ тако да се

$$C = c(2|1)p_1 \int_{R_2} f_1(x)dx + c(1|2)p_2 \int_{R_1} f_2(x)dx$$

минимизира. Узимајући у обзир да је простор узорка једнак унији области $R_1$ и $R_2$ то је

$$\int_{R_1} f_1(x)dx + \int_{R_2} f_2(x)dx = 1.$$

Сада је очекивани трошак погрешне алокације :

$$C = c(2|1)p_1\left[1 - \int_{R_1} f_1(x)dx\right] + c(1|2)p_2 \int_{R_1} f_2(x)dx,$$

односно :

$$C = \int_{R_1}\left[c(1|2)p_2 f_2(x) - c(2|1)p_1 f_1(x)\right]dx + c(2|1)p_1$$

По дефиницији су априорне вероватноће $p_1$ и $p_2$ ненегативни бројеви као и трошкови погрешне алокације. Функције густине вероватноћа су ненегативне функције које зависе од *X*. То значи да се минимум очекиваних трошкова

погрешне алокације постиже за оне вредности $X$ које припадају обалсти $R_1$ и за које је подинтегрална функција мања или једнака нули.

$$\left[c(1|2)p_2 f_2(x) - c(2|1)p_1 f_1(x)\right] \le 0$$

Одавде следи да област $R_1$ садржи оне тачке $X$ за које важи неједнакост

$$\frac{f_1(x)}{f_2(x)} \ge \left[\frac{c(1|2)}{c(2|1)}\right]\left[\frac{p_2}{p_1}\right]$$

а област $R_2$ садржи оне тачке $X$ за које важи неједнакост

$$\frac{f_1(x)}{f_2(x)} < \left[\frac{c(1|2)}{c(2|1)}\right]\left[\frac{p_2}{p_1}\right]$$

Области $R_1$ и $R_2$ дефинисане горњим неједнакостима минимизирају очекиване трошкове погрешне класификације. Када су трошкови погрешне алокације међусобно једнаки, тада су области дате следећим неједнакостима :

$$R_1 : \frac{f_1(x)}{f_2(x)} \ge \left[\frac{p_2}{p_1}\right]; \qquad R_2 : \frac{f_1(x)}{f_2(x)} < \left[\frac{p_2}{p_1}\right].$$

До истог резултата долазимо и минимизирањем стопе грешке $E$, односно максимизрањем вероватноће исправне алокације. Ако су априорне вероватноће једнаке међусобом, тада су области дефинисане неједнакостима :

$$R_1 : \frac{f_1(x)}{f_2(x)} \ge 1; \quad R_2 : \frac{f_1(x)}{f_2(x)} < 1.$$

Последњи случај дефиниције области се најчешће јавља у практичној примени. За нову опсервацију $x_0$ рачуна се вредност функције густине вероватноће, те ако је $f_1(x_0) \ge f_2(x_0)$, тада се $x_0$ алоцира у $G_j$, а ако је $f_1(x_0) < f_2(x_0)$, тада се $x_0$ алоцира у $G_2$. Ово правило алокације назива се правило највеће веродостојности.

### *5.5.1. [0, 1] вредносна логика као природно уопштење логичког закључивања*

*Syntactic Structured and Semantic Convex fuzzy* логика ($S^3C$) је конзистентна и непарадоксална логика. Насупрот другој fuzzy логици, $S^3C$ fuzzy логика има исте таутологије ($and/or$ контрадикције) попут *Bool*-ове логике. Операције над fuzzy скуповима су заправо fuzzy логичке операције над њиховим функцијама, тако да операције над fuzzy скуповима, који се базирају на $S^3C$ логици, имају исте особине као и операције над класичним скуповима – све основне операције

над "крутим" скуповима (на пример закон контрадикције и закон искључења трећег, идемпотенција итд.). [Radojević D., 2005;Radojevic: D.,2007.]

*5.5.1.1 Синтаксни ниво (старо)*

Елементарни искази $p_{i,}\ i=1,\ldots,n$, скуп елементарних исказа $\Omega=\{p_1,\ldots,p_n\}$ логички везници $\{\rightarrow,\wedge,\vee,\equiv,\neg\}$ и константе $\overline{0},\overline{1}$ су дефинисани као и у осталим fuzzy логикама. Правила за образовање **добро направљених формула** (well formed formulas **wffs**) су иста као и у другим *fuzzy* логикама:

Променљиве и константе су **wffs.**

Ако су $\varphi$ и $\psi$ **wffs** онда су $(\rho\rightarrow\psi),(\rho\wedge\psi),(\rho\vee\psi),(\rho\equiv\psi),\ \neg\rho$ такође **wffs.**

Не постоје друге **wffs.**

*5.5.1.2. Синтаксни ниво (ново)*

Уместо принципа истинитосне функционалности (камен спотицања у другим *fuzzy* логикама, дефинисан на семантичком нивоу) уводи се принцип структурне функционалности, дефинисан на синтаксном нивоу. Структура wffs је заснована на основним променљивама и Bool-овим функцијама. Структура основних променљивих (атомске функције) се дефинише на следећи начин:

Дефиниција – Структурна функција $\mu$ логичког атома $p\in\Omega$ (основне логичке тврдње, слова) је следећа скуповна функција:

$$\mu(p)(A)=\begin{cases}1\ p\in A\\ \qquad\quad ;\ A\in P(\Omega)\\ 0\ p\notin A\end{cases}$$

За случај скупа $\Omega=\{p_1,p_2\}$ вредности логичке структуре $p_i\ i=1,2$ су дате у следећој табели:

Табела 5.3. Вредности логичке структуре

| $A$ | $\mu(p_1)(A)$ | $\mu(p_2)(A)$ |
|---|---|---|
| $\varnothing$ | 0 | 0 |
| $\{p_1\}$ | 1 | 0 |
| $\{p_2\}$ | 0 | 1 |
| $\{p_1,p_2\}$ | 1 | 1 |

Структура логичког атома не зависи од његове истинитносне вредности.

Принцип структурне функционалности подразумева да вредност структурних функција (логичке структуре) делова логичке формуле јединствено одређује вредности структурне функције (логичка структура) саме формуле. То се постиже дефинисањем стуктурних функција везника (формално еквивалентним са истинитосним функцијама класичне логике) на следећи начин:

Табела 5.4. Структурне функције везника

| | **(-)** |
|---|---|
| 1 | 0 |
| 0 | 1 |
| | |

| $\Rightarrow$ | **0** | **1** |
|---|---|---|
| **0** | 1 | 1 |
| **1** | 0 | 1 |

| $\cap$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 0 |
| **1** | 0 | 1 |

| $\cup$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 1 |

| $\Leftrightarrow$ | **0** | **1** |
|---|---|---|
| **0** | 1 | 0 |
| **1** | 0 | 1 |

где је $\Rightarrow$ структурна функција од $\rightarrow$, $\cap$ од $\wedge$, $\cup$ од $\vee$, $\Leftrightarrow$ од $\equiv$ и $(-)$ од $\neg$.

Користећи принцип структурне функционалности, свака структурна функција $\mu$ се на јединствен начин проширује до структурне дефиниције свих формула на следећи начин:

$$\mu(\neg\rho)(A) = (-)\mu(\rho)(A)$$
$$\mu(\rho \rightarrow \psi)(A) = (\mu(\rho)(A) \Rightarrow \mu(\psi)(A))$$
$$\mu(\rho \rightarrow \psi)(A) = (\mu(\rho)(A) \cap \mu(\psi)(A))$$
$$\mu(\rho \rightarrow \psi)(A) = (\mu(\rho)(A) \cap \mu(\psi)(A))$$
$$\mu(\rho \rightarrow \psi)(A) = (\mu(\rho)(A) \Leftrightarrow \mu(\psi)(A))$$

где је $A \in \mathrm{P}(\Omega)$.

За случај скупа $\Omega = \{p_1, p_2\}$ логичке структуре логичких формула $\{\neg p_1, \neg p_2, p_1 \vee p_2, p_1 \wedge p_2, p_1 \Rightarrow p_2, p_1 \Leftrightarrow p_2\}$ дате су следећим табелама:

Табела 5.5. Логичке структуре логичких формула

| $A$ | $\mu(p_1)(A)$ | $\mu(p_2)(A)$ |
|---|---|---|
| $\varnothing$ | 1 | 1 |
| $\{p_1\}$ | 0 | 1 |
| $\{p_2\}$ | 1 | 0 |
| $\{p_1, p_2\}$ | 0 | 0 |

| $A$ | $\mu(p_1)(A)$ | $\mu(p_2)(A)$ |
|---|---|---|
| $\varnothing$ | 0 | 0 |
| $\{p_1\}$ | 0 | 1 |
| $\{p_2\}$ | 0 | 1 |
| $\{p_1, p_2\}$ | 1 | 1 |

| $A$ | $\mu(p_1)(A)$ | $\mu(p_2)(A)$ |
|---|---|---|
| $\varnothing$ | 1 | 1 |
| $\{p_1\}$ | 0 | 0 |
| $\{p_2\}$ | 1 | 0 |
| $\{p_1, p_2\}$ | 1 | 1 |

**Последица** - Структура логичке формуле је независна од истинитосне вредности својих логичких варијабли – атома.

**Последица** - Број компоненти структурне функције у случају $|\Omega| = n$ износи $2^n$.

**Дефиниција** – Структурни вектор $\vec{\mu}(\rho)$ логичке формуле $\rho$, има компоненте које су једнаке вредностима структурне функције те логичке формуле у датом редоследу (лексикографском или измењеном лексикографском на пример). Структурни вектор логичке формуле одговара колони те формуле у класичној *Bool*-овој табели истинитости. Врло важна особина структурних вектора, која следи из горе наведене дефиниције, дата је следећим тврђењем:

**Последица** - Свака $n$-арна логичка формула $\rho$ чија функција ($[0,1]$-вредносна, вишевредносна и/или $\{0,1\}$-вредносна) $\rho : \{0,1\}^n \to \{0,1\}$ врши

пресликавање на исти начин има исту структурну функцију, а самим тим и исти структурни вектор.

**Дефиниција** – $\vec{\mu}(n)$ је скуп структурних вектора свих $n$-арних логичких формула $\rho(n)$:

$$\vec{\mu}(n) = \{\vec{\mu}(\rho_i) \mid \rho_i \in \rho(n)\}; n\epsilon N_0.$$

Димензија структурног вектора $n$-арне логичке функције износи $2^n$ , а број $n$-арних $0-1$ структурних вектора је $2^n$. *Bool*-ова алгебра $B_\mu$ на скупу $\vec{\mu}(n)$свих $0-1$ структурних вектора $n$-арне логичке формуле је дефинисана као уређена четворка: $B_\mu = (\vec{\mu}(n), \vee, \wedge, \vdash)$, где су $\wedge, \vee$ бинарни оператори а $\neg$ унарни оператор на $\vec{\mu}(n)$ за које важе следеће особине:

Табела 5.6. Особине оператора

| | |
|---|---|
| $(B_1)$ | $\vec{\mu}(\rho) \vee \vec{\mu}(\rho) = \vec{\mu}(\rho)$ |
| | $\vec{\mu}(\rho) \wedge \vec{\mu}(\rho) = \vec{\mu}(\rho)$ |
| $(B_2)$ | $\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_2) = \vec{\mu}(\rho_2) \vee \vec{\mu}(\rho_1)$ |
| | $\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2) = \vec{\mu}(\rho_2) \wedge \vec{\mu}(\rho_1)$ |
| $(B_3)$ | $(\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2)) \vee \vec{\mu}(\rho_3) = \vec{\mu}(\rho_2) \vee (\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_3))$ |
| | $(\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2)) \wedge \vec{\mu}(\rho_3) = \vec{\mu}(\rho_2) \wedge (\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_3))$ |
| $(B_4)$ | $\vec{\mu}(\rho_1) \vee (\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2)) = \vec{\mu}(\rho_1)$ |
| | $\vec{\mu}(\rho_1) \wedge (\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_2)) = \vec{\mu}(\rho_1)$ |
| $(B_5)$ | $\vec{\mu}(\rho_1) \wedge (\vec{\mu}(\rho_2) \vee \vec{\mu}(\rho_3)) = (\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2)) \vee (\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_3))$ |
| | $\vec{\mu}(\rho_1) \vee (\vec{\mu}(\rho_2) \wedge \vec{\mu}(\rho_3)) = (\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_2)) \wedge (\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_3))$ |
| $(B_6)$ | $\vec{\mu}(\rho) \vee \vec{\mu}(0) = \vec{\mu}(\rho)$ |
| | $\vec{\mu}(\rho) \vee \vec{\mu}(1) = \vec{\mu}(1)$ |
| | $\vec{\mu}(\rho) \wedge \vec{\mu}(1) = \vec{\mu}(\rho)$ |
| | $\vec{\mu}(\rho) \wedge \vec{\mu}(0) = \vec{\mu}(0)$ |
| $(B_7)$ | $\vec{\mu}(\rho) \vee \vec{\mu}(\vdash\rho) = \vec{\mu}(1)$ |
| | $\vec{\mu}(\rho) \wedge \vec{\mu}(\vdash\rho) = \vec{\mu}(0)$ |
| $(B_8)$ | $\vec{\mu}(\vdash 1) = \vec{\mu}(0)$ |
| | $\vec{\mu}(\vdash(\vdash\rho)) = \vec{\mu}(\rho)$ |
| $(B_9)$ | $\vdash(\vec{\mu}(\rho_1) \vee \vec{\mu}(\rho_2)) = \vec{\mu}(\vdash\rho_1) \wedge \vec{\mu}(\vdash\rho_2)$ |
| | $\vdash(\vec{\mu}(\rho_1) \wedge \vec{\mu}(\rho_2)) = \vec{\mu}(\vdash\rho_1) \vee \vec{\mu}(\vdash\rho_2)$ |

$(B_1)$ Идемпотентност, $(B_2)$ комутативност, $(B_3)$ асоцијативност, $(B_4)$ апсорпција, $(B_5)$ дистрибутивност, $(B_6)$ универзалне границе, $(B_7)$ комплементарност, $(B_8)$ иволутивност и $(B_9)$ дуализација.

**Последица** - Све особине $(B_1)$-$(B_9)$ важе за $0-1$ структурне функције као компоненте структурних вектора.

Особине $(B_1)$-$(B_4)$ важе у свим решеткама. Због тога су *Bool*-ове алгебре решетке које су дистрибутивне $(B_5)$, ограничене $(B_6)$ и комплементарна $(B_7)$-$(B_9)$.

Поред формалне сличности између истинитосних функција и/или принципа истинитосне функционалности у класичној исказној логици и структурне функције и/или принципа структурне функционалности принципа у теорији $S^3C$ предикатске логике, постоје велике квалитативне разлике. Заправо, структурна функција и/или принцип структурне функционалности представљају основне особине, и не зависе од семантичке реализације логичке формуле ($[0,1]$-вредносна, вишевредносна и/или $\{0,1\}$-вредносна имплементација).

Структуре логичких закона, искључења трећег (структура логичке константе

$$\vec{\mu}(\rho) \vee \vec{\mu}(\neg\rho) = \vec{\mu}(\bar{1})$$

и контрадикције (структура логичке костанте

$$\vec{\mu}(\rho) \wedge \vec{\mu}(\neg\rho) = \vec{\mu}(\bar{0})$$

су независне од логичке формуле $\rho$ и њене семантичке реализације.

*5.5.1.3. Семантички ниво (ново)*

Логичка функција $e$ $n$-арне логичке формуле $\mu$ (валидација логичке формуле) је линеарна конвексна комбинација компонената њихове логичке структуре $(\mu(\rho)(A),\quad A\in \mathrm{P}(\Omega))$:

$$e_{\otimes}(\rho)(p_1,\ldots,p_n)=\sum_{A\in \mathrm{P}(\Omega)} \mu(\rho)(A)\phi_{\otimes}(A)(p_1,\ldots,p_n)$$

где су: $\phi_{\otimes}(A)(p_1,\ldots,p_n),\quad A\in \mathrm{P}(\Omega)$; базичне логичке функције.

Базичне логичке функције $\phi_{\otimes}(A):[0,1]^{|\Omega|}\to[0,1]$ имају следећу особину:

$$\sum_{A\in \mathrm{P}(\Omega)} \phi_{\otimes}(A)(p_1,\ldots,p_n)=1$$

и

$$\phi_{\otimes}(A)(p_1,\ldots,p_n)\geq 0$$

за $p_i \in [0,1], \quad i = 1,\ldots,n; \quad A \in \mathrm{P}(\Omega).$

**Дефиниција** – Базичне логичке функције се дефинишу на следећи начин:

$$\phi_{\otimes}(A)(p_1,\ldots,p_n) = \sum_{B \in \mathrm{P}(\Omega \setminus A)} (-1)^{|B|} \bigotimes_{p_i \in A \cup B} p_i$$

где је $\otimes$ оператор уопштеног производа ($t$-норма $S^3C$ логике).

Када је $\Omega = \{p_1, p_2\}$ базичне логичке функције су:

Табела 5.7. Базичне логичке функције

| $A$ | $\phi(A)(p_1, p_2)$ |
|---|---|
| $\varnothing$ | $1 - p_1 - p_2 + p_1 \otimes p_2$ |
| $\{p_1\}$ | $p_1 - p_1 \otimes p_2$ |
| $\{p_2\}$ | $p_2 - p_1 \otimes p_2$ |
| $\{p_1, p_2\}$ | $p_1 \otimes p_2$ |

**Дефиниција** – Уопштени $n$-производ, или $S^3C$ логичка $n$ триангуларна норма ($S^3C$ логичка $n$ $t$-норма) је бинарна операција на јединичном интервалу $[0,1]$, тј. функција $\otimes_{(n)} : [0,1]^2 \to [0,1]$ таква да за свако $p_1,\ldots,p_n \in [0,1]$ важи следећих пет аксиома:

$(T1)$ $\otimes_{(n)}(p_1, p_2) = \otimes_{(n)}(p_2, p_1)$ комутативност,

$(T2)$ $\otimes_{(n)}(p_1, \otimes_n(p_2, p_3)) = \otimes_{(n)}(\otimes_{(n)}(p_1, p_2), p_3)$ асоцијативност,

$(T3)$ $\otimes_{(n)}(p_1, p_2) \le \otimes_{(n)}(p_1, p_3) \quad p_2 \le p_3$ монотоност,

$(T4)$ $\otimes_{(n)}(p_1, 1) = p_1$ гранични услов,

$(T5)$ $\sum_{B \in \mathrm{P}(\Omega \setminus A)} (-1)^{|B|} \bigotimes_{p_i \in A \cup B} p_i \ge 0, \quad \forall A \in \mathrm{P}(\Omega)$ ненегативност

где је $\mathrm{P}(\Omega)$ партитивни скуп скупа $\Omega = \{p_1,\ldots,p_n\} \in [0,1]^n$.

**Последица** - На основу новог аксиома (T5), следи да је скуп могућих $n$-тригуларних норми $S^3C$ логике подскуп скупа познатих $t$-норми. *Frank*–ове $t$-норме задовољавају услов ненегативности за $n = 2$ и представљају пример 2 тригуларне норме $S^3C$ логике.

*5.5.1.4. Операције на Fuzzy скуповима*

$A$ – коначан скуп елементарних *fuzzy* скупова (*fuzzy* атома) тј. $A=\{A_1, A_2, \ldots, A_n\}$.

*P(A)* – Партитивни скуп скупа $A$ представља скуп свих подскупова елементарног *fuzzy* скупа укључујући и празан скуп $\varnothing$.

Нека је $A=\{A_1, A_2\}$; $P(A)=\{\varnothing, A_1, A_2, \{A_1, A_2\}\}$.

Логичка структура елементарног *fuzzy* скупа је скуповна функција припадности $\mu_A : P(A) \to \{0,1\}$ дефинисана следећим изразом:

$$\mu_A(S)=\begin{cases}1 & A\in S\\ & ;\ S\in P(A)\\ 0 & A\notin S\end{cases}$$

Логичка структура сложене скуповне формуле добија се на основу принципа структурне функционалности.

**Последица** - Структура сложене скуповне формуле је независна од вредности функција припадности својих елементарним *fuzzy* скупова – атома.

Функција припадности *fuzzy* скупа $A$ је уопштење карактеристичне функције класичних тврдих скупова, означава се са $A(x)$ где:

$$A: X \to [0,1],$$

Универзум $X$ је увек "*крут*" скуп и $x\in X$.

Функција припадности сложеног *fuzzy* скупа $F$ (састављеног од $A=\{A_1, A_2, \ldots, A_n\}$) у $x\in X$ је једнака линеарној конвексној комбинацији компоненти његове структуре $\mu_F(S);\ \ S\in P(A)$

$$F(x)=\sum_{S\in P(A)} \mu_F(S)\phi(S)\left(A_1(x),\cdots,A_n(x)\right)$$

где су $\phi(S)\left(A_1(x),\cdots,A_n(x)\right);\ \ S\in P(A)$ базичне логичке функције, дефинисане на следећи начин:

$$\phi_{\otimes}(S)\left(A_1(x),\ldots,A_n(x)\right)=\sum_{B\in P(A\setminus S)\,S\in P(A)} (-1)^{|B|} \bigotimes_{A_i\in S\cup B} A_i(x)$$

где је $\otimes$ оператор уопштеног производа ($t$-норма $S^3C$ логике), а $A_i(x)$ функција припадности *fuzzy* скупу $A_i$ у $x\in X$.

*5.5.1.5. Fuzzy комплемент*

Пошто је логичка структура *fuzzy* комплемента $F^c$ у функцији логичке структуре *fuzzy* скупа $F$

$$\mu_{F^c}(S)=1-\mu_F(S);\quad S\in P(A)$$

следи да је

$$F^c(x)=\sum_{S\in P(A)}\mu_{F^c}(S)\phi(S)\left(A_1(x),\ldots,A_n(x)\right)=1-F(x).$$

*5.5.1.6. Fuzzy пресек*

Функција припадности *fuzzy* пресека је:

$$(A\cap B)(x)=\sum_{S\in P(A)}\left(\mu_A(S)\wedge\mu_B(S)\right)\phi(S)\left(A(x),B(x)\right)$$

Закон контрадикције за *fuzzy* скупове:

$$\left(A\cap A^C\right)(x)=\sum_{S\in P(A)}\left(\mu_A(S)\wedge\mu_{A^c}(S)\right)\phi(S)\left(A(x)\right)=\sum_{S\in P(A)}\left(\mu_0(S)\right)\phi(S)\left(A(x)\right)\equiv 0$$

за сваку $t$-норму $S^3C$ логике.

*5.5.1.7. Fuzzy унија*

Функција припадности *fuzzy* уније је:

$$(A\cup B)(x)=\sum_{S\in P(A)}\left(\mu_A(S)\vee\mu_B(S)\right)\phi(S)\left(A(x),B(x)\right)$$

Закон искључења трећег за *fuzzy* скупове:

$$\left(A\cup A^C\right)(x)=\sum_{S\in P(A)}\left(\mu_A(S)\vee\mu_{A^c}(S)\right)\phi(S)\left(A(x)\right)=\sum_{S\in P(A)}\left(\mu_1(S)\right)\phi(S)\left(A(x)\right)\equiv 1$$

за сваку $t$-норму $S^3C$ логике.

*5.5.1.8. Комбинација операција*

Функција припадности било којег сложеног *fuzzy* скупа је:

$$SF(A_1,\ldots,A_n)(x)=\sum_{S\in P(A)}LF\left(\mu_{A_1},\ldots,\mu_{A_n}\right)(S)\phi(S)\left(\left(A_1(x),\ldots,A_n(x)\right)\right)$$

где су скуповне операције у $SF$ на *fuzzy* скуповима $A_i$ замењене одговарајућим логичким операцијама ($\cap$ са $\wedge$; $\cup$ са $\vee$; комплемент са негацијом) у $LF$ над функцијама припадности $\mu_{A_i}(S);\quad S\in P(A)$.

Очигледно је да је из операција над *fuzzy* скуповима које су засноване на $S^3C$ *fuzzy* логици (све таутологије класичне логике су сачуване) важе све основне особине операција над класичним скуповима:

Табела 5.8. Операције над класичним скуповима

| | |
|---|---|
| $(B_1)$ | $A\cup A=A;\quad A\cap A=A$ |
| $(B_2)$ | $A\cup B=B\cup A;\quad A\cap B=B\cap A$ |
| $(B_3)$ | $(A\cup B)\cup C=A\cup(B\cup C);\quad (A\cap B)\cap C=A\cap(B\cap C)$ |
| $(B_4)$ | $A\cup(A\cap B)=A;\quad A\cap(A\cup B)=A$ |
| $(B_5)$ | $A\cap(B\cup C)=(A\cap B)\cup(A\cap C);\quad A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ |
| $(B_6)$ | $A\cup X=X;\quad A\cap\varnothing=\varnothing$ |
| $(B_7)$ | $A\cap X=X;\quad A\cup\varnothing=A$ |
| $(B_8)$ | $A\cup A^c=X$ |
| $(B_9)$ | $A\cap A^c=\varnothing$ |
| $(B_{10})$ | $(A^c)^c=A$ |
| $(B_{11})$ | $(A\cup B)^c=A^c\cap B^c;\quad (A\cap B)^c=A^c\cup B^c$ |

$(B_1)$ Идемпотентност, $(B_2)$ комутативност, $(B_3)$ асоцијативност, $(B_4)$ апсорпција, $(B_5)$ дистрибутивност, $(B_6)$ апсорпција $X$ и $\varnothing$, $(B_7)$ идентитет, $(B_8)$ закон искључења трећег, $(B_9)$ закон контрадикције, $(B_{10})$ инволутивност, $(B_{11})$ *DeMorgan*-ови закони.

$S^3C$ логика примењена на операције *fuzzy* скупова задржава све основне особине операција над класичним скуповима за све могуће $t$-норме. Сходно томе нови приступ fuzzy скуповима је конзистентан и непарадоксалан.

*5.5.1.9. Спајање атрибута*

Проблеми сажимања многих релевантних облика (атрибута, симптома, карактеристика...) у једну вредност (степен важности, задовољење, сличност, подесност, компатибилност, оперативност, итд.) су врло често сукобљени у многим доменима *OR* оператора. Ови проблами су по својој природи логички проблеми и математичка логика би требала да буде главни алат за њихово

решавање. Класична {0, 1}-вредносна *Bool*-ова логика је погодна за решавање проблема који су *"црно-бели"* или дво-вредносних проблема. Међутим многи реални проблеми, са логичке тачке гледишта, су више-вредносни па чак и бесконачно-вредносни и/или [0, 1]-вредносни проблеми. Постоји јако велики број генерализација *Bool*-ове дво-вредносне логике у више-вредносну и/или у [0, 1]-вредносну логику. Такође, постоји и велики број разматрања ових генерализација. До сада, сви познати приступи били су само делимично комплементарни *Bool*-овој логици. [Radojević D., 2002;Radojević D.,2005.]

[0, 1] представља вредносну логику комплементарну *Bool*-овој {0, 1}-вредносној логици. Нова [0, 1]-вредносна логика је генерализација *Bool*-ове логике, тако да су све главне карактеристике сачуване, и штавише, представљен је нови поглед на класичну логику. [Radojević D., 2000.]

*N*-арна [0, 1]-вредносна логичка функција се састоји од два главна дела:

1. Структурно уређене функције логичке формуле и
2. Основних логичких функција.

Структурна функција *n*-арне псеудо-*Bool*-овске формуле (линеарна конвексна комбинација *n*-арне *Bool*-ове формуле) је псеудо-логичка структурна функција а одговарајући вектор је псеудо-струцтурни вектор. Псеудо-структурни вектор било које *n*-арне псеудо-логичке формуле може бити престављен као линеарно-конвексна комбинација струцтурних вектора *n*-арне логичке формуле.

Геометријски скуп свих логичких (0-1) структурних и псеудо-логички структурних вектора *n*-арне формуле је структурна хипер-коцка. У *n*-арном случају, структурна хипер-коцка има димензије $2^n$, тј. њен простор је дефинисан скупом $(0-1)^{2^n}$, помоћу $2^{2^n}$ врхова-логичких структурних вектора.

Базични вектори структурне хипер-коцке имају само једну компоненту различиту од нуле и једнаку један. Логичка функција чији је структурни верктор базични структурни вектор је базична логичка функција. Пошто се било који структурни и/или псеудоструктурни вектор може представити као линеарна комбинација одговарајућих базичних вектора- било која *n*-арна [0, 1]-вредносна логичка функција може бити представљена као линеарна комбинација одговарајућих *n*-арних базичних логичких функција.

Базична логичка функција зависи од вредности [0, 1]-вредносних атомских симбола као променљивих и изабраних континуално логичких оператора као параметара. За различите континуално логичке операторе постоје различите [0, 1]-вредносне логике. Два најзначајнија случаја континуално логичких оператора [0, 1]-вредносно логичке функције су: [Radojević D., 2000.]

1. *AND* оператор дефинисан као алгебарски производ и
2. *AND* оператор дефинисан стандардни пресек.

*N*-арна [0, 1]-вредносно логичка функција је линеарно конвексна комбинација компоненти њеног структурног (0-1 *OR* псеудо-логичког) вектора, а а базична логичка функција је тежински коефицијент одговарајућих компоненти структурног вектора.

Покушајмо да представимо структуру једне логичке формуле од три атрибута.

Почињемо креирањем функције припадности. Пођимо од следеће табеле:

Табела 5.9. Функције припадности

| | | **μ** |
|---|---|---|
| **1.** | 0 | $\mu(0) = \mu_0$ |
| **2.** | $\{a_1\}$ | $\mu(\{a_1\}) = \mu_1$ |
| **3.** | $\{a_2\}$ | $\mu(\{a_2\}) = \mu_2$ |
| **4.** | $\{a_3\}$ | $\mu(\{a_3\}) = \mu_3$ |
| **5.** | $\{a_1, a_2\}$ | $\mu(\{a_1, a_2\}) = \mu_{1,2}$ |
| **6.** | $\{a_1, a_3\}$ | $\mu(\{a_1, a_3\}) = \mu_{1,3}$ |
| **7.** | $\{a_2, a_3\}$ | $\mu(\{a_2, a_3\}) = \mu_{2,3}$ |
| **8.** | $\{a_1, a_2, a_3\}$ | $\mu(\{a_1, a_2, a_3\}) = \mu_{1,2,3}$ |

Из ове табеле можемо извести табелу атомских структурних вектора:

Табела 5.10. Атомски структурни вектори

| | $\boldsymbol{\mu_{a_1}}$ | $\boldsymbol{\mu_{a_2}}$ | $\boldsymbol{\mu_{a_3}}$ |
|---|---|---|---|
| $\boldsymbol{\mu_0}$ | 0 | 0 | 0 |
| $\boldsymbol{\mu_1}$ | 1 | 0 | 0 |
| $\boldsymbol{\mu_2}$ | 0 | 1 | 0 |
| $\boldsymbol{\mu_3}$ | 0 | 0 | 1 |
| $\boldsymbol{\mu_{1,2}}$ | 1 | 1 | 0 |
| $\boldsymbol{\mu_{1,3}}$ | 1 | 0 | 1 |
| $\boldsymbol{\mu_{2,3}}$ | 0 | 1 | 1 |
| $\boldsymbol{\mu_{1,2,3}}$ | 1 | 1 | 1 |

На основу ове табеле, без обзира каква логичка зависност важи међу атрибутима $a_1$, $a_2$, $a_3$ ми је можемо претворити у комбинацију структурне формуле и базичних логичких функција.

Покушајмо то да урадимо са неким *AND* оператором. Најједноставнији оператор који задовољава услов да буде *AND* оператор је свакако оператор пута (*).

Покушајмо да израчунамо структуру и базичне изразе за израз: $\boldsymbol{L = a_1 \wedge (a_2\, XOR\, a_3)}$

Табела 5.11. Структура и базични изрази

| | $\mu_{a_1}$ | $\mu_{a_2}$ | $\mu_{a_3}$ | $\mu_L$ | **базне функције** |
|---|---|---|---|---|---|
| $\mu_0$ | 0 | 0 | 0 | 0 | $(1-a_1)*(1-a_2)*(1-a_3)$ |
| $\mu_1$ | 1 | 0 | 0 | 0 | $a_1*(1-a_2)*(1-a_3)$ |
| $\mu_2$ | 0 | 1 | 0 | 0 | $(1-a_1)*a_2*(1-a_3)$ |
| $\mu_3$ | 0 | 0 | 1 | 0 | $(1-a_1)*(1-a_2)*a_3$ |
| $\mu_{1,2}$ | 1 | 1 | 0 | 1 | $a_1*a_2*(1-a_3)$ |
| $\mu_{1,3}$ | 1 | 0 | 1 | 1 | $a_1*(1-a_2)*a_3$ |
| $\mu_{2,3}$ | 0 | 1 | 1 | 0 | $(1-a_1)*a_2*a_3$ |
| $\mu_{1,2,3}$ | 1 | 1 | 1 | 0 | $a_1*a_2*a_3$ |

Уколико као оператор користимо поменуто пута (*), као крајњу формулу добијамо:

[$\mu_L$] x [вектор базних функција].

$$\mathbf{0}*(1-a_1)*(1-a_2)*(1-a_3)+\mathbf{0}*a_1*(1-a_2)*(1-a_3)+\mathbf{0}*(1-a_1)*a_2*(1-a_3)+\mathbf{0}*(1-a_1)*(1-a_2)*a_3+\mathbf{1}*a_1*a_2*(1-a_3)+\mathbf{1}*a_1*(1-a_2)*a_3+\mathbf{0}*(1-a_1)*a_2*a_3+\mathbf{0}*a_1*a_2*a_3 = a_1*a_2*(1-a_3)+a_1*(1-a_2)*a_3 = a_1a_2-a_1a_2a_3-a_1a_3-a_1a_2a_3 = a_1a_2-a_1a_3-2\,a_1a_2a_3$$

Оно што нас интересује јесте да ли овакав приступ обезбеђује основне таутологије, нпр. $a_1 \wedge (\backsim a_1) = 0$, проверимо коју ћемо струтуру добити за предложени израз:

Табела 5.12. Провера таутологије

| | $\mu_{a_1}$ | $\mu_{\backsim a_1}$ | $\mu_L$ | **базне функције** |
|---|---|---|---|---|
| $\mu_0$ | 0 | 1 | 0 | $(1-a_1)*(1-a_2)$ |
| $\mu_1$ | 1 | 0 | 0 | $a_1*(1-a_2)$ |
| $\mu_2$ | 0 | 1 | 0 | $(1-a_1)*a_2$ |
| $\mu_{1,2}$ | 1 | 0 | 0 | $a_1*a_2$ |

Табела нас доводи до закључка да је овим приступом обезбеђено да је ова таутологија увек тачна, јер је израз $a_1 \wedge (\backsim a_1)$ структурно једнак нули. [Radojević D., 2000.]

# 6. АПЛИКАТИВНИ МОДЕЛ

Овај програм је замишљен као презентациони софтвер. Програм је написан применом алата *The MathWorks MATLAB*® и омогућава решавање линеарних проблема помоћу класичне {0, 1}-вредносне логике и [0, 1]-вредносне логике. Помоћу овог програма могу се вршити и упоредне анализе добијених резултата ради њихове боље интерпретације.

Подаци се уносе у облику матрице, у којој врсте представљају вредности опсервација, а колоне - атрибуте. Треба унети и вектор припадности класи, који ће омогућити формирање модела. У програму постоји опција, која дозвољава да се учитају већ припремљени, раније коришћени подаци.

Следећи корак у даљој анализи је нормализација улазних података. Избором опције за нормализацију отвара се форма за нормализацију. Ова форма се састоји из падајуће листе са списком критеријума, графиком функције за нормализацију, и са два слајдера са стране. Уколико ништа од овога не дирамо извршиће се класична линеарна нормализација која вредности свих атрибута своди у границе затвореног интервала [0, 1], али такође можемо вршити различите врсте нормализације за сваки критеријум. Слајдерима се ова функција критеријума закривљује, а такође и црвени троуглићи се могу померати лево и десно, али фиксирани на *y=0* или *y=1*.

Програм омогућава да се на улазне податке (који су представљени као матрица чији су редови вредности опсервација, а колоне атрибути) након њихове нормализације примени проширење, и тако добије нови улаз над којим се примењује нека од линераних статистичких метода. Програм нема ограничење броја атрибута (урађен је за општи случај).

Проширењем се добија нова матрица која укључује нове атрибуте ($2^n$ n-почетни број атрибута) који представљју узајамне везе атрибута. Ове везе су добијене на следећи начин. Прво се израчунају атомски структурни вектори( $2^n$ ), затим се помоћу њих и базичних логичких функција добију изрази на основу којих се за сваку опсервацију проширује број атрибута на $2^n$ .

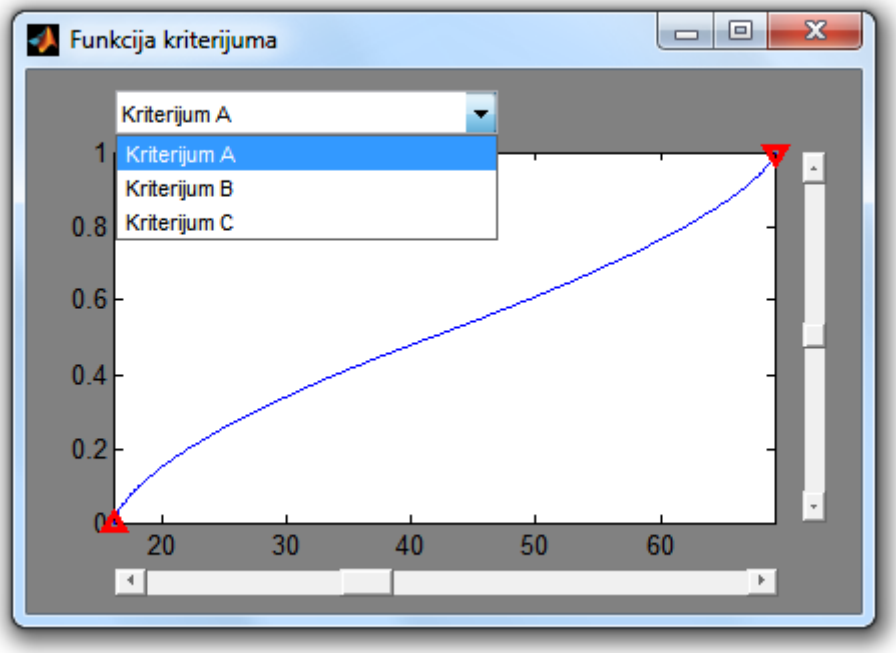
Програм користи and (&) оператор као базну логичку функцију који је имплементиран као производ (*) и као минимум (*min*). Овако добијени изрази помоћу атомских структурних вектора и логичке функције се примењују на вредности из сваке опсервације и тиме се добија нови улаз који садржи почетне вредности атрибута и вредност њихових зависности.

Следеће што можемо да урадимо је да на овако добијен улаз применимо неку статистичку методу (у овом случају дискриминациону анализу) и као резултат добијемо дискриминациону једначину и графички приказ резултата.

Једначина нам омогућава да нову опсервацију правилно класификујемо, а на графичком приказу се види полазна матрица и како су разврстани појединачни елементи ( помоћу боја се зна којој класи су припадали пре проширења, а помоћу вредности функције којој сада класи припадају). Као излаз приказујемо и број грешака, односно број колико елемената је у погрешној класи. Програм омогућава и да се примени дискриминациона анализа над почетним скупом, и тако добијемо излаз за класични приступ проблему.

***Нормализација***

Избором опције *Normalize* из подменија *Discriminant analysis* отвара се прозор за нормализацију као на слици:



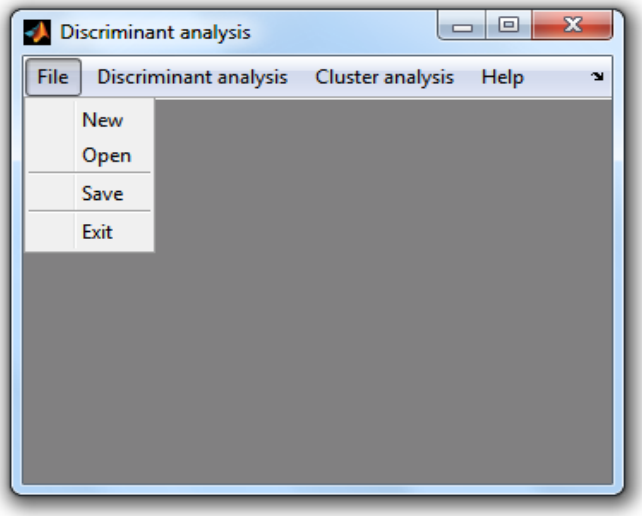

Слика 6.1. Прозор за нормализацију

Ова форма састоји се из падајуће листе са списком критеријума, графиком функције за нормализацију, и са два слајдера са стране.

Уколико ништа од овога не дирамо извршиће се класична нормализација, али такође можемо вршити различите врсте нормализације за сваки критеријум. Слајдерима се ова функција критеријума закривљује, а такође и црвени троуглићи се могу померати лево и десно, али фиксирани на *y=0* или *y=1*.

***File мени***

**Опције менија *File* су:**




Слика 6.2. *File* мени

New: Креира нову табелу, и омогућује унос података у њу...

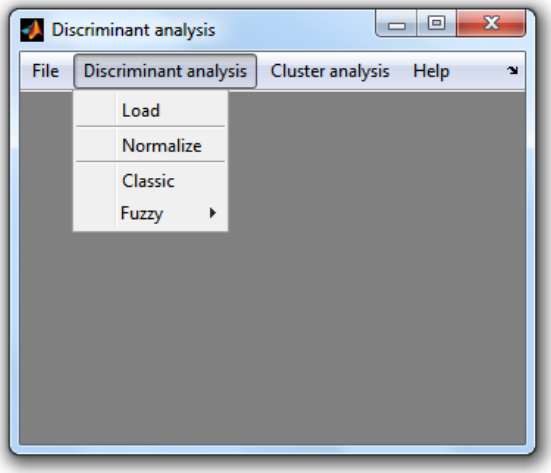
Open: Омогућује учитавање података у изабраној табели која већ постоји на хард диску...

Save: Меморише унете податке, под наведеним именом на изабраној локацији...

Exit: Излазак из програма. Затвара отворене прозоре и ослобађа заузету меморију...

***Discriminant analysis мени***

**Опције менија *Discriminant analysis* су:**




Слика 6.3. *Discriminant analysis* мени

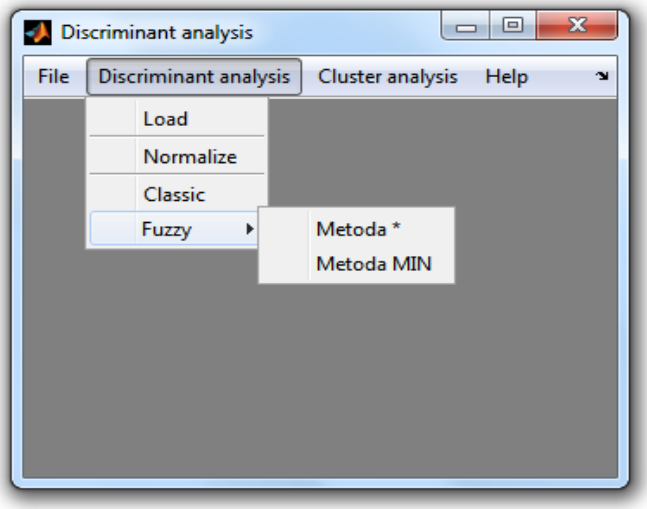
***Load***: Опцијом *Load* учитавамо унапред припремљене податке sa анализу.

***Normalize***: Избором опције *Normalize* из подменија *Discriminant analysis* отвара се прозор за нормализацију који је описан у пртходном поглављу 4.1.

***Classic***: Избором опције *Classic* из подменија *Discriminant analysis* спроводи се класична дискриминациона анализа над претходном учитаним подацима који су у следећем кораку нормирани.

***Fuzzy***

**Опције подменија *Fuzzy* су:**




Слика 6.4. Опције подменија *Fuzzy*

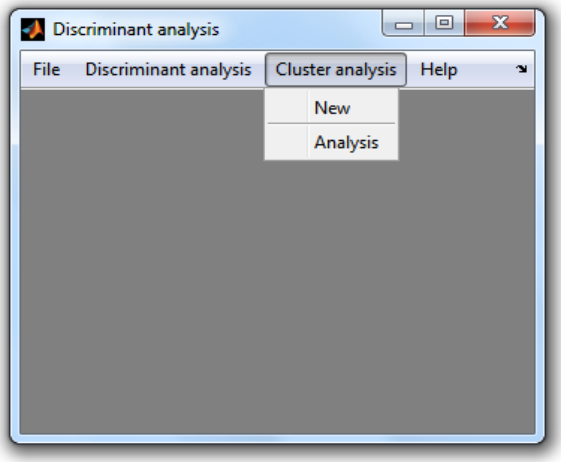
***Metoda ****: Овом опцијом се покреће програм који користи *AND* (&) оператор као базну логичку функцију који је имплементиран као производ (*).

***Metoda MIN***: Овом опцијом се покреће програм који користи *AND* (&) оператор као базну логичку функцију који је имплементиран као минимум *MIN* (*).

***Cluster analysis мени***

Овом анализом се утврђује којем кластеру припадају нове алтернативе, а на основу дискриминантне функције која је добијена дискриминантном анализом. Сами подаци за нове алтернативе морају бити из опсега у коме су и подаци на основу којих је одређена дискриминантна функција. Програм сам врши нормализацију на исти начин како су нормализовани подаци на основу којих је вршена дискриминантна анализа.

**Опције менија *Cluster analysis* су:**




Слика 6.5. Cluster analysis мени

***New***: За унос нових алтернатива потребно је из подменија *Cluster analysis* изабрати опцију *New*, након чега ће се отворити прозор у коме се уносе подаци за нове алтернативе.

***Analysis***: Избором опције *Analysis* из менија *Cluster analysis*, врши се одређивање припадности кластеру за претходно унете алтернативе. Програм сам врши нормализацију на исти начин како су нормализовани подаци на основу којих је вршена дискриминантна анализа. Након нормализације за нове алтернативе се израчуна вредност дискриминантне функције, и на основу те вредности одређује се припадност кластеру. Примењује се дискриминантна функција добијена по методи која је задња примењена.

# 7. СТУДИЈА ПРИМЕРА

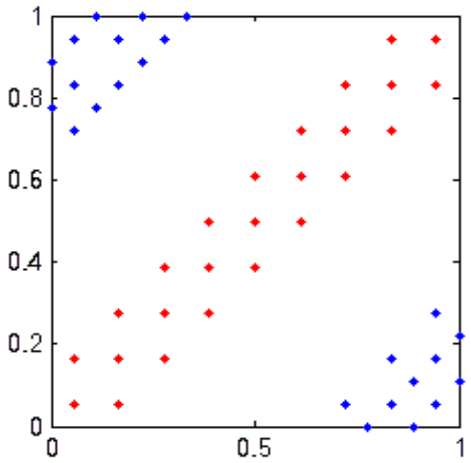
Експериментални део докторске дисертације представља процес методолошке имплементације теоријске основе дигиталних сертификата, у оквиру кога је извршено тестирање, мерење релеватних параметра и анализа добијених резултата.Експериментални приказ у различитим областима човековог живота, представља један од показатеља универзалности примене добијених резултата ове докторске дисертације.

## 7. 1. Вештачке променљиве

Нови приступ који је базиран на примени [0, 1]-вредносне логике може да решава проблеме који су до сада били нерешиви применом линеарне дискриминационе анализе. У прилог овом ставу наводимо следеће примере. Наредна два вештачка примера су конципирана тако да ће нам показати праву моћ [0, 1] вредносне логике. У првом примеру ће нагласак бити на бољем распознавању класа користећи [0, 1] вредносну логику када јој придружимо *fuzzy*. Други пример ће показати како се нови приступ успешно сналази и у граничним ситуацијама.

***Пример 1***

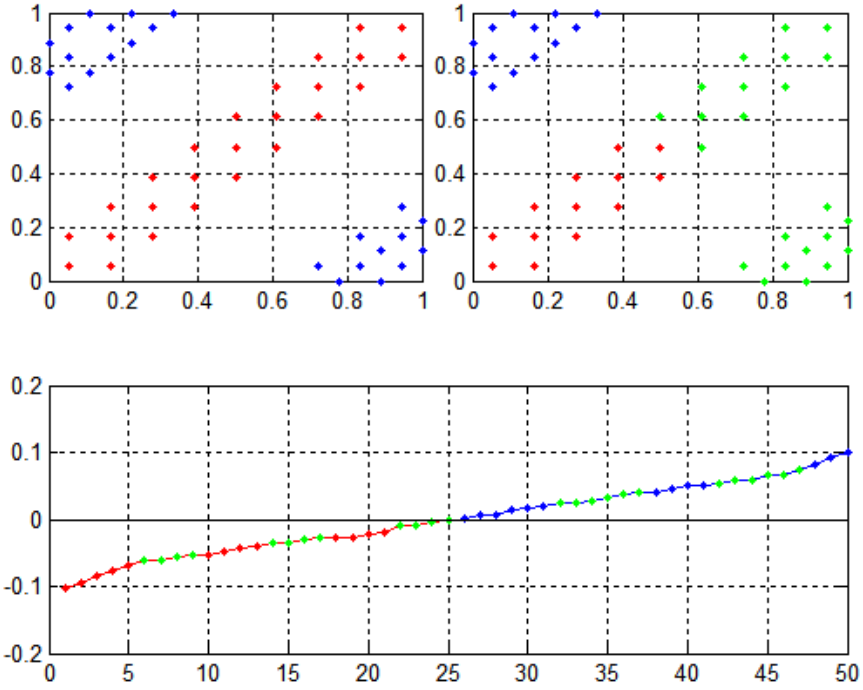
Нека је сваки објекат описан са два критеријума A и B и нека су класе у које су објекти сврстани следећег облика:



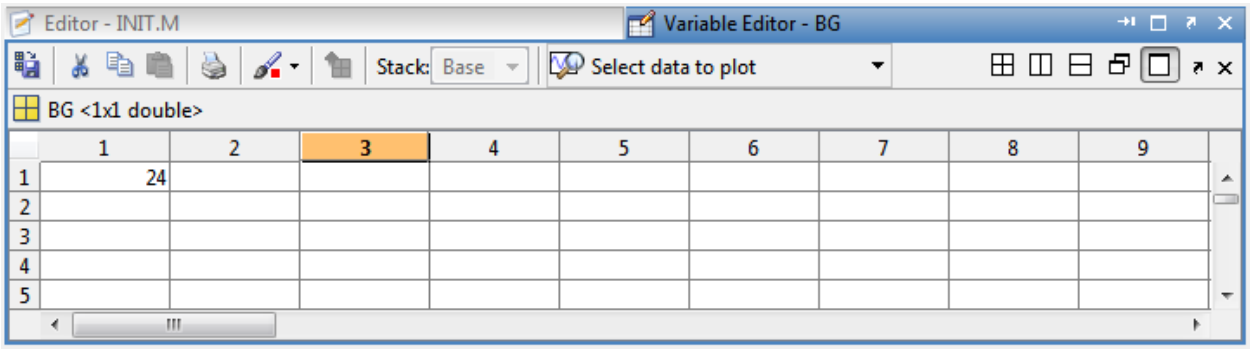

Слика 7.1. Класе објекта – пример 1

Као што се види са приказане слике 7.1. објекти су сврстани у две класе, иако се на први поглед види да можда постоје три класе, али ипак то неће бити случај. Прави задатак се намеће класичном приступу дискриминационој анализи. Класична дискринминациона анализа ће покушати да провуче праву, у овом конкретном случају, и тиме подели скуп на две класе. Управо ту ће доћи до грешке због, јер класичним приступом ће се појавити грешке. Управо зелене тачке на слици 7.1. показују број погрешно класификованих објеката.

Резултати дискриминационе анализе над полазним подацима класичним приступом приказани су на следећој слици:

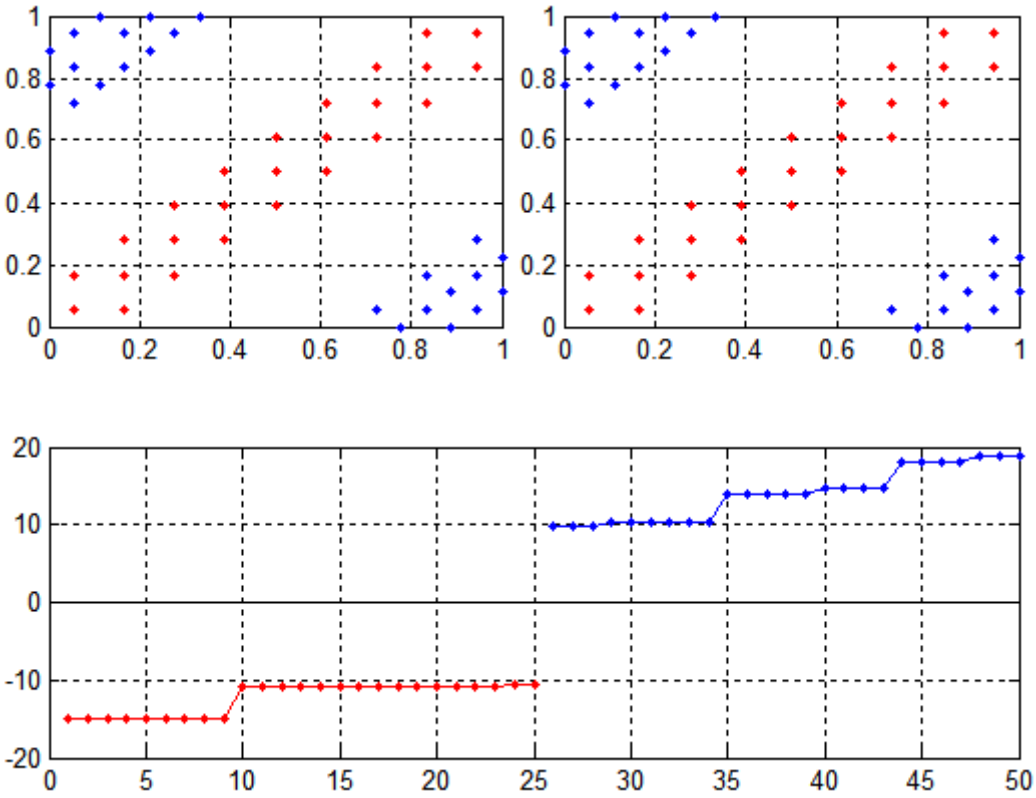



**Слика 7.2. Класичан приступ дискриминационој анализи – пример 1**

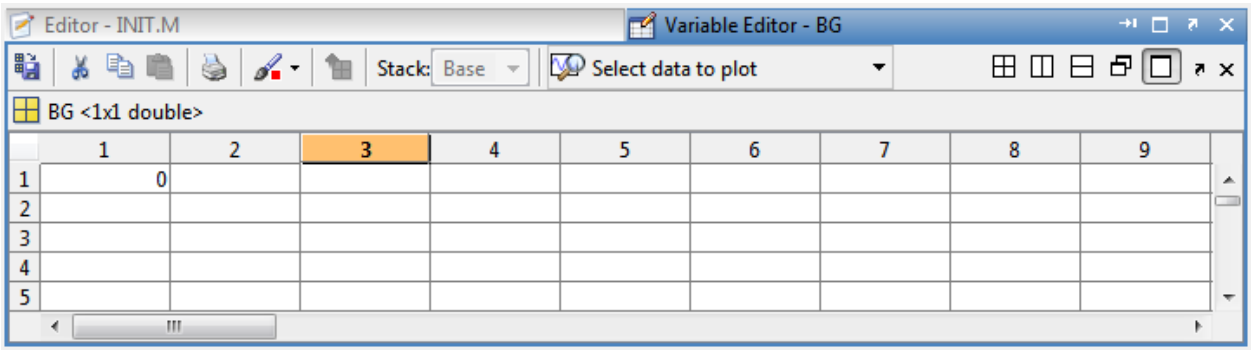



**Слика 7.3. Број грешака класичним приступом дискриминационој анализи – пример 1**

Резултати дискриминационе анализе над полазним подацима који су предпроцесирани применом [0, 1]-вредносне логике приказани су на следећој слици:




**Слика 7.4. Нови приступ дискриминационој анализи – пример 1**

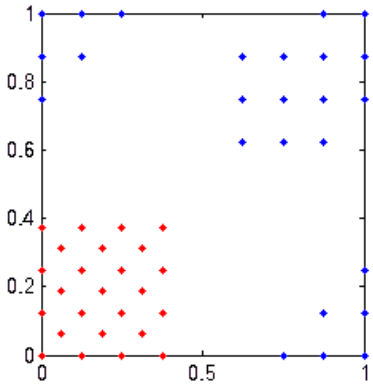



**Слика 7.5. Број грешака новим приступом дискриминационој анализи – пример 1**

За разлику од класичног приступа који је на скупу од 50 објеката погрешно сврстао 24 објекта, приступ заснован на примени [0, 1]-вредносне логике је у потпуности успео да раздвоји класе, тј. број грешака овог приступа је једнак нули.

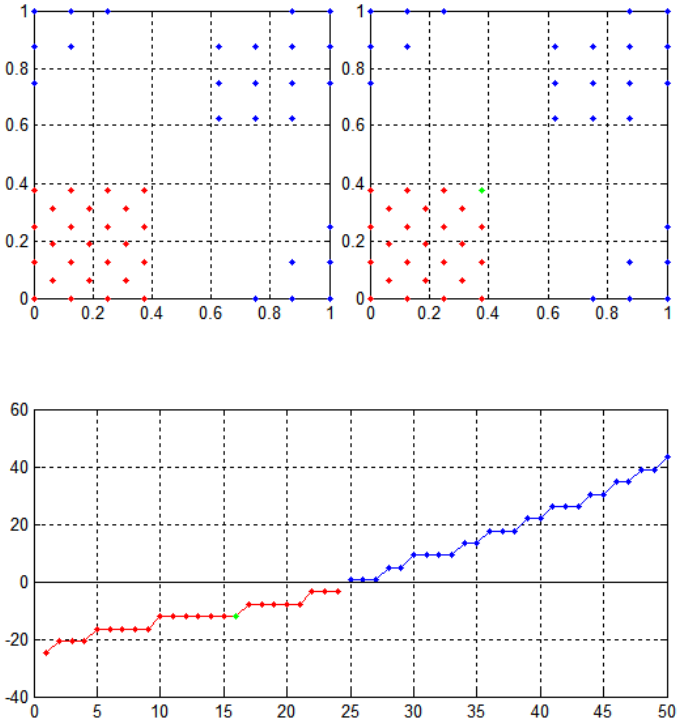
***Пример 2***

Нека је сваки објекат описан са два критеријума A и B и нека су класе у које су објекти сврстани следећег облика:




**Слика 7.6. Класе објекта – пример 2**

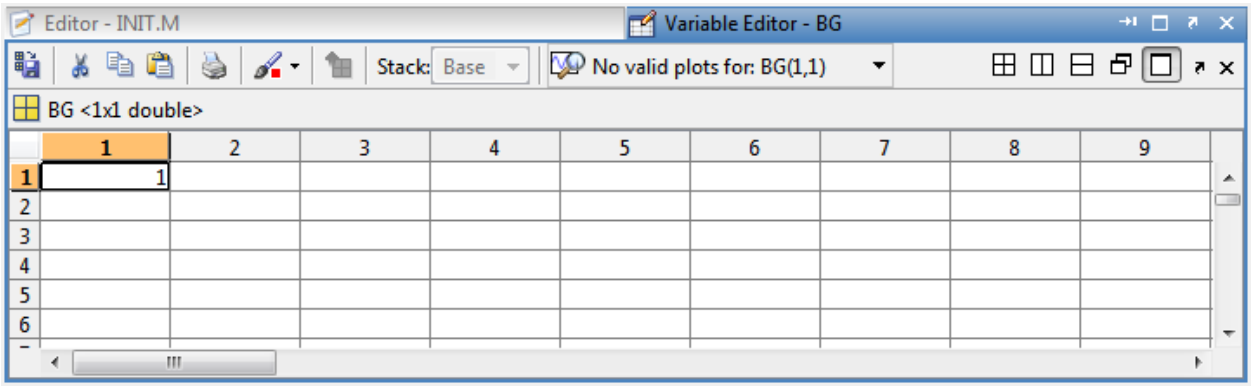
Резултати дискриминационе анализе над полазним подацима класичним приступом приказани су на следећој слици:




**Слика 7.7. Класичан приступ дискриминационој анализи – пример 2**

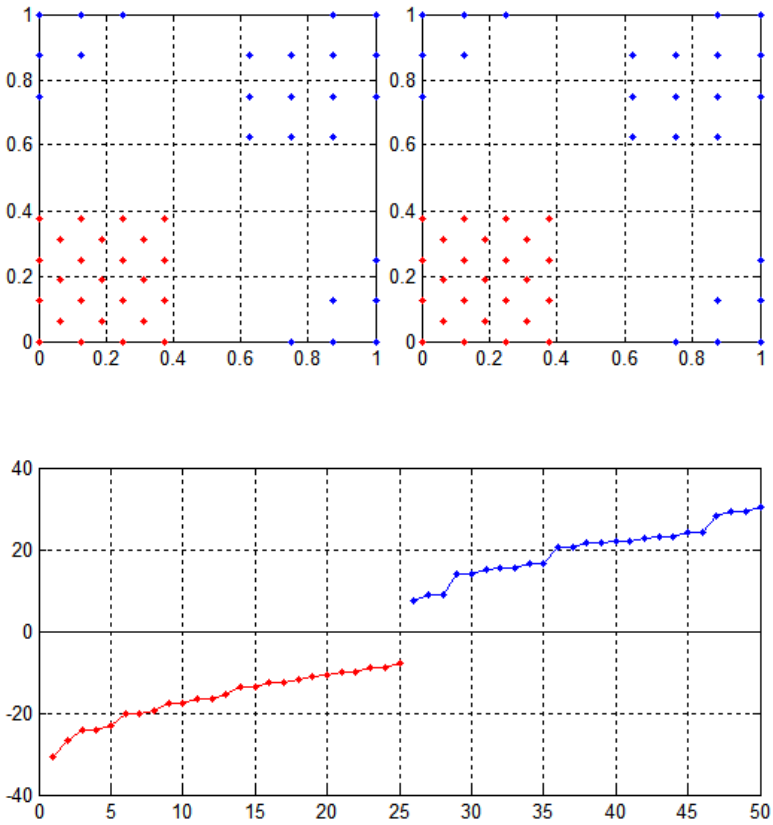
Као што се може видети, класичним приступом је направљена грешка управо тамо где смо и претпоставили. Зелена тачка на графику нам показује да

класичним приступом нисмо успели да класификујемо зелену тачку ни у једну припадајућу групу. До грешке је дошло зато што класичан приступ покушава да провуче праву или раван, уколико је тродимензионалан простор. Покушај да се све плаве тачке сврстају у једну класу наишао је на препреку јер, зелена тачка не припада плавој, већ црвеној групи. Ту на сцену ступа претпроцесирање података и боље могућности новог обраде података новим алгоритмом.

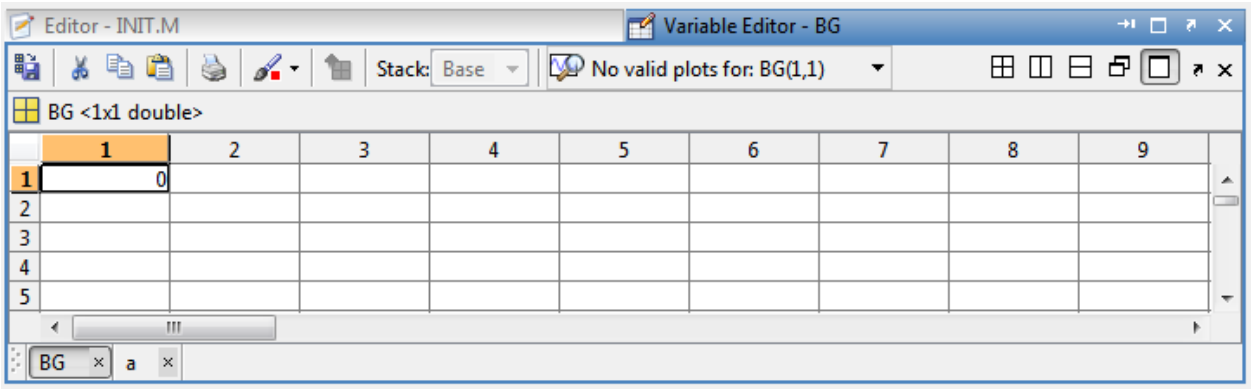



**Слика 7.8. Број грешака класичним приступом дискриминационој анализи – пример 2**

Резултати дискриминационе анализе над полазним подацима који су предпроцесирани применом [0, 1]-вредносне логике приказани су на следећој слици:



**Слика 7.9. Нови приступ дискриминационој анализи – пример 2**




**Слика 7.10. Број грешака новим приступом дискриминационој анализи – пример 2**

Попут прошлог примера на скупу од 50 објеката применом првог приступа погрешно је сврстан 1 објекат, док други приступ заснован на примени [0, 1]-вредносне логике у потпуности раздваја класе, тј. број грешака овог приступа је једнак нули.

### 7.2. Fuzzy метода

Свака оргнизација почива на одређеној хијерархији. Пословне организације, укључујући и банке заснивају своје пословање на класичној тронивојској хијерахији. Највиши ниво ове хијерархије чини врховни менаџмент који на основу анализа информација о успешности предузећа и кретања у окружењу формулише стратегију. Средњи ниво чини менаџмент који разрађује усвојену стратегију и формира одговарајућу политику реализације. Најнижи ниво чини менаџмент чији је посао повазан за извршење пословне политике. Највећи проблем овакво постављеног концептуалног модела јесте како пословне одлуке са врха реализовати на оним најнижим нивоима. На пример ако посматрамо банку, у којој један шалтерски службеник доноси одлуку о томе да ли ће комитенту одобрити кредит или не, како да будемо сигурни да је свака појединачна одлука овог службеника у складу са прокламованом стратегијом која је донета на врху ?

Кредитирање грађана се врши на основу слободних новчаних средстава банке (штедња грађана) и наменске штедње за добијање кредита, према актима пословне политике банке. Ми ћемо разматрати овај други случај. Зависно од пословне политике банке дају се следеће врсте кредита : потрошачки кредит за трајна потрошачка добра, потрошачки краткорочни кредити, дугорочни кредити и кредити за стамбену изградњу, дугорочни кредити за инвестиције у привредну делатност и дугорочни кредити за обнову средстава. У овом раду нећемо посебно

обрађивати различите врсте кредитирања, већ ћемо само разматрати, да ли комитенту одобрити кредит или не.

Претпоставимо, да је врховни менаџмент донео одлуку да се због велике кнкурентности, снизе критеријуми за давање кредита. Уколико се оваква наредба уручи шалтерском службенику, поставља се питање, да ли ће овај службеник дати кредите и оним комитентима који су сувише ризични, и који неће вратити позајмљена средства. Овакав потез би, наравно, изазвао директне трошкове који би пропорционално смањили остварени профит. С друге стране уколико службеник комитенту не одобри кредит, банка ће изгубити комитента, умањити репутацију и проузроковати још низ нажељених ефеката. Све ово указује на непоходност стварања једног другачијег модела, који ће омогућити, остваривање највећег могућег профита, уз најмањи могући ризик.

Када говоримо о банкама, правилан избор комитената којима ће бити одобрен кредит предстаља суштину успешног пословања, а дискриминациона анализа представља одличан алат који се у ту сврху може користити. На примеру који следи биће демонстрирана управо ова мултивариациона анализа, са посебним осврtом на снагу ове методе кад јој се придружи *„Fuzzy”* логика.

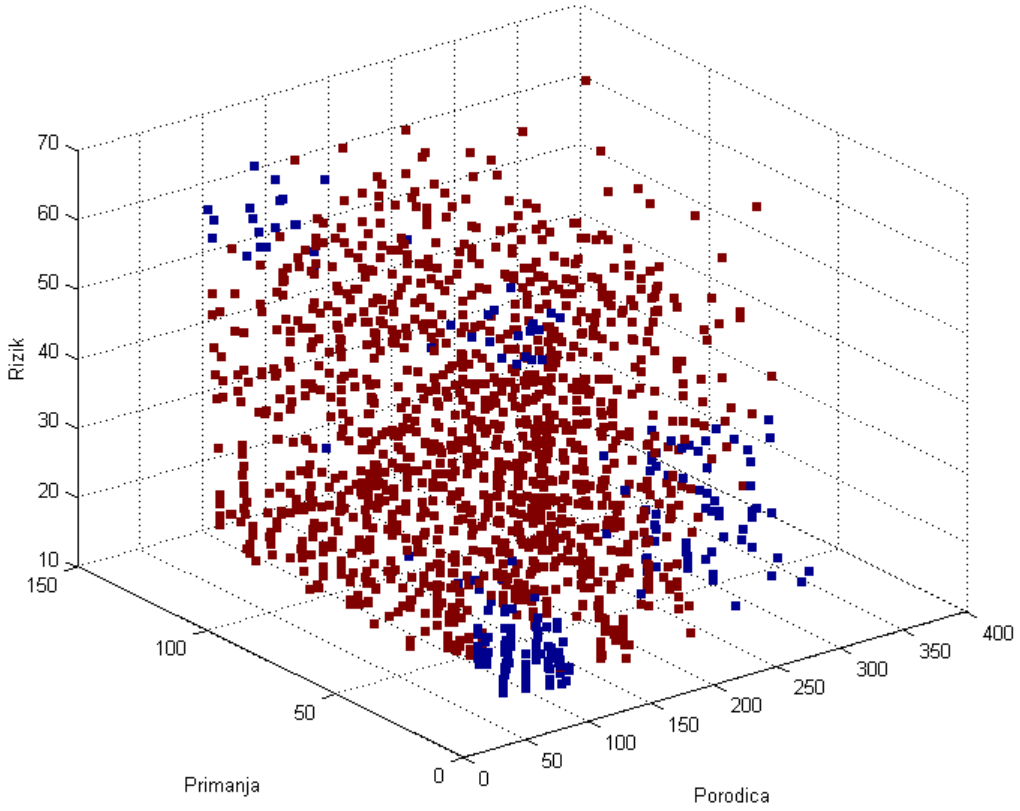



**График 7.1. Групе за доделу кредита**

Структуре основних података, везаних за активности кредитирања грађана, су : датотека корисника кредита (регистар комитената) и вођење партије за сваки дати кредит. Претпоставимо да једна банка прикупила податке за 1500 комитената који су досада добијали кредит, и то :

1. Примања
2. Спремност на ризик
3. Однос према породици

На графику су црвеном бојом означени комитенти који су своје кредите враћали на време, а плавом бојом они који то нису радили. На *графику 7.1.* се јасно распознаје неколико група оних којима не треба дати кредит. Прву групу чине они који имају мала примања, вероватно немају децу, млади су и нису спремни на ризик. Друга група је слична претходној само што је спремност на ризик код ове групе изузетно изражена. Разлоге зашто овим групама не треба дати кредит, вероватно не треба посебно износити. Између ове две групе налази се једна велика група која има сличне особине као претходне две, али је обележена зеленом бојом. То је вероватно група младих људи, на почетку каријере, без породице, са умереним односом према ризику, амбициозни са добром идејом. Треба уочити још једну групу којој не треба одобрити кредит, то су људи са великим примањима и спремни на ризик, а при томе нису породични људи. Последња група обојена плавом бојом, представља људе са великом породицом, просечним примањима и не баш спремне на ризик. Остали комитенти углавном припадају оној групи којој треба одобрити кредит.

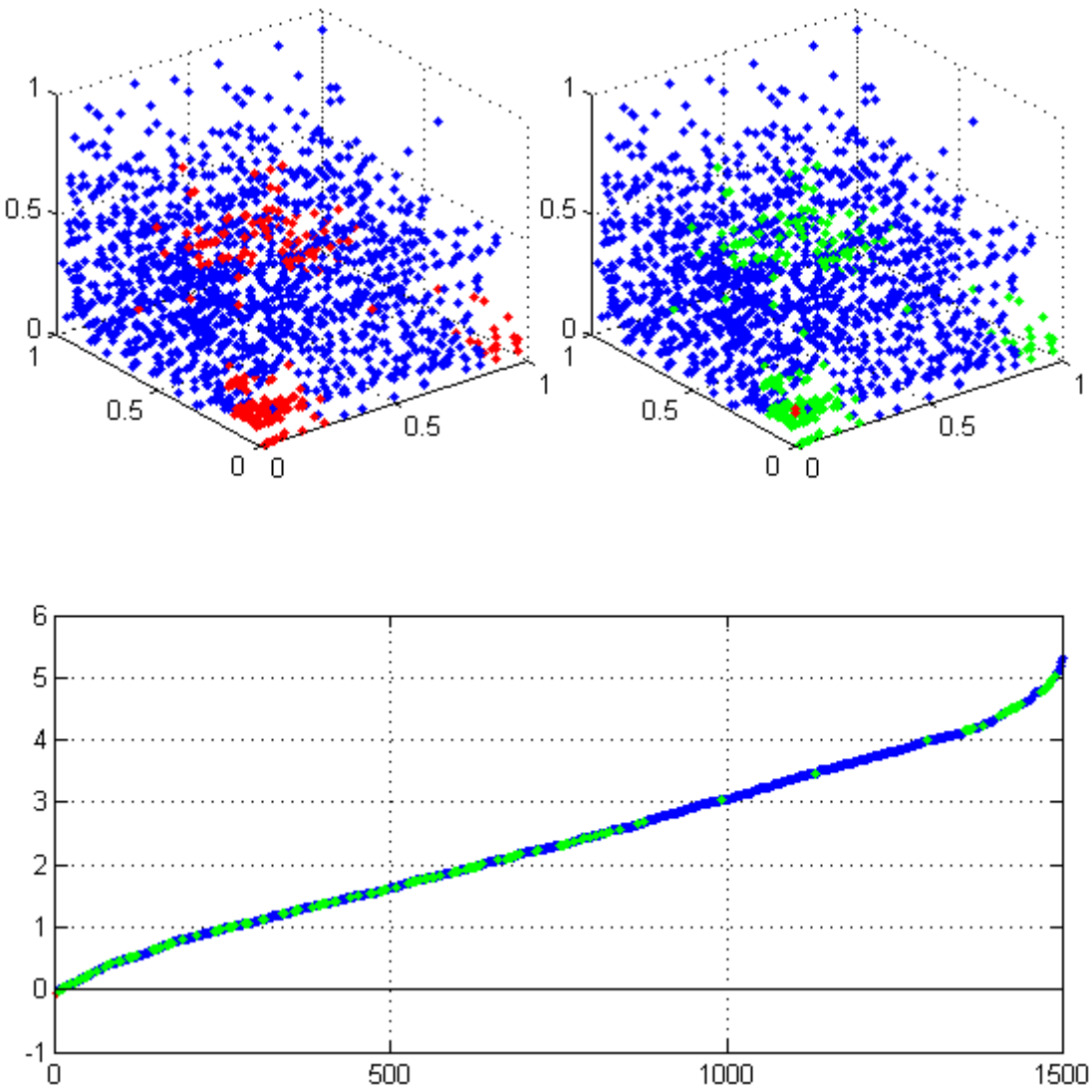
Наведене податке ћемо обрадити, помоћу:

1. Класичне
2. „*Fuzzy*” методе пута (*)
3. „*Fuzzy*” методе *min*

и добијене резултате анализирати.

### *7.2.1. Класична метода*

Након обраде података помоћу класичне медоде добијени су следећи резултати:

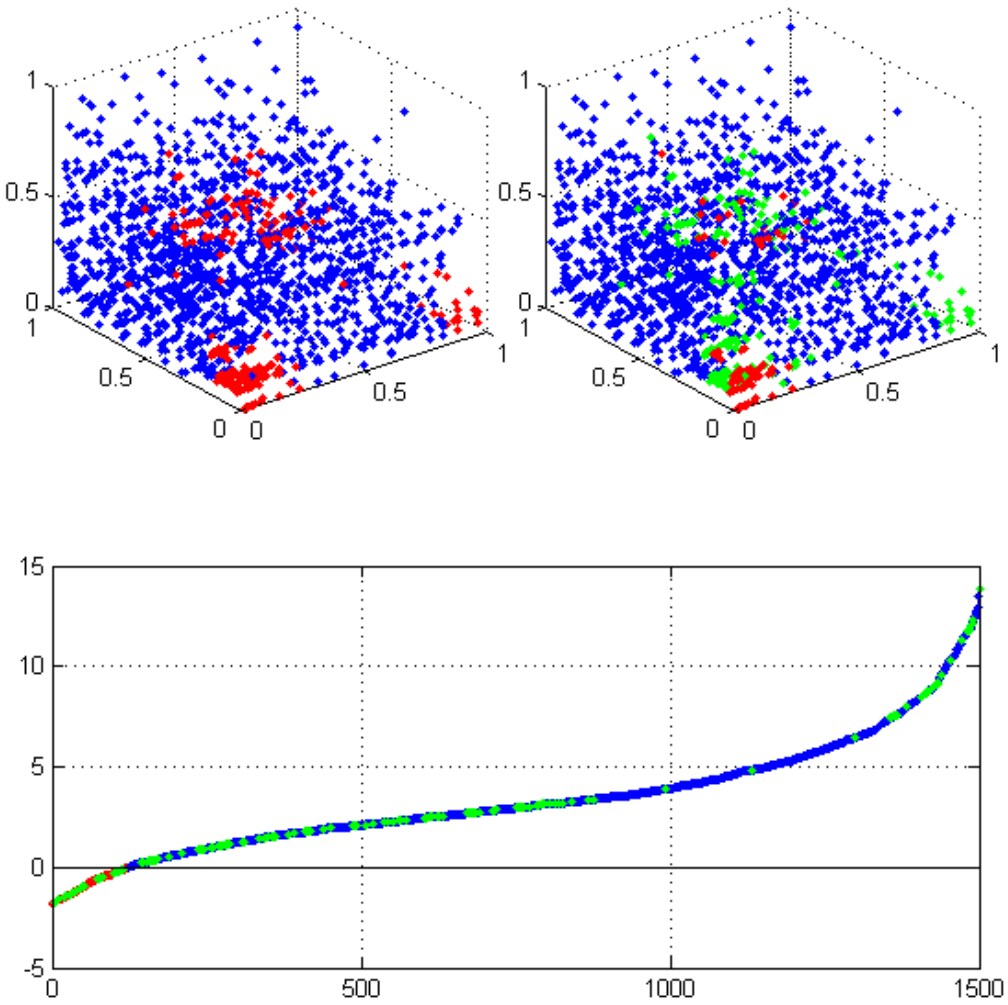



**слика 7.11. Класична дискриминациона анализа – пример 3**

На графику се јасно види да класична дискриминациона анализа није у стању да посматрани скуп података подели на одговарајуће кластере. На графику су зеленим тачкама обележени објекти који су погрешно класификовани, види се да су сви објекти који припадају групи оних којима не треба дати кредит сврстани у погрешну групу. Дискриминациона функција добијена на овај начин је потпунао неупотребљива.

### *7.2.2. „Fuzzy" метода пута (*)*

Након обраде података „*Fuzzy*" методом пута (*) добијени су следећи резултати:

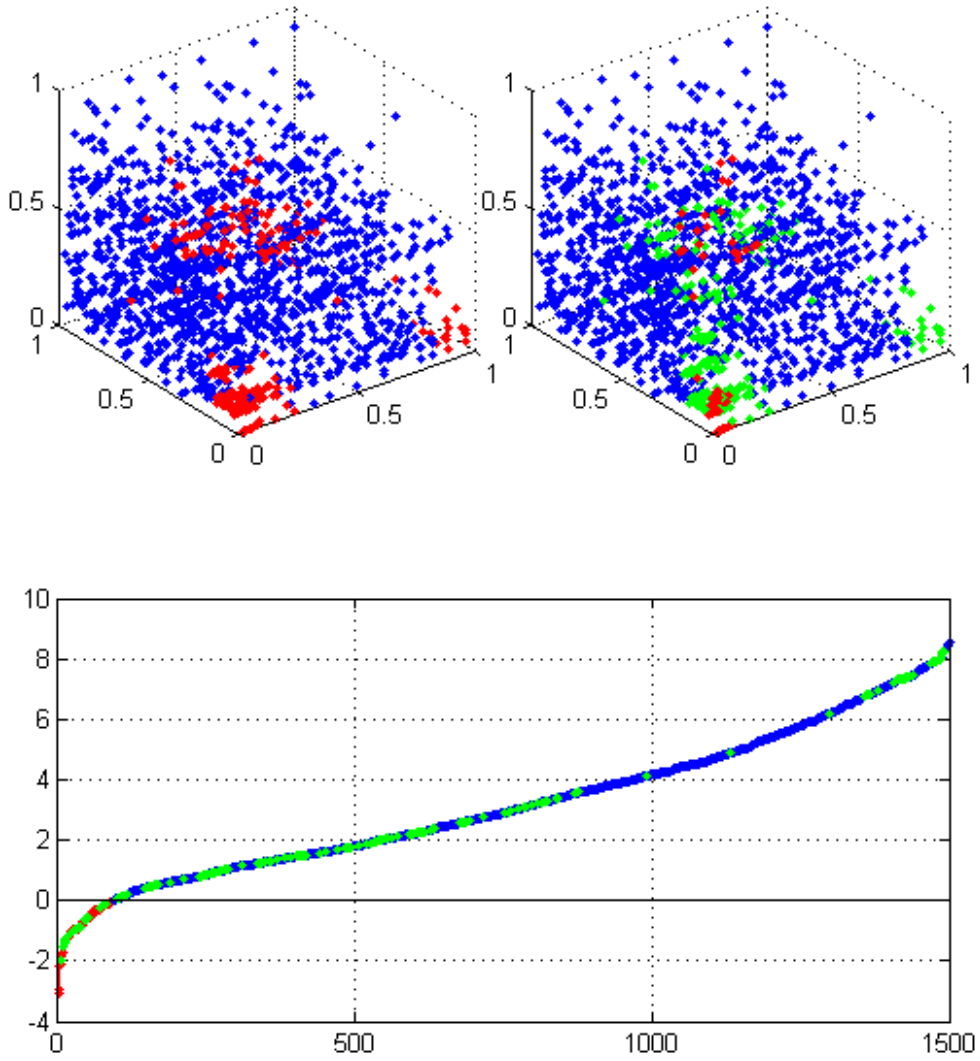



**Слика 7.12. „Fuzzy" методе пута (*)**

На графику се види да „*Fuzzy*" дискриминациона анализа у којој је операција „*AND*" имплементирана преко операције пута (*) успела да препозна постојање друге групе, оне којој припадају комитенти којима не треба дати кредит. На графику су зеленим тачкама обележени објекти који су погрешно класификовани, види се да је број оваквих објеката знатно смањен у односу на предходну методу. Дискриминациона функција добијена на овај начин би већ могла да послужи службеницима да одреде да ли комитенту треба одобрити кредит или не.

### *7.2.3. „Fuzzy" метода min*

Након обраде података „*Fuzzy*" методом *min* добијени су следећи резултати:




**Слика 7.13. „Fuzzy" методе *min***

На графику се види да *„Fuzzy"* дискриминациона анализа у којој је операција *„AND"* имплементирана преко функције „*min*", такође успела да препозна постојање друге групе, оне којој припадају комитенти којима не треба дати кредит. На графику су зеленим тачкама обележени објекти који су погрешно класификовани, види се да је број оваквих објеката знатно смањен у односу на класичну методу, али је број грешака ипак већи у односу на предходну методу. Ово указује на логички однос између компоненти. Дискриминациона функција добијена на овај начин би већ могла да послужи службеницима да одреде да ли комитенту треба одобрити кредит или не, али је предходна метода ипак дала боље резултате.

### 7.3. Класична метода

Пример који ћемо сада описати базиран је на ткз. “ADSL Tone diagnostics” или ти “АДСЛ дијагностика сигнала”. На сваком ADSL рутеру можемо да приступимо страници на којој можемо да тестирамо ADSL конекцију. За наш пример узећемо податке из једног таквог теста. За потребе примера и бољег разумевања узорка описаћемо основне елементе и променљиве које можемо добити из једног оваквог теста. Изглед једне такве странице види се на слици која следи.

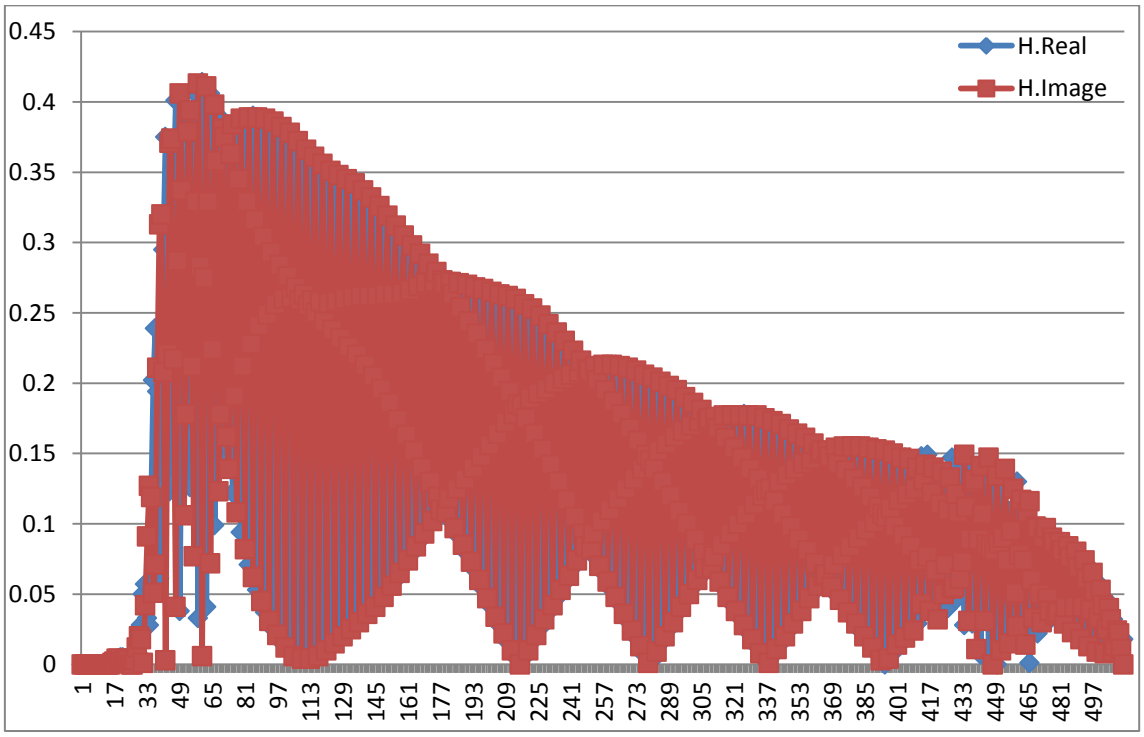

Слика7.14. Пример странице ADSL дијагностике

Елемнти ADSL тестирања конекције:

1. Start – Покретање дијагностичког теста
2. Downstream/Upstream – Показује проток података ка и од ADSL рутера
3. Hlin Scale – Приказује скалирајући фактор за H.Real и H.Image променљиве у целобројној вредности
4. Loop Attenuation (dB) – Приказује опадање везе ADSL рутера и провајдера у децибелима
5. Signal Attenuation (dB) – Приказује опадање сигнала везе који је одређен фреквенцијом у децибелима
6. SNR Margin (dB) – Приказује шум везе у децибелима
7. Attainable Rate (Kbps) – Приказује опадање везе провајдера у килобитима по секунди
8. Output Power (dBm) – Приказује излазну снагу јединице у децибелима по миливату

9. Tone Number – Приказује број ADSL сигнала (Опсег: 0-255)
10. H.Real – Приказује реални део функције преносног канала сваког под-носиоца сигнала
11. H.Image – Приказује имагинарни део функције преносног канала сваког под-носиоца сигнала
12. SNR – Приказује SNR (Шум) сваког под-носиоца сигнала изражен у децибелима
13. Hlog – Приказује амплитуду одговора функције преносног канала сваког под-носиоца, изражену у децибелима

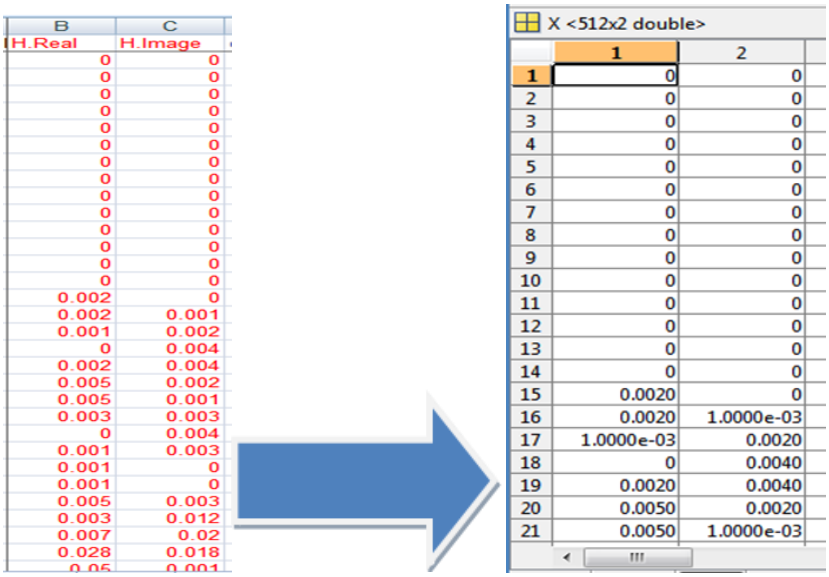
За наш пример узећемо податке из колона H.Real и H.Image. То ће бити наш узорак. Грубом анализом ових података са графика који следи можемо видети да ове променљиве покушавају да се усагласе и да имају исту вредност што на крају и успевају и тиме постижу стабилност система. Али то је један процес у коме има честих искакања из система променљиве H.Real што се на графику може видети као плаве тачке.




Графикон 7.2. Приказ реалног сигнала и сигнала слике

Дакле наш задатак би био да на основу довољно великог узорка предвидимо искакања из система са најмањом могућом грешком. За то ћемо користити програм за дискриминациону анализу побољшан Fuzzy логиком који је већ раније описан у овом раду и видећемо да ли је погодан и за овакав тип задатака.

Полазни подаци H.real и H.image смештени су у матрицу X[512x2] :



| B | C |
|---|---|
| H.Real | H.Image |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0 | 0 |
| 0.002 | 0 |
| 0.002 | 0.001 |
| 0.001 | 0.002 |
| 0 | 0.004 |
| 0.002 | 0.004 |
| 0.005 | 0.002 |
| 0.005 | 0.001 |
| 0.003 | 0.003 |
| 0 | 0.004 |
| 0.001 | 0.003 |
| 0.001 | 0 |
| 0.001 | 0 |
| 0.005 | 0.003 |
| 0.003 | 0.012 |
| 0.007 | 0.02 |
| 0.028 | 0.018 |

X <512x2 double>

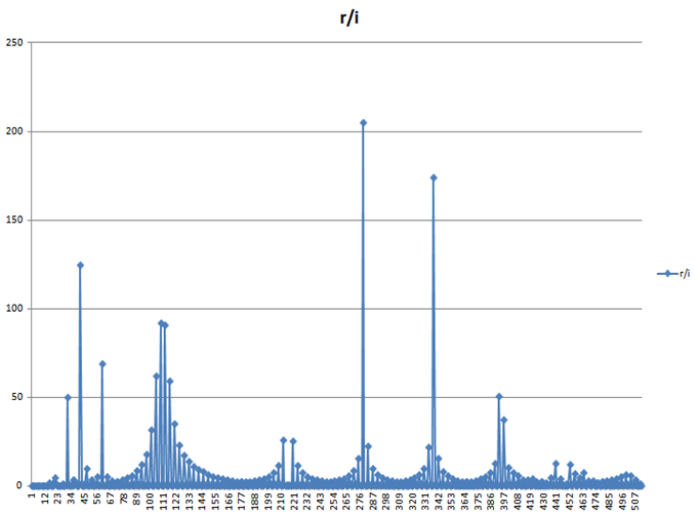
| | 1 | 2 |
|---|---|---|
| 1 | 0 | 0 |
| 2 | 0 | 0 |
| 3 | 0 | 0 |
| 4 | 0 | 0 |
| 5 | 0 | 0 |
| 6 | 0 | 0 |
| 7 | 0 | 0 |
| 8 | 0 | 0 |
| 9 | 0 | 0 |
| 10 | 0 | 0 |
| 11 | 0 | 0 |
| 12 | 0 | 0 |
| 13 | 0 | 0 |
| 14 | 0 | 0 |
| 15 | 0.0020 | 0 |
| 16 | 0.0020 | 1.0000e-03 |
| 17 | 1.0000e-03 | 0.0020 |
| 18 | 0 | 0.0040 |
| 19 | 0.0020 | 0.0040 |
| 20 | 0.0050 | 0.0020 |
| 21 | 0.0050 | 1.0000e-03 |

Слика 7.15. Трансформација матрице података

Због потребе програма (дискриминационе анализе) потребна је била груба класификација података матрице X[512x2] у кластере. Коришћена је уграђена функција classify (podaci,trening,grupa).

За класификасцију података из полазне матрице X[512x2], ти подаци су сместени у матрицу podaci која мора да има исти број колаона као и матрица trening. Матрица trening се састоји од 20 записа из полазне матрице X[512x2] који су репрезентативни и који припадају једној од две будуће групе.

Записи су изабрани на основу графика:




y <512x1 double>

| | 1 |
|---|---|
| 186 | 2 |
| 187 | 1 |
| 188 | 1 |
| 189 | 1 |
| 190 | 2 |
| 191 | 1 |
| 192 | 1 |
| 193 | 1 |
| 194 | 2 |
| 195 | 1 |
| 196 | 1 |
| 197 | 1 |
| 198 | 2 |
| 199 | 1 |
| 200 | 1 |
| 201 | 1 |
| 202 | 2 |
| 203 | 1 |
| 204 | 2 |
| 205 | 1 |
| 206 | 2 |

Слика 7.16. Нормална расподела испада система

Након изврсавања функције classify добили смо матрицу Y[512x1] која има исти број редова као матрица X[512x2]. Заправо сваки запис из матрице X[512x2] кореспондира са сваким редом из матрице Y[512x1] и тиме одређује припадност групи .

Сада имамо све потребне податке да би их пропустили кроз програм за дискриминациону анализу.

Наведене податке ћемо обрадити, помоћу:

1. Класичне

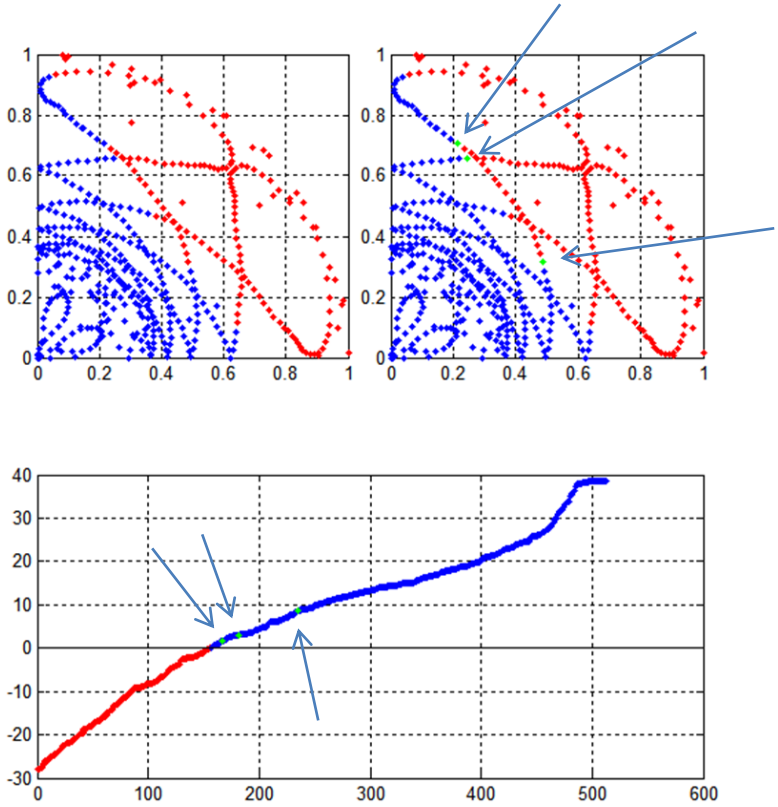
2. „Fuzzy" методе пута (*)

3. „Fuzzy" методе min

и добијене резултате анализирати.

### *7.3.1. Класична дискриминациона анализа (Classic)*

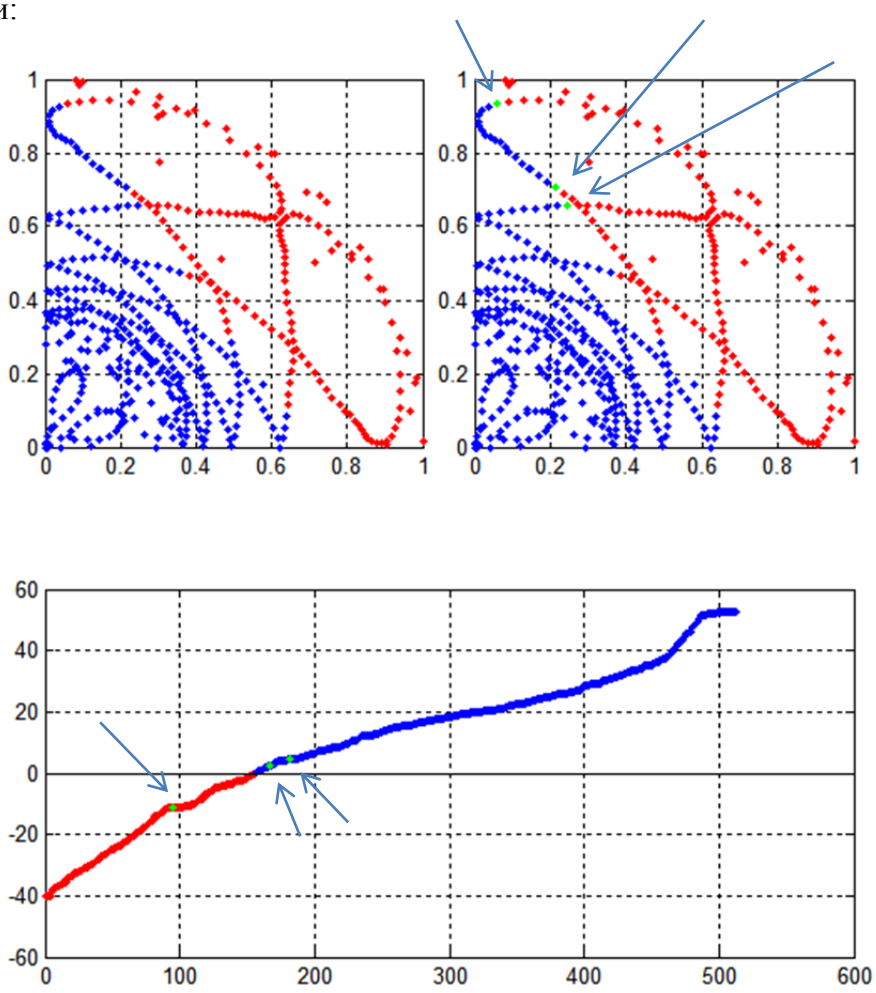
Након обраде података помоћу класичне медоде добијени су следећи резултати:




Слика 7.17. Број грешака Classic 3 (зелене тачке на графику)

### *7.3.2. Fuzzy-Метода* (пута)*

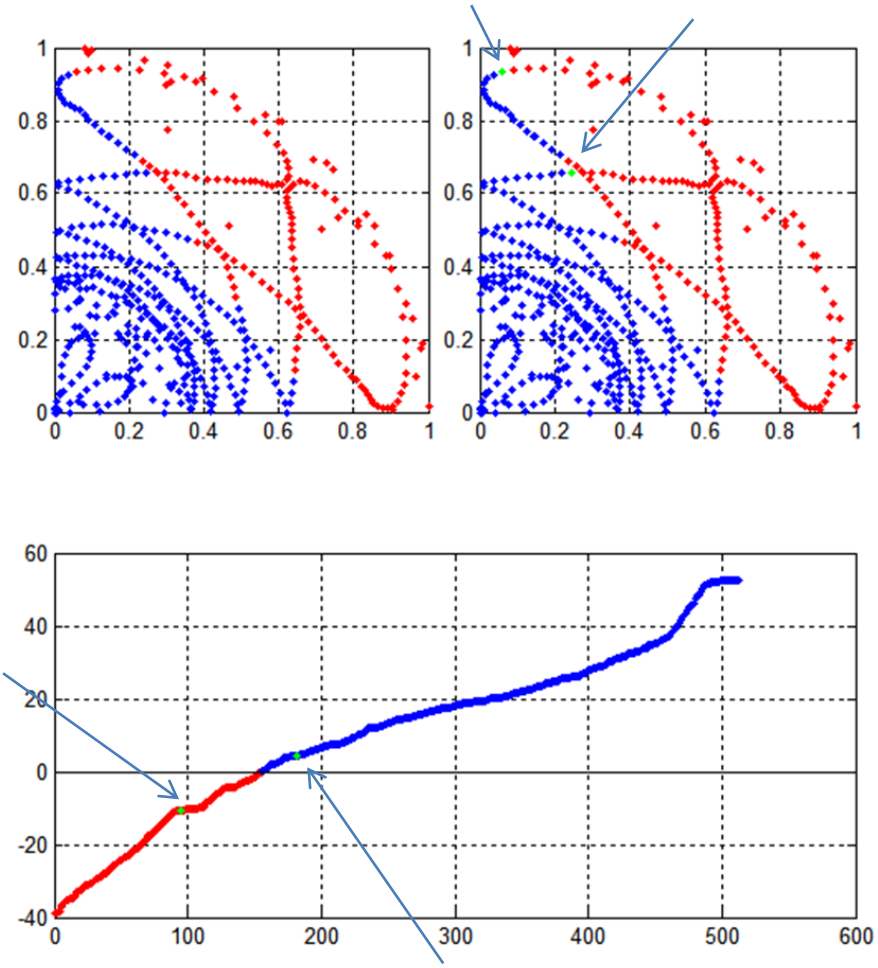
Након обраде података „Fuzzy" методом пута (*) добијени су следећи резултати:




Слика 7.18. Број грешака Fuzzy 3 (зелене тачке на графику)

### *7.3.3. Fuzzy-Метода min*

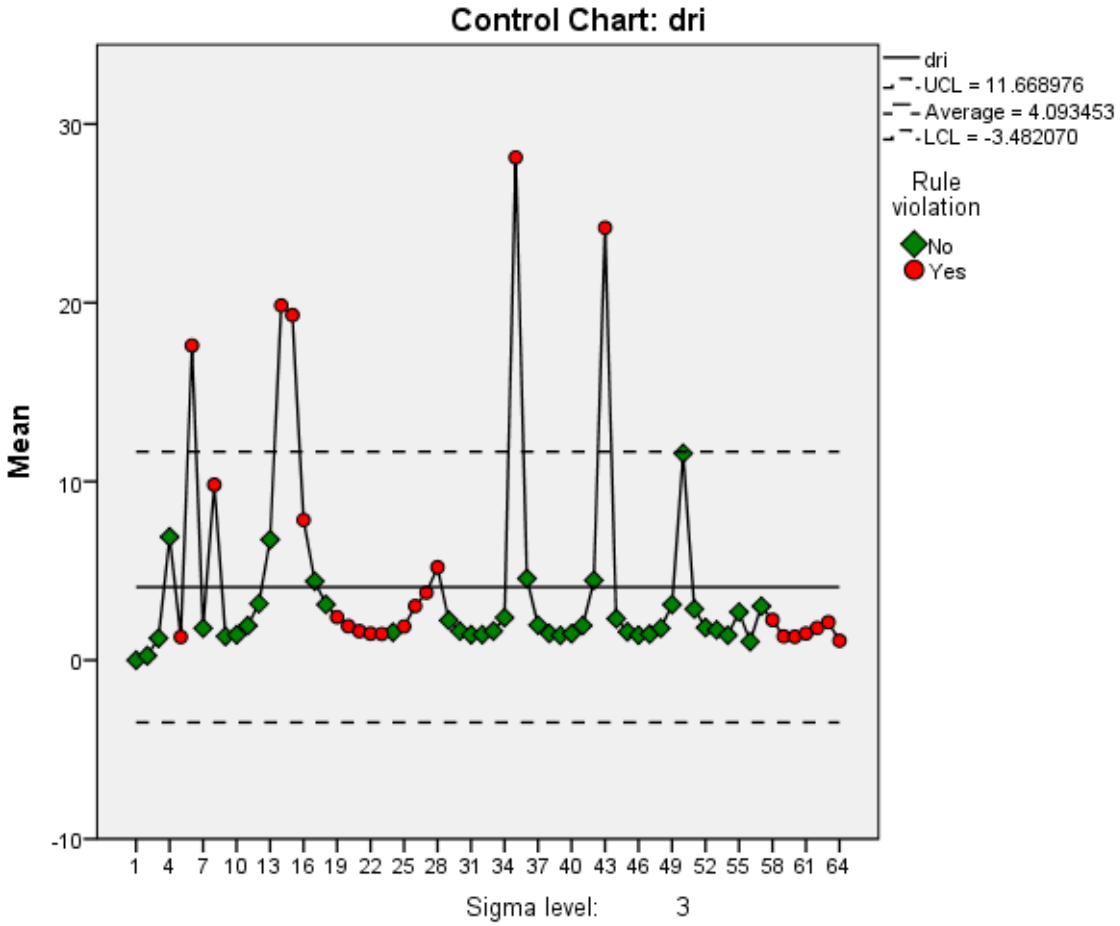
Након обраде података „Fuzzy" методом min добијени су следећи резултати:




Слика 7.19. Број грешака Min 2 (зелене тачке на графику)

### *7.3.4. Статистичка контрола процеса*

Наведени пример разматран је и кроз стандардну процедуру статистичке контроле процеса, ради откривања критичног понашања система. У претходним примерима кључни испади система су се базирали на две до три грешке, и као ретки догађаји систем је на основу понашања детектовао критичне тачке. Методом статистичке контроле процеса уочава се више критичних тачака система, које пре свега делују да су у складу са очекивањима, али само понашање (без обзира што се налазе у границама очекиваног) представља критично понашање. Резултати нарушавања правила статистичке конторолe процеса приказани су на слици 7.20.

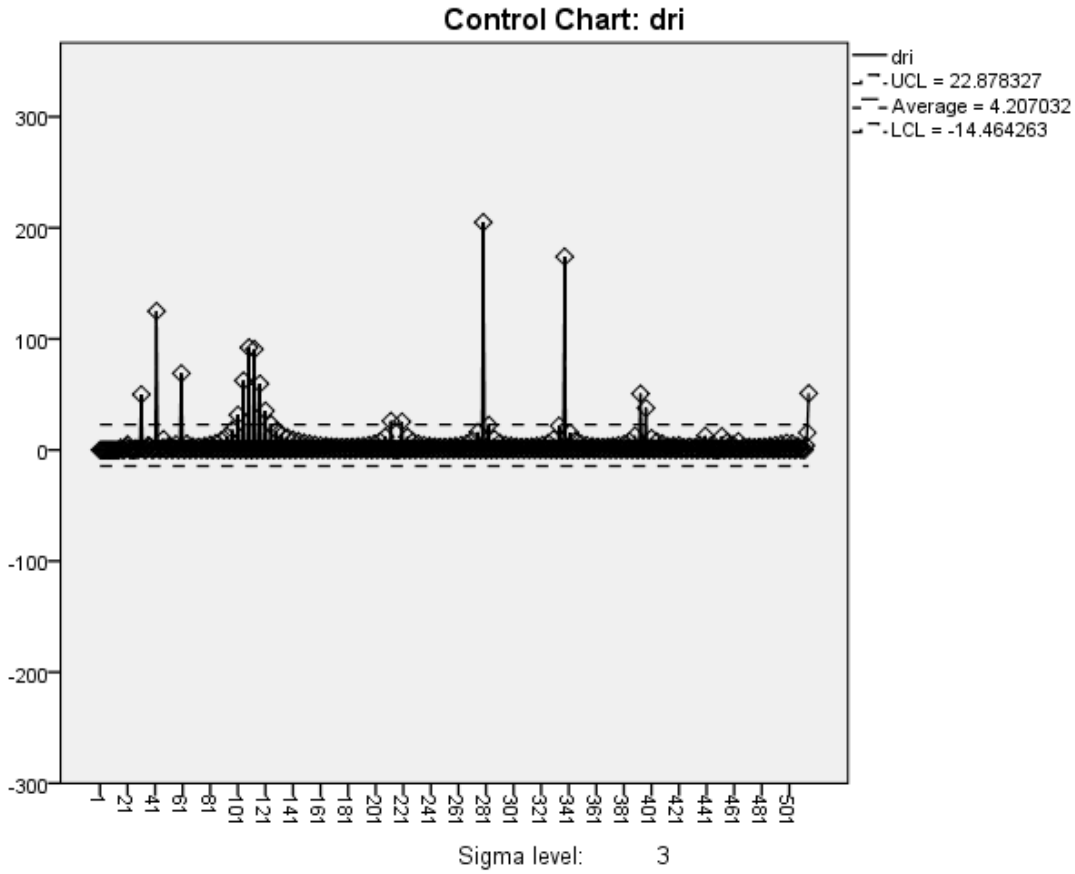



Слика 7.20. Нарушавање правила статистичке контроле процеса

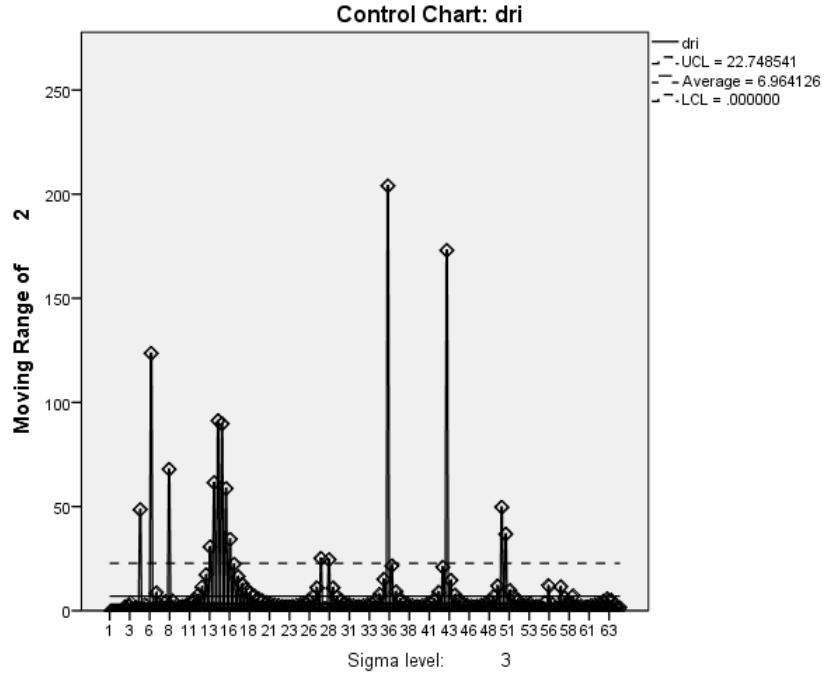
Приказани резултати показују да критичне вредности процеса су озбиљно нарушене у 5 случајева, док се серија података од 19 до 28 и од 58 до 64 бајта је нарушила правила иако се налазе у границама очекиваног. Систем је и даље у ван равнотежног стања што представља меру опреза, због могућности рањивости система у том периоду.

Према СП графикону, можемо на основу приказаних резултата уочити 15 критичних места система, у којим је дошло до озбиљног нарушавања система усклађивања. Резултати о наведеним бајтовима где је дошло до нарушавања приказани су на слици 7.21. Поредећи са предходним резултатима, можемо закључити да методе статистичке контроле процеса су обазривијег карактера и врше сигнализацију испада на нивоу сумње.

Посматрањем померања рангова (Слика 7.22.) ради у радикализације постојећих резултата, можемо само да потврдимо добијене резултате и да закључимо да можемо рећи да је систем био у критичној ситуацији чак 15 тачака (бајтова). Овиме статистички процес контроле сертификације сигнала је био на много већем нивоу обазривости.




Слика 7.21. СП графикон нарушавања система



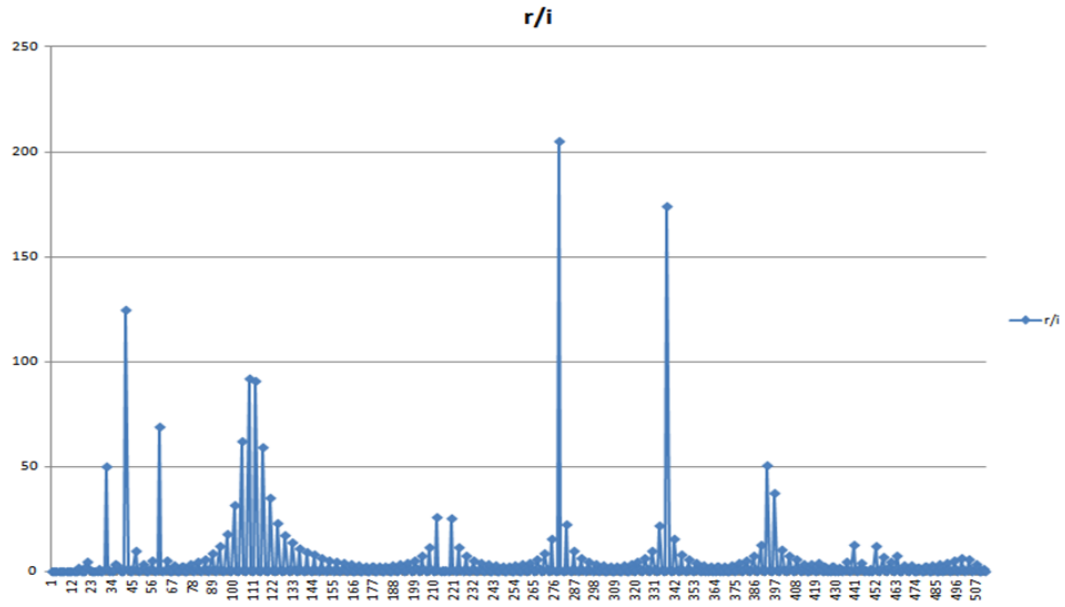

Слика 7.22. Метод покретних рангова

### *7.3.5. Анализа*

Подаци у овом примеру, тј. објекти који испадају из система имају Нормалну расподелу, а да би дискриминациона анализа добро радиала, требало би да подаци испуњавају следеће услове који су везани за улазне податке:

1. Групе (кластери, класе) треба да имају бар приближно нормалну расподелу;
2. Узорци треба да буду случајни;
3. Матрице варијације и коваријације треба да за сваку групу буду исте;
4. Почетни подаци морају да буду тачно квалификовани (подељени у групе)

Услов под тачком 1. је испуњен али  излазни подаци нису очекивани. Најбоље се показала метода MIN зато што је направила једну грешку мање у класификовању у односу на остале методе али то није довољно јер су скупови исувише неодређени. Много мање њих би требало да припада другој групи нпр.. А то може да се види из графика који следи где се види да објекти који искачу из система имају приближно Нормалну расподелу.




Слика 7.23. Испади из равнотеже

Групе би требало да се ломе на 50-ом подеоку на у-оси, или мање, негде око 30-ог подеока, али се то не дешава у случају дискриминационе анализе и то вероватно из више разлога.

1. Могуће је да је почетна класификација и груба подела у 2 групе лоше урађена, Можда узорак за тренинг групу мора да буде већи.

2. Можда зато што је цео узорак мали. (мада то не би требало да утиче, јер алгоритам ради добро и на мањим узорцима)
3. Можда због тога што улазни подаци немају Нормалну расподелу.

На крају можемо констатовати да за овакав тип проблема ова методологија нија најпогоднија или подаци морају боље да се претпроцесирају што је вероватно. Можда би за улазне податке требало узети не и однос основних података и онда их пропустити кроз алгоритам.

У односу на претходно приказане резултате, метода статистичке контроле процеса је у већој мери детектовала нарушавање система, са значајним елементима сигнализације и у оним тренутцима када процес није деловао као нарушен. Детектовање свих потенцијалних нарушавање система чино је да анализирање података се подигне на један квалитативно виши ниво чиме се обезбеђује већа сигурност и сталан опрез за појаву нарушавања интегритета система. У основи није довољно само пратити да ли је систем у задатим границама већ и само понашање података представља значајан показатељ угрожености система.

Предности статистичке контроле процеса је очигледна управо са аспекта аутоматизације праћења процеса сертификације система и раног система узбуњивања које се огледа у двоструком нарушавњу правила понашања и то:

1. Испад изван задатих граница
2. Атипична понашања унутар граница

Двоструки степен контроле унапредио је претходно приказане методе детекције критичних тачака понашања

# 8. ЗАКЉУЧАК

У докторској дисертацији, детаљно су описане основне карактеристике система за примену јавних кључева (PKI систем) и функције CA, као и начин њихове реализације. Истакнути су концептуални ставови, описани су међународни стандарди који се користе и приказане су основне карактеристике архитектуре једног сопствено реализованог софтверско-хардверског система за генерисање криптографских кључева, производњу дигиталних сертификата и персонализацију меморијских медијума или smart картица, тј. система за потпуну подршку рада PKI система као једног могућег предлога за реализацију CA .

Сертификационо тело (CA – Certification Authority) представља највишу тачку поверења у читавом PKI систему. Основни задатак CA је да процедуром дигиталног потписа на бази асиметричног криптографског алгоритма и свог тајног кључа, који мора бити најстроже чувана тајна, гарантује везу између јавног кључа и идентитета одређеног субјекта за потребе електронске размене података у оквиру IS. Сваки субјекат има могућност да верификује дигитални потпис CA, на бази јавног кључа асиметричног криптографског алгоритма CA, који је познат свим корисницима.

CA издаје дигиталне сертификате на основу захтева за учешће у електронској размени података у IS, које субјекти подносе у регистрационим телима (RA) или директно преко web портала CA, путем http комуникације. Дигитални сертификати су у форми, прописаној стандардом ITU-T X.509 v3. CA је одговорно за управљање базом података свих издатих сертификата и те информације су доступне свим субјектима. Читав садржај дигиталног сертификата се потписује асиметричним криптографским алгоритмом са тајним кључем CA и добијени дигитални потпис се прикључује садржају сертификата.

**Приказана решења у оквиру докторске дисертације дата су у односу на:**

1. Полазну претпоставку која се заснива на дефинисању и развијању активности дигиталних сертификата и његовог специфичног облика везаног за електронско окружење, ради његовог развоја и примене. Тиме је приказан нови приступ у начину пружања електронских услуга.
2. Постављени циљ истраживања, је изградња модела који је базиран на статистичкој анализи ефикасности примене PKI система и дигиталних сертификата.Анализа нам је дефинисала потребе пословања PKI ускладу са развојом електронских услуга, примене статистичких метода ради мерења постигнутих резултата.

3. Апликациони модел представља примену дигиталних сертификата, где су дефинисне активности које имају стратешку улогу у унапређењу електронског пословања, одређивању степена значаја активности и мерења ефекта његове примене.На оваквом апликативно модулу уз примену статистчких анализа дошли смо до циљне архитектуре PKI система, који је дао најбоље резулате у практичној примени савременим пословним окружењима.

**Решења полазних хипотеза у докторској дисертацији**

Основна хипотеза овог истраживања је да на основу статистичких метода и анализа доступних реалних података из процеса PKI система могуће је препознати латентне параметре система, чија би адекватна идентификација и примена квалитативно допринела побољшању процеса управљања дигиталним сертификатима PKI система у електронском пословању. Другим речима, могуће је извршити аутоматизацију кључних процеса управљања дигиталним сертификатима одабраног PKI система, путем статистичких метода, са циљем да се обједине у одговарајући статистички модел.

За равој дигиталних сертификата, пресудне су информације, јер пружају податке на основу којих корисници електронских сервиса, доносе ефикасније и ефективније одлуке, и самим тим повећавају степен задовољства живота.

Дигитални сертификати треба да учине своје пословање ближе корисницима електронских сервиса, да утичу на модернизацију и побољшање квалитета услуга, на побољшање ефикасности, транспаретности и ефективности рада.

1. Подршка различитим политикама рада PKI система

PKI систем мора омогућити подршку за примену различитих безбедносних политика крајњег корисника. Ове политике утичу на формат и екстензије које се користе у дигиталним сертификатима и које се конфигуришу применом алата едитора безбедносне политике (security policy editor). Политике могу такође да садрже информације о пословној регистрацији које се не појављују у самом сертификату али су сакупљене и безбедно сачуване за време регистрационог процеса.

2. Безбедност система

У структури PKI система, CA представља тачку највишег поверења, али истовремено и тачку највишег ризика. Основни и најважнији захтев који се поставља пред CA је чување тајности тајног кључа CA за примену асиметричног криптографског алгоритма којим се врши дигитални потпис издатих дигиталних сертификата, и чување тајности осталих криптографских кључева који се додељују овлашћеним учесницима у IS CA. Стога се, поред криптографских техника, морају применити и друге мере из области физичке и организационе

заштите како би се остварила свеукупна безбедност PKI система. Поменуте мере се односе на просторије, запослена лица и уређаје.

3. Скалабилност

PKI систем мора подржати евентуално проширивање система додавањем одређених модула без потребе заустављања рада система. Другим речима, ако се дата организација проширује, или ако се захтеви за PKI технологијом повећавају, све се то може решити додавањем одговарајућих специфичних PKI модула.

- Предности система увођења дигиталних сертификата огледају се у следећем:
  - брзо и ефикасно деловање у циљу аутоматизованог прикупљања података, праћења и приказ ситуације, одлучивања, правовремене реализација одлуке и доношења практичних решења,
  - повећање управљачких и безбедносних перформанси PKI апликација које користе софтверске и хардверске криптографске механизме, што редукује трошкове и повећава ниво контроле,
  - могућност коришћења дигиталних сертификата од стране великог броја корисника истовремено, применом Web сервиса.

**Научни и стручни допринос докторске дисертације је:**

Истраживањем, које је спроведено за израду докторске дисертације, даје се научни и стручни допринос.

Научни допринос се огледа у систематизацији сазнања до којих се дошло симулацијом кроз имплементирани сегмент дигиталних сертификата. Потреба за применом квалификованих дигиталних сертификата у Републици Србији се огледа у његовом све већем афирмисању, као и у интензивном развоју елктронских сервиса у електронском пословању.У домаћој литератури ова област није заступљена у довољној мери, па обрада ове теме са теоријског аспекта представља још један допринос ове дисертације.

Као што је већ речено, PKI системи, представљају комбинацију хардверских и софтверских елемената за реализацију функција система са применом јавних кључева, као и правила, процедуре и институције надлежне за њихову примену. Основна функција PKI система је поуздано успостављање дигиталног идентитета свих овлашћених корисника датог IS, специфицираног у облику дигиталног сертификата

Функционалне целине PKI система треба да обезбеде:

- Поверење у једнозначну везу између идентитета овлашћеног субјекта CA и јавног кључа који му је додељен – што се постиже механизмом дигиталног сертификата кога ће потписати CA,

- Највиши криптолошки квалитет јавних и тајних кључева за асиметричне криптографске алгоритме, као и кључева за симетричне криптографске алгоритме,
- Највишу безбедност CA које издаје дигиталне сертификате и опционо.

Задатак ове дисертације био је да представи предности једне од техника SOFT COMPUTING–а, [0, 1]-вредносне логике у односу на класичну {0, 1}-вредносну логику, кроз употребу статистичког алата за дискриминациону анализу.

Идеја да се проширењем класичног приступа {0, 1}-вредносне логике на [0, 1]- вредносну логику и применом истог статистичког апарата могу добити доста бољи резултати предтављала је суштину овог рада. Показало се да неки проблеми нису били решиви класичним приступом, док су решења добијена новим приступом бивала не само квалитетнија, већ и са малим процентом грешке.

Стручни допринос у докторској дисертацији се огледа у апликативном решењу. Програм је написан применом алата "The MathWorks MATLAB®" омогућује упоредни преглед резултата добијених применом класичног {0, 1} вредносног приступа и новог [0, 1] вредносног приступа дискриминационој анализи.

Развијени програм омогућује упоредни преглед резултата добијених применом класичног и новог приступа дискриминационој анализи. Обе анализе обрађивале су исте улазне скупове података. Излазни резултати добијени применом технике SOFT COMPUTING–а пружају бољи увид у посматрану појаву, јер у анализу укључују и логичке комбинације атрибута, а не само атрибуте, као што то чини класичан приступ.

Овом докторском дисертацијом није завршено истраживање утицаја квалификованог електронског сертификата, већ се проширују видици којима се ствара основа за изградњу статистичког модела у он-лајн окружењу. Овој проблематици се мора приступати са нарочитом пажњом око сигурности и аутентичности података који се размењују електронским путем. На ова питања национална тела покушавају да нађу оптималне одговоре, кроз доношење правних аката, у складу са Директивом Европске уније о електронским потписима и Законом о електронском пословању и електронском потпису, и треба да буде акредитовано од стране надлежног органа задуженог за послове акредитације сертификационих тела.

# 9. ЛИТЕРАТУРА


[1] Adams C. , Lloyd S., Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, Addison Wesley, 2002.

[2] Adams C., Lloyd S., Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, Addison-Wesley, 2003.

[3] Adams C., Farrell S., Kause T., Mononen T., Internet X.509 Public Key Infrastructure Certificate Management Protocols, Network Working Group Request for Comments, RFC 4210, September 2005,

[4] Anderson R.L., Bancroft T.A.: Statistical Theory in Research, McGraw-Hill Book Company, Inc., New York, 1952 .

[5] Aldrich, H. E., Organizations Evolving, Sage Publications, Thousand Oaks, California, 2000.

[6] Barari T., Implementing Online Certificate Status Protocol, Available at: http://hosteddocs.ittoolbox.com/TB100104.pdf. ( 12.05.2009.)

[7] Bishop M., An Overview of Computer Security, Addison Wesley, 2005.

[8] Boeyen S., Howes T., Richard P., Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, Network Working Group Request for Comments, RFC 2559, April 1999.

[9] Boeyen S., Howes T., Richard P., Internet X.509 Public Key Infrastructure LDAPv2 Schema, Network Working Group Request for Comments, RFC 2587, June 1999.

[10] Brian Komar, Windows Server 2003 PKI Certificate Security, 2004 .

[11] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, 1996.

[12] Burr W.E., Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations, TWG-98-59, September 1998.

[13] Campbell C.M., Design and Specification of Cryptographic Capabilities, IEEE Computer Society Magazine, v.16, n.6, Nov 1978.

[14] CERT Cordination Center, CERT/CC Statistics 1988-2006, Carnegie Mellon University Available at: http://www.cert.org/stats/cert_stats.html. (15.10.2009.)

[15] CERT, Securing Network Servers, 2000, Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf. (05.05.2009).

[16] Chabaud F., On the Security of Some Crytposystems Based on Error-Correcting Codes, Springer-Verlag, 1995.

[17] Chen L. and Pederson T.P.:New Group Signature Schemes , Springer-Verlag, 1995.

[18] Chokhani S., Ford W., Internet X.509 Public Key Infrastructure Certificate

Policy and Certification Practices Framework, Network Working Group Request for Comments, RFC 2527, May 1999.
[19] Choudhury S., Bhatnager K., Haque W., Public Infrastructure Key Infrastructure Implementation and Design, M&T Books, New York, 2002.
[20] Contini S., Rivest R., at all, The Security of the RC6 Block Cipher, 1998, ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/security.pdf, (17.04.2010.)
[21] Cooper D. A., Model of Certificate Revocation, Computer Security Division National Institute of Standardsand Technology, Available at: http://csrc.nist.gov/pki/documents/acsac99.pdf, (24.10.2010.)
[22] Cooper M. et al., Internet X.509 Public Key Infrastructure: Certification Path Building, Network Working Group Request for Comments, RFC 4158, September 2005.
[23] Cooper D. A., A More Efficient Use of Delta-CRLs, Computer Security Division National Institute of Standards and Technology, Gaithersburg, 2005,Available at: http://csrc.nist.gov/pki/documents/sliding_window.pdf, (07.09.2010.)
[24] Un, C. A. and Cuervo-Cazurraw, A. (2004), 'Strategies for knowledge creation in firms', British Journal of Management 15: S27-41.
[25] Čisar P., Metode otkrivanja malfunkcija internet saobraćaja u elektronskom poslovanju, doktorska disertacija, Ekonomski fakultet, Subotica, 2010.
[26] Daeman J., Cipher and Hash Function Design, Ph.D.Thesis, Katholieke Universiteit Leuven, Mar 95.
[27] Daeman J., Govaerts R., and Vandewalle J., Resynchronization Weaknesses in Synchronous Stream Ciphers, Advanes in Cryptology-EUROCRYPT 93 Proceedings, Springer-Verlag, 1994.
[28] Davies D.W. and Parkin G.I.P., The Average Size of the Key Stream in Output Feedback Encipherment, Cryptography, Proceedings of the Workshop on Cryptography, Burg Feuerstein Germany, March 1982.
[29] Davies D.W. and Parkin G.I.P., The Average Size of the Key Stream in Output Feedback Mode, Advances in Cryptology:Proceedings of Crypto 82, Plenum Press 1983.
[30] Diffie, W., Hellman, M. Multiuser Cryptographic Techniques, IEEE Transactions on Information Theory, November 1976.
[31] Diffie W., Hellman M.: New directions in cryptography, IEEE Trans ,1978.
[32] Djordjević M., :Metode SOFT COMPUTING-a u analizi podataka, Master rad, FON, 2011.
[33] Drucker, P. F., Post-Capitalist Society, Harper Business, 1993.
[34] Dworkin M., Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38a, National Institute of Standards and Technology, December 2001, Available at: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf. (07.12.2010.)

[35] Eastlake D., Jones P., US Secure Hash Algorithm 1 (SHA1), Network Working Group Request for Comments, RFC 3174, 2001, Available at: http://www.ietf.org/rfc/rfc3174. (06.09.2010.)
[36] Zakon o elektronskom potpisu, Službeni glasniki Republike Srbije, broj 135, 2004
[37] FIPS PUB 81, Des modes of operation, Federal Information Processing Standards Publication 81, Available at: http://www.itl.nist.gov/fipspubs/fip81.htm (08.09.2009.)
[38] FIPS 180-1, Secure Hash Standard, Federal Information Processing Standards Publication FIPS PUB 180-1, Computer Systems Laboratory National Institute of Standards and Technology 1995, Available at: http://www.itl.nist.gov/fipspubs/fip180-1.htm (09.02.2010.)
[39] FIPS 186-1, Digital signature standard, U.S. Department Of Commerce/National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS-186-1 with Change Notice 1, 2000, Available at: http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf (11.11.2010.)
[40] FIPS PUB 180-2, Secure Hash Standard, Federal Information Processing Standards Publication FIPS PUB 180-2, National Institute of Standards and Technology, 2002, Available at: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (05.10.2010.)
[41] Gardiner, B, E-Business Security in RAG Order, School of Computing Dublin Institute of Technolog, Ireland, 2003.
[42] Golod A., PKI registratio, Information Security Management Handbook, CRC Press LCC, 2003.
[43] Gisela Meister, Application Interface for Smart Cards as Secure Signature Generation Device, 2002.
[44] Guannela G., Means for and Method for Secret Signalling, U.S.Patent #2, 405, 500, 6 Aug 1946.
[45] Housley R., Hoffman P., Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP, Network Working Group Request for Comments, RFC 2585 May, 1999.
[46] Housley R., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)Profile, Network Working Group Request for Comments, RFC 3280, April 2002.
[47] ISO/IEC 9594-8/ITU-T Recommendation X.509, Information Technology - Open Systems Interconne - ction: The Directory: Authentication Framework, 1997 edition.
[48] Yager R. R., Filev D. "Essential of Fuzzy Modelling and Control", Wiley 1994

[49] John R. Vacca, Public Key Infrastructure: Building Trusted Applications and Web Services, 2004.
[50] Johner H., Fujiwara S., Yeung A. S., at al, .Deploying a Public Key Infrastructure, IBM Redbooks, SG24-5512-00, IBM, 2000. Available at: http://www. ibm.com/redbooks,
[51] Kacprzyk J., "Multistage Fuzzy Control", Wiley 1994
[52] Kostić M., Zaštita podataka u sistemu zvanične statistike – doktorska disertacija, 2006.
[53] Kumar, I., Cryptology, Laguna Hills, CA: Aegean Park Press, 1997.
[54] Klir G. J., Yuan Bo "Fuzzy Sets and Fuzzy Logic – Theory and Applications", Prentice Hall 1995
[55] Kuhn D.R., Hu V. C., Polk W. T., Chang S.-J., Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST Special Publication SP 800-32, National Institute of Standards and Technology, 2001.Available at: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf. (25.04.2011.)
[56] Lok, P., Hung, R.Y., Walsh, P., Wang, P., and Crawford, J. (2005), " An Integrative Framework for Measuring the Extent toWhich Organizational Variables Influence the Success of Process Improvement Programmes" , Journal of Management Studies, Vol.42, No.7, pp.1356-1381.
[57] Linderman, K., Schroeder, R. G., Zaheer, S., Choo, A. S. 2003. Six Sigma: A goaltheoretic perspective. Journal of Operations Management, 21(2): 193-203
[58] Linderman, K., Schroeder, R. G., Choo, A. S. 2006. Six Sigma: The role of goals in improvement teams. Journal of Operations Management, 24(6): 779-790.
[59] Markovic M.,Tehnike zaštite podataka i kriptografski protokoli u savremenim racunarskim mrežama, skripata, Fakultet za poslovnu informatiku, Singidunum, Beograd, 2004.
[60] Markovic M.,Zaštita računarskih i poslovnih sistema,skripata,Fakultet za poslovnu informatiku, Aperion, Banja Luka, 2009.
[61] Marković, M., Djorđević, G., Unkašević, T., 2002, Influence of key length in possible optimization of RSA algorithm implementation on signal processor, in Proc. of ICEST 2002, Oct., 1-4, pp. 23.26.
[62] Marković, M., Đorđević, G., Unkašević, T., 2003, On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length, in Proceedings of WISP 2003, Budapest, Sept. 2003, pp. 73-77.
[63] Matsui M., Linear Cryptanalysis Method for DES cipher (III), 1994
[64] McCullagh A., Caelli W., Non-Repudiation in the Digital Environment, First Monday, volume 5, number 8, August 2000, Available at: http://firstmonday.org/issues/issue5_8/mccullagh/index.html (07.09.2011.)

[65] McNab C., Network Security Assessment, O'Reilly, 2004.
[66] Menezes A., Oorschot van P. C., Vanstone S. A., Handbook of Applied Cryptography, CRC Press, 1997.
[67] Mell P., Kent K., Nusbaum J., Guide to Malware Incident Prevention and Handling, NIST Special Publication SP 800-83, National Institute of Standards and Technology, 2005, Available at: http://csrc.nist.gov/ publications/nistpubs/800-83/SP800-83.pdf
[68] Merkle, R.C. and Hellman, H.E.:On securty of Multiple Encryption, 1981
[69] Moses T., PKI trust models, 2003.
[70] Myers M., Adams C., Solo D., Kemp D., Internet X.509 Certification Request Message Format, Network Working Group Request for Comments, RFC 2511, March 1999
[71] Myers E.D., STU-III-Multilevel Secure Computer Interface, 1994.
[72] NSA, Guide to Securing Microsoft Windows 2000 (including 2000 Server), National Security Agency, Available at: http://nsa1.www.conxion.com/win2k/index.html (10.09.2010.)
[73] Oakland J., Statistical Process Control, Sixth Edition, Elsevier, Great Britain, 2008
[74] Oppliger, R., 1998, Internet and Intranet Security, Artech House, ISBN 0-89006-829.
[75] Oppliger, R., 2000, Security Technologies for the World Wide Web, Artech House, Boston, London
[76] Oppliger R., Security Technologies for the World Wide Web, Second Edition, Artech House, 2003
[77] Otuteye E., Framework for E-Business Information Security Management, University of New Brunswick, Canada, 2002.
[78] Pande P.S., The Six Sigma Way, 2000., McGraw-Hill
[79] Pande P.S., Neuman R.P., and Cavanagu R.R., (2000) The Six Sigma Way, McGraw-Hill
[80] Pande P.S., L Holpp (2001) "What is Six Sigma?" McGraw-Hill Trade.
[81] Pfleeger, C.P., Pfleeger, S.L., Security in Computing, Prentice Hall, Upper Saddle River, New Jersey, 2002.
[82] PKS, Privredna Komora Srbije, Politika Sertifikacije, Kvalifikovani Elektronski Sertifikati, verzija: 1.4.2, Beograd, jul, 2009.
[83] Pleskonić D. Macek N, Djordjević B, Carić M., Sigurnost računarskih sistema i mreža, 2007
[84] Preneel B., Nuttin M., Rijmen V., and Buelens J., Cryptanalysis of the CFB mode of the DES with a Reduced Number of Rounds, Advances in Cryptology-CRYPTO 93, Proceedings, Springer-Verlag, 1994.
[85] Prodanovic R., Ugrožavanje bezbednosti u elektronskom poslovanju, Simpozijum YUINFO 2007, Kopaonik, 2007.
[86] Prodanovic R, Petrovic M, Digitalni sertifikat: nosilac zaštite u

elektronskom poslovanju, SymOrg 2006, Zlatibor, 2006.
[87] Public Key Infrastructure: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, Proceedings, June 16-17, 2008.
[88] Radojičić Z.,Statistički model ocenjivanja na subjektivno procenjenim karakteristikama – doktorska disertacija', 2007.
[89] Radojičić Z., Statističko merenje intenziteta pojava', Magistarski rad, 2001.
[90] Radojević D., New [0,1]-valued logic: A natural generalization of Boolean logic, Yugoslav Journal of OperationalResearch - YUJOR, Belgrade, Vol. 10, No 2, 185-216, 2000.
[91] Radojević D., Interpolative relations and interpolative preference structures, Yugoslav Journal of OperationalResearch - YUJOR , Belgrade, Vol. 15, No 2, 2005.
[92] Radojević D., Logical measure - structure of logical formula, in Technologies for Constructing IntelligentSystems 2: Tools, Springer, pp 417-430, 2002.
[93] Radojević: D., Interpolative realization of Boolean algebra as consistent frame for gradation and/or fuzziness,Studies in Fuzziness and Soft Computing: Forging New Frontiers: Fuzzy Pionee D. Radojević, "Interpolative Relation base for Graduation and/or Fuzziness", Forging New Frontiers: Fuzzy Pioneers II Studies in Fuzziness and Soft Computing, Edits. M.Nikravesh, J. Kacprzyk and L. A. Zadeh, Springer-Verlag, march 2007,
[94] Radojević D., Petrović B. "Uvod u fazi logiku i sisteme", skripta, FON, Beograd 1998-2004
[95] Ramakrishnan, S., Drayer, C., Tsai, P.F., and Srihari, K., Using simulation with design for Six Sigma in a server manufacturing environment, Proceedings of the 2008 Winter Simulation Conference, Miami, USA, 2008.
[96] Rasis D., Gitlow H.S., and Popovich E., "Paper Organizers International: A Fictitious Six Sigma Green Belt Case Study, I", Quality Engineering, 15 (2003) 127-146
[97] Rasis D., Gitlow H.S., and Popovich E., "Paper Organizers International: A Fictitious Six Sigma Green Belt Case Study, II", Quality Engineering, 15 (2003) 259-274.
[98] RFC 3280 "Internet X.509 PKI Certificate and Certificate Revocation List Profile ", 2002.
[99] RFC 3447 "PKI Standard #1: RSA Cryptography Specification V2.1", Feb 2003.
[100] RFC 3739 "Internet X.509 PKI Qualified Certificate Profile", March 2004.
[101] Rescorla, E. SSL and TLS: Designing and Building Secure Systems. Reading, MA: Addison-Wesley, 2001.

[102] Robshaw M.J.B., RC6 and the AES, 2001, Available at:: ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/rc6+aes.pdf, (14.11.2010.)
[103] Rosing M., Implementing Elliptic Curve Cryptography, Manning Publications, 1998
[104] Rivest R.L. et al., The RC6 block cipher,1977,Available at: http://www.secinf.net/cryptography/ The_RC6_Block_Cipher.html.
[105] Rivest R.L., Shamir A., and Adleman L.M., A Method for Obtaining Digital Singatures and Publc-Key Cryptosystems, Communnications of the ACM.v.21, n.2, Feb 1978.
[106] Rivest R.L., Shamir A., and Adleman L.M., On Digital Signatures and Public Key Cryptosystems, MIT Labaratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979
[107] Rivest R.L., The MD5 Message Digest Algorithm, RFC 1321, Apr 1992.
[108] Rivest R.L., Robshaw M.J.B., Sidney R., Yin Y.L., The RC6 Block Cipher , 1998. Available at: www.rsa.com/rsalabs/aes/, (15.02.2011.)
[109] Savage J.E., Some Simple Self-Synchronizing Digital Data Scramblers, Bell System Technical Journal, v.46, n.2, Feb 1967.
[110] Schneier B., One –Way –Hash Functions, Dr.Dobbs Journal, v.16, n.9, Sep, 1991
[111] Schneier B., Applied Cryptography, Second Edition, Protocols, Algorithms and Source Code in C, Joh Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore,1996.
[112] Sertifikaciono Telo, Integrisanog Komorskog Sistema Srbije, Beograd, maj, 2004.
[113] Souppaya M., Harris A., McLarnon M., Selimis N., Guide to Securing Windows 2000 Professional, NIST Special Publication 800-43, National Institute of Standards and Technology, 2002, Available at: http://csrc.nist.gov/itsec/NIST_Win2KPro.pdf (04.03.2010.)
[114] Stallings W., Network and internetwork security:principels and practice, PRENTEICE HALL, 1995 .
[115] Stallings W., Cyptography and Network Security Principles and Practices, Prentice Hall, 2005
[116] Stinson D., Cryptogrophy Theory and Practice, CRC Prress Ins, Boca Ration, Florida, 1996.
[117] TabachnickT.P., Fidell, S.L, : Using Multivarijate Statistics, Cambridge, 1989,Harper....htp://www.urban.csuohio.edu /sanda/syl/803/803s06.pdf
[118] Tracy M., Jansen W., McLarnon M., Guidelines on Securing Public Web Servers, NIST Special Publication 800-44, 2002, National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/drafts.html#sp800-44-version2 (06.05.2010.)
[119] Tuttle S., Ehlenberger A., et al., Understanding LDAP Design and

Implementation, IBM Redbooks, IBM, 2004. Available at: http://www.ibm.com/redbooks

[120] Tsai, C-R., Non-Repudiation In Practice, Citigroup Information Security Office, http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/6.pdf (27.08.2010.)

[121] Vuković N, Statistička analiza, 2000.

[122] Zigon, J.: How to Measure White-Collar Employee Performance. Media, PA: Zigon Performance Group, 1995.

[123] Zigon, J.: Measuring the Hard Stuff: Teams and Other Hard-to-Measure Work President, Zigon Performance Group, www.zigonperf.com , 1998.

[124] Zigon, J.: Performance Measurement Examples—CD-ROM. Media, PA: Zigon Performance Group, 1999.

[125] [http://www.indicators.scot.nhs.uk] (12.11.2009.)

[126] [htp://www.ffiec.gov/pdf/authentication_guidance.pdf] (03.10.2009.)

# ПРИЛОГ

| Tone Number | H.Real | H.Image | e | dri | dir | enimg | bit | sbits |
|---|---|---|---|---|---|---|---|---|
| 0 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 0 | 1 |
| 1 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 1 | 1 |
| 2 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 2 | 1 |
| 3 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 3 | 1 |
| 4 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 4 | 1 |
| 5 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 5 | 1 |
| 6 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 6 | 1 |
| 7 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 7 | 1 |
| 8 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 0 | 2 |
| 9 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 1 | 2 |
| 10 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 2 | 2 |
| 11 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 3 | 2 |
| 12 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 4 | 2 |
| 13 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | #DIV/0! | 5 | 2 |
| 14 | 0.002 | 0.000 | 0.002 | 0.000 | 0.000 | #DIV/0! | 6 | 2 |
| 15 | 0.002 | 0.001 | 0.001 | 2.000 | 0.500 | 1.000 | 7 | 2 |
| 16 | 0.001 | 0.002 | -0.001 | 0.500 | 2.000 | -0.500 | 0 | 3 |
| 17 | 0.000 | 0.004 | -0.004 | 0.000 | 0.000 | -1.000 | 1 | 3 |
| 18 | 0.002 | 0.004 | -0.002 | 0.500 | 2.000 | -0.500 | 2 | 3 |
| 19 | 0.005 | 0.002 | 0.003 | 2.500 | 0.400 | 1.500 | 3 | 3 |
| 20 | 0.005 | 0.001 | 0.004 | 5.000 | 0.200 | 4.000 | 4 | 3 |
| 21 | 0.003 | 0.003 | 0.000 | 1.000 | 1.000 | 0.000 | 5 | 3 |
| 22 | 0.000 | 0.004 | -0.004 | 0.000 | 0.000 | -1.000 | 6 | 3 |
| 23 | 0.001 | 0.003 | -0.002 | 0.333 | 3.000 | -0.667 | 7 | 3 |
| 24 | 0.001 | 0.000 | 0.001 | 0.000 | 0.000 | #DIV/0! | 0 | 4 |
| 25 | 0.001 | 0.000 | 0.001 | 0.000 | 0.000 | #DIV/0! | 1 | 4 |
| 26 | 0.005 | 0.003 | 0.002 | 1.667 | 0.600 | 0.667 | 2 | 4 |
| 27 | 0.003 | 0.012 | -0.009 | 0.250 | 4.000 | -0.750 | 3 | 4 |
| 28 | 0.007 | 0.020 | -0.013 | 0.350 | 2.857 | -0.650 | 4 | 4 |
| 29 | 0.028 | 0.018 | 0.010 | 1.556 | 0.643 | 0.556 | 5 | 4 |
| 30 | 0.050 | 0.001 | 0.049 | 50.000 | 0.020 | 49.000 | 6 | 4 |
| 31 | 0.057 | 0.042 | 0.015 | 1.357 | 0.737 | 0.357 | 7 | 4 |
| 32 | 0.033 | 0.091 | -0.058 | 0.363 | 2.758 | -0.637 | 0 | 5 |
| 33 | 0.028 | 0.127 | -0.099 | 0.220 | 4.536 | -0.780 | 1 | 5 |
| 34 | 0.117 | 0.119 | -0.002 | 0.983 | 1.017 | -0.017 | 2 | 5 |
| 35 | 0.202 | 0.051 | 0.151 | 3.961 | 0.252 | 2.961 | 3 | 5 |
| 36 | 0.239 | 0.071 | 0.168 | 3.366 | 0.297 | 2.366 | 4 | 5 |
| 37 | 0.194 | 0.211 | -0.017 | 0.919 | 1.088 | -0.081 | 5 | 5 |
| 38 | 0.061 | 0.313 | -0.252 | 0.195 | 5.131 | -0.805 | 6 | 5 |
| 39 | 0.125 | 0.320 | -0.195 | 0.391 | 2.560 | -0.609 | 7 | 5 |
| 40 | 0.295 | 0.208 | 0.087 | 1.418 | 0.705 | 0.418 | 0 | 6 |
| 41 | 0.375 | 0.003 | 0.372 | 125.000 | 0.008 | 124.000 | 1 | 6 |
| 42 | 0.314 | 0.221 | 0.093 | 1.421 | 0.704 | 0.421 | 2 | 6 |
| 43 | 0.123 | 0.371 | -0.248 | 0.332 | 3.016 | -0.668 | 3 | 6 |
| 44 | 0.129 | 0.374 | -0.245 | 0.345 | 2.899 | -0.655 | 4 | 6 |
| 45 | 0.336 | 0.217 | 0.119 | 1.548 | 0.646 | 0.548 | 5 | 6 |
| 46 | 0.401 | 0.041 | 0.360 | 9.780 | 0.102 | 8.780 | 6 | 6 |
| 47 | 0.287 | 0.287 | 0.000 | 1.000 | 1.000 | 0.000 | 7 | 6 |
| 48 | 0.038 | 0.406 | -0.368 | 0.094 | 10.684 | -0.906 | 0 | 7 |
| 49 | 0.233 | 0.337 | -0.104 | 0.691 | 1.446 | -0.309 | 1 | 7 |
| 50 | 0.397 | 0.106 | 0.291 | 3.745 | 0.267 | 2.745 | 2 | 7 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 51 | 0.371 | 0.178 | 0.193 | 2.084 | 0.480 | 1.084 | 3 | 7 |
| 52 | 0.164 | 0.379 | -0.215 | 0.433 | 2.311 | -0.567 | 4 | 7 |
| 53 | 0.126 | 0.394 | -0.268 | 0.320 | 3.127 | -0.680 | 5 | 7 |
| 54 | 0.355 | 0.212 | 0.143 | 1.675 | 0.597 | 0.675 | 6 | 7 |
| 55 | 0.407 | 0.077 | 0.330 | 5.286 | 0.189 | 4.286 | 7 | 7 |
| 56 | 0.251 | 0.329 | -0.078 | 0.763 | 1.311 | -0.237 | 0 | 8 |
| 57 | 0.033 | 0.413 | -0.380 | 0.080 | 12.515 | -0.920 | 1 | 8 |
| 58 | 0.302 | 0.283 | 0.019 | 1.067 | 0.937 | 0.067 | 2 | 8 |
| 59 | 0.414 | 0.006 | 0.408 | 69.000 | 0.014 | 68.000 | 3 | 8 |
| 60 | 0.309 | 0.275 | 0.034 | 1.124 | 0.890 | 0.124 | 4 | 8 |
| 61 | 0.041 | 0.411 | -0.370 | 0.100 | 10.024 | -0.900 | 5 | 8 |
| 62 | 0.248 | 0.329 | -0.081 | 0.754 | 1.327 | -0.246 | 6 | 8 |
| 63 | 0.406 | 0.072 | 0.334 | 5.639 | 0.177 | 4.639 | 7 | 8 |
| 64 | 0.346 | 0.224 | 0.122 | 1.545 | 0.647 | 0.545 | 0 | 9 |
| 65 | 0.099 | 0.398 | -0.299 | 0.249 | 4.020 | -0.751 | 1 | 9 |
| 66 | 0.199 | 0.358 | -0.159 | 0.556 | 1.799 | -0.444 | 2 | 9 |
| 67 | 0.390 | 0.123 | 0.267 | 3.171 | 0.315 | 2.171 | 3 | 9 |
| 68 | 0.368 | 0.178 | 0.190 | 2.067 | 0.484 | 1.067 | 4 | 9 |
| 69 | 0.144 | 0.381 | -0.237 | 0.378 | 2.646 | -0.622 | 5 | 9 |
| 70 | 0.157 | 0.375 | -0.218 | 0.419 | 2.389 | -0.581 | 6 | 9 |
| 71 | 0.372 | 0.162 | 0.210 | 2.296 | 0.435 | 1.296 | 7 | 9 |
| 72 | 0.380 | 0.139 | 0.241 | 2.734 | 0.366 | 1.734 | 0 | 10 |
| 73 | 0.177 | 0.363 | -0.186 | 0.488 | 2.051 | -0.512 | 1 | 10 |
| 74 | 0.122 | 0.384 | -0.262 | 0.318 | 3.148 | -0.682 | 2 | 10 |
| 75 | 0.354 | 0.191 | 0.163 | 1.853 | 0.540 | 0.853 | 3 | 10 |
| 76 | 0.386 | 0.108 | 0.278 | 3.574 | 0.280 | 2.574 | 4 | 10 |
| 77 | 0.202 | 0.345 | -0.143 | 0.586 | 1.708 | -0.414 | 5 | 10 |
| 78 | 0.094 | 0.388 | -0.294 | 0.242 | 4.128 | -0.758 | 6 | 10 |
| 79 | 0.337 | 0.212 | 0.125 | 1.590 | 0.629 | 0.590 | 7 | 10 |
| 80 | 0.389 | 0.082 | 0.307 | 4.744 | 0.211 | 3.744 | 0 | 11 |
| 81 | 0.221 | 0.329 | -0.108 | 0.672 | 1.489 | -0.328 | 1 | 11 |
| 82 | 0.071 | 0.389 | -0.318 | 0.183 | 5.479 | -0.817 | 2 | 11 |
| 83 | 0.322 | 0.228 | 0.094 | 1.412 | 0.708 | 0.412 | 3 | 11 |
| 84 | 0.390 | 0.062 | 0.328 | 6.290 | 0.159 | 5.290 | 4 | 11 |
| 85 | 0.235 | 0.316 | -0.081 | 0.744 | 1.345 | -0.256 | 5 | 11 |
| 86 | 0.053 | 0.389 | -0.336 | 0.136 | 7.340 | -0.864 | 6 | 11 |
| 87 | 0.310 | 0.241 | 0.069 | 1.286 | 0.777 | 0.286 | 7 | 11 |
| 88 | 0.389 | 0.045 | 0.344 | 8.644 | 0.116 | 7.644 | 0 | 12 |
| 89 | 0.246 | 0.304 | -0.058 | 0.809 | 1.236 | -0.191 | 1 | 12 |
| 90 | 0.037 | 0.388 | -0.351 | 0.095 | 10.486 | -0.905 | 2 | 12 |
| 91 | 0.299 | 0.249 | 0.050 | 1.201 | 0.833 | 0.201 | 3 | 12 |
| 92 | 0.387 | 0.031 | 0.356 | 12.484 | 0.080 | 11.484 | 4 | 12 |
| 93 | 0.253 | 0.293 | -0.040 | 0.863 | 1.158 | -0.137 | 5 | 12 |
| 94 | 0.025 | 0.386 | -0.361 | 0.065 | 15.440 | -0.935 | 6 | 12 |
| 95 | 0.289 | 0.256 | 0.033 | 1.129 | 0.886 | 0.129 | 7 | 12 |
| 96 | 0.384 | 0.021 | 0.363 | 18.286 | 0.055 | 17.286 | 0 | 13 |
| 97 | 0.258 | 0.284 | -0.026 | 0.908 | 1.101 | -0.092 | 1 | 13 |
| 98 | 0.016 | 0.382 | -0.366 | 0.042 | 23.875 | -0.958 | 2 | 13 |
| 99 | 0.280 | 0.260 | 0.020 | 1.077 | 0.929 | 0.077 | 3 | 13 |
| 100 | 0.380 | 0.012 | 0.368 | 31.667 | 0.032 | 30.667 | 4 | 13 |
| 101 | 0.260 | 0.276 | -0.016 | 0.942 | 1.062 | -0.058 | 5 | 13 |
| 102 | 0.009 | 0.378 | -0.369 | 0.024 | 42.000 | -0.976 | 6 | 13 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 103 | 0.272 | 0.261 | 0.011 | 1.042 | 0.960 | 0.042 | 7 | 13 |
| 104 | 0.375 | 0.006 | 0.369 | 62.500 | 0.016 | 61.500 | 0 | 14 |
| 105 | 0.260 | 0.268 | -0.008 | 0.970 | 1.031 | -0.030 | 1 | 14 |
| 106 | 0.005 | 0.372 | -0.367 | 0.013 | 74.400 | -0.987 | 2 | 14 |
| 107 | 0.265 | 0.259 | 0.006 | 1.023 | 0.977 | 0.023 | 3 | 14 |
| 108 | 0.369 | 0.004 | 0.365 | 92.250 | 0.011 | 91.250 | 4 | 14 |
| 109 | 0.257 | 0.263 | -0.006 | 0.977 | 1.023 | -0.023 | 5 | 14 |
| 110 | 0.004 | 0.366 | -0.362 | 0.011 | 91.500 | -0.989 | 6 | 14 |
| 111 | 0.261 | 0.255 | 0.006 | 1.024 | 0.977 | 0.024 | 7 | 14 |
| 112 | 0.363 | 0.004 | 0.359 | 90.750 | 0.011 | 89.750 | 0 | 15 |
| 113 | 0.252 | 0.259 | -0.007 | 0.973 | 1.028 | -0.027 | 1 | 15 |
| 114 | 0.004 | 0.361 | -0.357 | 0.011 | 90.250 | -0.989 | 2 | 15 |
| 115 | 0.258 | 0.250 | 0.008 | 1.032 | 0.969 | 0.032 | 3 | 15 |
| 116 | 0.358 | 0.006 | 0.352 | 59.667 | 0.017 | 58.667 | 4 | 15 |
| 117 | 0.247 | 0.258 | -0.011 | 0.957 | 1.045 | -0.043 | 5 | 15 |
| 118 | 0.008 | 0.356 | -0.348 | 0.022 | 44.500 | -0.978 | 6 | 15 |
| 119 | 0.257 | 0.244 | 0.013 | 1.053 | 0.949 | 0.053 | 7 | 15 |
| 120 | 0.353 | 0.010 | 0.343 | 35.300 | 0.028 | 34.300 | 0 | 16 |
| 121 | 0.241 | 0.257 | -0.016 | 0.938 | 1.066 | -0.062 | 1 | 16 |
| 122 | 0.012 | 0.351 | -0.339 | 0.034 | 29.250 | -0.966 | 2 | 16 |
| 123 | 0.258 | 0.238 | 0.020 | 1.084 | 0.922 | 0.084 | 3 | 16 |
| 124 | 0.350 | 0.015 | 0.335 | 23.333 | 0.043 | 22.333 | 4 | 16 |
| 125 | 0.235 | 0.258 | -0.023 | 0.911 | 1.098 | -0.089 | 5 | 16 |
| 126 | 0.018 | 0.348 | -0.330 | 0.052 | 19.333 | -0.948 | 6 | 16 |
| 127 | 0.259 | 0.232 | 0.027 | 1.116 | 0.896 | 0.116 | 7 | 16 |
| 128 | 0.347 | 0.020 | 0.327 | 17.350 | 0.058 | 16.350 | 0 | 17 |
| 129 | 0.229 | 0.260 | -0.031 | 0.881 | 1.135 | -0.119 | 1 | 17 |
| 130 | 0.023 | 0.345 | -0.322 | 0.067 | 15.000 | -0.933 | 2 | 17 |
| 131 | 0.261 | 0.226 | 0.035 | 1.155 | 0.866 | 0.155 | 3 | 17 |
| 132 | 0.344 | 0.025 | 0.319 | 13.760 | 0.073 | 12.760 | 4 | 17 |
| 133 | 0.223 | 0.261 | -0.038 | 0.854 | 1.170 | -0.146 | 5 | 17 |
| 134 | 0.028 | 0.342 | -0.314 | 0.082 | 12.214 | -0.918 | 6 | 17 |
| 135 | 0.262 | 0.220 | 0.042 | 1.191 | 0.840 | 0.191 | 7 | 17 |
| 136 | 0.339 | 0.030 | 0.309 | 11.300 | 0.088 | 10.300 | 0 | 18 |
| 137 | 0.217 | 0.262 | -0.045 | 0.828 | 1.207 | -0.172 | 1 | 18 |
| 138 | 0.033 | 0.337 | -0.304 | 0.098 | 10.212 | -0.902 | 2 | 18 |
| 139 | 0.262 | 0.213 | 0.049 | 1.230 | 0.813 | 0.230 | 3 | 18 |
| 140 | 0.335 | 0.036 | 0.299 | 9.306 | 0.107 | 8.306 | 4 | 18 |
| 141 | 0.209 | 0.262 | -0.053 | 0.798 | 1.254 | -0.202 | 5 | 18 |
| 142 | 0.038 | 0.332 | -0.294 | 0.114 | 8.737 | -0.886 | 6 | 18 |
| 143 | 0.262 | 0.205 | 0.057 | 1.278 | 0.782 | 0.278 | 7 | 18 |
| 144 | 0.329 | 0.041 | 0.288 | 8.024 | 0.125 | 7.024 | 0 | 19 |
| 145 | 0.201 | 0.262 | -0.061 | 0.767 | 1.303 | -0.233 | 1 | 19 |
| 146 | 0.044 | 0.326 | -0.282 | 0.135 | 7.409 | -0.865 | 2 | 19 |
| 147 | 0.262 | 0.196 | 0.066 | 1.337 | 0.748 | 0.337 | 3 | 19 |
| 148 | 0.323 | 0.048 | 0.275 | 6.729 | 0.149 | 5.729 | 4 | 19 |
| 149 | 0.191 | 0.263 | -0.072 | 0.726 | 1.377 | -0.274 | 5 | 19 |
| 150 | 0.052 | 0.319 | -0.267 | 0.163 | 6.135 | -0.837 | 6 | 19 |
| 151 | 0.263 | 0.186 | 0.077 | 1.414 | 0.707 | 0.414 | 7 | 19 |
| 152 | 0.315 | 0.056 | 0.259 | 5.625 | 0.178 | 4.625 | 0 | 20 |
| 153 | 0.180 | 0.263 | -0.083 | 0.684 | 1.461 | -0.316 | 1 | 20 |
| 154 | 0.060 | 0.312 | -0.252 | 0.192 | 5.200 | -0.808 | 2 | 20 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 155 | 0.264 | 0.174 | 0.090 | 1.517 | 0.659 | 0.517 | 3 | 20 |
| 156 | 0.308 | 0.065 | 0.243 | 4.738 | 0.211 | 3.738 | 4 | 20 |
| 157 | 0.169 | 0.264 | -0.095 | 0.640 | 1.562 | -0.360 | 5 | 20 |
| 158 | 0.070 | 0.305 | -0.235 | 0.230 | 4.357 | -0.770 | 6 | 20 |
| 159 | 0.265 | 0.163 | 0.102 | 1.626 | 0.615 | 0.626 | 7 | 20 |
| 160 | 0.301 | 0.074 | 0.227 | 4.068 | 0.246 | 3.068 | 0 | 21 |
| 161 | 0.157 | 0.266 | -0.109 | 0.590 | 1.694 | -0.410 | 1 | 21 |
| 162 | 0.079 | 0.298 | -0.219 | 0.265 | 3.772 | -0.735 | 2 | 21 |
| 163 | 0.268 | 0.152 | 0.116 | 1.763 | 0.567 | 0.763 | 3 | 21 |
| 164 | 0.295 | 0.084 | 0.211 | 3.512 | 0.285 | 2.512 | 4 | 21 |
| 165 | 0.146 | 0.269 | -0.123 | 0.543 | 1.842 | -0.457 | 5 | 21 |
| 166 | 0.088 | 0.292 | -0.204 | 0.301 | 3.318 | -0.699 | 6 | 21 |
| 167 | 0.270 | 0.140 | 0.130 | 1.929 | 0.519 | 0.929 | 7 | 21 |
| 168 | 0.288 | 0.093 | 0.195 | 3.097 | 0.323 | 2.097 | 0 | 22 |
| 169 | 0.135 | 0.271 | -0.136 | 0.498 | 2.007 | -0.502 | 1 | 22 |
| 170 | 0.098 | 0.285 | -0.187 | 0.344 | 2.908 | -0.656 | 2 | 22 |
| 171 | 0.271 | 0.130 | 0.141 | 2.085 | 0.480 | 1.085 | 3 | 22 |
| 172 | 0.282 | 0.102 | 0.180 | 2.765 | 0.362 | 1.765 | 4 | 22 |
| 173 | 0.124 | 0.272 | -0.148 | 0.456 | 2.194 | -0.544 | 5 | 22 |
| 174 | 0.106 | 0.279 | -0.173 | 0.380 | 2.632 | -0.620 | 6 | 22 |
| 175 | 0.272 | 0.119 | 0.153 | 2.286 | 0.438 | 1.286 | 7 | 22 |
| 176 | 0.275 | 0.110 | 0.165 | 2.500 | 0.400 | 1.500 | 0 | 23 |
| 177 | 0.113 | 0.273 | -0.160 | 0.414 | 2.416 | -0.586 | 1 | 23 |
| 178 | 0.114 | 0.271 | -0.157 | 0.421 | 2.377 | -0.579 | 2 | 23 |
| 179 | 0.272 | 0.108 | 0.164 | 2.519 | 0.397 | 1.519 | 3 | 23 |
| 180 | 0.267 | 0.118 | 0.149 | 2.263 | 0.442 | 1.263 | 4 | 23 |
| 181 | 0.102 | 0.272 | -0.170 | 0.375 | 2.667 | -0.625 | 5 | 23 |
| 182 | 0.121 | 0.263 | -0.142 | 0.460 | 2.174 | -0.540 | 6 | 23 |
| 183 | 0.272 | 0.097 | 0.175 | 2.804 | 0.357 | 1.804 | 7 | 23 |
| 184 | 0.259 | 0.125 | 0.134 | 2.072 | 0.483 | 1.072 | 0 | 24 |
| 185 | 0.091 | 0.271 | -0.180 | 0.336 | 2.978 | -0.664 | 1 | 24 |
| 186 | 0.129 | 0.254 | -0.125 | 0.508 | 1.969 | -0.492 | 2 | 24 |
| 187 | 0.271 | 0.085 | 0.186 | 3.188 | 0.314 | 2.188 | 3 | 24 |
| 188 | 0.249 | 0.132 | 0.117 | 1.886 | 0.530 | 0.886 | 4 | 24 |
| 189 | 0.079 | 0.270 | -0.191 | 0.293 | 3.418 | -0.707 | 5 | 24 |
| 190 | 0.137 | 0.244 | -0.107 | 0.561 | 1.781 | -0.439 | 6 | 24 |
| 191 | 0.269 | 0.073 | 0.196 | 3.685 | 0.271 | 2.685 | 7 | 24 |
| 192 | 0.239 | 0.140 | 0.099 | 1.707 | 0.586 | 0.707 | 0 | 25 |
| 193 | 0.067 | 0.268 | -0.201 | 0.250 | 4.000 | -0.750 | 1 | 25 |
| 194 | 0.144 | 0.235 | -0.091 | 0.613 | 1.632 | -0.387 | 2 | 25 |
| 195 | 0.267 | 0.060 | 0.207 | 4.450 | 0.225 | 3.450 | 3 | 25 |
| 196 | 0.229 | 0.148 | 0.081 | 1.547 | 0.646 | 0.547 | 4 | 25 |
| 197 | 0.054 | 0.267 | -0.213 | 0.202 | 4.944 | -0.798 | 5 | 25 |
| 198 | 0.152 | 0.224 | -0.072 | 0.679 | 1.474 | -0.321 | 6 | 25 |
| 199 | 0.266 | 0.047 | 0.219 | 5.660 | 0.177 | 4.660 | 7 | 25 |
| 200 | 0.219 | 0.156 | 0.063 | 1.404 | 0.712 | 0.404 | 0 | 26 |
| 201 | 0.041 | 0.265 | -0.224 | 0.155 | 6.463 | -0.845 | 1 | 26 |
| 202 | 0.161 | 0.214 | -0.053 | 0.752 | 1.329 | -0.248 | 2 | 26 |
| 203 | 0.264 | 0.034 | 0.230 | 7.765 | 0.129 | 6.765 | 3 | 26 |
| 204 | 0.209 | 0.164 | 0.045 | 1.274 | 0.785 | 0.274 | 4 | 26 |
| 205 | 0.028 | 0.263 | -0.235 | 0.106 | 9.393 | -0.894 | 5 | 26 |
| 206 | 0.168 | 0.204 | -0.036 | 0.824 | 1.214 | -0.176 | 6 | 26 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 207 | 0.263 | 0.022 | 0.241 | 11.955 | 0.084 | 10.955 | 7 | 26 |
| 208 | 0.199 | 0.172 | 0.027 | 1.157 | 0.864 | 0.157 | 0 | 27 |
| 209 | 0.016 | 0.262 | -0.246 | 0.061 | 16.375 | -0.939 | 1 | 27 |
| 210 | 0.175 | 0.194 | -0.019 | 0.902 | 1.109 | -0.098 | 2 | 27 |
| 211 | 0.261 | 0.010 | 0.251 | 26.100 | 0.038 | 25.100 | 3 | 27 |
| 212 | 0.189 | 0.178 | 0.011 | 1.062 | 0.942 | 0.062 | 4 | 27 |
| 213 | 0.005 | 0.260 | -0.255 | 0.019 | 52.000 | -0.981 | 5 | 27 |
| 214 | 0.182 | 0.185 | -0.003 | 0.984 | 1.016 | -0.016 | 6 | 27 |
| 215 | 0.258 | 0.000 | 0.258 | 0.000 | 0.000 | #DIV/0! | 7 | 27 |
| 216 | 0.180 | 0.184 | -0.004 | 0.978 | 1.022 | -0.022 | 0 | 28 |
| 217 | 0.005 | 0.256 | -0.251 | 0.020 | 51.200 | -0.980 | 1 | 28 |
| 218 | 0.187 | 0.175 | 0.012 | 1.069 | 0.936 | 0.069 | 2 | 28 |
| 219 | 0.255 | 0.010 | 0.245 | 25.500 | 0.039 | 24.500 | 3 | 28 |
| 220 | 0.170 | 0.189 | -0.019 | 0.899 | 1.112 | -0.101 | 4 | 28 |
| 221 | 0.016 | 0.253 | -0.237 | 0.063 | 15.813 | -0.937 | 5 | 28 |
| 222 | 0.191 | 0.164 | 0.027 | 1.165 | 0.859 | 0.165 | 6 | 28 |
| 223 | 0.250 | 0.021 | 0.229 | 11.905 | 0.084 | 10.905 | 7 | 28 |
| 224 | 0.159 | 0.193 | -0.034 | 0.824 | 1.214 | -0.176 | 0 | 29 |
| 225 | 0.026 | 0.248 | -0.222 | 0.105 | 9.538 | -0.895 | 1 | 29 |
| 226 | 0.195 | 0.153 | 0.042 | 1.275 | 0.785 | 0.275 | 2 | 29 |
| 227 | 0.245 | 0.032 | 0.213 | 7.656 | 0.131 | 6.656 | 3 | 29 |
| 228 | 0.148 | 0.196 | -0.048 | 0.755 | 1.324 | -0.245 | 4 | 29 |
| 229 | 0.037 | 0.242 | -0.205 | 0.153 | 6.541 | -0.847 | 5 | 29 |
| 230 | 0.198 | 0.142 | 0.056 | 1.394 | 0.717 | 0.394 | 6 | 29 |
| 231 | 0.239 | 0.042 | 0.197 | 5.690 | 0.176 | 4.690 | 7 | 29 |
| 232 | 0.136 | 0.200 | -0.064 | 0.680 | 1.471 | -0.320 | 0 | 30 |
| 233 | 0.047 | 0.236 | -0.189 | 0.199 | 5.021 | -0.801 | 1 | 30 |
| 234 | 0.201 | 0.130 | 0.071 | 1.546 | 0.647 | 0.546 | 2 | 30 |
| 235 | 0.233 | 0.053 | 0.180 | 4.396 | 0.227 | 3.396 | 3 | 30 |
| 236 | 0.124 | 0.203 | -0.079 | 0.611 | 1.637 | -0.389 | 4 | 30 |
| 237 | 0.058 | 0.230 | -0.172 | 0.252 | 3.966 | -0.748 | 5 | 30 |
| 238 | 0.204 | 0.117 | 0.087 | 1.744 | 0.574 | 0.744 | 6 | 30 |
| 239 | 0.226 | 0.063 | 0.163 | 3.587 | 0.279 | 2.587 | 7 | 30 |
| 240 | 0.111 | 0.206 | -0.095 | 0.539 | 1.856 | -0.461 | 0 | 31 |
| 241 | 0.069 | 0.223 | -0.154 | 0.309 | 3.232 | -0.691 | 1 | 31 |
| 242 | 0.207 | 0.105 | 0.102 | 1.971 | 0.507 | 0.971 | 2 | 31 |
| 243 | 0.220 | 0.074 | 0.146 | 2.973 | 0.336 | 1.973 | 3 | 31 |
| 244 | 0.099 | 0.208 | -0.109 | 0.476 | 2.101 | -0.524 | 4 | 31 |
| 245 | 0.079 | 0.216 | -0.137 | 0.366 | 2.734 | -0.634 | 5 | 31 |
| 246 | 0.210 | 0.093 | 0.117 | 2.258 | 0.443 | 1.258 | 6 | 31 |
| 247 | 0.213 | 0.084 | 0.129 | 2.536 | 0.394 | 1.536 | 7 | 31 |
| 248 | 0.087 | 0.210 | -0.123 | 0.414 | 2.414 | -0.586 | 0 | 32 |
| 249 | 0.088 | 0.209 | -0.121 | 0.421 | 2.375 | -0.579 | 1 | 32 |
| 250 | 0.211 | 0.082 | 0.129 | 2.573 | 0.389 | 1.573 | 2 | 32 |
| 251 | 0.206 | 0.093 | 0.113 | 2.215 | 0.451 | 1.215 | 3 | 32 |
| 252 | 0.076 | 0.212 | -0.136 | 0.358 | 2.789 | -0.642 | 4 | 32 |
| 253 | 0.098 | 0.202 | -0.104 | 0.485 | 2.061 | -0.515 | 5 | 32 |
| 254 | 0.212 | 0.070 | 0.142 | 3.029 | 0.330 | 2.029 | 6 | 32 |
| 255 | 0.198 | 0.102 | 0.096 | 1.941 | 0.515 | 0.941 | 7 | 32 |
| 256 | 0.065 | 0.213 | -0.148 | 0.305 | 3.277 | -0.695 | 0 | 33 |
| 257 | 0.106 | 0.195 | -0.089 | 0.544 | 1.840 | -0.456 | 1 | 33 |
| 258 | 0.213 | 0.059 | 0.154 | 3.610 | 0.277 | 2.610 | 2 | 33 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 259 | 0.191 | 0.110 | 0.081 | 1.736 | 0.576 | 0.736 | 3 | 33 |
| 260 | 0.053 | 0.213 | -0.160 | 0.249 | 4.019 | -0.751 | 4 | 33 |
| 261 | 0.114 | 0.187 | -0.073 | 0.610 | 1.640 | -0.390 | 5 | 33 |
| 262 | 0.213 | 0.048 | 0.165 | 4.438 | 0.225 | 3.438 | 6 | 33 |
| 263 | 0.182 | 0.118 | 0.064 | 1.542 | 0.648 | 0.542 | 7 | 33 |
| 264 | 0.043 | 0.212 | -0.169 | 0.203 | 4.930 | -0.797 | 0 | 34 |
| 265 | 0.122 | 0.178 | -0.056 | 0.685 | 1.459 | -0.315 | 1 | 34 |
| 266 | 0.211 | 0.036 | 0.175 | 5.861 | 0.171 | 4.861 | 2 | 34 |
| 267 | 0.174 | 0.125 | 0.049 | 1.392 | 0.718 | 0.392 | 3 | 34 |
| 268 | 0.031 | 0.211 | -0.180 | 0.147 | 6.806 | -0.853 | 4 | 34 |
| 269 | 0.129 | 0.168 | -0.039 | 0.768 | 1.302 | -0.232 | 5 | 34 |
| 270 | 0.210 | 0.024 | 0.186 | 8.750 | 0.114 | 7.750 | 6 | 34 |
| 271 | 0.164 | 0.132 | 0.032 | 1.242 | 0.805 | 0.242 | 7 | 34 |
| 272 | 0.019 | 0.209 | -0.190 | 0.091 | 11.000 | -0.909 | 0 | 35 |
| 273 | 0.136 | 0.159 | -0.023 | 0.855 | 1.169 | -0.145 | 1 | 35 |
| 274 | 0.208 | 0.013 | 0.195 | 16.000 | 0.063 | 15.000 | 2 | 35 |
| 275 | 0.154 | 0.139 | 0.015 | 1.108 | 0.903 | 0.108 | 3 | 35 |
| 276 | 0.007 | 0.206 | -0.199 | 0.034 | 29.429 | -0.966 | 4 | 35 |
| 277 | 0.142 | 0.149 | -0.007 | 0.953 | 1.049 | -0.047 | 5 | 35 |
| 278 | 0.205 | 0.001 | 0.204 | 205.000 | 0.005 | 204.000 | 6 | 35 |
| 279 | 0.144 | 0.145 | -0.001 | 0.993 | 1.007 | -0.007 | 7 | 35 |
| 280 | 0.003 | 0.204 | -0.201 | 0.015 | 68.000 | -0.985 | 0 | 36 |
| 281 | 0.148 | 0.139 | 0.009 | 1.065 | 0.939 | 0.065 | 1 | 36 |
| 282 | 0.203 | 0.009 | 0.194 | 22.556 | 0.044 | 21.556 | 2 | 36 |
| 283 | 0.134 | 0.152 | -0.018 | 0.882 | 1.134 | -0.118 | 3 | 36 |
| 284 | 0.015 | 0.201 | -0.186 | 0.075 | 13.400 | -0.925 | 4 | 36 |
| 285 | 0.154 | 0.130 | 0.024 | 1.185 | 0.844 | 0.185 | 5 | 36 |
| 286 | 0.200 | 0.020 | 0.180 | 10.000 | 0.100 | 9.000 | 6 | 36 |
| 287 | 0.124 | 0.157 | -0.033 | 0.790 | 1.266 | -0.210 | 7 | 36 |
| 288 | 0.025 | 0.198 | -0.173 | 0.126 | 7.920 | -0.874 | 0 | 37 |
| 289 | 0.160 | 0.120 | 0.040 | 1.333 | 0.750 | 0.333 | 1 | 37 |
| 290 | 0.196 | 0.030 | 0.166 | 6.533 | 0.153 | 5.533 | 2 | 37 |
| 291 | 0.115 | 0.162 | -0.047 | 0.710 | 1.409 | -0.290 | 3 | 37 |
| 292 | 0.036 | 0.195 | -0.159 | 0.185 | 5.417 | -0.815 | 4 | 37 |
| 293 | 0.164 | 0.109 | 0.055 | 1.505 | 0.665 | 0.505 | 5 | 37 |
| 294 | 0.193 | 0.041 | 0.152 | 4.707 | 0.212 | 3.707 | 6 | 37 |
| 295 | 0.105 | 0.166 | -0.061 | 0.633 | 1.581 | -0.367 | 7 | 37 |
| 296 | 0.046 | 0.190 | -0.144 | 0.242 | 4.130 | -0.758 | 0 | 38 |
| 297 | 0.168 | 0.100 | 0.068 | 1.680 | 0.595 | 0.680 | 1 | 38 |
| 298 | 0.188 | 0.050 | 0.138 | 3.760 | 0.266 | 2.760 | 2 | 38 |
| 299 | 0.095 | 0.170 | -0.075 | 0.559 | 1.789 | -0.441 | 3 | 38 |
| 300 | 0.055 | 0.186 | -0.131 | 0.296 | 3.382 | -0.704 | 4 | 38 |
| 301 | 0.171 | 0.089 | 0.082 | 1.921 | 0.520 | 0.921 | 5 | 38 |
| 302 | 0.183 | 0.060 | 0.123 | 3.050 | 0.328 | 2.050 | 6 | 38 |
| 303 | 0.085 | 0.173 | -0.088 | 0.491 | 2.035 | -0.509 | 7 | 38 |
| 304 | 0.063 | 0.181 | -0.118 | 0.348 | 2.873 | -0.652 | 0 | 39 |
| 305 | 0.173 | 0.079 | 0.094 | 2.190 | 0.457 | 1.190 | 1 | 39 |
| 306 | 0.178 | 0.068 | 0.110 | 2.618 | 0.382 | 1.618 | 2 | 39 |
| 307 | 0.075 | 0.174 | -0.099 | 0.431 | 2.320 | -0.569 | 3 | 39 |
| 308 | 0.072 | 0.175 | -0.103 | 0.411 | 2.431 | -0.589 | 4 | 39 |
| 309 | 0.175 | 0.069 | 0.106 | 2.536 | 0.394 | 1.536 | 5 | 39 |
| 310 | 0.171 | 0.077 | 0.094 | 2.221 | 0.450 | 1.221 | 6 | 39 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 311 | 0.064 | 0.176 | -0.112 | 0.364 | 2.750 | -0.636 | 7 | 39 |
| 312 | 0.081 | 0.168 | -0.087 | 0.482 | 2.074 | -0.518 | 0 | 40 |
| 313 | 0.176 | 0.059 | 0.117 | 2.983 | 0.335 | 1.983 | 1 | 40 |
| 314 | 0.165 | 0.085 | 0.080 | 1.941 | 0.515 | 0.941 | 2 | 40 |
| 315 | 0.054 | 0.177 | -0.123 | 0.305 | 3.278 | -0.695 | 3 | 40 |
| 316 | 0.088 | 0.161 | -0.073 | 0.547 | 1.830 | -0.453 | 4 | 40 |
| 317 | 0.177 | 0.048 | 0.129 | 3.688 | 0.271 | 2.688 | 5 | 40 |
| 318 | 0.158 | 0.093 | 0.065 | 1.699 | 0.589 | 0.699 | 6 | 40 |
| 319 | 0.043 | 0.177 | -0.134 | 0.243 | 4.116 | -0.757 | 7 | 40 |
| 320 | 0.097 | 0.154 | -0.057 | 0.630 | 1.588 | -0.370 | 0 | 41 |
| 321 | 0.177 | 0.038 | 0.139 | 4.658 | 0.215 | 3.658 | 1 | 41 |
| 322 | 0.151 | 0.100 | 0.051 | 1.510 | 0.662 | 0.510 | 2 | 41 |
| 323 | 0.033 | 0.177 | -0.144 | 0.186 | 5.364 | -0.814 | 3 | 41 |
| 324 | 0.103 | 0.147 | -0.044 | 0.701 | 1.427 | -0.299 | 4 | 41 |
| 325 | 0.178 | 0.028 | 0.150 | 6.357 | 0.157 | 5.357 | 5 | 41 |
| 326 | 0.143 | 0.107 | 0.036 | 1.336 | 0.748 | 0.336 | 6 | 41 |
| 327 | 0.023 | 0.177 | -0.154 | 0.130 | 7.696 | -0.870 | 7 | 41 |
| 328 | 0.110 | 0.139 | -0.029 | 0.791 | 1.264 | -0.209 | 0 | 42 |
| 329 | 0.177 | 0.018 | 0.159 | 9.833 | 0.102 | 8.833 | 1 | 42 |
| 330 | 0.136 | 0.114 | 0.022 | 1.193 | 0.838 | 0.193 | 2 | 42 |
| 331 | 0.013 | 0.177 | -0.164 | 0.073 | 13.615 | -0.927 | 3 | 42 |
| 332 | 0.117 | 0.132 | -0.015 | 0.886 | 1.128 | -0.114 | 4 | 42 |
| 333 | 0.175 | 0.008 | 0.167 | 21.875 | 0.046 | 20.875 | 5 | 42 |
| 334 | 0.128 | 0.120 | 0.008 | 1.067 | 0.938 | 0.067 | 6 | 42 |
| 335 | 0.003 | 0.175 | -0.172 | 0.017 | 58.333 | -0.983 | 7 | 42 |
| 336 | 0.122 | 0.124 | -0.002 | 0.984 | 1.016 | -0.016 | 0 | 43 |
| 337 | 0.174 | 0.001 | 0.173 | 174.000 | 0.006 | 173.000 | 1 | 43 |
| 338 | 0.120 | 0.125 | -0.005 | 0.960 | 1.042 | -0.040 | 2 | 43 |
| 339 | 0.006 | 0.173 | -0.167 | 0.035 | 28.833 | -0.965 | 3 | 43 |
| 340 | 0.128 | 0.116 | 0.012 | 1.103 | 0.906 | 0.103 | 4 | 43 |
| 341 | 0.171 | 0.011 | 0.160 | 15.545 | 0.064 | 14.545 | 5 | 43 |
| 342 | 0.111 | 0.130 | -0.019 | 0.854 | 1.171 | -0.146 | 6 | 43 |
| 343 | 0.015 | 0.171 | -0.156 | 0.088 | 11.400 | -0.912 | 7 | 43 |
| 344 | 0.132 | 0.107 | 0.025 | 1.234 | 0.811 | 0.234 | 0 | 44 |
| 345 | 0.169 | 0.020 | 0.149 | 8.450 | 0.118 | 7.450 | 1 | 44 |
| 346 | 0.103 | 0.135 | -0.032 | 0.763 | 1.311 | -0.237 | 2 | 44 |
| 347 | 0.024 | 0.167 | -0.143 | 0.144 | 6.958 | -0.856 | 3 | 44 |
| 348 | 0.137 | 0.098 | 0.039 | 1.398 | 0.715 | 0.398 | 4 | 44 |
| 349 | 0.166 | 0.029 | 0.137 | 5.724 | 0.175 | 4.724 | 5 | 44 |
| 350 | 0.094 | 0.139 | -0.045 | 0.676 | 1.479 | -0.324 | 6 | 44 |
| 351 | 0.034 | 0.164 | -0.130 | 0.207 | 4.824 | -0.793 | 7 | 44 |
| 352 | 0.141 | 0.089 | 0.052 | 1.584 | 0.631 | 0.584 | 0 | 45 |
| 353 | 0.162 | 0.038 | 0.124 | 4.263 | 0.235 | 3.263 | 1 | 45 |
| 354 | 0.085 | 0.143 | -0.058 | 0.594 | 1.682 | -0.406 | 2 | 45 |
| 355 | 0.043 | 0.161 | -0.118 | 0.267 | 3.744 | -0.733 | 3 | 45 |
| 356 | 0.145 | 0.081 | 0.064 | 1.790 | 0.559 | 0.790 | 4 | 45 |
| 357 | 0.159 | 0.047 | 0.112 | 3.383 | 0.296 | 2.383 | 5 | 45 |
| 358 | 0.076 | 0.146 | -0.070 | 0.521 | 1.921 | -0.479 | 6 | 45 |
| 359 | 0.051 | 0.157 | -0.106 | 0.325 | 3.078 | -0.675 | 7 | 45 |
| 360 | 0.148 | 0.072 | 0.076 | 2.056 | 0.486 | 1.056 | 0 | 46 |
| 361 | 0.155 | 0.056 | 0.099 | 2.768 | 0.361 | 1.768 | 1 | 46 |
| 362 | 0.068 | 0.150 | -0.082 | 0.453 | 2.206 | -0.547 | 2 | 46 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 363 | 0.059 | 0.152 | -0.093 | 0.388 | 2.576 | -0.612 | 3 | 46 |
| 364 | 0.151 | 0.063 | 0.088 | 2.397 | 0.417 | 1.397 | 4 | 46 |
| 365 | 0.150 | 0.064 | 0.086 | 2.344 | 0.427 | 1.344 | 5 | 46 |
| 366 | 0.059 | 0.152 | -0.093 | 0.388 | 2.576 | -0.612 | 6 | 46 |
| 367 | 0.067 | 0.148 | -0.081 | 0.453 | 2.209 | -0.547 | 7 | 46 |
| 368 | 0.153 | 0.055 | 0.098 | 2.782 | 0.359 | 1.782 | 0 | 47 |
| 369 | 0.146 | 0.071 | 0.075 | 2.056 | 0.486 | 1.056 | 1 | 47 |
| 370 | 0.050 | 0.154 | -0.104 | 0.325 | 3.080 | -0.675 | 2 | 47 |
| 371 | 0.074 | 0.143 | -0.069 | 0.517 | 1.932 | -0.483 | 3 | 47 |
| 372 | 0.154 | 0.046 | 0.108 | 3.348 | 0.299 | 2.348 | 4 | 47 |
| 373 | 0.141 | 0.078 | 0.063 | 1.808 | 0.553 | 0.808 | 5 | 47 |
| 374 | 0.042 | 0.155 | -0.113 | 0.271 | 3.690 | -0.729 | 6 | 47 |
| 375 | 0.081 | 0.138 | -0.057 | 0.587 | 1.704 | -0.413 | 7 | 47 |
| 376 | 0.155 | 0.037 | 0.118 | 4.189 | 0.239 | 3.189 | 0 | 48 |
| 377 | 0.135 | 0.084 | 0.051 | 1.607 | 0.622 | 0.607 | 1 | 48 |
| 378 | 0.033 | 0.155 | -0.122 | 0.213 | 4.697 | -0.787 | 2 | 48 |
| 379 | 0.087 | 0.132 | -0.045 | 0.659 | 1.517 | -0.341 | 3 | 48 |
| 380 | 0.155 | 0.029 | 0.126 | 5.345 | 0.187 | 4.345 | 4 | 48 |
| 381 | 0.129 | 0.090 | 0.039 | 1.433 | 0.698 | 0.433 | 5 | 48 |
| 382 | 0.024 | 0.155 | -0.131 | 0.155 | 6.458 | -0.845 | 6 | 48 |
| 383 | 0.093 | 0.126 | -0.033 | 0.738 | 1.355 | -0.262 | 7 | 48 |
| 384 | 0.155 | 0.020 | 0.135 | 7.750 | 0.129 | 6.750 | 0 | 49 |
| 385 | 0.122 | 0.096 | 0.026 | 1.271 | 0.787 | 0.271 | 1 | 49 |
| 386 | 0.016 | 0.154 | -0.138 | 0.104 | 9.625 | -0.896 | 2 | 49 |
| 387 | 0.099 | 0.119 | -0.020 | 0.832 | 1.202 | -0.168 | 3 | 49 |
| 388 | 0.154 | 0.012 | 0.142 | 12.833 | 0.078 | 11.833 | 4 | 49 |
| 389 | 0.115 | 0.101 | 0.014 | 1.139 | 0.878 | 0.139 | 5 | 49 |
| 390 | 0.008 | 0.153 | -0.145 | 0.052 | 19.125 | -0.948 | 6 | 49 |
| 391 | 0.104 | 0.112 | -0.008 | 0.929 | 1.077 | -0.071 | 7 | 49 |
| 392 | 0.152 | 0.003 | 0.149 | 50.667 | 0.020 | 49.667 | 0 | 50 |
| 393 | 0.109 | 0.107 | 0.002 | 1.019 | 0.982 | 0.019 | 1 | 50 |
| 394 | 0.000 | 0.152 | -0.152 | 0.000 | 0.000 | -1.000 | 2 | 50 |
| 395 | 0.109 | 0.105 | 0.004 | 1.038 | 0.963 | 0.038 | 3 | 50 |
| 396 | 0.151 | 0.004 | 0.147 | 37.750 | 0.026 | 36.750 | 4 | 50 |
| 397 | 0.102 | 0.111 | -0.009 | 0.919 | 1.088 | -0.081 | 5 | 50 |
| 398 | 0.008 | 0.150 | -0.142 | 0.053 | 18.750 | -0.947 | 6 | 50 |
| 399 | 0.114 | 0.098 | 0.016 | 1.163 | 0.860 | 0.163 | 7 | 50 |
| 400 | 0.149 | 0.014 | 0.135 | 10.643 | 0.094 | 9.643 | 0 | 51 |
| 401 | 0.095 | 0.117 | -0.022 | 0.812 | 1.232 | -0.188 | 1 | 51 |
| 402 | 0.015 | 0.147 | -0.132 | 0.102 | 9.800 | -0.898 | 2 | 51 |
| 403 | 0.117 | 0.092 | 0.025 | 1.272 | 0.786 | 0.272 | 3 | 51 |
| 404 | 0.147 | 0.019 | 0.128 | 7.737 | 0.129 | 6.737 | 4 | 51 |
| 405 | 0.085 | 0.121 | -0.036 | 0.702 | 1.424 | -0.298 | 5 | 51 |
| 406 | 0.023 | 0.146 | -0.123 | 0.158 | 6.348 | -0.842 | 6 | 51 |
| 407 | 0.125 | 0.084 | 0.041 | 1.488 | 0.672 | 0.488 | 7 | 51 |
| 408 | 0.139 | 0.024 | 0.115 | 5.792 | 0.173 | 4.792 | 0 | 52 |
| 409 | 0.079 | 0.125 | -0.046 | 0.632 | 1.582 | -0.368 | 1 | 52 |
| 410 | 0.029 | 0.140 | -0.111 | 0.207 | 4.828 | -0.793 | 2 | 52 |
| 411 | 0.131 | 0.074 | 0.057 | 1.770 | 0.565 | 0.770 | 3 | 52 |
| 412 | 0.148 | 0.043 | 0.105 | 3.442 | 0.291 | 2.442 | 4 | 52 |
| 413 | 0.068 | 0.131 | -0.063 | 0.519 | 1.926 | -0.481 | 5 | 52 |
| 414 | 0.043 | 0.142 | -0.099 | 0.303 | 3.302 | -0.697 | 6 | 52 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 415 | 0.149 | 0.077 | 0.072 | 1.935 | 0.517 | 0.935 | 7 | 52 |
| 416 | 0.143 | 0.038 | 0.105 | 3.763 | 0.266 | 2.763 | 0 | 53 |
| 417 | 0.069 | 0.122 | -0.053 | 0.566 | 1.768 | -0.434 | 1 | 53 |
| 418 | 0.035 | 0.140 | -0.105 | 0.250 | 4.000 | -0.750 | 2 | 53 |
| 419 | 0.101 | 0.067 | 0.034 | 1.507 | 0.663 | 0.507 | 3 | 53 |
| 420 | 0.133 | 0.032 | 0.101 | 4.156 | 0.241 | 3.156 | 4 | 53 |
| 421 | 0.065 | 0.114 | -0.049 | 0.570 | 1.754 | -0.430 | 5 | 53 |
| 422 | 0.053 | 0.137 | -0.084 | 0.387 | 2.585 | -0.613 | 6 | 53 |
| 423 | 0.117 | 0.050 | 0.067 | 2.340 | 0.427 | 1.340 | 7 | 53 |
| 424 | 0.137 | 0.071 | 0.066 | 1.930 | 0.518 | 0.930 | 0 | 54 |
| 425 | 0.040 | 0.110 | -0.070 | 0.364 | 2.750 | -0.636 | 1 | 54 |
| 426 | 0.063 | 0.133 | -0.070 | 0.474 | 2.111 | -0.526 | 2 | 54 |
| 427 | 0.147 | 0.054 | 0.093 | 2.722 | 0.367 | 1.722 | 3 | 54 |
| 428 | 0.141 | 0.055 | 0.086 | 2.564 | 0.390 | 1.564 | 4 | 54 |
| 429 | 0.046 | 0.121 | -0.075 | 0.380 | 2.630 | -0.620 | 5 | 54 |
| 430 | 0.059 | 0.108 | -0.049 | 0.546 | 1.831 | -0.454 | 6 | 54 |
| 431 | 0.136 | 0.061 | 0.075 | 2.230 | 0.449 | 1.230 | 7 | 54 |
| 432 | 0.117 | 0.073 | 0.044 | 1.603 | 0.624 | 0.603 | 0 | 55 |
| 433 | 0.028 | 0.149 | -0.121 | 0.188 | 5.321 | -0.812 | 1 | 55 |
| 434 | 0.066 | 0.112 | -0.046 | 0.589 | 1.697 | -0.411 | 2 | 55 |
| 435 | 0.144 | 0.031 | 0.113 | 4.645 | 0.215 | 3.645 | 3 | 55 |
| 436 | 0.081 | 0.089 | -0.008 | 0.910 | 1.099 | -0.090 | 4 | 55 |
| 437 | 0.029 | 0.129 | -0.100 | 0.225 | 4.448 | -0.775 | 5 | 55 |
| 438 | 0.077 | 0.131 | -0.054 | 0.588 | 1.701 | -0.412 | 6 | 55 |
| 439 | 0.141 | 0.011 | 0.130 | 12.818 | 0.078 | 11.818 | 7 | 55 |
| 440 | 0.104 | 0.089 | 0.015 | 1.169 | 0.856 | 0.169 | 0 | 56 |
| 441 | 0.007 | 0.141 | -0.134 | 0.050 | 20.143 | -0.950 | 1 | 56 |
| 442 | 0.096 | 0.107 | -0.011 | 0.897 | 1.115 | -0.103 | 2 | 56 |
| 443 | 0.127 | 0.031 | 0.096 | 4.097 | 0.244 | 3.097 | 3 | 56 |
| 444 | 0.101 | 0.085 | 0.016 | 1.188 | 0.842 | 0.188 | 4 | 56 |
| 445 | 0.003 | 0.147 | -0.144 | 0.020 | 49.000 | -0.980 | 5 | 56 |
| 446 | 0.074 | 0.083 | -0.009 | 0.892 | 1.122 | -0.108 | 6 | 56 |
| 447 | 0.122 | 0.000 | 0.122 | 0.000 | 0.000 | #DIV/0! | 7 | 56 |
| 448 | 0.110 | 0.081 | 0.029 | 1.358 | 0.736 | 0.358 | 0 | 57 |
| 449 | 0.000 | 0.134 | -0.134 | 0.000 | 0.000 | -1.000 | 1 | 57 |
| 450 | 0.090 | 0.086 | 0.004 | 1.047 | 0.956 | 0.047 | 2 | 57 |
| 451 | 0.124 | 0.010 | 0.114 | 12.400 | 0.081 | 11.400 | 3 | 57 |
| 452 | 0.070 | 0.090 | -0.020 | 0.778 | 1.286 | -0.222 | 4 | 57 |
| 453 | 0.012 | 0.139 | -0.127 | 0.086 | 11.583 | -0.914 | 5 | 57 |
| 454 | 0.091 | 0.074 | 0.017 | 1.230 | 0.813 | 0.230 | 6 | 57 |
| 455 | 0.109 | 0.015 | 0.094 | 7.267 | 0.138 | 6.267 | 7 | 57 |
| 456 | 0.091 | 0.095 | -0.004 | 0.958 | 1.044 | -0.042 | 0 | 58 |
| 457 | 0.024 | 0.125 | -0.101 | 0.192 | 5.208 | -0.808 | 1 | 58 |
| 458 | 0.095 | 0.051 | 0.044 | 1.863 | 0.537 | 0.863 | 2 | 58 |
| 459 | 0.130 | 0.027 | 0.103 | 4.815 | 0.208 | 3.815 | 3 | 58 |
| 460 | 0.080 | 0.078 | 0.002 | 1.026 | 0.975 | 0.026 | 4 | 58 |
| 461 | 0.015 | 0.117 | -0.102 | 0.128 | 7.800 | -0.872 | 5 | 58 |
| 462 | 0.093 | 0.074 | 0.019 | 1.257 | 0.796 | 0.257 | 6 | 58 |
| 463 | 0.109 | 0.014 | 0.095 | 7.786 | 0.128 | 6.786 | 7 | 58 |
| 464 | 0.047 | 0.108 | -0.061 | 0.435 | 2.298 | -0.565 | 0 | 59 |
| 465 | 0.001 | 0.116 | -0.115 | 0.009 | 116.000 | -0.991 | 1 | 59 |
| 466 | 0.089 | 0.060 | 0.029 | 1.483 | 0.674 | 0.483 | 2 | 59 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 467 | 0.098 | 0.033 | 0.065 | 2.970 | 0.337 | 1.970 | 3 | 59 |
| 468 | 0.081 | 0.098 | -0.017 | 0.827 | 1.210 | -0.173 | 4 | 59 |
| 469 | 0.022 | 0.097 | -0.075 | 0.227 | 4.409 | -0.773 | 5 | 59 |
| 470 | 0.092 | 0.050 | 0.042 | 1.840 | 0.543 | 0.840 | 6 | 59 |
| 471 | 0.086 | 0.030 | 0.056 | 2.867 | 0.349 | 1.867 | 7 | 59 |
| 472 | 0.044 | 0.090 | -0.046 | 0.489 | 2.045 | -0.511 | 0 | 60 |
| 473 | 0.029 | 0.097 | -0.068 | 0.299 | 3.345 | -0.701 | 1 | 60 |
| 474 | 0.086 | 0.047 | 0.039 | 1.830 | 0.547 | 0.830 | 2 | 60 |
| 475 | 0.083 | 0.038 | 0.045 | 2.184 | 0.458 | 1.184 | 3 | 60 |
| 476 | 0.045 | 0.090 | -0.045 | 0.500 | 2.000 | -0.500 | 4 | 60 |
| 477 | 0.036 | 0.087 | -0.051 | 0.414 | 2.417 | -0.586 | 5 | 60 |
| 478 | 0.086 | 0.035 | 0.051 | 2.457 | 0.407 | 1.457 | 6 | 60 |
| 479 | 0.086 | 0.037 | 0.049 | 2.324 | 0.430 | 1.324 | 7 | 60 |
| 480 | 0.032 | 0.087 | -0.055 | 0.368 | 2.719 | -0.632 | 0 | 61 |
| 481 | 0.040 | 0.081 | -0.041 | 0.494 | 2.025 | -0.506 | 1 | 61 |
| 482 | 0.087 | 0.029 | 0.058 | 3.000 | 0.333 | 2.000 | 2 | 61 |
| 483 | 0.079 | 0.041 | 0.038 | 1.927 | 0.519 | 0.927 | 3 | 61 |
| 484 | 0.026 | 0.084 | -0.058 | 0.310 | 3.231 | -0.690 | 4 | 61 |
| 485 | 0.041 | 0.076 | -0.035 | 0.539 | 1.854 | -0.461 | 5 | 61 |
| 486 | 0.082 | 0.023 | 0.059 | 3.565 | 0.280 | 2.565 | 6 | 61 |
| 487 | 0.073 | 0.041 | 0.032 | 1.780 | 0.562 | 0.780 | 7 | 61 |
| 488 | 0.020 | 0.080 | -0.060 | 0.250 | 4.000 | -0.750 | 0 | 62 |
| 489 | 0.042 | 0.069 | -0.027 | 0.609 | 1.643 | -0.391 | 1 | 62 |
| 490 | 0.077 | 0.018 | 0.059 | 4.278 | 0.234 | 3.278 | 2 | 62 |
| 491 | 0.066 | 0.041 | 0.025 | 1.610 | 0.621 | 0.610 | 3 | 62 |
| 492 | 0.015 | 0.074 | -0.059 | 0.203 | 4.933 | -0.797 | 4 | 62 |
| 493 | 0.040 | 0.061 | -0.021 | 0.656 | 1.525 | -0.344 | 5 | 62 |
| 494 | 0.070 | 0.013 | 0.057 | 5.385 | 0.186 | 4.385 | 6 | 62 |
| 495 | 0.057 | 0.039 | 0.018 | 1.462 | 0.684 | 0.462 | 7 | 62 |
| 496 | 0.011 | 0.065 | -0.054 | 0.169 | 5.909 | -0.831 | 0 | 63 |
| 497 | 0.036 | 0.052 | -0.016 | 0.692 | 1.444 | -0.308 | 1 | 63 |
| 498 | 0.059 | 0.009 | 0.050 | 6.556 | 0.153 | 5.556 | 2 | 63 |
| 499 | 0.046 | 0.033 | 0.013 | 1.394 | 0.717 | 0.394 | 3 | 63 |
| 500 | 0.009 | 0.053 | -0.044 | 0.170 | 5.889 | -0.830 | 4 | 63 |
| 501 | 0.029 | 0.042 | -0.013 | 0.690 | 1.448 | -0.310 | 5 | 63 |
| 502 | 0.047 | 0.008 | 0.039 | 5.875 | 0.170 | 4.875 | 6 | 63 |
| 503 | 0.036 | 0.025 | 0.011 | 1.440 | 0.694 | 0.440 | 7 | 63 |
| 504 | 0.008 | 0.040 | -0.032 | 0.200 | 5.000 | -0.800 | 0 | 64 |
| 505 | 0.019 | 0.032 | -0.013 | 0.594 | 1.684 | -0.406 | 1 | 64 |
| 506 | 0.032 | 0.009 | 0.023 | 3.556 | 0.281 | 2.556 | 2 | 64 |
| 507 | 0.027 | 0.013 | 0.014 | 2.077 | 0.481 | 1.077 | 3 | 64 |
| 508 | 0.010 | 0.024 | -0.014 | 0.417 | 2.400 | -0.583 | 4 | 64 |
| 509 | 0.007 | 0.022 | -0.015 | 0.318 | 3.143 | -0.682 | 5 | 64 |
| 510 | 0.017 | 0.011 | 0.006 | 1.545 | 0.647 | 0.545 | 6 | 64 |
| 511 | 0.018 | 0.000 | 0.018 | 0.000 | 0.000 | #DIV/0! | 7 | 64 |
| Average | | | | 4.093 | 3.536 | | | |
| Stdev | | | | 15.647 | 10.669 | | | |
| +/-3STDEV | | | | 51.034 | 35.544 | | | |

**Биографија**

Мр Аца Алексић је рођен 03.10.1957. године у Београду, где је уписао Електротехничку школу "Никола Тесла", усмерење ваздухопловна електроника и завршио са одличним успехом. Студије на Факултету организационих наука уписао је школске 1976/1977. године на кибернетском смеру, а дипломирао је у априлу 1981. године одбраном дипломског рада „Примена табела одлучивања у симулационим моделима" код професора др Бранка Лазаревића, оцењеним оценом десет (10), са просечном оценом 8.60 током студија. Континуитет образовања наставио је на последипломским студијама и, након положених испита, пријавио је и одбранио магистарску тезу под насловом "Развој организације и савремене друштвене промене", маја 2005 године, под вођством ментора професора др Живка Дулановића. Након дипломирања 1981.године, започела је његова успешна радна каријера и то на следећим пословима и задацима:

Главни инжењер за информатику од 1981. до 1988. год., у Техногасу;Самостални саветник, Начелник центра за информатику, Помоћник директора за информатику и наплату прихода од1988. до 1997 год.,у Савезној управи царина СР Југославије; Начелник управе информатике и аналитике,Предавач информационих технологија од 1998. до 2003. год., у Ресору државне безбедности, Републичког министарства унтрашњих послова Републике Србије; Саветник председника компаније за информационе технологије од октобра 2003. до 2005. год,у Цитроену Србија; Директор центра за информатику и електронско пословање,Секретар удружења информатичке делатности ПКС од априла 2005. до 2007. год., у Привредној Комори Србије;Начелник службе за информационе и комуникационе технологије у Директорату цивилног ваздухопловства Републике Србије од октобара 2007 до 2010. год.;Директор сектора за откривање превара у осигурању, спречавање прања новца и финасирање тероризма, у Компанији Дунав Осигурање А.Д. од јануара 2010 до 2011. године. Од августа 2011. године ради као Помоћник генералног директора за информационе технологије, у „Дунав РЕ".

**Прилог 1.**

# Изјава о ауторству

Потписани-а Аца С. Алексић

број уписа 465/09

**Изјављујем**

да је докторска дисертација под насловом

Статистички модел аутоматизованог управљања дигиталним сертификатима

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

**Потпис докторанда**

У Београду, 30.04.2012

**Прилог 2.**

# Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора __Аца С. Алексић_____

Број уписа _____467/09_____

Студијски програм _____

Наслов рада Статистички модел аутоматизованог управљања дигиталним сертификатима

Ментор __др Зоран Радојичић, ванредни професор _____

Потписани __Аца С. Алексић_____

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

**Потпис докторанда**

У Београду, 30.04.2012.

**Прилог 3.**

# Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Статистички модел аутоматизованог препознавања дигиталног идентитета

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

**Потпис докторанда**

У Београду, 9. 5. 2022

Душан К

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.