УНИВЕРЗИТЕТ СИНГИДУНУМ
БЕОГРАД
ДЕАПАРТМАН ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ

# УНАПРЕЂЕЊЕ ПРОТОКОЛА ЗА РАЗМЕНУ КЉУЧЕВА НА БАЗИ ЛИЧНИХ ИДЕНТИФИКАЦИОНИХ ДОКУМЕНАТА ПОШИЉАОЦА И ПРИМАОЦА

ДОКТОРСКА ДИСЕРТАЦИЈА

ментор:
проф. др. Младен Веиновић

студент:
Александар Мишковић
број индекса: 2010460065

Београд, 2019.

SINGIDUNUM UNIVERSITY
BELGRADE
DEPARTMENT FOR POSTGRADUATE STUDIES

# IMPROVING KEY EXCHANGE PROTOCOLS BASED ON SENDER AND RECEIVER ELECTRONIC IDENTIFICATION DOCUMENTS

DOCTORAL DISSERTATION

Mentor:
Mladen Veinović

Student:
Aleksandar Mišković

Belgrade, 2019.

***Страхиње***

**ЗАХВАЛНИЦА**

Ова докторска дисертација је настала као резултат дугогодишњих истраживања под руководством проф. др Младена Веиновића.

Свако научно истраживање је и истраживање сопствених граница и моћи. Ментори су ту да би нас својим знањем и искуством подстакли да померамо границе, а породица и пријатељи да би нам давали смисао, љубав и снагу.

Хвала мом ментору, проф. др Младену Веиновићу, на несебичној помоћи и подршци у свим фазама израде ове дисертације, као и на безграничном поверењу, корисним саветима, како током израде дисертације тако и током наше дугогодишње сарадње.

Хвала мојој највећој подршци и животној снази супрузи Јасмини на безграничном стрпљењу, подршци и разумевању током израде докторске дисертације.

Децембар 2019.

Београд

Аутор

# Сажетак

Предмет рада докторске дисертације је сагледавање актуелних проблема везаних за појмове размена криптографских кључева и аутентификација корисника система за тајну комуникацију. Рад се бави анализом постојећих решења у области истраживања и развијањем сопственог система за тајну комуникацију.

Научни циљ дисертације је унапређење протокола за размену криптографских кључева на бази личних идентификационих докумената. Извршена је анализа постојећих приступа у области истраживања с циљем да се побољша ниво заштите приликом тајне комуникације и добије основа за развој сопственог система. Комбиновањем криптографских метода које обезбеђују поверљивост, аутентичност и интегритет, уз примену стеганографских метода за размену информација на скривен начин, корисницима предложеног система се пружа могућност да на ефикасан и сигуран начин размењују тајне поруке.

Анализом резултата истраживања закључено је да постоји оправданост употребе личних идентификационих докумената за размену криптографских кључева који се користе у тајној комуникацији.

Кључне речи: размена криптографских кључева, тајна комуникација, лични идентификациони документ, стеганографија

# Abstract

The subject of the doctoral dissertation is looking at current issues related to the concepts of cryptographic key exchange and authentication of users of a secret communication system. The paper deals with the analysis of the existing solutions in the field of research and development of own secret communication system.

The scientific goal of the dissertation is to improve the protocol for exchanging cryptographic keys based on electronic identification (eID). Analysis of the existing approaches in the research was carried out in order to improve the level of protection during secret communication and to provide the basis for the development of own system. By combining cryptographic methods that ensure confidentiality, authenticity and integrity, along with the use of steganographic methods for information exchange in a secret way, users of the proposed system are given the opportunity to exchange secret messages in an efficient and secure manner.

By analysing the research findings, it has been concluded that it is justified to use electronic identification for exchanging cryptographic keys used in secret communication.

Keywords: cryptographic keys exchange, secret communication, electronic identification, steganography

# Садржај

# Списак слика

# 1. Увод

До данас је развијен велики број комплетних сервиса којима се штити приватност и који гарантују висок степен заштите размењених информација. Неки од ових сервиса су бесплатни и могу се користити без икаквих ограничења, док се други могу користити уз одређену новчану надокнаду. Међутим, у данашње време постоје разне методе за прислушкивање комуникационог канала преко кога се врши размена информација. Након откривања шифроване комуникације и пресретања шифрованих порука, постоји вероватноћа да ће неко покушати да изврши криптоанализу истих. У сврху смањивања вероватноће откривања шифроване комуникације најчешће се користи нека од опште познатих стеганографских метода. Употребом стеганографије потенцијалним нападачима се знатно отежава процес разоткривања тајне комуникације јер се од њих скрива информација да је до комуникације уопште и дошло.

Ово је послужило као основа за сагледавање актуелних проблема у овој области, као и за анализу постојећих решења за заштиту. На основу утврђених проблема и недостатака постојећих решења за заштиту, предложен је сопствени модел заштите који се, као такав, по први пут користи као комплетан систем за приватну, тј. тајну комуникацију.

Комбиновањем криптографских метода које обезбеђују тајност, аутентичност и интегритет, уз примену стеганографских метода за размену информација на скривен начин, корисници тајне комуникације могу на ефикасан и сигуран начин да размењују тајне поруке, уверени да оне нису у међувремену промењене од стране неког трећег лица и да су тајни кључеви којима се обезбеђује тајност размењени на сигуран начин.

Слање тајних кључева јавним комуникационим каналом, као што је то интернет, се сматра небезбедним. Сходно томе, предложени модел користи лична идентификациона документа грађана Републике Србије, на којима су уписана два квалификована дигитална сертификата издата од стране сертификационог тела МУП Републике Србије (*MUPCA*). Уз помоћ програма развијеног у Јава програмском језику приступа се квалификованим дигиталним сертификатима на којима се налазе два пара *RSA* кључева. Ови кључеви се могу користити за дигитално потписивање и шифровање, респективно, а у предложеном моделу они се користе за шифровање тајних кључева, којима се обезбеђује тајност, и аутентификацију корисника тајне комуникације. *RSA* алгоритам који се у овом случају користи сматра се погодним и практичним за дигитално потписивање и шифровање.

Развој програма који за шифровање и дешифровање користи *RSA* кључ, који се налазе на квалификованом дигиталном сертификату личног

идентификационог документа, треба да укаже на једноставност употребе предложеног система за тајну комуникацију и широк спектар могућности које се нуде крајњим корисницима. Такође, важно је напоменути да постоје програмски алати које нуди *MUPCA* у оквиру својих услуга, који врше дигитално потписивање и очитавање личног идентификационог документа, међутим, не постоји јавно доступан програмски алат којим би се извршило шифровање *RSA* кључем који се налази на личном идентификационом документу грађана Републике Србије.

# 1.1. Очекивани доприноси

## 1.1.1. Стручни допринос

Основни допринос овог рада, на основу разматраних искустава из теорије и праксе, огледа се у развоју и примени једног новог свеобухватног система за тајну комуникацију који унапређује протокол за размену криптографских кључева. Предложени систем за тајну комуникацију користи квалификоване дигиталне сертификате са личних идентификационих докумената грађана Републике Србије за дистрибуцију тајних кључева, којима се обезбеђује тајност, и аутентификацију корисника тајне комуникације.

Употребом личних идентификационих докумената грађана Републике Србије се обезбеђује широка доступност предложеног система тајне комуникације, а применом програма развијеног у Јава програмском језику, који ће бити јавно доступан свим грађанима Републике Србије, се знатно олакшава употреба личних идентификационих докумената у тајној комуникацији.

Посебан допринос се огледа у томе што је у овом раду развијен нови програм у Јава програмском језику, коришћењем стандардне методологије и алата за софтверско моделовање, ради проширивања функционалности постојећих апликација за дигитално потписивање и шифровање коришћењем личних идентификационих докумената грађана Републике Србије.

## 1.1.2. Научни допринос

Научни допринос овог рада огледа се у анализи постојећих решења, где ће се јасно указати на предности и недостатке тих решења. Резултати ове анализе треба да омогуће јасно сагледавање тренутног стања у области истраживања и да дају основу за предлагање новог система тајне комуникације који унапређује евентуалне недостатке постојећих решења.

У складу са до сада наведеним, очекивани доприноси овог рада су:

- Нови протокол за размену тајних кључева на бази личних идентификационих докумената пошиљаоца и примаоца.
- Не постоји потреба да се смешта и чува велики број тајних кључева који се могу компромитовати.
- За сваку нову комуникацијску сесију генерише се нови тајни кључ који корисници тајне комуникације лако и сигурно размењују.
- Остварује се потпуна *end-to-end* заштита за сваку комуникацију и за сваки пар учесника у тајној комуникацији.
- Нови протокол је отпоран на велики број напада на мрежи.

Резултати рада на овој докторској дисертацији биће објављени у више радова у часописима међународног значаја и саопштени на више научних скупова у земљи и иностранству. Поједине идеје су већ изложене на међународним стручним конференцијама и часописима.

## 1.2. Методе које ће се примењивати у истраживању

Методологија истраживања у овом раду обухватаће сложен и организован поступак полазећи од логичких начела и принципа по утврђеним фазама.

У истраживању и прикупљању примарних и секундарних података, биће коришћене методе из групе основних, опште научних, посебних и из групе статистичких метода за прикупљање података.

Сложеност предмета истраживања захтева примену:

- аналитичких основних метода: метод анализе, метод апстракције, метод специјализације и метод дедукције;
- синтетичких основних метода: синтезу, конкретизацију, генерализацију и индукцију;
- општих научних метода: хипотетичко-дедуктивну, аналитичко-дедуктивну, компаративну, статистичку и методу моделовања.

Овај избор истраживачких метода је употребљен да се истраживање и ток истраживачког процеса у свим фазама, тј. идентификацији и дефинисању проблема, планирању дизајна истраживања, сакупљању, обради и анализи података, као и формулацији закључака, коректно спроведе у складу са основним принципима научно истраживачког рада. Применом ових метода, како показују досадашњи резултати истраживања, могуће је валидно остварење научног и друштвеног циља истраживања. Приступ истраживању је интердисциплинаран и синтетички у том смислу што се ни једном методолошком поступку не даје искључива предност.

У прикупљању података примениће се: истраживање, анкета и метода анализе садржаја докумената.

Анализа ће бити остварена на два нивоа :

- на нивоу експерименталне анализе реалних субјеката и
- на нивоу секундарне анализе резултата ранијих истраживања и адекватне литературе.

## 1.3. Циљ истраживања

Циљ показује основну сврху истраживања. Он може имати непосредно практични, друштвени, теоријски и научни значај.

Што се тиче теоријског и научног циља истраживања, у предложеној докторској дисертацији поред анализе теоријских модела и принципа за тајну размену информација, биће извршена детаљна анализа постојећих приступа у овој области. Резултати анализе треба да укажу на предности и мане постојећих система, с циљем да се побољша ниво заштите приликом тајне размене информација и добије основа за развој сопственог модела који би ефикасно одговорио на евентуалне недостатке постојећих решења.

Практични циљ овог истраживања огледа се у развоју и примени једног новог свеобухватног модела за тајну комуникацију, који се као такав, по први пут користи за приватну, тј. тајну комуникацију. Предложени нови модел за тајну комуникацију корисницима пружа могућност коришћења стеганографских метода у комбинацији са личним идентификационим докуменатима.

Спроведена анкета међу студентима прве године Високе техничке школе струковних студија у Крагујевцу, студијског програма Информатике, одмах након уписа, указује на то да развој новог модела за тајну комуникацију треба да допринесе већој друштвеној прихватљивости, која треба да подстиче кориснике да користе средства за заштиту приватности која су им лако доступна. С подизањем опште свести о једноставности употребе предложеног модела и указивањем на широк спектар могућности који се нуде крајњим корисницима друштвени циљ овог истраживања би био у потпуности задовољен.

## 1.4. Научне хипотезе

Хипотезе које чине основу овог рада:

- Развојем новог свеобухватног модела за тајну комуникацију који обједињује употребу личних идентификационих докумената са

стеганографским методама побољшава се ниво заштите приликом тајне размене информација.
- Реализовани модел треба да обезбеди једноставност употребе, која треба да подстиче кориснике да користе средства за заштиту приватности која су им лако доступна и мора да представља систем са јасним параметрима за тајну комуникацију у који се може имати поверења.
- Примена личних идентификационих докумената у комбинацији са неком стеганографском методом потенцијалном нападачу у великој мери отежава процес разоткривања тајне комуникације, а самим тим умањује се и вероватноћа да ће доћи до криптоанализе шифрованих информација.

Посебне хипотезе:

- Корисници који желе да примењују предложени модел за тајну комуникацију морају да користе услуге "треће стране од поверења", тј. сертификационг тела које издаје квалификоване дигиталне сертификате на личним идентификационим документима.
- *RSA* кључ од 2048 бита који се користи у личним идентификационим документима грађана Републике Србије се још увек сматра безбедним.

# 1.5. Структура докторске дисертације

Докторска дисертација се састоји из 8 (осам) поглавља: Увод, Преглед у области истраживања, Теоријске основе истраживања, Преглед постојећих решења, Модел предложеног решења, Евалуација предложеног решења, Закључак и Литература.

У првом поглављу је описан предмет истраживања, назначени су мотиви за израду једног новог решења за тајну комуникацију, наведени су очекивани доприноси, приказана је методологија истраживања, дате су научне хипотезе и циљ истраживања.

Друго поглавље представља преглед у области истраживања. Методолошки су анализирани научни радови из врхунских међународних часописа, научни радови са релевантних међународних конференција и скупова, објављених књига и стандарда.

У трећем поглављу су описане теоријске основе које су релевантне за област истраживања. Дат је кратак преглед савремене криптографије, уз историјски осврт ка развоју криптографских система, као и теоретске основе стеганографије.

Четврто поглавље представља преглед постојећих решења која се већ користе и која су релевантна за област истраживања. Дат је приказ софтверских решења и описане су њихове предности и уочени недостаци. Број постојећих решења је сведен на она која

су се користила за поређење са предложеним решењем за тајну комуникацију из ове дисертације.

Пето поглавље описује предложено решење за тајну комуникацију и приказује метод његове примене. Дат је опис проблема који је био и мотив за рад на овој докторској дисертацији.

Шестим поглављем су приказани резултати симулација модела који су довели до развоја новог система за тајну комуникацију, приказана су поређења предложеног решења са већ постојећим решењима описаним у поглављу четири. Приказани резултати спроведене анкете са изведеним закључцима који су проистекли из исте. Дат је критички осврт на делове система за тајну комуникацију који могу да утичу на безбедну употребу истог и дате смернице за унапређење недостатака.

Седмо поглавље је закључак где су јасно издвојени научни и стручни доприноси ове докторске дисертације и предложени су правци даљих истраживања

У осмом поглављу је дат списак литературе која је коришћена у овај докторској дисертацији.

# 2. Преглед у области истраживања

Безбедна размена криптографских кључева је тема о којој се у науци и професионалној употреби криптографије стално говори. Може се рећи да је то једна од најслабијих карика у изградњи једног система за тајну комуникацију. Познато је да постоји велики број за сада доказано безбедних решења, која су при том и ефикасна у пракси. О размени криптографских кључева написан велики број научних радова. Многа од тих решења су представљена само у теорији, нека су недоступна за широку јавну употребу, а постоје и она решења која су комерцијално доступна. Поред безбедне и ефикасне размене кључева област истраживања ове дисертације покрива и област тајне комуникације, стеганографију и електронска идентификациона документа (енгл. *Electronic identity – eID*).

Лични идентификациони документ са чипом грађана Републике Србије (Биометријска лична карта) је у посебном фокусу овог истраживања јер спада у групу *eID*. Проширена примена *eID*, поред очигледне и једноставне идентификације, је тренутно у тренду како код нас, тако и свуда у свету. Портали електронске управе, на државном и локалном нивоу, који се развијају код нас у земљи омогућавају грађанима да велики део административних ствари заврше преко интернета са својих кућних рачунара. Међутим, лични идентификациони документ са чипом можемо посматрати као паметну картицу (енгл. *smart card*) пошто у себи има интегрисан електронски чип са којим је могуће спровести и низ других нетипичних активности, што ће бити и приказано у овом поглављу и дисертацији уопште.

Преглед у области истраживања ове докторске дисертације може се свести на следеће категорије, које су у великом броју научних радова на неки начин међусобно повезане:

1. размена кључева,
2. тајна комуникација,
3. стеганографија и
4. електронски идентификациони документ.

Један од најновијих приступа у области размене кључева је протокол за дистрибуцију кључева на сигуран и ефикасан начин путем групне комуникације која је заснована на Ади Шамировој[1] шеми дељења тајне [1]. Анализом других протокола аутори су дошли до закључка да је њихова шема отпорна на пасивне нападе који подразумевају прислушкивање и надгледање комуникационог канала, напад "поновног слања" (енгл. *replay attack*) где нападач лажно понавља пренос

[1] Ади Шамир, израелски криптограф, један је од проналазача *RSA* алгоритма.

података који је већ коришћен у комуникацији, као и напад лажног представљања у којем нападач преузима идентитет једне од легитимних страна у комуникацији.

Свеобухватан преглед радова из области истраживања [2], чији је фокус био на научним радовима који се баве управљањем и дистрибуцијом кључева у мобилним и *Cloud* мрежама, се анализом: садржаја, приказаних резултата, перформанси, доприноса у области истраживања, друштвене корисности и другим факторима, издвојило више радова. Као релевантни за област истраживања ове докторске дисертације издвајају се радови који се баве: сигурном комуникацијом међу корисницима друштвених мрежа, генерисањем и опозивом кључева на *Cloud* просторима за складиштење података и решавањем проблема "цурења" (енгл. *leakage*) тајног кључа успостављањем ефикасне провере идентитета [3, 4 и 5].

Постоје разне иницијативе земаља широм света за побољшање система који би могли назвати електронски здравствени систем (енгл. *e-health*), међу којима се издвајају Аустралија, Велика Британија, Канада, САД, Холандија и Сингапур. Предложени систем елиминише сложену процедуру управљања дигиталним сертификатима на начин који не угрожава сигурност једног сложеног система као што је то инфраструктура јавних кључева [6]. Сличан приступ и нову ефикасну имплементацију дељења дигиталног сертификата стандардног формата X.509 између уређаја као што су то паметни телефони и персонални рачунари приказан је као пример за пословно окружење [7].

Сигурносни протокол заснован на инфраструктури јавних кључева предложен је за имплементацију сигурносних механизама у операцијама преноса података између сателита. Протокол је експериментално развијен и имплеметиран како би показао да се протоколом заснованом на инфраструктури јавних кључева решава проблем безбедносних захтева и обезбеђују сервиси аутентификације, интегритета и поверљивости података [8]. Размена кључева у мобилним *Ad hoc* мрежама (енгл. *MANET*), где сваки чвор у мрежи генерише своје парове јавних и приватних кључева ослања се на принципе асиметричне криптографије. Предност оваквог начина размене кључева се огледа, према тврдњама аутора, у томе што се креира више независних сертификата које потписује више различитих чворова у мрежи [9]. Упркос успешној примени инфраструктуре јавних кључева уочени су и недостаци који се огледају у томе да постоји могућност фалсификовања дигиталних сертификата. За решавање поменутог недостатка предложено је неколико ефикасних решења. Група аутора [10] је предложила ефикасно решење које омогућава *TLS* серверу (*Transport Layer Security – TLS*) да детектује напад који има за циљ да проузрокује фалсификовање дигиталног сертификата, као и да сазна одакле напад потиче. Анализа [11] и поређење симетричне криптографије са асиметричном криптографијом, као и осврт на предности и недостатке инфраструктуре јавних кључева, подстакла је аутора да предложи решење које задовољава безбедносне стандарде у *Cloud* технологијама.

Асиметрични алгоритам који се највише користи у комбинацији са инфраструктуром јавних кључева је *RSA*. Решења и примери који стреме ка побољшању имплементације и примене једног овако робусног алгоритма су бројни. Софтверско решење применом *C#* програмског језика у комбинацији са *SQL Server 2008 R2* које има за циљ да убрза алгоритам током преноса података између различитих комуникационих мрежа, приказано је кроз нов метод за размену кључева између два мрежна уређаја [12]. Diffie-Hellman протокол за размену кључева је послужио као основа многим ауторима да развију своје методе за размену кључева у асиметричној криптографији. Скраћено се често у литератури он назива и *DHKE* (*Diffie–Hellman Key Exchange*). *DHKE* је био основа за развој новог протокол, јасног концепта и практичне примене на мрежи, који пружа заштиту приватности и представља нове правце примене у *IKE* (*Internet Key Exchange*) стандарду [13].

Идентификација и аутентификација корисника су важни сервиси који се примењују у националним службама електронске управе. Ове службе су у неким земљама достигле висок степен развоја у којима битну улогу имају електронска идентификациона документа (енгл. *electronic identification – eID*). У оквиру стратегије за развој, имплементацију сервиса е-управе и прихватања *eID* од стране пружаоца услуга, национална служба за е-управу Аустрије је развила нов модул под називом *MOA-ID*. Група аутора је искористила *MOA-ID* како би представила три различита приступа о томе како се примена аустријске *eID* може сигурно преместити у *Cloud* без кршења било каквих аспеката приватности или заштите података. На основу евалуације предложених приступа предложен је модел који се ослања на различите криптографске методе, уз минималну промену сервиса за идентификацију и аутентификацију аустријске *eID*, и омогућава сигурну употребу *eID* у несигурном окружењу [14, 15].

Група аутора [16] је уочила и приказала претње које су описане као напад "ослушкивања" (енгл. *sniffing*) терминала који очитава паметну картицу и напад којим се врши промена поруке непосредно пре потписивања дигиталним потписом. Своје истраживање су завршили предлогом новог протокола који користи основе протокола за временско означавање (енгл. *timestamping protocol*).

Сигурна шема за аутентификацију заснована на шпанским *eID* приказана је на примеру аутомобилских *Ad hoc* мрежа (engl. *Vehicle Ad Hoc Networks – VANETs*) [17]. Аутори су представили сигуран протокол који омогућава возилима власти (полиција, и томе сл.) да брзо и на захтев преко *VANET* мреже добију стварни идентитет возача. Евалуација предложеног протокола је извршена на симулационом моделу који је показао да је предложени протокол имао 60–70% успешних детекција идентитета возача возила. Група аутора [18] је такође користила шпански *eID* како би представила систем за потврду идентитета помоћу бежичне *NFC* (*Near Field Communication*) технологије уз помоћ криптографских метода.

Федеративно управљање идентитетом је метода која је представљена са циљем лакшег управљања ентитетима који сарађују међусобно без централизоване контроле. Ово се односи пре свега на Европску унију која има наслеђене *eID* системе својих чланица. Представљено је обједињено европско решење за *eID* које има за циљ да опслужује око 500 милиона људи, а у плану је и проширење на издавању *eID* за компаније. Након евалуације која је подразумевала проверу перформанси и скалабилности предложеног решења, дошло се до закључка да је предложено решење изводљиво узимајући у обзир и сигурносна ограничења [19]. Поменута метода и креирање *eIDAS* (*electronic IDentification, Authentication, and trust Services – eIDAS*) била је предмет истраживања групе аутора [20] која је посматрала сценарио у коме се захтева да се прво спроведе сервис ауторизације, а након тога аутентификација. Ово се односи превасходно на контролу приступа неком мрежном сервису, где пружалац услуге води рачуна о контроли приступа пре него што се изврши аутентификација корисника. Понуђена су решења која се примењују на апликативном и транспортном мрежном слоју, респективно. Многе земље, које су увеле *eID*, користе решења која за потврду о идентитету врше обелодањивање свих податак који се налазе на *eID* [21, 22]. Наравно ово представља проблем који залази у домен заштите приватности грађана, па су аутори предложили један модел који селективно открива потребне податке по потреби.

Велики број европских земаља почела је да користи *eID* за апликације које су издате од стране државне управе и од стране приватних компанија. Један од таквих примера је немачки eID који представља паметну картицу могућношћу бесконтактног очитавања, која има за циљ да заштити приватност корисника користећи јаку криптографску аутентификацију између корисника и пружаоца услуга. Предложено је коришћење псеудонимне аутентификације за приступ сервису услуга уз очитавање само потребних података, што је представљено као мера заштите приватних податак корисника [23]. Рад [24] који такође узима у разматрање аустријски *eID* али овога пута у сегменту мобилних технологија приказује како се један нови поступак аутентификације користи као средство да се премости јаз између различитих врста уређаја и услуга. Приказана је евалуација решења, у току пробног коришћења компоненте, које доноси сигурну аутентификацију на "паметним" телефонима.

Слабости и рањивост система који примењују *eID* разматран је на случају естонске *eID* [25]. 2017. године је откривен сигурносни ризик на естонском *eID*, тј. у алгоритамска грешка унутар *RSA* библиотеке која се налази на чипу *eID*. Преко 800000 естонских *eID* и више од 200000 чипова које је произвела компанија *Infineon* је било од 2014. године под ризиком. Ажурирање дигиталних сертификата на даљину је омогућило Естонији да превазиђе ову кризу.

Многи аутори су за прикривање информација користили различите технике стеганографије [26]. С обзиром да нападач није свестан постојања комуникације у

неком комуникационом каналу учинило се као врло интересантно за истраживања. Група аутора [27] је користила стеганографски метод заснован на дискретним косинусним трансформацијама у циљу скривања тајних информација у најмање битним битовима. Они су користили ниске и средње фреквенције за анализу њихових перформанси помоћу *PSNR* (енгл. *Peak Signal to Noise Ratio*) и *MSE* (*Mean Square Error*) метода. Истраживања су показала да средња фреквенција има већу способност прикривања, као и бољи однос сигнала и шума, на основу чега су закључили да предложени стеганографски алат омогућава релативно висок капацитет уградње, без битног визуелног изобличења слике и да се при том одржава тачност скривених података. Аутори [28] су предложили стеганографску технику за побољшање квалитета стего слике као и повећање стеганографске способности. Предложена метода се ослања на минимизирање тајне поруке што је више могуће пре уградње. Алгоритам, назван од стране аутора *DCT-M3*, користи разлике између два *DCT* (енгл. *discrete cosine transform*) коефицијената за уградњу тајне поруке у *JPEG* слику. Добијени резултати су показали да предложени алгоритам знатно смањује број промена на *JPEG* слици током уградње порука различите дужине. На основу спроведених анализа закључили су да алгоритам *DCT-M3* даје боље резултате у поређењу са најчешће кориштеном LSB (енгл. *least significant bit*) техником стеганографије.

Стеганографија која примењује *JPEG* слику за сигурност визуелних садржаја на мрежним друштвеним мрежама је веома актуелно поље истраживања, где су осетљиви садржаји уграђени у *JPEG* слике, задржавајући свој визуелни квалитет. Истраживачи су до сада користили корелациони простор боја, као што је *RGB*, где промена једног параметра утиче на укупни квалитет стего слика, смањујући на тај начин његову погодност за стеганографске алгоритме. Адаптивни метод *LSB* супституције употребом некорелисаног простора у боји смањиће шансе откривања помоћу система људског вида. У предложеној шеми, улазна слика пролази кроз програм за кодирање слика, што као резултат даје шифровану слику, која се затим се конвертује у *HSV* простор боја погодан за даљу обраду. Идеја за коришћење *HSV* простора боја за скривање података потиче из његових својстава која се огледају у декорелацији, економичности у обради, бољем квалитету слике и погодности за стеганографију. Квантитативни и квалитативни експериментални резултати предложеног модела и његове примене, као и сигурност и приватност визуелних садржаја на мрежним друштвеним мрежама, потврђују његову ефикасност за разлику од најсавременијих (*state-of-the-art*) метода [29].

Група аутора [30] је дала нову и ефикасну методологију коришћењем *JPEG* слика у стеганографији, применом методе *LSB*. Овај систем стеганографије се комбинује са *RSA* алгоритмом. Према тврдњи аутора, коришћење стеганографске методе штити пренете податке од "цурења" у комуникационом каналу, поготово када се користи вишеструки пренос података који се односи на дељење стего носача између већег броја корисника.

Комбиновање реверзибилног скривања податак и шифровања, како би се добила максимална сигурност, представљено је као нов приступа за остваривање сервиса поверљивости, интегритета и аутентификације [31]. Предложени метод користи стеганографију са A-S [32] секвенцијалним алгоритмом за шифровање. Предложени метод је веома брз и пружа високу сигурност. Резултат испитивања показује да је предложена метода врло ефикасна и добро изведена.

У раду [33] представљен је стеганографски алат *CrypSteg* за уметање података у слике који комбинује криптографију и стеганографију у једном алгоритму. Ова метода показује свој већи капацитет за скривање података од осталих метода јер уграђује 4 бита информација у блок од 4 x 4 пиксела. Овај алат се примењује на оним сликама чији су пиксели хомогено распршени и користан је за утискивање мале количине података. Експериментални резултати показују да је метода веома ефикасна нарочито када се примењује на оне бинарне слике чији су пиксели у боји распоређени врло једнолико.

Анализа актуелних стеганографских техника и метода примењених на различитим мултимедијалним фајловима, са акцентом на примени стеганографије у *JPEG* сликама, приказана је уз примену различитих трансформационих техника [34]. Поред метода за прикривање информација дат је преглед метода за детекцију утиснутих информација, тј. стегоанализа. Група аутора је [35] предложила коришћење алата *StegApp* с којим би се скривала тајна порука, чиме би се добила *JPEG* слика као стего носач, која би након тога била смањена на веома малу величину и као таква била уметнута у *Microsoft Word* документ.

# 3. Теоријске основе истраживања

Потреба да се размена информација учини бржом и ефикаснијом подстакла је развој информационо-комуникационих технологија. Развој све већег броја телекомуникационих и интернет сервиса, довео је до пораста броја корисника тих услуга, а самим тим повећала се и количина размењених информација. Информације које се размењују путем јавног комуникационог канала могу бити компромитоване уколико нису заштићене на адекватан начин. Упоредо са развојем информационо-комуникационих технологија развијају се и начини за заштиту размењених информација.

Размена информација на сигуран начин, који подразумева да исте буду доступне само ономе коме су и послате, одувек је представљала потребу, још од времена старих цивилизација. Познато је да израз "Криптографија" потиче из грчког језика и да представља науку о "тајном писању" [36]. Гледано кроз историју криптографија се у почетку искључиво користила у војне и дипломатске сврхе. Људи су се на разне домишљате начине трудили да размена порука буде неразумљива некој трећој страни која би била у могућности да пресретне послату поруку. У време античке државе Спарте забележено је коришћење система за шифровање званог Скитале. Након тога, за време Римљана користио се шифарски систем Цезарова шифра, назван по Гај Јулије Цезару. Хронологија појављивања и коришћења шифарских система је забележена у многим књигама и уџбеницима, а међу првима која се појавила је књига Дејвида Кана[1] "Разбијачи шифара" (енгл. *The Codebreakers*), за коју се сматра да је подстакла нове ауторе да пишу и издају нове радове о криптографији иако је америчка Национална агенција за безбедност (енгл. *National Security Agency – NSA*) покушавала то да сузбије [37].

Поред класичних криптографских метода које се користе за размену информација уз помоћ шифровања, за прикривену размену информација развијене су стеганографске методе којима се скривају информације унутар неке датотеке. Стеганографија се суштински разликује од криптографије иако се обе науке користе како би се сачувала тајност података. Коришћењем стеганографије могуће је избећи напад "човек у средини" [38] јер се нападачима знатно отежава процес разоткривања тајне комуникације тиме што се од њих скрива информација да је до комуникације уопште и дошло. Као и криптографија, стеганографија се такође користи од давнина када су се људи користили разним триковима за прикривање порука, нпр.: коришћење невидљивог мастила, разне ознаке на самим словима која

[1] Дејвид Кан (David Kahn) амерички писац, историчар и новинар који је написао хронологију криптографије од старог Египта па све до 1967. године када је књига и објављена.

су написана, и томе сл. У данашње време, употребом рачунара, могуће је поруке сакривати тако што се оне утискују у различите дигиталне датотеке.

# 3.1. Криптографија

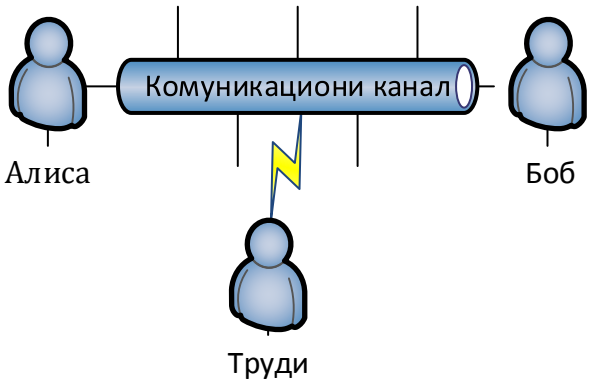
Годинама уназад криптографија је представљала средство за заштиту која се примењивала углавном у војним оквирима, која је била под директним надзором државних органа. Развојем рачунара и интернета криптографија је, можемо рећи, постала свеприсутна у јавним оквирима, иако је и даље остала доминантно војна технологија [39].

Без обзира у коју сврху се користи, основна сврха коришћења криптографије је да обезбеди тајност. Међутим, применом криптографије можемо да задовољимо и друге захтеве који се постављају испред појма безбедна комуникација: аутентификација, интегритет и непорецивост.

## 3.1.1. Основна правила

У циљу представљања криптографских принципа у литератури се дефинишу одређени појмови као што су: пошиљалац (енгл. *sender*), прималац (енгл. *receiver*), комуникациони канал, отворен текст (енгл. *plaintext*), шифрован текст (енгл. *ciphertext*), кључ (енгл. *key*), уљез (енгл. *intruder*), итд.

Веома често се у литератури, у циљу једноставнијег представљања проблема, пошиљалац и прималац представљају као Алиса и Боб, а уљез као Труди, међутим, то не мора да значи да се ради о људима већ то могу бити било који уређаји (рачунари, мобилни телефони, и томе сл.) или пак процеси на самим тим уређајима. Ово се може и представити графички, слика 3.1:



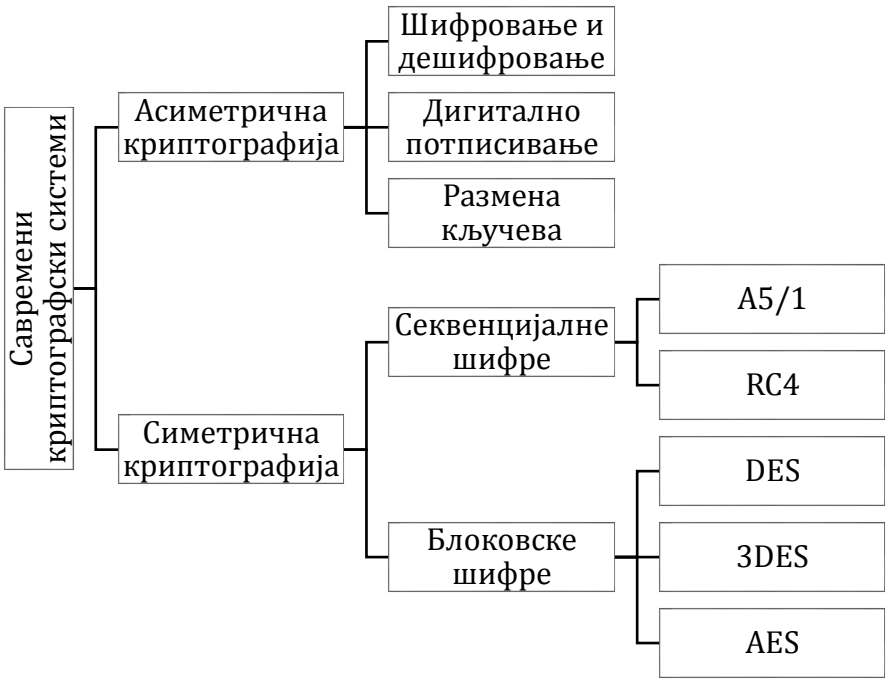

Слика 3.1. Комуникација између Алисе и Боба уз присуство уљеза Труди

Тајност поруке коју Алиса шаље Бобу може да се обезбеди шифровањем исте помоћу неког криптографског алгоритма и одговарајућег кључа. Аутентификација или провера идентитета треба да обезбеди да Боб буде сасвим сигуран да је порука

коју је добио стигла од Алисе, тј. да Труди није успела да се умеша у комуникацију и представи као Алиса, а самим тим и превари Боба. Интегритет је сервис од веома велике важности јер се с њим гарантује да порука коју је Алиса послала Бобу није у међувремену промењена, тј. да Труди није пресрела поруку, изменила њен садржај и тако измењену поруку послала Бобу. Немогућност порицања, тј. непорецивост, је сервис који треба да заштити Боба у случају да се Алиса предомисли и након неког времена почне да тврди да она поруку уопште није ни послала Бобу.

Да би наведене сервисе Алиса и Боб могили да спроведу у дело морају да тоураде уз помоћ одговарајућег криптографског протокола. Криптографски протокол представља један алгоритам или низ корака који прецизно описују интеракцију између корисника, било да се ради о два или више учесника у комуникацији [40]. Пре него што успоставе комуникацију Алиса и Боб се договарају и бирају одговарајући криптографски протокол, начин на који ће да размене кључеве који се користе у криптографском алгоритму и друге кораке који ће да им омогуће заштићену комуникацију. Избор криптографског протокола зависи, пре свега, од начина на који Алиса и Боб желе да остваре сигурну комуникацију и они се могу дефинисати као:

- Комуникација уз примену симетричне криптографије.
- Комуникација уз примену криптографије са јавним кључем – асиметрична криптографија.




Слика 3.2. Подела савремених криптографских система

На слици 2. је приказана подела савремених криптографских система са набрајањем неких од познатијих реализација тих система. Побројани су неки од практично сигурних криптографских алгоритама. Познато је, математички

доказано, да апсолутно сигурни криптографски систем представља једнократна бележница (енгл. *one-time pad - OTP*) који се и користио у ближој историји али који није практичан за већину данашњих ситуација у којима се одвија комуникација између два корисника [41].

Једнократна бележница је непрактична за примену у већини данашњих комуникационих технологија из разлога што дужина кључа за шифровање мора да буде исте дужине као и текст (порука) који се шифрује. Друго ограничење је избор самих кључева за шифровање који мора да задовољи одређене стандарде по питању случајности и јединствености, а није ни једноставно управљати с њима јер се, по правилу, један кључ може употребити само једном након чега се уништава. Употребом једнократне бележнице није могуће проверити идентитет пошиљаоца, а такође се мора водити рачуна да пошиљалац и прималац буду савршено синхронизовани јер у супротном порука коју прималац буде добио неће имати никаквог смисла. Примена једнократне бележнице данас има смисла једино у комуникационим каналима који захтевају веома висок ниво безбедности.

Како је апсолутну сигурност веома тешко остварити у данашње време се, у већини случајева, користе криптографски алгоритми који обезбеђују висок ниво заштите али који не задовољавају претпоставку апсолутне сигурности. Такви системи су довољно добри и поуздани да се оствари практична безбедност комуникационог канала и погодни су да се користе у рачунарским системима. Њих другим речима називамо рачунарски сигурни шифарски системи и њихова сигурност се заснива на претпоставци да противник не располаже са довољно рачунарске снаге и времена да би у реалном времену могао на неки начин да наруши њихову безбедност и обезбеди себи откривање тајне поруке, делом или у целости, или пак да дође до откривања криптографског кључа.

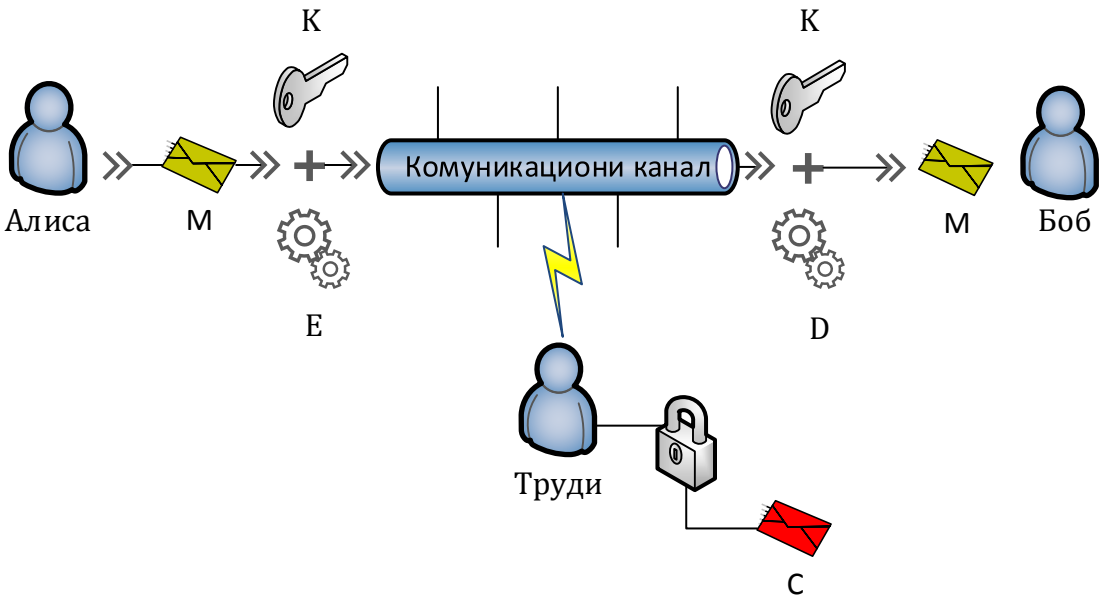
Претпоставља се да државне агенције, нпр. *CIA*, *NSA*, *BND*, *SIS* (*MI6*) и њима сличне своје криптографске алгоритме држе у тајности. Међутим, основни принцип криптоанализе, који је поставио холандски криптограф и лингвиста *Auguste Kerckhoffs* још у XIX веку, гласи да сигурност једног криптографског система треба да зависи искључиво од тајности криптографског кључа, а да је криптографски алгоритам, који се користи у поступку шифровања, опште познат. Овај фундаментални принцип се данас користи у савременој криптографији, осим могућих изузетака који се односе на државне агенције, и поузданост модерних криптографских алгоритама је вишеструко проверавана и доказивана. Када се криптографски алгоритам представи на такав начин да буде јавно доступан свима он постаје предмет научних анализа стручњака из целог света, од војних до академских, и на тај начин се врло лако открива колико је одређени поступак поуздан и да ли је отпоран на разне нападе из домена криптоанализе. На овај начин се заправо верификује његова сигурност.

Појам криптоанализа се односи на поступке који се спроводе над шифрованим текстом или поруком у циљу откривања текста или поруке, дела

текста или поруке, откривање поступка којим је извршено шифровање, откривање тајног кључа или било какве друге информације везане за шифровани текст или поруку. Увек се полази од претпоставке да противник који врши криптоанализу има неограничене ресурсе на располагању (новац, знање, рачунарске ресурсе, ...) и да има неограничено време да спроводи разне технике криптоанализе. Оно што ми једино можемо да тврдимо да је наш криптографски систем сигуран уколико је најбољи познати напад на њега напад под називом потпуна претрага кључева. Потребно је још нагласити да се дешифровање разликује од криптоанализе јер дешифровање подразумева акцију коју предузима прималац како би прочитао шифровану поруку, док криптоанализа подразумева напад на криптографски систем [42].

### 3.1.2. Симетрична криптографија

Савремени криптографски системи који користе алгоритме за шифровање симетричним кључем користе идеје које су се користиле у класичној криптографији: транспозиција (премештање) и супституција (замена). Предности које је донела савремена технологија, поготово с развојем савремених рачунара, омогућила је криптографима да креирају далеко сложеније алгоритме који се далеко брже извршавају од оних који су се користили у класичној криптографији. Принцип по коме се извршава један алгоритам за шифровање симетричним кључем приказан на слици 3:




Слика 3.3. Алгоритам за шифровање симетричним кључем приказан

Претпоставићемо да Алиса и Боб деле тајни кључ (K) и да Алиса жели да пошаље поруку (M) Бобу путем отвореног комуникационог канала [43]. Труди има могућност и одговарајуће ресурсе да пресретне шифровану поруку (C) коју Алиса шаље Бобу, међутим, Труди нема тајни кључ и није у могућности да види шта је у

поруци написано. Уколико су Алиса и Боб испоштовали фундаменталне принципе криптографије, сигурност њихове тајне комуникације зависи од тајног кључа који су користили за шифровање (E) и дешифровање (D) поруке. Математички записано:

$$E_K(M) = C$$

$$D_K(C) = M$$

тј. ове функције имају следеће својство:

$$D_K\big(E_K(M)\big) = M$$

Поред очигледних предности које доноси примена симетричне криптографије у виду брзине извршавања криптографског алгоритма, количине података који могу да се шифрују и сигурности који пружају, постоји и неколико недостатака на које Алиса и Боб морају да мисле унапред, пре него што успоставе тајну комуникацију. Уколико се Алиса и Боб налазе на удаљеним локацијама, нпр. Европа и Америка, договор око успостављања сигурног комуникационог канала је веома компликован, поготово ако узмемо и Труди у обзир.

Пре свега, Алиса и Боб морају да се договоре у вези криптосистема који ће да користе, након тога се договарају о кључу и начинима како ће исти у тајности да размене. Треба имати на уму да се овде не размењује само један кључ, већ већи број кључева који не смеју бити компромитовани. Уколико се ради о више корисника, не само о Алиси и Бобу, проблем размене кључева се додатно усложњава. Овај проблем се решава на различите начине, личном доставом, увођењем центра за дистрибуцију кључева (енгл. *Key Distribution Center – KDC*) који у целу причу уводи и "трећу страну од поверења" (енгл. *Trusted Third Party – TTP*), коришћењем криптографије са јавним кључем, итд. Поред размене кључева веома битна ствар у њиховој тајној комуникацији су сервиси аутентификације у циљу спречавања напада "човек у средини" и евентуално, уколико за тим има потребе, непорицања.

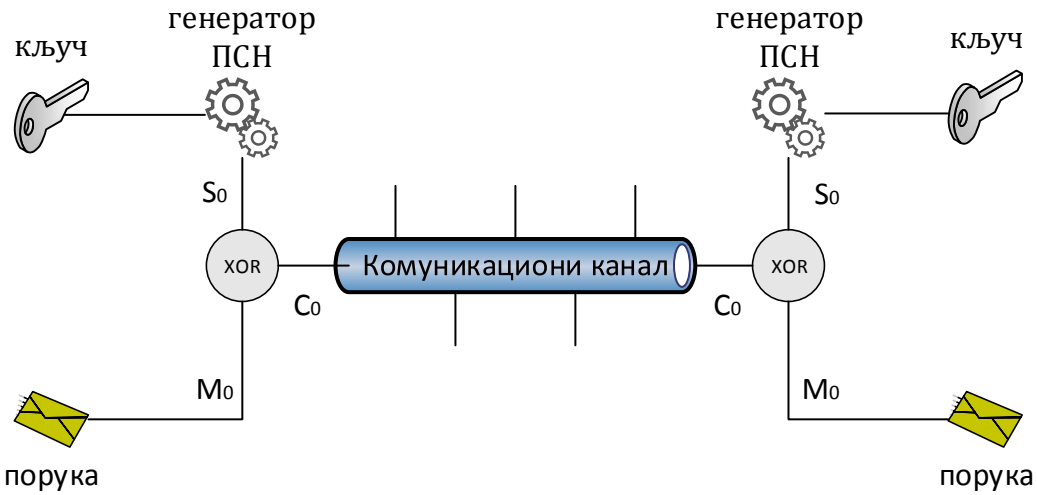
На основу начина на који обрађују податке савремене алгоритме за шифровање симетричним кључем делимо на две групе:

- Алгоритми који шифрују токове података, тј. секвенцијални шифарски системи (енгл. *stream ciphers*).
- Алгоритми који шифрују блокове података, тј. блоковски шифарски системи (енгл. *block ciphers*).

#### 3.1.2.1. Секвенцијални шифарски системи

Карактеристика секвенцијалних шифарских система је да са тајним кључем *K* иницијализује низ псеудослучајних знакова $S = [s_0, s_1, s_2, \ldots, s_i]$ које генерише генератор псеудослучајних низова. Са тако добијеним псеудослучајним низом S шифрује се *XOR* операцијом ток података $M = [m_0, m_1, m_2, \ldots, m_i]$ који представља низ карактера поруке која се шаље. Тако генерисани карактери представљају низ

шифрованих карактера $C = [c_0, c_1, c_2, \ldots, c_i]$, који се другим именом зове шифрат [44]. Дешифровање се врши на идентичан начин обрнутим поступком од шифровања. За сваку успоставу везе између пошиљаоца и примаоца користи се нови сесијски кључ који се користи заједно са тајним кључем за добијање псеудослучајног низа.




Слика 3.4. Секвенцијални шифарски систем – почетно стање

Секвенцијални шифарски системи нуде знатно боље перформансе у поређењу са блоковским шифарским системима, бар за фактор 4 – 5 ако се тај фактор мери брзином. Међутим, сигурност модерних секвенцијалних шифарских система није толико добра као код алгоритама који шифрују блокове података. Већина секвенцијалних шифарских система који су широко распрострањени, попут *RC4* и *A5/1*, имају сигурносне слабости [45, 46].

Алгоритми који шифрују токове података, иако имају одређене сигурносне слабости, користе се најчешће за специјалне намене, попут *RC4* у рачунарским мрежама или *A5/1* у мобилним *GSM* мрежама.

### 3.1.2.2. Блоковски шифарски системи

Алгоритми који шифрују блокове података деле поруку на блокове тачно одређене величине и шифрује их тајним кључем који је исте величине као и генерисани блок података. Заправо, блоковски алгоритам користи два улаза, кључ и блок бита који су исте величине чиме се добија шифрован блок, такође исте величине. На излазу се шифрован блок трансформише тајним кључем поново у отворен текст [47].

Два опште прихваћена принципа за дизајнирање практичних шифарских система, према сугестији Клода Шенона[2], су принципи конфузије (енгл. *confusion*) и дифузије (енгл. *diffusion*). Блоковски шифарски системи комбинују та два основна принципа чиме се добија задовољавајућа комплексност алгоритма. Својство

[2] Амерички научник и инжењер који је поставио основне принципе о теорији информација.

конфузије треба да обезбеди минималну статистичку везу између поруке и шифрата, док својство дифузије треба да обезбеди да сваки бит поруке утиче на што већи део шифрата. Блоковски шифарски системи, у зависности од избора алгоритма који се користи, задовољавају својства и циљеве везано за сигурност и ефикасност, а најчешће се реализују софтверски [38, 40].

Најзаступљенији алгоритми који се користе у блоковским шифарским системима су DES (енгл. *Data Encryption Standard*), његова побољшана верзија 3DES (енгл. *Triple Data Encryption Standard*) и AES (енгл. *Advanced Encryption Standard*). Иако је избор *DES* алгоритма за шифровање пратило низ контраверзних ситуација у које је била умешана америчка агенција *NSA*, која је била одговорна за то да се иницијална величина кључа за шифровање смањи на 56 бита чиме је сам алгоритам знатно ослабљен, *DES* је постао опште прихваћени стандард за шифровање средином '70-их и '80-их година XX века. Што се тиче саме умешаности *NSA* агенције у креирање *DES* алгоритма, постоје одређена мишљења да је *NSA* заправо ојачала *DES* алгоритам заменом тзв. *S*-кутија које су нудиле заштиту против до тада непознатих криптоаналитичких напада. У сваком случају, *DES* алгоритам је успешно одолевао 30-ак година интензивним криптоаналитичким нападима читаве научне заједнице, а данас је постао рањив само због мале дужине кључа (56 бита) који се користи.

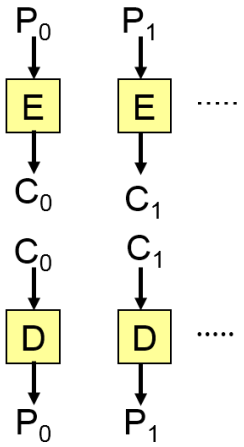
Крајем '90-их амерички Национални институт за стандарде и технологију (енгл. *National Institute of Standards and Technology – NIST*) покренуо је процес за избор новог криптографског стандарда. Овога пута сам процес избора новог стандарда је био транспарентан и укључивао је велики број предлога послатих од стране научне и стручне јавности широм света. *NSA* је и овога пута учествовала у избору новог стандарда али овога пута само као један од судија. Изабран је криптографски алгоритам који су развили Јоан Дајмен (*Joan Daemen*) и Винсент Рејмен (*Vincent Rijmen*), белгијски криптографи, који је првобитно по њиховим именима био назван *Rijndael*. *NIST* је 2001. године прогласи овај алгоритам победником који је назван *AES*. О овом алгоритму је доступно пуно информација и може се тврдити да у историји ниједан криптографски алгоритам није био испитиван као *AES*. Отпоран је на све познате нападе и шифрује блокове величине 128 бита кључевима од 128, 192 и 256 бита, што значи да *AES*-ом можемо шифровати блок од 128 бита кључем од 256 бита.

Веома битан параметар који користе сви алгоритми који шифрују блокове података је начин на који то раде. Начин рада блоковског система за шифровање директно утиче како ће се шифровани блокови спајати у коначан шифрат. Такође, одабир овог параметра директно утиче на брзину рада блоковског шифарског система. Постоје многи режими који се користе у блоковским шифарским системима, а међу њима се издвајају:

- Режим "електронске кодне књиге" (енгл. *Electronic CodeBook – ECB*).
- Режим уланчавања блокова (енгл. *Cipher Block Chaining – CBC*).

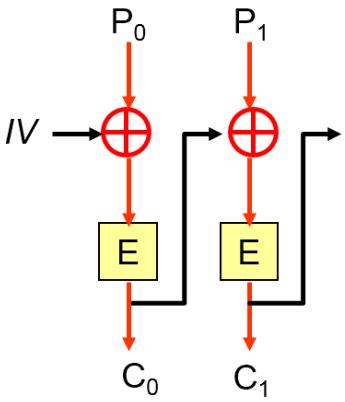
- Режим бројача (енгл. *CounTeR mode – CTR*).

Режим *ECB* је једноставан и популаран начин примене блоковске шифре. У овом режиму рада један блок отвореног текста се претвара у исти блок шифрата. Такав начин шифровања је идентичан шифровању са кодном књигом, који се раније користио кроз историју, па одатле и потиче назив "електронска кодна књига", слика 3.5. Блокови отвореног текста се шифрују независно, могуће је шифровати прво блокове у средини, затим на крају текста, па тек онда оне на почетку текста. Међутим, постоји озбиљан недостатак у примени овог режима који наводи на то да се овај режим шифровања не би требао примењивати у пракси. Можемо да претпоставимо да нападач зна део отвореног текста и да поседује неколико шифрованих блокова. Нападач сада може да покрене напад превођења кодне књиге иако не зна тајни кључ јер свако подударање шифрованог блока са блоком отвореног текста отвара нови блок [37, 38].



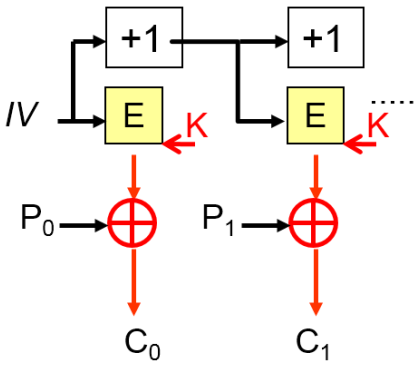

Слика 3.5. *ECB* режима рада

Режим *CBC* је најчешће коришћени режим шифровања који блоковској шифри додаје механизам повратне спреге чиме се добија да је резултат шифровања претходног блока заправо улазна вредност за шифровање наредног блока. Почетни блок у *CBC* режиму шифровања се сабира (*XOR*) са иницијалним вектором *IV* који се генерише на потпуно случајан начин, а његова дужина одговара величини блока и користи се само за генерисање првог блока шифрата. Предност оваквог начина коришћења блоковске шифре се огледа у томе да исти блок отвореног текста неће одговарати истом блоку шифрата. Ова особина *CBC* режима шифровања даје додатни ниво сложености шифрованим подацима. *CBC* режим шифровања је безбеднији од *ECB* режима шифровања.




Слика 3.6. *CBC* режима рада

Режим *CTR* је специфичан по томе што омогућава потпуну независност између блокова. Пошто су сви блокови независни једни од других могу се паралелно обрађивати што убрзава израчунавање шифрата из блока отвореног текста и обрнуто. Као и код *CBC* режима и овде се употребљава иницијални вектор *IV* који се шифрује, а затим сабира (*XOR*) са блоком отвореног текста. Почетна вредност бројача је број један и за сваки наредни блок вредност бројача и иницијалног вектора се увећава за један [48].




Слика 3.7. *CTR* режима рада

Може се закључити да се *CTR* режим понаша као секвенцијална шифра.

### 3.1.3. Асиметрична криптографија

Рад који су *Whitfield Diffie* и *Martin Hellman* објавили 1976. године представљао је идеју криптографије у којој није било неопходно да две стране у шифрованој комуникацији поседују исти кључ [48]. Две године касније *Kohnfelder* је у свом дипломском раду [50] представио појам сертификата као дигитално потписаног податка који везује јавни кључ са особом којој тај кључ припада, док су *Rivest*, *Shamir* і *Adleman* пронашли метод практичне реализације асиметричне криптографије [51], по којима је назван најпознатији алгоритам асиметричне криптографије – *RSA*. Ово су биле основне идеје које су уз појаву интернета довеле

до развоја асиметричних шифарских система, који се сматрају за једно од највећих историјских достигнућа у криптографији.

Принцип коришћења два кључа, јавног и приватног, је приказан на примеру комуникације између Алисе и Боба, слика 3.8:


Слика 3.8. Принцип слања шифроване поруке у асиметричној криптографији

Карактеристика и основна разлика асиметричне криптографије у односу на симетричну криптографију је та да се у асиметричној криптографији користе различити кључеви за шифровање и дешифровање података. Често се за асиметричну криптографију у литератури наводи да је то криптографија са јавним кључем (енгл. *Public Key Cryptography*). Објављивањем једног кључа који постаје јавни податак не угрожава се тајност другог кључа. Суштина је у томе да се јавни кључ користи за шифровање, а приватни кључ, који се увек чува у тајности, користи за дешифровање. Користећи нотацију која је наведена за шифровање и дешифровање код симетричних криптографских система, математички записано асиметрична криптографија, уз додатак да јавни кључ обележавамо са ЈК, а приватни кључ са ПК, се користи на следећи начин:

$$E_{\text{ЈК}}(M) = C_1$$

$$D_{\text{ПК}}(C_1) = M$$

Шифровање приватним кључем, што се искључиво користи код дигиталног потписивања математички може да се прикаже као:

$$E_{\text{ПК}}(M) = C_2$$

$$D_{\text{ЈК}}(C_2) = M$$

Први корак у комуникацији је да Алиса затражи од Боба његов јавни кључ ($ЈК_{Боб}$). Боб без икакве бојазни свој јавни кључ може да објави или да га пошаље Алиси путем отвореног комуникационог канала. Алиса сада може да шифрује поруку Бобовим јавним кључем са одговарајућим асиметричним алгоритмом и да тако шифровану поруку пошаље Бобу. Труди је могла да преузме Бобов јавни кључ и да пресретне Алисину шифровану поруку, међутим, Труди не може да дође до отвореног текста јер Бобов јавни кључ служи само за шифровање порука. Када Боб прими шифровану поруку од Алисе он ће уз помоћ свог приватног кључа ($ПК_{Боб}$) и одговарајућег асиметричног алгоритма да дешифрује и прочита поруку. Алиса у сваком тренутку може да тражи од Боба да се представи како би се уверила да се Труди није умешала у њихову комуникацију. Боб то ради на врло једноставан начин тако што шифрује поруку, нпр. "*Ја сам Боб*", својим приватним кључем и шаље је Алиси. Алиса ту поруку може да дешифрује само са Бобовим јавним кључем чиме се потврђује Бобов идентитет. Труди то такође може да уради али она сем чињенице коју већ зна, да је Боб послао ту поруку, не може да дође ни до којег другог битног податка везаног за шифровану поруку или кључа којим је она шифрована.

Само је мали број асиметричних алгоритама истовремено и сигуран и практичан. Од сигурних и практичних алгоритама с јавним кључем неки су погодни само за шифровање, док су поједини погодни само за дигиталне потписе. Само три алгоритма добро функционишу и за шифровање и за дигиталне потписе: *RSA*, *ElGamal* и *Rabin*. Сви ови алгоритми су спори, они шифрују и дешифрују податке много спорије него симетрични алгоритми, а то је обично преспоро да би се обављало масовно шифровање података [37].

Особине асиметричних алгоритама које произилазе из једноставности коришћења, омогућиле су низ функционалности које се тешко или никако користе у симетричним шифарским системима. Аутентификација, интегритет, тајност и непорецивост су четири кључне услуге која на једном месту обезбеђује асиметрична криптографија. Рад асиметричних криптографских алгоритама се заснива на математичким једносмерним функцијама са замком. Ове функције имају специфичну особину да се лако израчунавају у једном смеру, док је инверзна операција, односно израчунавање у супротном смеру практично неизводљиво. Замка која се помиње се односи на особину која омогућава ономе ко поседује јавни и приватни кључ да дешифрује шифроване поруке.

Факторизација производа веома великих простих бројева је прави пример за једносмерну функцију. Лако се израчунава производ два велика проста броја $p$ и $q$, $N = p \times q$, међутим, веома је тешко из производа $N$ израчунати факторе $p$ и $q$ уколико су они непознати ономе ко покушава да их израчуна. [52, 38].

#### 3.1.3.1 *RSA* асиметрични алгоритам

Већ је напоменуто да се у асиметричној криптографији користе два кључа, јавни и приватни кључ. *RSA* приватни кључ се генерише уз помоћ два насумично изабрана велика проста броја, нпр. за кључ од 2048 бита бирају се прости бројеви од 1024 бита [53, 54]. Сигурност *RSA* алгоритма се заснива на претпоставци да је немогуће извршити факторизацију производа два велика насумично изабрана проста броја на чиниоце. Ради се дакле о претпоставци јер не постоје математички докази који би процес факторизације једног тако великог броја скратио и учинио бржим.

За израчунавање приватног кључа се користи модуларна аритметика. У литератури параметри за израчунавање кључева се најчешће означавају са $p$ и $q$. Препорука је да се прости бројеви за ова два параметра изаберу тако да имају одређене особине које њихов производ, који се иначе означава са $n$, чини тешким за факторисање. Због упрошћеног приказа се најчешће бирају мали прости бројеви с којима се приказује поступак израчунавања приватног кључа [38, 55, 56, 57]. Важно је напоменути да параметри $p$ и $q$ никада не смеју да буду разоткривени и да је због тога добра пракса да се они униште након израчунавања јер се сигурност приватног кључа заснива на тајности ова два параметра.

Процес израчунавања се може приказати на једноставан начин, уз чињеницу да се јавни кључ обележава са $e$, а приватни кључ са $d$. Приликом израчунавања приватног кључа потребно је изабрати јавни кључ на тај начин да буде задовољен услов да су $e$ и производ $\varphi$ узајамно прости. Најмањи заједнички делилац бројева $e$ и $\varphi$ обележавамо са *gcd* (енгл. *greatest common divisor* – *gcd*). Упоредо са теоретским, биће приказан и практичан део израчунавања.

За показни пример бирамо да је $p = 11$, а $q = 47$.

$$n = p \times q$$

$$n = 11 \times 47 = 517$$

$$\varphi = (p - 1) \times (q - 1)$$

$$\varphi = (11 - 1) \times (47 - 1) = 460$$

$$e = 13$$

$$gcd(e, \varphi) = 1$$

$$gcd(13, 460) = 1$$

$$d = e^{-1}\ mod\ \varphi$$

$$d = 13^{-1}\ mod\ 460 = 177$$

Сада $e$ и $n$ могу да се јавно објаве, $d$ се чува у тајности, а $p$ и $q$ се уништавају.

Алгоритми за факторизацију се стално унапређују, међутим, не толиком брзином да би се могло рећи да је *RSA* кључ дужине од 2048 бита угрожен. Ова дужина кључа је у великој мери још увек у комерцијалној употреби и по препорукама, које је објавио *NIST* у 2019. години [58], он задовољава минималну безбедносну снагу.

*RSA* алгоритам је веома спор јер се користе веома велики бројеви што у знатној мери успорава процес шифровања и дешифровања. Ова чињеница у пракси значи да се са *RSA* алгоритмом неће шифровати поруке које садрже много текста, већ кратке поруке које би могле да буду носиоци тајних кључева симетричне криптографије. *RSA* алгоритам је погодан и за дигитално потписивање, чиме се обезбеђују сервиси аутентификације, интегритета и непорецивости. Потребно је напоменути да се дигитално потписивање врши са приватним кључем. Комерцијална употреба *RSA* алгоритма подразумева употребу инфраструктуре јавних кључева, што у целу причу уводи и "трећу страну од поверења".

### 3.1.3.2 Сертификациона тела

Сложени систем уз помоћ кога се одвија сигурна комуникација назива се Инфраструктура јавних кључева (*Public Key Infrastructure – PKI*). Основа сваког *PKI* система је сертификационо тело (*Certification Authority – CA* ). Сертификационо тело је најважнији модул и основа поверења сваког *PKI* система [59].

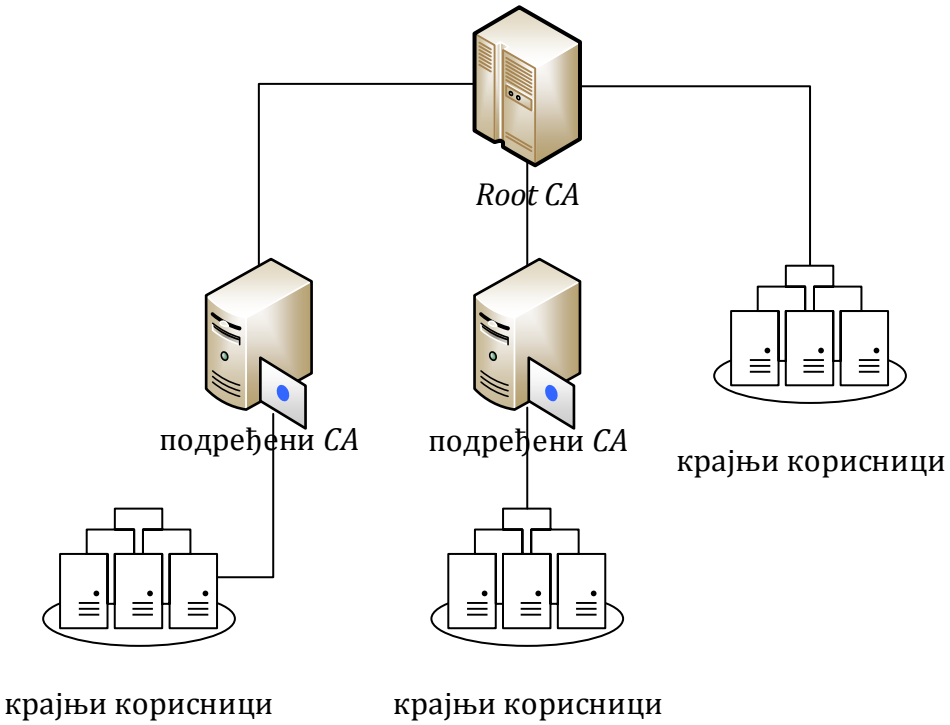
*PKI* систем је изграђен као комбинација хардверских и софтверских решења, криптографских алгоритама и услуга које у потпуности омогућавају државним организацијама, компанијама и појединцима да обезбеде сигурност својих комуникација и пословних трансакција. Овакав систем интегрише дигиталне сертификате, криптографију јавног кључа и сертификациона тела у комплетну мрежну сигурносну архитектуру које обухвата издавање дигиталних сертификата појединим корисницима [60].

Сертификационо тело је неопходно у процесу издавања дигиталних сертификата јер представља институцију од поверења. Поверење је основа сигурних комуникација. Заправо, свака врста идентификације, која је први критеријум сигурних комуникација, је заснована на поверењу. Људе и предмете које непосредно познајемо идентификујемо директно. Људе и предмете које не познајемо директно идентификујемо преко неког другог. Потпуне странце у службеним контактима идентификујемо преко идентификационих докумената. Овим документима верујемо јер их је издала установа којој верујемо. Иста та установа је издала и наше идентификационе документе. Ми верујемо и идентификационим документима које је издала нека друга установа, а не наша, на основу тога што је наша установа којој верујемо рекла да верује тој другој установи (нпр. пасоши). Наведени примери представљају моделе поверења. Постоји више формалних подела модела поверења у свету дигиталних сертификата али би се основна подела могла направити на директно и индиректно поверење [61, 62].

Модел директног поверења односи се, пре свега, на то да дигиталном сертификату верујемо јер знамо коме припада, односно на неки начин смо се уверили да дигитални сертификат припада свом наведеном власнику. Овакав модел поверења нема велику практичну примену осим за ужи круг људи који се међусобно познају. Асиметрична криптографија омогућава људима који се не познају сигурну и поверљиву електронску комуникацију. Овакав вид комуникације имплицира модел индиректног поверења. Модел индиректног поверења се дели у две главне групе [61] које заправо представљају моделе поверења које људи користе у приватним и пословним контактима.

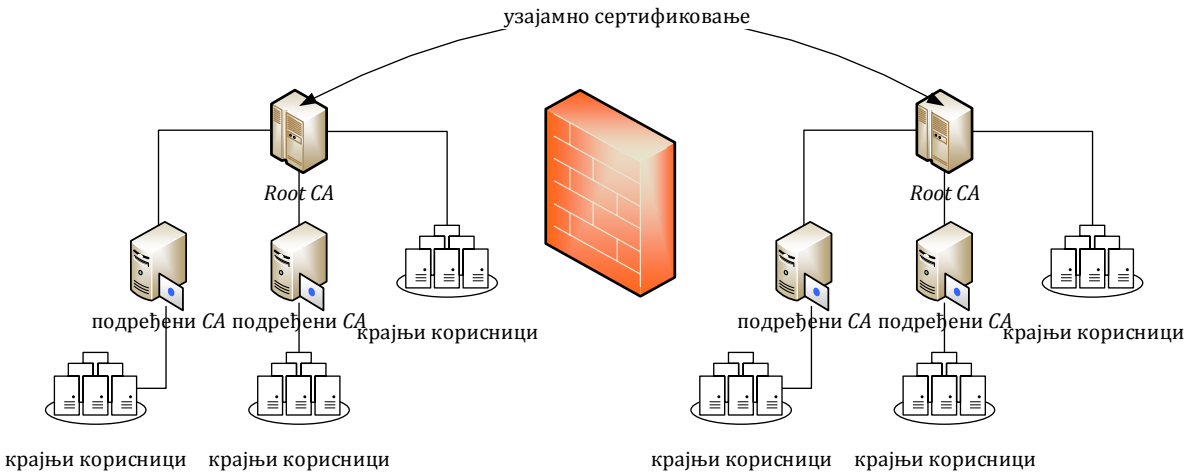
Када комуницирају међусобно људи често верују у препоруке других људи које врло добро познају. Ако овакав вид поверења пренесемо на дигиталну сертификацију могли би смо да успоставимо мрежу поверења (*Web of Trust*). Међутим, у овакво успостављеној мрежи поверења дигиталне сертификате не потписује *CA* већ корисници овакве мреже се узајамно сертификују. Наравно, одмах се уочава и ограничење у коришћењу оваквог система јер није применљив ван оквира уског круга људи који се међусобно познају и верују једни другима. За разлику од оваквог модела, у пословним и њима сличним комуникацијама, сервиси државне електронске управе, корисници се ослањају на неку организацију која гарантује за идентитет својих чланова.

Класичан хијерархијски модел поверења је заснован на једној врховној сертификационој установи (*Root CA*) од које потичу сви сертификати унутар једне мреже поверења, слика 3.9.




Слика 3.9. Хијерархијски модел поверења

*Root CA*, као врховно тело од поверења, коме сви корисници те мреже верују, у најчешћем броју случајева издаје сертификате подређеним сертификационим установама, које даље могу да издају сертификате установама које су подређене директно њој или пак крајњим корисницима. Међутим, *Root CA* може такође, што је заправо ређи случај, да дигиталне сертификате издаје директно крајњим корисницима. Издавање сертификата на овај начин, унутар мреже поверења за коју је надлежна *Root CA* представља један ланац повезивања у коме корисници овакве мреже од поверења могу да буду сигурну и идентитет других корисника исте те мреже. Једни начин да се корисници ове мреже од поверења повежу са корисницима друге мреже од поверења је да се оствари узајамно сертификовање врховних сертификационих тела (*cross-certification*), слика 3.10 [62].




Слика 3.10. Узајамно сертификовање - *cross-certification*

*Root CA* по правилу не би требало да буде повезан на мрежну инфраструктуру – интернет. Потребно је да се налази у посебно заштићеној просторији која је отпорна и на електро-магнетно зрачење и постоји низ строгих правила по којима ради. Сертификационо тело мора да подржава различите хардверске елементе као што су "паметне" (*smart*) картице, *HSM* модули (*hardware security module*), *USB* токени, итд. Сертификационо тело, такође, мора да подржава различите алгоритме за симетрично и асиметрично шифровање, а неопходно је да подржи следеће алгоритме за дигитално потписивање: *RSA*, *DSA* и *ECDSA*.

Технички гледано сертификационо тело треба да обавља следеће задатке:

- регистрацију корисника (може то да ради и регистрационо тело),
- иницијализацију корисника (може то да ради и регистрационо тело),
- сертификацију корисника,
- међусобно сертификовање,
- потхрањивање кључева,
- ажурирање кључева,
- опозивање сертификата и
- вођење евиденције о опозваним сертификатима.

### 3.1.3.3. Принцип рада сертификационог тела

*CA* најчешће представља државну институцију или компанију које задужено за издавање дигиталних сертификата крајњим корисницима. Што се тиче самих корисника, *CA* представља тзв. "трећу страну од поверења" (енгл. *Trusted Tthird Party – TTP*) којој сви корисници верују. *CA* поверење гради на принципу пирамиде, на чијем се самом врху налази *Root CA*. Једино *Root CA* може самом себи да потпише дигитални сертификат и оно најчешће сертификује подређене *CA* (*Intermediate CA – ICA*) која под одређеним условима издају и повлаче дигиталне сертификате крајњим корисницима.

Приликом издавања дигиталног сертификата крајњем кориснику *CA* мора да изврши потпуну проверу података о крајњем кориснику како би исти били уписани у корисников дигитални сертификат потписан од стране *CA* чиме се гарантује тачност података. Све поступке везане за проверу и регистрацију нових корисника *CA* може да препусти телу под називом регистрациони тело (енгл. *Registration Authority – RA*). Издати дигитални сертификат гарантује да је јавни кључ који је записан у дигиталним сертификату и који може бити јавно објављен у власништву корисника коме је дигитални сертификат и издат. Овом се успоставља поверење између крајњих корисника ове мреже од поверења јер сви корисници знају да је гарант *Root CA* [64].

Важна карика у ланцу поверења које ствара једно сертификационо тело и листа опозваних сертификата (*Certificate Revocation List – CRL*). Дигиталним сертификатима издатим од стране *CA* може да истекне рок важења, да корисник сам поднесе захтев за укидање дигиталног сертификата, да дође до компромитације приватног кључа који је записан у дигиталном сертификату и да због тога дигитални сертификат мора да буде опозван, итд. Сви ти разлози доводе до тога да сертификационо тело мора да направи једну листу или електронски репозиторијум који ће да садржи листу свих опозваних сертификата и да је јавно објављује како би била доступна свим учесницима у његовој мрежи поверења.

Сертификационо тело најчешће јавно објављује документе који регулишу његов рад и односе се на разна правила из домена његовог рада. Ти документи се по правили зову Политика сертификације (енгл. *Certificate Policy – CP*) и Практична правила рада сертификационог тела (*Certificate Practice Statement – CPS*).

*PKI* са припадајућим системима корисницима обезбеђује поуздан сервис за пренос информација у дистрибуираним системима тиме што обезбеђује [65]:

- Аутентификацију учесника у комуникацији.
- Интегритет размењених порука.
- Непорецивост јер нико не може да тврди да поруку није послао.
- Тајност јер поруке могу да се шифрују кључевима записаним на дигиталном сертификату.

Иако је доста ствари регулисан према строгим правилима општи стандард који се односи на поделу *PKI* система не постоји.

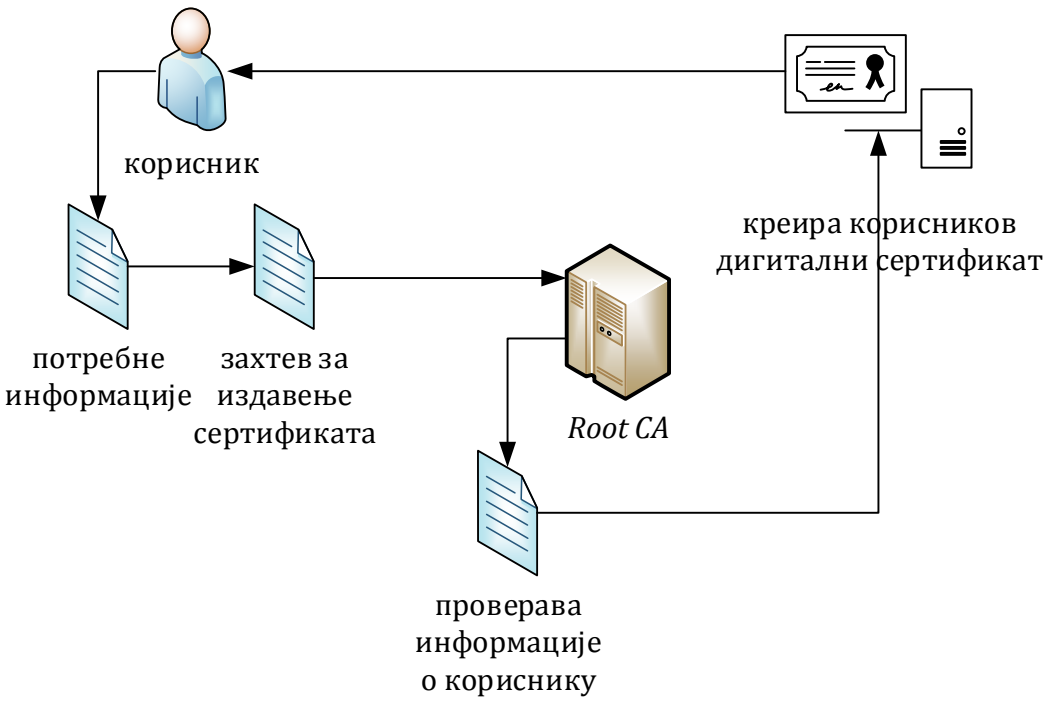
### 3.1.3.4. Дигитални сертификат

Дигитални сертификат је дигитално потписан документ који повезује јавни кључ са особом којој тај кључ припада (власником јавног кључа). Као што својим личним идентификационим документом доказујемо свој идентитет на разним местима као што су државна управа, банке, поште, и томе сл., дигиталним сертификатом доказујемо свој идентитет на интернету. Сертификат се дигитално потписује да би се обезбедио његов интегритет. Интегритет дигиталног сертификата гарантује потписник, а потписник је у овом случају *CA*.

Дигитални сертификат најчешће садржи:

- податке о власнику сертификата,
- јавни кључ власника сертификата,
- период важења сертификата,
- име издавача (сертификационо тело које је издало сертификат),
- серијски број сертификата и
- дигитални потпис издавача.

Добијање сертификата од *CA*:




Слика 3.11. Шематски приказ издавања дигиталног сертификата

*CA* је установа која складишти информације о идентитету физичких и правних лица. Кориснику који почиње са комуникацијом прво захтева од другог учесника да му потврди свој идентитет. Њему је довољно да провери преко

установе која је издала сертификат да ли је он још увек валидан и да ли он заиста припада ономе с ким жели да комуницира. Из дигиталног сертификата лако може да преузме јавни кључ и да започне са тајном комуникацијом. [66].

Дигитални сертификати према намени издавања се деле на: личне – за грађане, пословне – правне субјекте и тела државне управе. Према нивоима сигурности сврставају се у 3 категорије:

- Стандардна – ниво који је прикладан за ризике и последице који немају већу важност. То може бити приступ тајним подацима за које вероватноћа злонамерног приступа није велика. За овај сигурносни ниво се подразумева да је вероватноћа да корисници буду злонамерни мала.
- Средња - овај ниво је прикладан за околине у којима су ризици и последице компромитовања података умерени. Може се користити у трансакцијама које имају знатну новчану вредност или ризик од фалсификовања, или у онима у које је укључен приступ тајним информацијама за које је вероватноћа злонамерног приступа знатна.
- Висока - ниво прикладан за употребу у трансакцијама у којима је угроженост података висока или су последице пропуста у систему заштите велике. То су трансакције врло високе вредности или са великим ризиком од фалсификовања.

### 3.1.3.5. Структура дигиталног сертификата

Најзаступљенији формат сертификата који се користи у *PKI* системима је *X.509*. Овај формат дефинишу *ISO* и *ITU-T* [67]. *X.509* формат подржавају водећи *PKI* -омогућени протоколи и апликације као што су *SSL*, *IPSec*, *S/MIME*, *Privacy Enhaced Mail* (*PEM*) и *SET*. Други формат сертификата који није стандардизован од стране званичних институција али је довољно заступљен да га је неопходно споменути је *PGP* [68]. Овај формат се користи у врло раширеном софтверском пакету истог назива *PGP* (*Prety Good Privacy*).

| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 0b 7c ad 5f 69 1d 72 bd |
| Signature algorithm | sha512RSA |
| Signature hash algorithm | sha512 |
| Issuer | MUPCA Gradjani 3, MUPCA... |
| Valid from | Thursday, November 26, 2... |
| Valid to | Thursday, November 26, 2... |
| Subject | АЛЕКСАНДАР МИШКОВИЋ... |

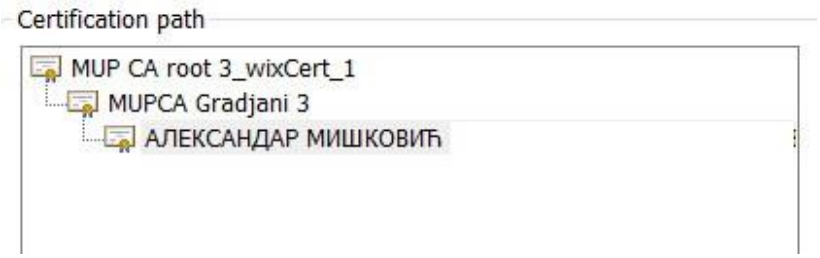
| Field | Value |
|---|---|
| Public key | RSA (2048 Bits) |
| Basic Constraints | Subject Type=End Entity, P... |
| Enhanced Key Usage | Secure Email (1.3.6.1.5.5.... |
| Authority Key Identifier | KeyID=66 2d c5 52 9e 23 0... |
| Subject Key Identifier | 94 1d d7 e3 7f 78 01 fd 45 ... |
| CRL Distribution Points | [1]CRL Distribution Point: D... |
| Qualified Certificate Sta... | 30 14 30 08 06 06 04 00 8... |
| Authority Information A... | [1]Authority Info Access: A... |

Слика 3.12. *X.509 ver3* стандардни сертификат

Сертификати издати од стране *PKI* системима по формату *X.509* дефинишу формат и поља у којима се уписују информације о издатом сертификату, слика 3.12.

Поља од посебног значаја су:

- Верзија: У овом примеру се ради о сертификату верзије 3.
- Серијски број сертификата: *CA* издаје јединствени серијски број.
- Алгоритам потписивања и криптографска хеш функција: Идентификација дигиталног потписа који користи *CA*.
- Издавач: *CA* које је издало дигитални сертификат, записан по стандарду *X.500*, који дефинише стабло или структуру директоријума чиме се дефинише ланац сертификације, слика 3.13.
- Период важења: У овим пољима је записан датум издавања и престанка важења дигиталног сертификата.
- Име корисника: Име и презиме корисника коме је издат дигитални сертификат, такође записан по стандарду *X.500*.
- Јавни кључ: У приказаном примеру ради се о *RSA* кључу за дигитално потписивање.
- Проширења: Ова поља садрже додатне информације о *CA*, кориснику, екстензије које садржи дигитални сертификат, листи опозваних сертификата итд.




Слика 3.13. Ланац сертификације

У свету постоји велики број компанија које користе *X.509 ver3* стандардни сертификат. Међу њима су и светски познате *VISA* и *MasterCard*.

### 3.1.3.6. Издавање дигиталног сертификата

Да би сертификационо тело издало дигитални сертификат кориснику морају да се изврше следеће процедуре:

- преузимање личних податке од корисника,
- преузимање јавног кључа корисника или генерисање истог од стране *CA* (чешћи случај),
- форматирање преузетих података на стандардан начин (нпр. *X.509 ver3* формат),
- дигитално потписивање форматираних података.

*CA* јавни кључ може да добије од самог корисника и да га сертификује или да генерише пар асиметричних кључева (јавни и приватни кључ) за сваког корисника па да их дистрибуира заједно са сертификатом. Уколико корисник сам генерише

пар асиметричних кључева може да захтева од *CA*, само у одређеним случајевима који се могу ретко срести у практичној промени, да му изда дигитални сертификат који садржи његов јавни кључ. Овај метод је добар са становишта безбедности корисника јер се приватни кључ увек чува само на једној локацији тј. код самог корисника. Међутим, поменути разлози могу се оправдати само са становишта корисника. Са становишта *CA* сигурније је да само *CA* буде надлежно за генерисање парова асиметричних кључева јер се једино на тај начин може контролисати и одржати квалитет генерисаних кључева као и спровођење процедура за безбедно чување истих.

Корисник се обраћа *CA* захтевом за издавање сертификата (енгл. *certification request*). Како се све у вези *PKI* система ради по одговарајућим стандардима и процедурама, тако постоји и стандард који прописује како ће корисник да поднесе захтев за издавање сертификата. Најчешће коришћени стандард за подношење захтева носи ознаку *PKCS#10*.

Први корак у процесу пријављивања је регистрација при којој се проверава идентитет крајњег корисника који подноси захтев за сертификатом. Ниво провере идентитета зависи од типа сертификата за који се подноси захтев. За сваки тип сертификата дефинисан је одговарајући документ који се назива политика сертификације. Иницијализација је следећи корак у регистрацији у оквиру кога крајњи корисник и сертификационо тело размењују неопходне информације за даљу комуникацију [64]:

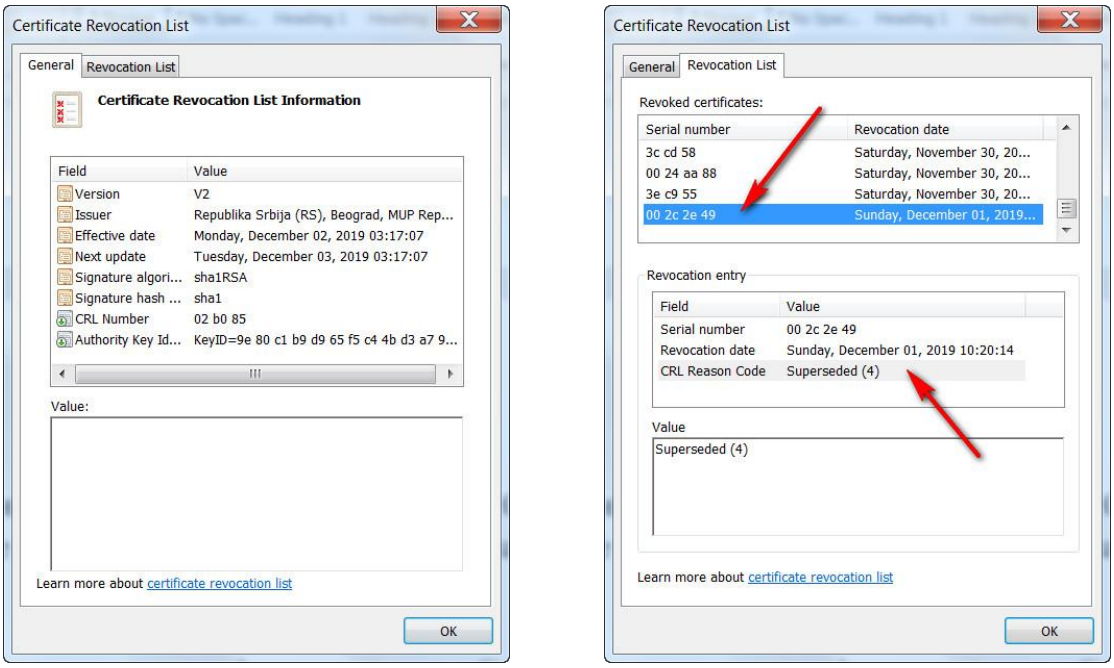
- како ће се одвијати сама комуникација,
- како ће се дистрибуирати сертификати,
- на који начин се успоставља сигурна комуникација између крајњих корисника и сертификационог тела,
- како се генерише и доставља пар асиметричних кључева итд.

### 3.1.3.7. Листа опозваних сертификата

Као што је већ напоменуто, дигитални сертификат има датум издавања и датум када истом истиче валидност. Колико дуго ће један сертификат да важи зависи од унутрашње политике коју *CA* спроводи према одговарајућим, унапред прописаним, правилима. Већ је напоменуто да постоје различите ситуације када дигиталном сертификату престаје употреба. *CA* је дужан да све опозване сертификате чува и јавно објављује у виду *CRL* преко одговарајућег дигиталног репозиторијума. *CRL* мора да буде дигитално потписана од стране *CA* које је дужно да је редовно ажурира и објављује. Начин на који то *CA* ради и у којим временским оквирима није на прецизан начин стандардизовано и зависи искључиво од унутрашње политике коју спроводи *CA*. Низом правила [69] дефинисан је начин издавања *CRL*, одговарајући управљачки протокол и низ операционих протокола (*HTTP, LDAP,...*) за достављање *CRL* до клијената. [66].

Проверу дигиталних сертификата, а самим тим и јавних кључева, корисници *PKI* система раде преко *CA* тела или преко неког другог тела које је ауторизовано од стране *CA* тела. *CRL* омогућује ентитетима који комуницирају у датом *PKI* систему проверу валидности дигиталних сертификата друге стране у комуникацији [70].

*PKI* системи који користе *X.509 ver3* сертификат, *CRL* својим корисницима доставља најчешће коришћењем *LDAP* (*Lightweight Directory Access Protocol – LDAP*) протокола. слика 3.14. Такође су заступљени методи слања *CRL* од стране *CA* тела или повлачења *CRL* од стране корисника са репозиторијума на коме се она објављује. *CRL* је који корисницима омогућава да виде низ података, а међу битније се убрајају датуми објављивања *CRL* и датум објављивања нове *CRL*, слика 3.14.




Слика 3.14. Приказ *CRL* листе

Постоје и разни други начини за проверу опозваних сертификата, а који ће да се користи највише зависи од прописа и правила којима се дефинише рад једног *PKI* система. Познати су протоколи који корисницима могу у реалном времену да да ју одговор да ли је дигитални сертификат повучен или не. Један од таквих протокола је *OCSP* (*Online Certificate Status Protocol*) протокол који користи две методе за добијање информације о валидности дигиталног сертификата. *OCSP* сервер такође периодично преузима или прима информације од *CA* тела о валидности дигиталних сертификата који се даље корисницима прослеђује у реалном времену [71]. Начини на који овај протокол може бити имплементиран у *PKI* систем је дефинисан и одобрен од стране *IESG* (*Internet Engineering Steering Group – IESG*)[72].

## 3.2. Стеганографија

Историјски гледано стеганографија и криптографија имају исту временску линију. Постоје историјски записи у којима је наведено да се стеганографија користила од давнина, око 500. године пре нове ере. Како што је то случај код криптографије и стеганографија се користила у готово свим ратним сукобима кроз историју. Њена примене није била ограничена само на војну употребу у ратним сукобима, већ се може рећи да се стеганографија користила тамо где се слање шифрованих порука забрањено и кажњиво. Много је таквих примера и данас у свету, тако да се стеганографија и даље користи. На жалост, сврха скривања порука нема увек племениту мисију, као што је то нпр. борба против угњетавања и тираније.

Развој модерне стеганографије се, као и код криптографије, поклапа са развојем рачунара. Модерна стеганографија се данас користи не само за скривање информација од потенцијалних нападача, већ је своју примену нашла и у областим заштите интелектуалне својине, маркетиншким активностима које се посебно ослањају на коришћење мултимедије (нпр. пласирање реклама путен видео преноса неког важног догађаја, спортске манифестације, и томе сл.). Са растом популарности и употребе модерне стеганографије развијају се и технике стегоанализе, чији је циљ да скривање информација открију.

Стеганографија се суштински разликује од криптографије иако се обе науке користе како би се сачувала тајност података. Међутим, за стеганографију се може рећи да је то наука о "невидљивој" комуникацији, , слика 3.15. У односу на критографију чији је циљ да тајна комуникација остане безбедна чак и ако је откривена, стеганографија има за циљ да сакрије само присуство тајне комуникације од потенцијалних нападача или посматрача уопште [73].


Слика 3.15. Модел стеганографског система

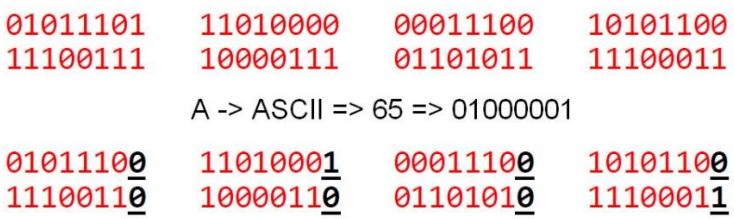
Концепт стеганографије, тј. скривања тајне поруке, се може описати помоћу тзв. појма "проблем затвореника", којим је описана тајна комуникација уз посредовање "треће стране" која је за тај вид комуникације веома заинтересована

[74]. Тајност поруке која је утиснута у стего носач се обезбеђује тајним кључем који се користи у одређеном стеганографском алгоритму. Када крајњи корисник преузме стего објекат, исти се распакује уз помоћ претходно дефинисаног тајног кључа и стеганографског алгоритма. На тај начин, крајњи корисник долази до тајне поруке. Постоје три врсте стеганографских система:

- Стеганографски системи који не користе тајне кључеве или лозинке.
- Стеганографски системи који користе тајни кључ за заштиту.
- Стеганографски системи који користе јавни кључ за заштиту.

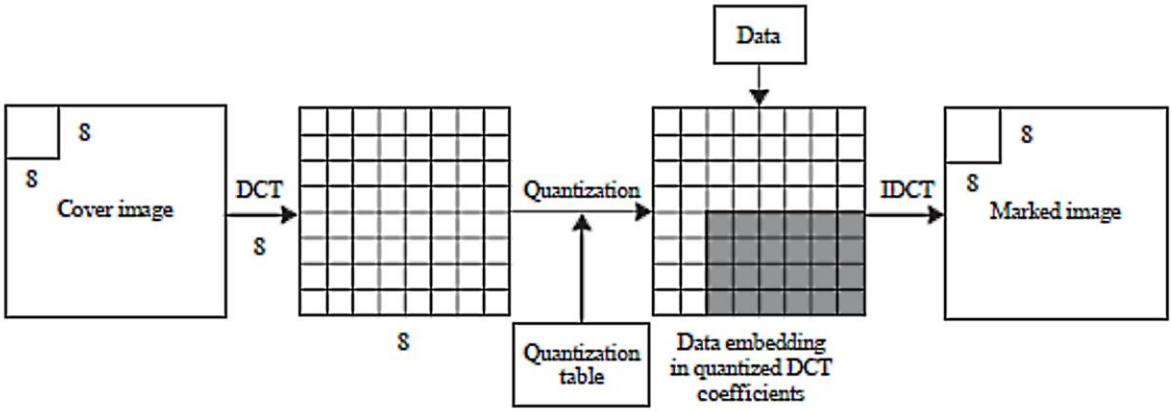
Стеганографске технике које се данас користе морају да задовоље одређене критеријуме како би тајна порука заиста била скривена у неком стего објекту. Пре свега се мора водити рачуна о капацитету који стего носач, односно покривач, поседује. Једноставно речено, постоји могућност да у стего носач уметнете поруку веома велике дужине али ће такав поступак знатно изменити изглед оригиналног фајла који бити уочљив и визуелним прегледањем истог. Технике које се користе у стеганографији су бројне, међутим, постоји неколико које се својом популарношћу, брзином трансформације, робусношћу и томе сл. издвајају од осталих. Ниједна од ових техника не гарантује потпуну безбедност, тј. функционалну методу која ће утиснути тајну информацију тако да она са сигурношћу буде "невидљива" бројним алатима који су развијени за стегоанализу. С обзиром на изнете чињенице могу се издвојити следеће стеганографске технике[75]:

- Најмање значајан бит (енгл. *Least Significant Bit – LSB*). Техника мења најмање значајне битове у стего носачу са битовима тајне поруке, слика 3.16. Најчешће се користи за мењање дигиталних слика. Међутим овај метод не пружа висок ниво сигурности јер се мењају статистичка својства коришћених датотека за стего носаче.




Слика 3.16. Уметање слова "A" у 8 бајтова стего носача

- Дискретна косинусна трансформација (енгл. *Discrete Cosine Transformation – DCT*). *DCT* коефицијенти се користе за компресију која се базира на Фуријеовој трансформацији, тј. на дискретној Фуријеовој трансформацији, трансформишући их из просторног домена у фрекфентни домен. *DCT* може да раздвоји слику на компоненте високе, средње и ниске фреквенције [76]. Најчешће се користи за уметање тајне поруке у *JPEG* слике, слика 3.17 [77].




Слика 3.17. *DCT* помоћу *JPEG* модела компресије помоћу блока величине 8 x 8 пиксела

Као што је већ напоменуто иако је употреба стеганографије, као и криптографије, потпуно легална и легитимно је право сваког појединца да те технике користи, постоје одређене ситуације када су ове технике биле и злоупотребљаване у циљу извршавања терористичких и дугих врста напада на објекте и људе. Као резултат тога, потреба за откривањем стеганографских података постала је важно питање за агенције које су задужене за безбедност у оквиру својих држава. Покушај да се открије употреба стеганографије назива се стеганализом где се открива присуство скривених података. Због огромног броја техника скривања подата употребом стеганографије, откривање свих скривених података је веома тежак задатак. Детектовање скривених податак у некој мултимедијалној датотеци може бити веома дуг процес, који неће успети да у временском интервалу важног за безбедност открије скривену поруку.

Упркос свему, може се рећи да стеганографија има више него корисну улогу у данашњем друштву које је усмерено на коришћење мултимедијалних извора података (телевизија, радио, интернет, ...). Сходно томе, најзначајнија и најчешћа употреба стеганографије је употреба дигиталних водених печата којима се штите ауторска права[38].

# 4. Преглед постојећих решења

Криптографија у области заштите података има веома дугу историју коришћења. Опште је познато да је криптографија доминанто војна технологија која се с развојем интернета, пре свега, а у новије време и паметних телефона своју примену проширила на пословне али и сервисе јавне управе. Криптографију више не користе само одређене државне структуре, обавештајне пре свега, већ је она постала лако доступна за коришћење и обичним људима, тј. појединцима који имају потребу да примене један од сервиса које криптографија нуди.

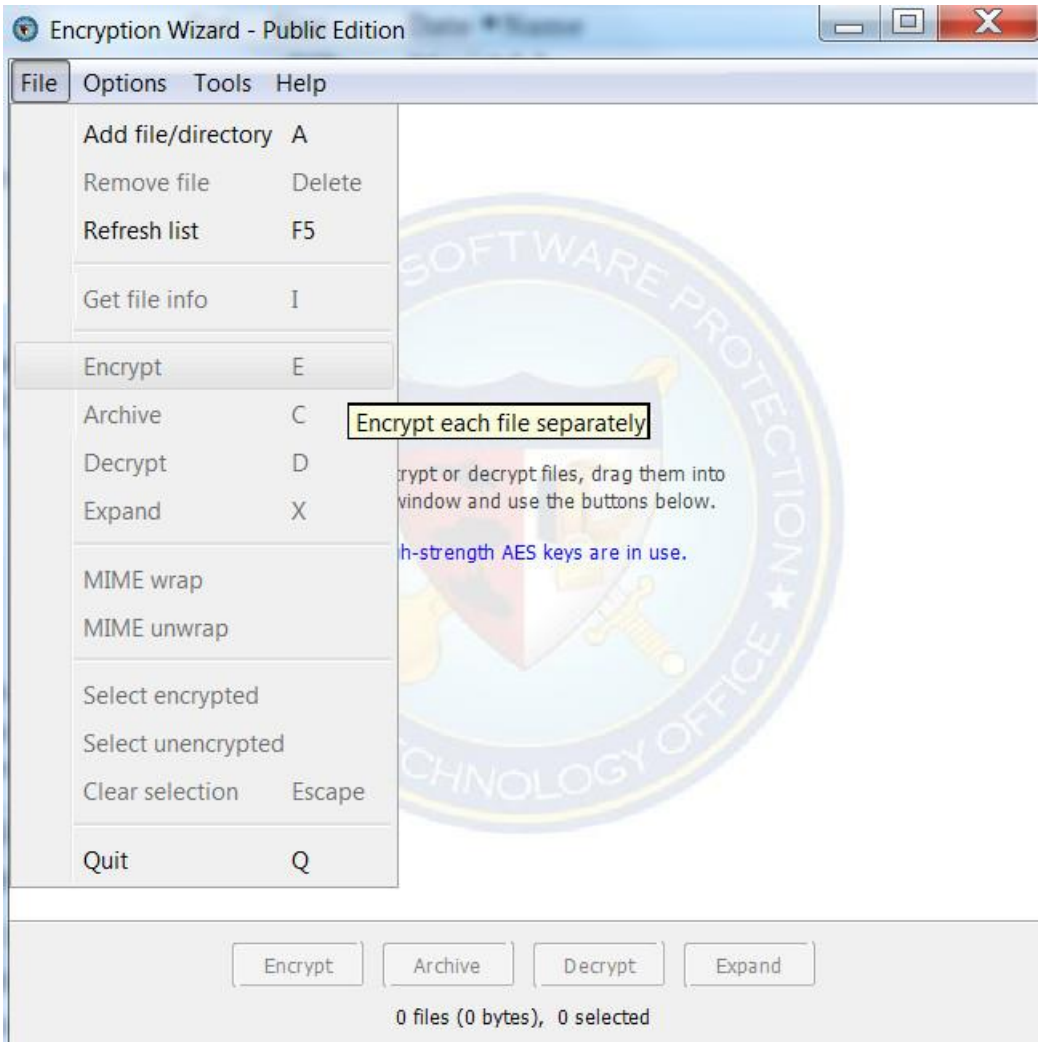
Стеганографија, која такође има дугачку историју као и криптографија, се такође користи како би се остварила заштита информација. Међутим, сам концепт заштите које се користи у стеганографији се разликује од принципа на којима функционише криптографија. Док се у криптографији тежи ка остваривању сервиса тајности података, стеганографија има за циљ да постојање информације о нечему сакрије на одређени начин од ока посматрача. Један од напада на комуникационе канале којим се размењују тајне поруке или информације уопште, а који се односи на прекидање комуникационог канала или онемогућавање корисника да размењују информације, стеганографија успешно решава.

Упоредо са развојем криптографије, развијала се и стеганографија. То је довело до спајања криптографских метода са методама стеганографије у вишенаменске системе за тајну комуникацију. Циљ креирања оваквих система је више него очигледан јер постоји потреба ка сервису који би могао да обезбеди тајност, интегритет и аутентификацију и који при том не одаје никакве информације о томе да су се побројани сервиси уопште и користили. Најчешће се у оваквим хибридним решењима користе сервиси симетричне криптографије којима се обезбеђује тајност, док се неком од стеганографских метода врши утискивање тајне поруке или информације у стего носач. Стего носачи у данашње време су најчешће мултимедијалне датотеке или датотеке које се лако преносе и деле преко јавног комуникационог канала као што је то интернет. Од свих мултимедијалних датотека највише се примењују дигиталне фотографије које се кодирањем трансформишу на такав начин да визуелно не изгледају другачије од оригинала. Међутим, као што постоје технике за криптоанализу, постоје и технике којима се врши стегоанализа, тј. детекција аномалија у стего носачу.

У овом поглављу ће бити описани само неки од бројних алата који пружају сервисе из домена области истраживања ове докторске дисертације. Одабрани алати су се користили како би се извршила валидација предложеног протокола за размену криптографских кључева на бази личних идентификационих докумената.

# 4.1. Encryption Wizard

*Encryption Wizard* као и остале алате који су развијени од стране *AFRL* (енгл. *Air Force Research Laboratory*), који је део Министарства одбране САД (енгл. *Department of Defence – DoD*), би требало да користе америчко Министарство одбране и остатак савезне владе, међутим, понуђена је и јавна верзије овог софтвера заједници отвореног кода (у ограниченој верзији), слика 4.1.




Слика 4.1. Изглед *Encryption Wizard* апликације

*Encryption Wizard* је алат које је развијен коришћењем Јава програмског језика за једноставно, лако и брзо шифровање фајлова (датотека) и програмских фасцикли (фолдера) у целини. Јава програмски језик је коришћен како би се развила мултиплатформска апликација која може да ради на готово свим познатим оперативним системима. Програм се уз минимално предзнање криптографских појмова веома лако користи. На врло једноставан начин корисници овог програма могу да изаберу жељене дужине, 128 или 256 бита, *AES* кључа, слика 4.2.


Слика 4.2. Одабир дужине *AES* кључа у *Encryption Wizard* апликацији

Уколико корисник жели да користи сервис аутентификације у оквиру апликације може да генерише сопствени дигитални сертификат, слика 4.3.


Слика 4.3. Одабир параметара за формирање дигиталног сертификата

Понуђене су различите опције за избор дужине *RSA* кључа и *SHA* хеш функције. На слици су одабрани исти параметри који се налазе на квалификованом дигиталном сертификату издатом од стране *MUPCA*, који се користи у систему за тајну комуникацију описаном у поглављу 5.

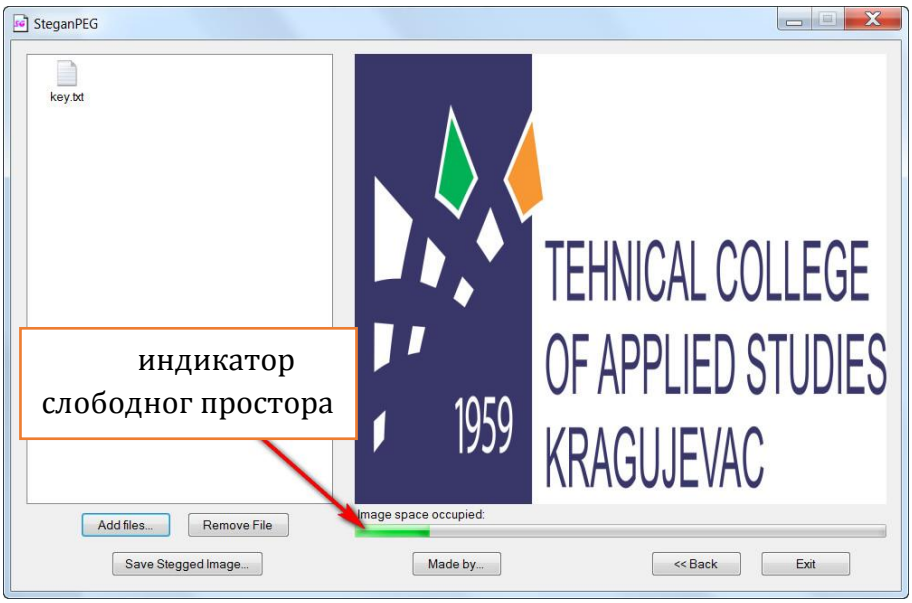
*Encryption Wizard* алат може да се употреби за један од два предложена начина за коришћење предложеног решења за тајну комуникацију, који су описани у поглављу 5 ове докторске дисертације.


Слика 4.4. Верзија *Encryption Wizard* апликације

Верзија софтвера који је коришћен током истраживања спроведених у оквиру ове докторске дисертације приказана је на слици 4.4.

## 4.2. SteganPEG

*SteganPEG* је апликација која користи дискретну косинусну трансформацију (*DCT*) за сакривање одабране датотеке у *JPEG* слику без битније промене саме у *JPEG* слике, слика 4.5.




Слика 4.5. Изглед *SteganPEG* апликације након постављених улазних датотека

Софтвер је једноставан за употребу и не захтева од корисника никакво предзнање везано за криптографију. Подржава рад само са у *JPEG* сликама и софтвер може да сакрије више датотека у једној *JPEG* слици. Постоји индикатор који означава колико је још простора преостало за утискивање у одабраној *JPEG* слици. Заштита се своди на једноставно укуцавање лозинке и овај софтвер је погодан само за скривање мање битних датотека. Аутор је дао изворни код тако да свако може слободно да настави развој овог софтвера и да га прилагоди својим потребама.

## 4.3. StegApp tool

*StegApp tool* је креиран као једна Веб апликација која се заснива на заштити тајне поруке скривањем у сликама формата *JPEG*, *PNG*, *BMP*, *GIF* и *TIF*. Аутор је представио свој програм у истакнутом научном међународном часопису (по категоризацијо КоБСОН-а) [35]. Апликација ради на принципу *DCT* и захтева претходну пријаву на Веб страници апликације путем email-а. Након добијања ауторизације од администратора сајта корисник може да врши скривање тајне поруке која је записана у *.txt* формату. Принцип рада саме апликације је приказан на слици 4.6.


Слика 4.6. Шематски приказ тајне комуникације помоћу *StegApp* апликације

Кораци које Алиса предузима да би послала тајну поруку су:

1. Пријављивање на *StegApp* Веб апликацију;
2. Додавање датотеке која ће бити стего носач на сервер Веб апликације;

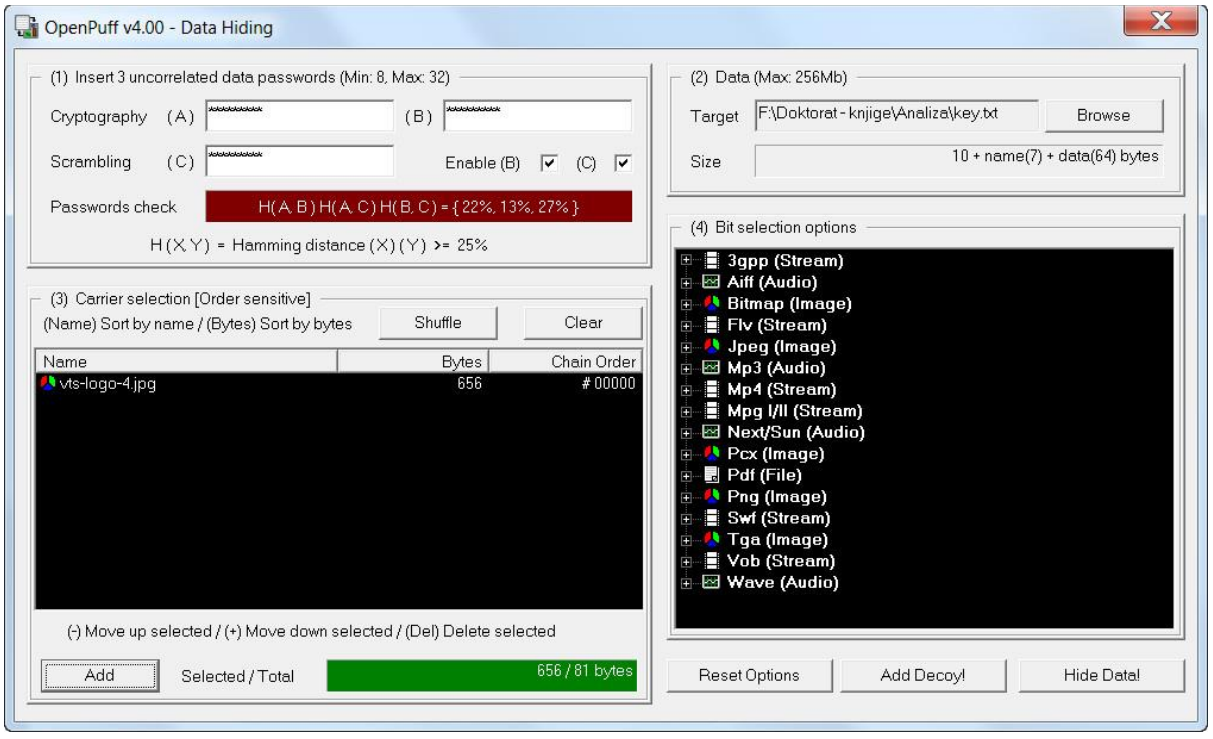
3. Уписивање тајне лозинке (шифре) која се користи у *StegApp* апликацији при заштити стего носача;
4. Додавање текстуалне поруке која ће бити утиснута у стего носач;
5. Преузимање стего носача са *StegApp* Веб странице на свој рачунар;
6. Слање стего носача (стего објекат) путем интернета Бобу.

Кораци које Боб предузима да би прочитао тајну поруку су:

1. Преузимање стего носача (стего објекат) од Алисе;
2. Пријављивање на *StegApp* Веб апликацију;
3. Додавање стего носача на сервер Веб апликације;
4. Уписивање тајне лозинке (шифре) ради откривања текстуалне поруке;
5. Преузимање текстуалне поруке са *StegApp* Веб странице на свој рачунар.

## 4.4. OpenPuff

*OpenPuff* је веома моћан и свеобухватан алат који је публикован под лиценцом отвореног кода. Овај алат обухвата велики број дигиталних датотека које је могуће користити као стего носач. Могуће је комбиновати више дигиталних датотека како би се утиснула веома велика датотека слика 4.7.




Слика 4.7. Коришћење стеганографије у *OpenPuff* апликацији

Иницијалним покретањем нуди се одабир начина коришћења *OpenPuff* апликације. Постоје три избора, а у складу са предметом истраживања у овој докторској дисертацији је коришћен део софтвера намењен за стеганографију.

Програм дозвољава коришћење три лозинке, минималне и максималне вредности за исте се крећу од 8 до 32 карактера, али корисник може да изабере да користи само једну лозинку. Максимална величина датотеке која може бити утиснута зависи од величине стего носача али је она пројектована тако де не може да пређе границу од 256 *MB*. *OpenPuff* је једина апликација која комбинује симетричну криптографију са стеганографском техником која се користи адаптивним нелинеарним кодирањем битова стего носача.

## 4.5. Сертификационо тело МУП-а Републике Србије

Сертификационо тело *MUPCA* изградило је инфраструктуру јавних кључева на бази имплементације решења које је пројектовала компанија *NetSeT*. *MUPCA* издаје квалификоване дигиталне сертификате грађанима Републике Србије на личним идентификационим документима са чипом. Стандарди којих се придржава *MUPCA* приликом издавања квалификованих дигиталних сертификата су[1]:

- *ETSI ESI TS 101 862 „Qualified Certificate Profile",*
- *RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile",*
- *RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",*
- *ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons"*

*MUPCA* издаје сертификате у формату *X.509v3*. Криптографски параметри, тј. асиметрични парови кључева се генеришу помоћу хардверских генератора случајних бројева који су реализовани на криптографским хардверским уређајима тзв. HSM (енгл. *hardware security module*) модул. Сопствени сертификат *MUPCA* потписује *RSA* кључем дужине 4096 бита, док се грађанима Републике Србије издају квалификовани дигитални сертификати који у себи садрже два пара *RSA* кључева од 2048 бита.

Детаљни прописи који прописују рад *MUPCA*, Политика сертификације и Практична правила рада сертификационог тела, су доступни на Веб страници сертификационог тела *MUPCA*.

[1] Доступно на: http://ca.mup.gov.rs/

# 5. Модел предложеног решења

До данас је развијен велики број комплетних сервиса којима се штити приватност и који гарантују висок степен заштите размењених информација. Постоји више познатих начина за размену тајних кључева путем несигурног комуникационог канала.

Нов приступ који ће бити представљен у овој дисертацији унапређује сигурност протокола за размену тајних криптографских кључева тако што се додаје још један сигурносни корак у тајној комуникацији корисника. Стеганографија, која се користи у предложеном систему, треба да сакрије од потенцијалног нападача информацију да је до било какве комуникације између два корисника дошло. Потенцијални нападач поред стегоанализе, како би утврдио да некаква тајна комуникација постоји, мора да изврши и криптоанализу како би дошао до отвореног текста послате поруке која у себи садржи тајни кључ. Применом предложеног система се поред прикривене комуникације уз помоћ стеганографије, врши и безбедна дистрибуција тајних кључева коришћених за шифровање поруке али и аутентификација корисника, респективно.

Безбедна дистрибуција тајних кључева и аутентификација корисника се врши помоћу асиметричне криптографије, коришћењем квалификованих дигиталних сертификата који се налазе на личним идентификационим документима грађана Републике Србије. Предложеним унапређењем корисници добијају комплетан систем за тајну комуникацију који се, као такав, по први пут користи.

## 5.1. Опис проблема

Прислушкивање комуникационих канала, поготово интернета, више не представља непознат појам и у данашње време је то постала јавно позната чињеница о којој се у више наврата писало и говорило у јавности.

Актуелни случајеви попут портала "Викиликс"[1] (енгл. *WikiLeaks*), за који се сматра да га је оснивао Јулијан Асанж (енгл. *Julian Assange*), а поготово полемика коју је изазвао Едвард Сноуден (енгл. *Edward Snowden*) изношењем чињеница о

[1] Непрофитна међународна организација преко које су узбуњивачи широм света објављивали, и још увек објављују, тајна документа и материјале који су на други начин недоступни широј светској јавности. На порталу *WikiLeaks* могу се пронаћи и документа и тајне депеше везано за нашу земљу.

постојању великог броја тајних пројеката надзирања од стране САД[2] (*United States of America*) су довољни разлози да се тврди како слободна комуникација у свету, без нечијег надзора, не постоји. Уколико је важно да комуникација буде тајна, макар се то односило и за неки краћи период, употребиће се неки од сервиса који то могу обезбедити. Сваки од тих сервиса подразумева употребу криптографије.

Вероватноћа да неко надзире и прислушкује комуникациони канал је велика, а размена шифрованих информација може да скрене пажњу на исте. Након откривања шифроване комуникације и пресретања шифрованих порука, постоји вероватноћа да ће неко покушати да изврши криптоанализу истих. У сврху смањивања вероватноће откривања шифроване комуникације најчешће се користи нека од опште познатих стеганографских метода. Употребом стеганографије потенцијалним нападачима се знатно отежава процес разоткривања тајне комуникације јер се порука која садржи информацију утискује у стего објекат чиме се оригинална датотека, тј. стего носач, тек незнатно мења.

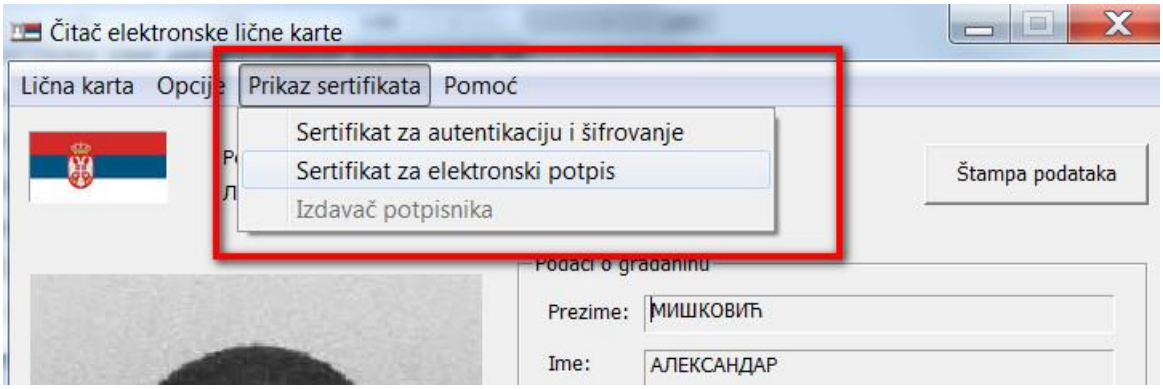
С обзиром на чињеницу да се у данашње време размењује велика количина мултимедијалног садржаја путем разних друштвених мрежа, сервиса за размену фотографија и видео фајлова, интернет форума, и томе сл., потенцијални нападач који прислушкује комуникациони канал мора да прикупи сав размењени мултимедијални садржај и да изврши стегоанализу свих датотека како би евентуално открио тајну комуникацију између два корисника.

С друге стране, развојем и унапређивањем информационих система постали смо сведоци примене електронских докумената у државној администрацији, банкарству, правосуђу и осталим сферама друштва, а комуницирање у отвореним мрежама без директног личног контакта је постала свакодневница. Ово су само неки од примера примене савремених комуникационих технологија који захтевају нове облике утврђивања идентитета и заштите података. Заштита поверљивих информација веома се успешно спроводи уз помоћ симетричних шифарских система, док се за утврђивање аутентичности и интегритета најчешће користе асиметрични шифарски системи. Ови сервиси ће бити основ за коришћење предложеног система за тајну комуникацију, док ће се коришћењем стеганографије прикривати да је до тајне комуникације уопште и дошло чиме се отежава процес разоткривања тајне комуникације, а самим тим умањује се и вероватноћа да ће доћи до криптоанализе шифрованих информација.

[2] *Glenn Greenwald*, новинар британског дневног листа *The Guardian*, први је објавио низ чланака, према тврдњама и документима које му је презентовао Едвард Сноуден, да су САД покренуле и користиле низ тајних пројеката за надзор готово читавог интернета али и других светских институција и организација. Објављени су кодни називи тајних пројеката записаних у преко 9000 тајних докумената. Поред америчке агенције *NSA*, у објављеним документима се помињу се и британске, немачке и израелске тајне службе.

## 5.2. Предложено решење и његова примена

Један од највећих проблема који се јавља приликом успостављања тајне комуникације је сигурна размена криптографских кључева. Проблем који настаје када корисници треба да размене тајни кључ путем јавног комуникационог канала као што је то нпр. интернет, у предложеном систему ове дисертације разрешен је употребом асиметричне криптографије. Наиме, коришћењем Јава програмског језика, развијен је метод који приступа квалификованим дигиталним сертификатима који се налазе на личним идентификационим документима са чипом грађана Републике Србије. Квалификовани дигитални сертификати који се користе у предложеном систему садрже два пара *RSA* кључева величине 2048 бита, слика 5.1, један за шифровање и аутентификацију, а други за дигитално потписивање. Квалификоване дигиталне сертификате грађанима републике Србије бесплатно издаје сертификационо тело *MUPCA*[3].




Слика 5.1. Очитавање квалификованих дигиталних сертификата који се налазе на личном идентификационом документу

Предложени систем за тајну комуникацију своју сигурност заснива на шифровању тајног кључа, који се користи у симетричној криптографији, са *RSA* јавним кључем за шифровање који се налази на квалификованом дигиталном сертификату. Пре операције шифровања документ, који садржи тајни кључ, се дигитално потписује чиме се врши аутентификација корисника предложеног система за тајну комуникацију, а самим тим се потврђује и интегритет размењених порука којима се дистрибуирају тајни кључеви. Утискивањем ове шифроване и дигитално потписане поруке у стего објекат, који се касније поставља на неки од сервиса јавне комуникације, се прикрива да је до размене тајних порука између корисника уопште и дошло. На овај начин корисници тајне комуникације могу на

[3] На основу увида у регистар сертификационих тела за издавање квалификованих дигиталних сертификата Републике Србије, може се утврдити да је сертификационо тело МУП РС (*MUPCA*) једно од пет сертификационих тела које издају квалификоване дигиталне сертификате. Такође, МУП РС је једино сертификационо тело које издаје квалификоване дигиталне сертификате на електронским идентификационим документима грађана Републике Србије.

ефикасан и сигуран начин да размењују тајне поруке, уверени да оне нису у међувремену промењене од стране неког трећег лица и да су тајни кључеви који се користе за шифровање порука размењени на сигуран начин.

Корисници предложеног система могу да изаберу нека од стеганографских решења која у себи интегришу и симетричне алгоритме за шифровање, који су описани у поглављу 4 ове дисертације. Тада би се предложени систем за размену тајних кључева помоћу личних идентификационих докумената користио за пренос тајних кључева који се користе у тим стеганографским решењима. Мана оваквих готових решења је у томе што корисници немају могућност избора алгоритма за симетрично шифровање. Такође, у неким системима немају могућност избора дужине тајног кључа, већ морају да се задовоље оним што нуди један такав хибридни систем.

Међутим, предложени систем за размену тајних кључева помоћу личних идентификационих докумената не условљава кориснике да користе такве хибридне системе, већ им дозвољава да сами одаберу алгоритам за симетрично шифровање. На овај начин корисници би могли, поред избора система за симетричну криптографију, да сами генеришу кључеве који ће да се користе у симетричном алгоритму за шифровање, а стеганографске алате да користе за прикривање и пренос порука које садрже информацију о тајном криптографском кључу коришћеном у симетричној криптографији.

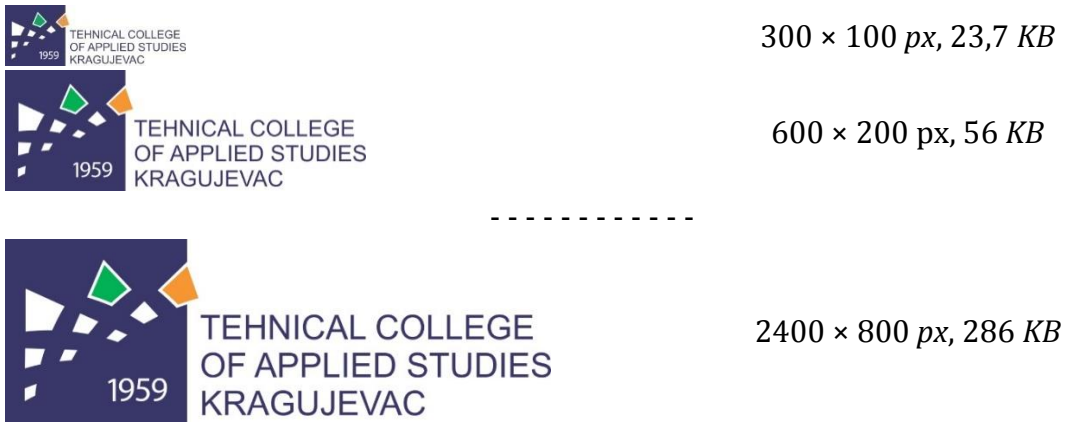
### 5.2.1. Примена и имплементација стеганографије

Потребно је напоменути да карактеристике стеганографских алата нису узимане у озбиљну евалуацију с обзиром на чињеницу да они, у овој докторској дисертацији, служе за представљање предложеног концепта дистрибуције тајних кључева и аутентификације корисника тајне комуникације помоћу личних идентификационих докумената.

Стеганографски алати који су тренутно доступни за бесплатну употребу нуде врло једноставне и ефикасне начине за скривање тајних порука унутар *JPEG* слика. *JPEG* формат је одабран да буде стего носач као један од најпопуларнијих формата за приказивање слика (фотографија) на интернету. Међутим, постоје различите методе које се користе за стегоанализу, којима се може открити присуство тајне поруке у на изглед обичној *JPEG* слици. У ту сврху се користе визуелна детекција, статистичка детекција или анализа хистограма, структурна детекција или детекција необичних структура.

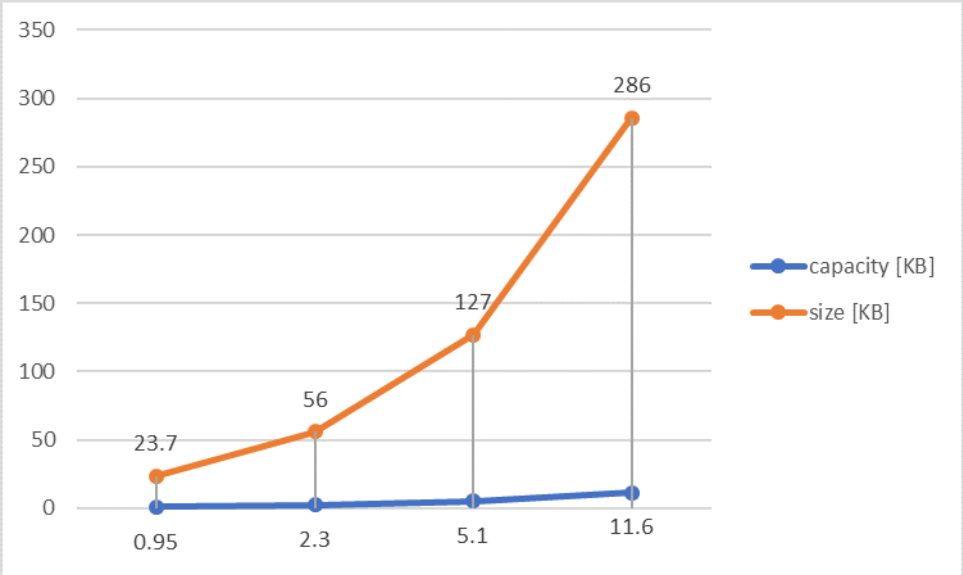
Промену *JPEG* слике коришћењем фреквентног домена приказали су у свом раду *Cheddad* et al. [78] Они су у свом раду дали преглед различитих софтвера који се могу користити у ту сврху и критички анализирали перформансе истих. Један од закључака до кога су дошли доводи у спрегу стеганографске технике и њихову отпорност на могуће нападе са величином поруке која се скрива у *JPEG* слици. Овај

рад је послужио као идеја да се спроведе слична анализа у овој дисертацији. Анализом резултата добијених коришћењем стеганографских алата који су доступни за слободну употребу, а који су описани у поглављу 4, добијени су резултати који показују да је капацитет *JPEG* слике за скривање података у директној вези са величином саме *JPEG* слике, слика 5.2 и 5.3.




Слика 5.2. Апроксимација *JPEG* слике над којом је вршена анализа капацитета за скривање података

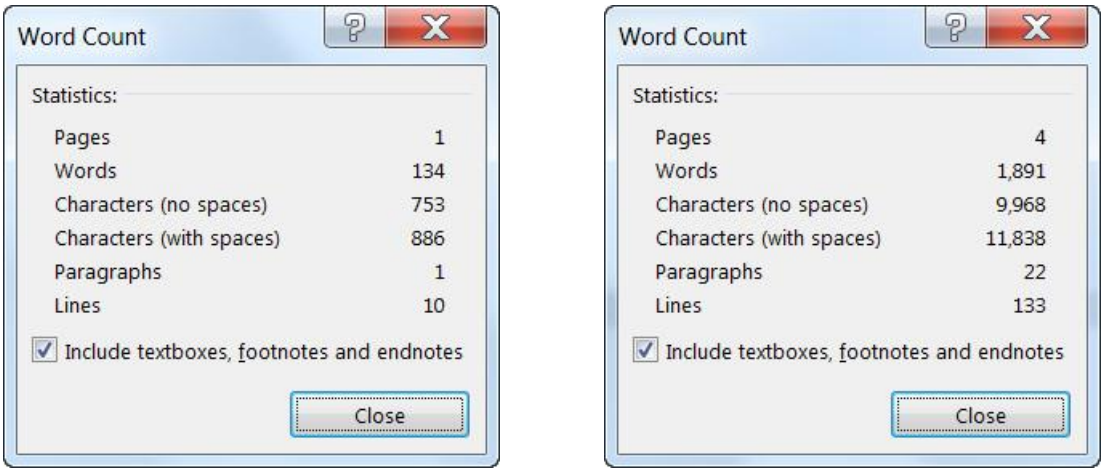
Међутим, ова анализа је показала да пораст величине *JPEG* слике не утиче пуно на вредност која представља капацитет *JPEG* слике за скривање података. Капацитет за скривање поруке незнатно расте у односу на пораст величине саме *JPEG* слике, слика 3. Узимајући у обзир да је *JPEG* слика стего носач мора се водити рачуна да се она не сме променити тако да својим изгледом, статистичким својствима и структуром указује на чињеницу да у себи садржи скривену поруку.




Слика 5.3. Дијаграм зависности капацитета за скривање тајних података и величине *JPEG* слике у *KB*

Анализа је започета са *JPEG* сликом величине 23.7 *KB* (што одговара слици величине 300 × 100 пиксела), а завршена је са *JPEG* сликом величине 286 *KB* (што

одговара слици величине 2400 × 800 пиксела). Дужина текстуалне поруке која је уписивана у *JPEG* слику најмање величине је 134 речи или 886 карактера са размацима, док се у највећу *JPEG* слику, величине 286 *KB*, уписивала порука од 1891 реч или 11838 карактера са размацима. Број речи и карактера са размацима који су наведени је добијен бројачем из *Microsoft Word* документа, слика 5.4.




Слика 5.4. Статистички приказ порука записаних у најмањој и највећој слици

Ако се узме у обзир да корисник може да бира симетрични алгоритам за шифровање и да се претпостави да је изабрао *AES* кључ од 256 бита, на основу представљених података о величини текстуалне поруке може се рећи да се овај изабрани кључ може утиснути у најмањи стего носач, величине 23,7 *KB*, без икаквог утицаја на изглед, статистичка својства и структуру одабране *JPEG* слике. Овај закључак произилази из чињенице да порука најмање величине конвертована у *Base64* кодни формат садржи 1184 карактера без размака, док *AES* кључ од 256 бита представљен у истом том кодном формату садржи 44 карактера без размака. Када се *AES* кључ од 256 бита, сачуван у *Base64* кодном формату, шифрује *RSA* кључем од 2048 бита који се налази на личном идентификационом документу број карактера онда износи 344, слика 5.5.

```
ANBdWqyHV4HhCOYBKXSP2Im0A7F3gQ9DzTUZP+VEtrRceaB/IAP8cRbD9ppUwGVi4QPgGYNj0v9j8Fj
WZ4zMTct6XdqB7G9ZcshtYl9hXUO8Bgwue5N4vn+p9SvNQkipwiUtGFV8zffQmjjl8y8AiShbQmmJFQvK
xwrpZk9gNUDB0otNY3y/ccjwbZLL11upliNoEILxy1D6gnAecMYXnmHeDizcqkErqO6Vc6+7rDjuzYnox4u
Vb1gOLpE3+lE025lDzots7pXZ9fzIn1cakNK/jRqQ/mWZCSBUIfpf8HhLT/mEPA/k4AlekOz07P0Sdw2w71
t20utn8iFo7L29Bw==
```

Слика 5.5. *AES* кључ у шифрованом облику

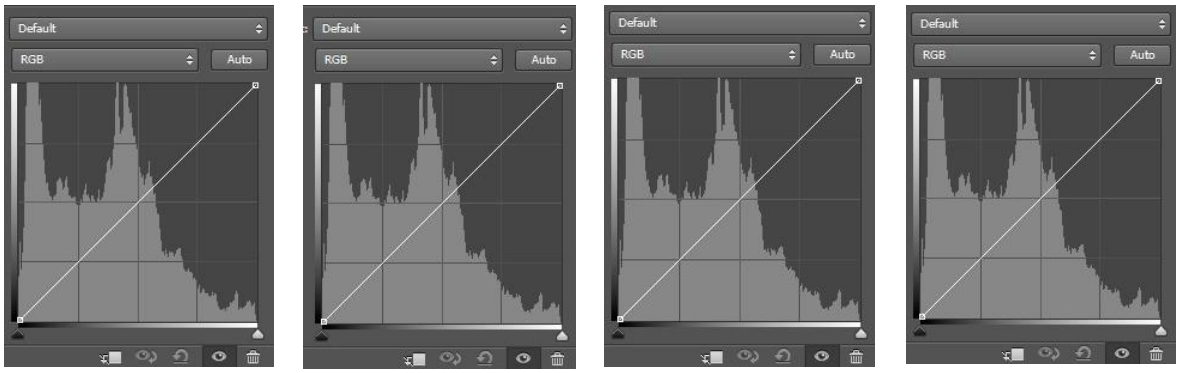
Употребом неколико јавно доступних стеганографских алата, који се могу бесплатно користити, дошло се до закључка да су ови алати врло ефикасни приликом утискивања релативно кратких порука у *JPEG* слике већих димензија. Нпр. слика која је коришћена у горе поменутом експерименту је величине 286 *KB* тј. 2400 × 800 пиксела према приказаним подацима из анализе је могла да се употреби за утискивање шифрованог *AES* кључа од 256 бита. Ова слика је

послужила као стего носач, а за утискивање тајне поруке која садржи шифровани *AES* кључ употребљени су следећи стеганографски алати: *StegApp tool*, *OpenPuff tool* и *SteganPEG tool*. Као што је већ напоменуто карактеристике ових стеганографских алата нису узимане у озбиљну евалуацију, а они су детаљно представљени у поглављу 4 ове дисертације.

Према приказаним резултатима, слика 5.6 и 5.7, може се закључити да квалитет оригиналне *JPEG* слике није нимало промењен утискивањем поруке која у себи садржи 344 карактера. Потребно је напоменути да према анализи капацитета за скривање података изабрана *JPEG* слика може да послужи као стего носач за поруку од 9968 карактера без размака, што је и приказано на слици 4. Ово је веома битна напомена јер се шифровањем *RSA* кључем од 2048 бита број речи који могу да стану у такву поруку смањује, што се види на примеру шифрованог *AES* кључа чијих се 44 карактера без размака, шифровањем *RSA* кључем добија 344 карактера без размака.


Оригинал *StegApp tool* *OpenPuff tool* *SteganPEG tool*

Слика 5.6. Графички приказ квалитета *JPEG* слике путем опције *Curves* у програму *Photoshop*




Оригинал *StegApp tool* *OpenPuff tool* *SteganPEG tool*

Слика 5.7. Графички приказ квалитета *JPEG* слике путем опције *Levels* у програму *Photoshop*

За анализу *JPEG* слике, оригинала и стего носача коришћен је програм *Photoshop* и његове опције *Curves* и *Levels*. Упоређиван је оригинална *JPEG* слика са *JPEG* сликом након стеганографског поступка утискивања поруке у исту. Као крајњи закључак ове анализе намеће се чињеница да је капацитет *JPEG* слике за

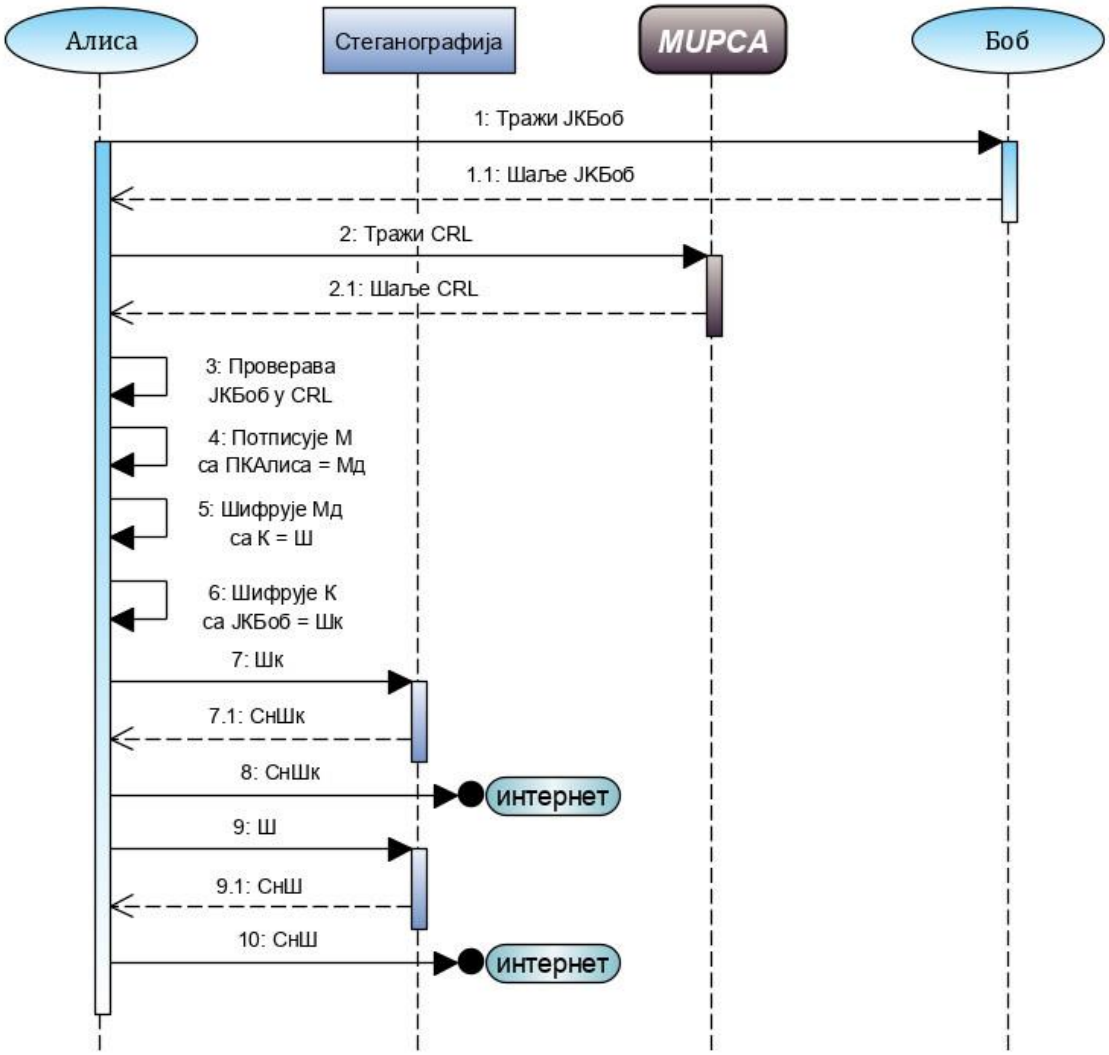
скривање тајне поруке од великог значаја за утискивање тајне поруке у *JPEG* слику. Од њега у великој мери зависи колико података, изражених у *KB*, може да се сакрије у некој *JPEG* слици, а да се њен изглед не промени. О овој чињеници корисници стеганографије морају посебно да воде рачуна како тајна комуникација не би била разоткривена.

### 5.2.2. Предложено решење и његова имплементација

Размена тајних кључева која подразумева да се корисници тајне комуникације сусретну на некој локацији и да их лично размене се сматра добром праксом. Међутим, овакав начин размене тајних кључева иако је добар није увек и практичан, поготово ако корисници који желе тајно да комуницирају не живе у истом граду, држави или пак на истом континенту. Слање тајних кључева јавним комуникационим каналом, као што је то интернет, се сматра небезбедним јер увек постоји вероватноћа да је јавни комуникациони канал прислушкиван од неке треће стране. Питање које се намеће је: "Како Алиса и Боб могу на сигуран начин да размене тајне кључеве?". Додатан проблем је и то што Боб мора бити уверен да комуницира са Алисом, и обрнуто, а не са неком непознатом особом која се представља као неко од њих.

Организације које припадају разним државама, нпр. амбасаде, тајне службе, војска, па чак и велике интернационалне корпорације које имају неограничена или велика новчана средства, инфраструктуру, обучене појединце за овакве послове, и томе сл., немају проблем да тајне кључеве размене на било који начин. Појединци, мале организације, у које спадају и непрофитне организације, и њима сл. могу лично да размењују тајне кључеве уколико им локацијски услови погодују за то. Међутим, уколико је удаљеност међу корисницима који желе да тајно комуницирају велика или се корисници у оваквом виду комуникације никада пре нису ни срели, пружена им је могућност да користе неки од јавно доступних сервиса за размену тајних кључева, који при том обезбеђују и сервис аутентификације. На ову чињеницу се указује у овој докторској дисертацији, а предложено решење за размену тајних кључева треба то да им и омогући.

Шема предложеног система тајне комуникације, секвенцијални дијаграм, која укључује лична идентификациона документа грађана Републике Србије, приказана је на сликама 5.8 и 5.9 – кораци које преузимају Алиса и Боб. Предложени систем тајне комуникације користи лична идентификациона документа са чипом, на којима су уписана два квалификована дигитална сертификата издата од стране *MUPCA*. На овим сертификатима се налазе два пара *RSA* кључева, што је приказано на слици 5.1. Ови кључеви се могу користити за дигитално потписивање и шифровање, респективно, а у предложеном моделу они се користе за шифровање тајних кључева коришћених у симетричним алгоритмима за шифровање и аутентификацију корисника тајне комуникације.




Слика 5.8. Кораци које предузима Алиса у предложеном решењу

Кораци које Алиса предузима у оваквом систему су следећи:

1. Алиса преузима дигитални сертификат од Боба, на коме је записан Бобов јавни кључ ($ЈК_{Боб}$), и врши проверу његове валидности преко *CRL*[4] издате од стране *MUPCA*. Провера се врши како би Алиса била сигуран да је Бобов дигитални сертификат валидан.

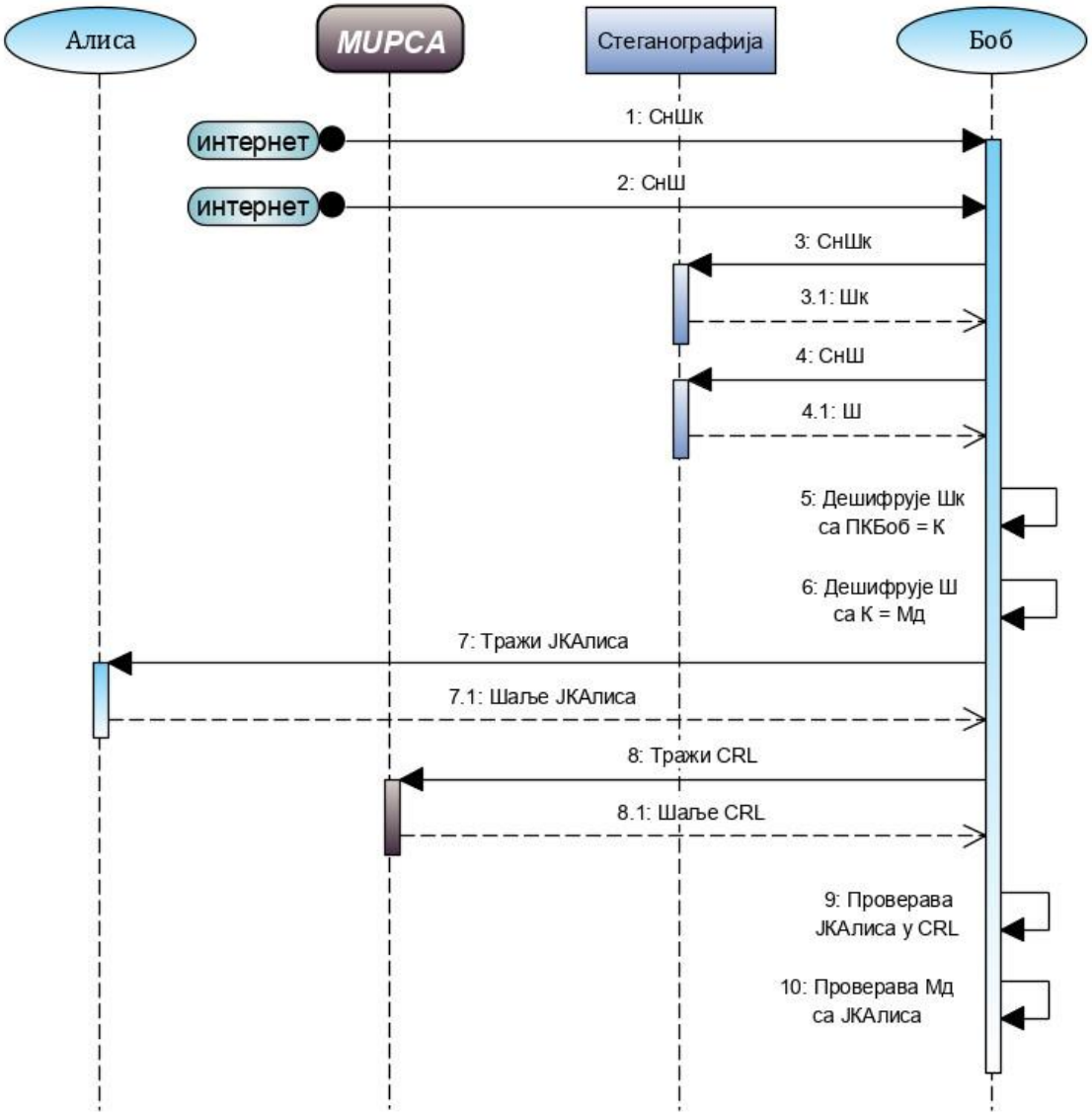
2. Текстуалну поруку (М), коју жели да пошаље Бобу, Алиса прво дигитално потписује чиме се добија дигитално потписана порука ($М_Д$). Алиса не жели да Боб на било који начин посумња да она није имала увид у поруку пре шифровања исте или да је М на неки начин измењен без Алисиног знања. Потписивање поруке Алиса ради са својим приватним кључем ($ПК_{Алиса}$) који се налаз на њеном личном идентификационом документу. Шифровање $М_Д$ Алиса обавља алгоритмом симетричне криптографије чиме се добија шифрат (Ш).

[4] Листа повучених сертификата: http://ca.mup.gov.rs/CRL.html

3. Тајни кључ (К) који се користио за шифровање $М_д$, Алиса шифрује са $ЈК_{Боб}$ чиме се добија шифрована порука у којој је записан тајни кључ ($Ш_К$). На тај начин Алиса је уверена да само Боб може да дешифрује $Ш_К$ јер само Боб поседује приватни кључ који се налази на његовом личном идентификационом документу ($ПК_{Боб}$).

3. Алиса користи стеганографију ради утискивања $Ш_К$ у одабрану *JPEG* слику. Таква слика постаје стего носач ($С_НШ_К$) и Алиса је поставља на своју Веб страницу или је дистрибуира на неки други начин, водећи рачуна о томе да користи портале који не врше додатну компресију приликом слања *JPEG* слика (нпр. *Facebook*).

4. Шифровану поруку, тј. Ш, Алиса може Бобу да пошаље директно путем комуникационог канала, међутим, Алиса може да понови трећи корак са неком другом *JPEG* сликом чиме би она постала нови стего носач ($С_НШ$) и тиме у потпуности прикрије да је до било какве тајне комуникације и дошло.




Слика 5.9. Кораци које предузима Боб у предложеном решењу

Кораци које Боб предузима у оваквом систему су следећи:

1. Боб прати шта Алиса објављује на својим Веб страницама и преузима *JPEG* слике од којих једна у себи садржи тајну поруку, тј. преузима $С_{Н}Ш$, а друга садржи тајни кључ, тј. преузима $С_{Н}Ш_{К}$.

2. Како би добио Ш и $Ш_{К}$ Боб мора да користи исти стеганографски алат који је користила Алиса.

3. Боб дешифрује $Ш_{К}$ са $ПК_{Боб}$ како би дошао до К. Сада када има К може да дешифрује Ш и дође до $М_{Д}$. Како би се уверио да је порука коју је добио стигла од Алисе у неизмењеном облику провериће да ли је исправан дигитални потпис којим је Алиса потписала поруку чиме се спроводи сервис аутентификације.

4. Боб преузима Алисин дигитални сертификат, на коме је записан Алисин јавни кључ ($ЈК_{Алиса}$), и врши проверу његове валидности преко *CRL* издате од стране *MUPCA*. Уколико је дигитални потпис валидан Боб може да буде сигуран да је то заиста порука коју му је Алиса послала јер је само Алиса могла М да потпише са $ПК_{Алиса}$.

#### 5.2.2.1. Имплементација предложеног решења

Један корисник у оваквом виду комуникације не мора да поседује било каква претходна сазнања о другом кориснику комуникације. Све информације, које су му потребне да отпочне комуникацију, налазе се на квалификованом дигиталном сертификату. Подразумева се да квалификовани дигитални сертификати за обе стране у комуникацији морају да буду издати од стране *MUPCA* и да обе стране у комуникацији верују "трећој страни од поверења", тј. сертификационом телу које им је сертификате и издало.

Уз помоћ програма развијеног у Јава програмском језику приступа се квалификованим дигиталним сертификатима на којима се налазе два пара *RSA* кључева. *RSA* алгоритам се сматра спорим алгоритмом, он шифрује и дешифрује податке много спорије него симетрични алгоритми. Међутим, како се у овом случају он не користи за шифровање података већег обима, у смислу величине текстуалне поруке, он се сматра погодним и практичним за шифровање тајних кључева који се користе за симетрично шифровање. Такође, важно је напоменути да постоје програми које нуди *MUPCA* у оквиру својих услуга, који врше дигитално потписивање и очитавање електронског идентификационог документа.

Исто тако, важно је напоменути да не постоји јавно доступан алат или програм којим би се извршило шифровање *RSA* кључем који се налази на електронском идентификационом документу грађана Републике Србије, чиме се врши проширивање функционалности личних идентификационих докумената са чипом грађана Републике Србије. Програм који је развијен у Јава програмском језику узима *RSA* пар кључева који се налазе на квалификовано дигиталном сертификату намењеном за аутентификацију и шифровање.

Коришћењем стандардне методологије и алата за софтверско моделовање, ради проширивања функционалности личних идентификационих докумената са чипом грађана Републике Србије, развијен је програм у Јава програмском језику, слика 5.10. Алгоритам који је значајан за овај програм приказан је псеудо кодом у следећим корацима:

```
function main(args):
    /* configuration */
    loadPkcs11ProviderIntoSystem(cfg)
    KeyStore keyStore = connectIDAndCreateKeyStore(pinCode, PKCS11)
    String alias = getAlias(KeyStore)

    /* encryption */
    X509Certificate certificate = keyStore.getCertificate(alias)
    String text = readFileIntoText(fileLocation)
    byte[] encryptedData = encryptText("RSA", text)
    writeEncryptedTextIntoFile(encryptData, fileLocation)

    /* decryption */
    PrivateKey privateKey = keyStore.getKey(alias);
    String encryptedText = readEncryptedFileIntoText(fileLocation)
    byte[] decryptedData = decryptText("RSA", encryptedText)
    writeDecryptedTextIntoFile(decryptedData, fileLocation)

```

Слика 5.10. Псеудо код предложеног решења

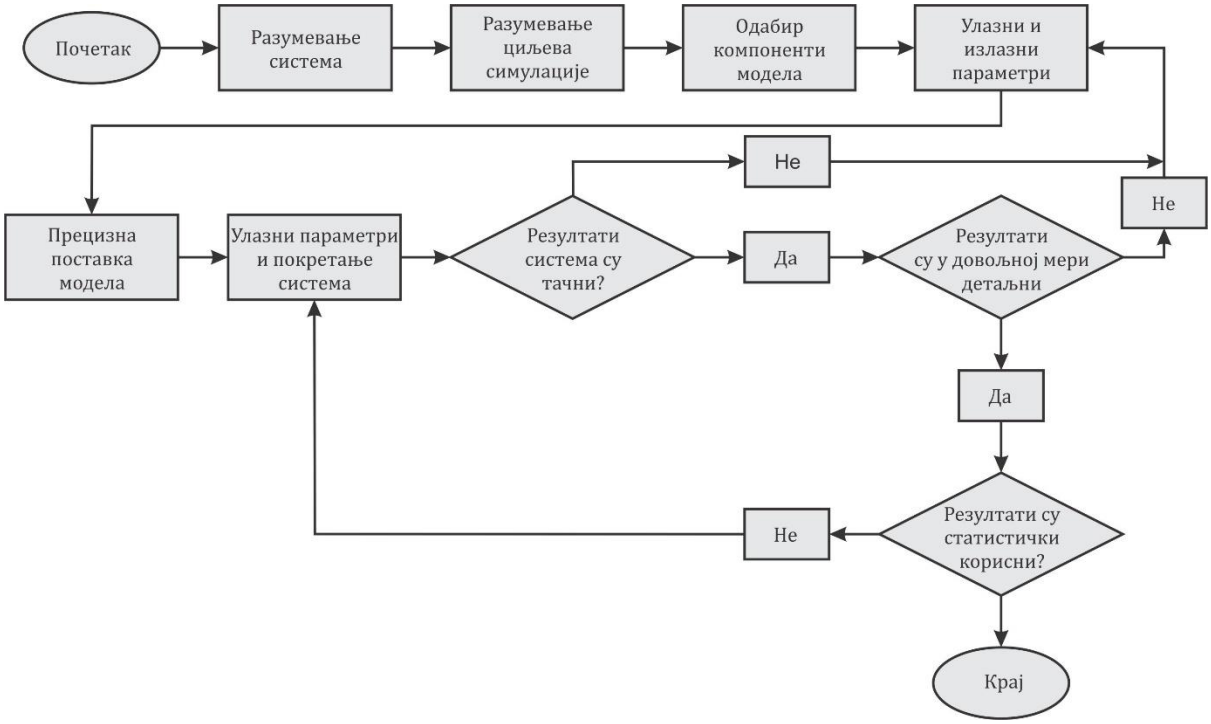
Детаљан приказ кода развијеног у Јава програмском језику биће дат у прилогу ове докторске дисертације.

# 6. Евалуација предложеног решења

Поред евалуације предложеног система за размену криптографских кључева и његове имплементације, извршена је анализа фаза планирања и резултата добијених преко симулационих модела. За потребе ове докторске дисертације, са аспекта социјалних активности, спроведена је анкета која је имала за циљ добијање одговора везаних за:

1. Општу информисаност таргетиране групе испитаника о појму квалификовани дигитални сертификат.
2. Мотивација таргетиране групе испитаника да користи системе за заштиту приватности.

За израду симулационих модела, статистичку обраду и приказивање добијених резултата коришћен је софтверски пакет *OPNET IT Guru Academic Edition*, а у завршној фази истраживања и *Riverbed Modeler Academic Edition*. Симулациона методологија која је примењивана и на основу које су донети одређени закључци приказана је на слици 6.1. Анализом литературе [79, 80] извршен је одабир компоненти симулационог модела, улазни и излазни параметри, као и начин приказивања резултата добијених на крају симулација.



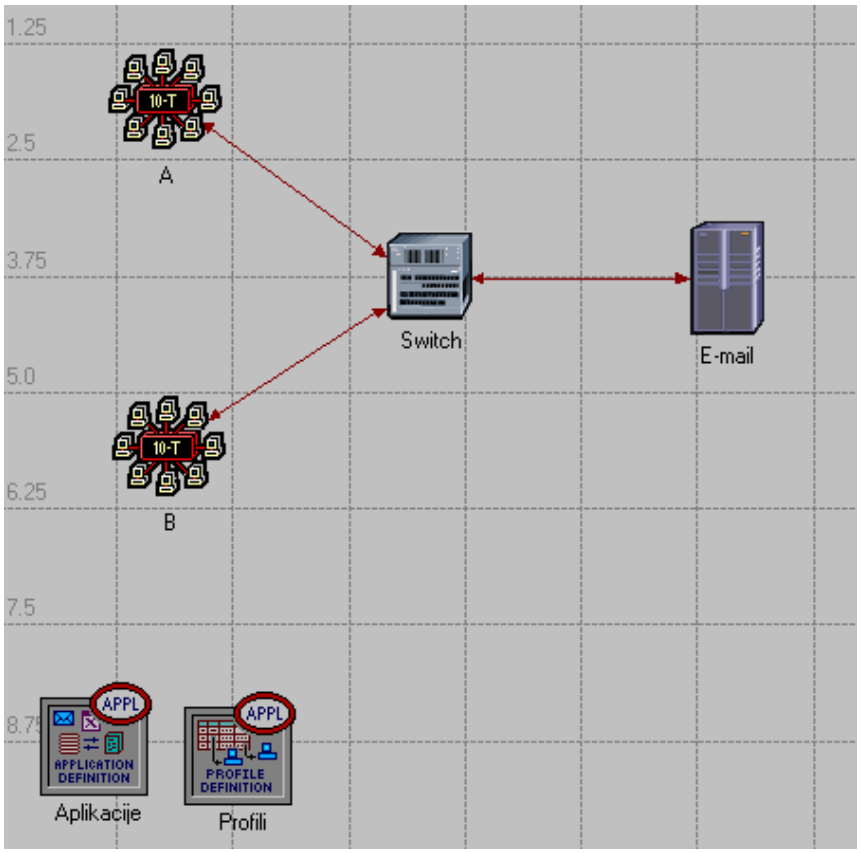

Слика 6.1. Дијаграм контроле тока одлучивања у симулационом моделу

# 6.1. Приказ експерименталних резултата

Имплементација и примена једног система за тајну комуникацију који при том обезбеђује и аутентификацију корисника не представља једноставан процес. Шифровање и дигитално потписивање порука увећава њихову величину, мерено у *KB*, што је и очекивано због самог начина на који ови процеси функционишу. Међутим, чињеница да су дигитално потписане и шифроване поруке које се размењују знатно веће од рутински размењених порука је од битне важности за развој једног система за тајну комуникацију који има за циљ да ту чињеницу да сакрије од потенцијалног нападача.

## 6.1.1. Симулација система за сигурну размену *email* порука

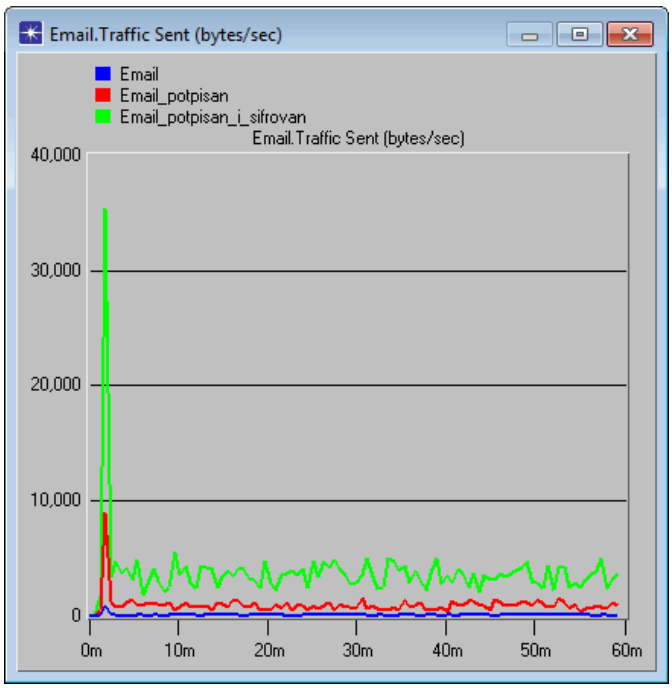
У првом симулационом моделу извршена је апроксимација тајне комуникације на тај начин што су се за размену шифрованих и аутентификованих порука користиле *email* поруке, слика 6.2.



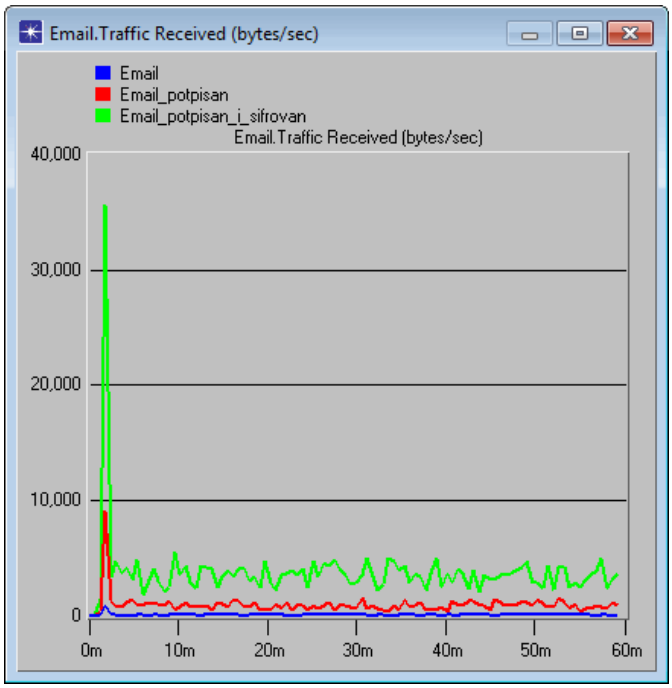

Слика 6.2. Симулациони модел за размену тајних порука

Овим симулационим моделом представљена је размена *email* порука између две групе корисника преко једног сервера. Симулација је изведена коришћењем три иста сценарија са различитим улазним параметрима у трајању од 60 минута. За први симулациони сценарио коришћена је уобичајена размена *email* порука

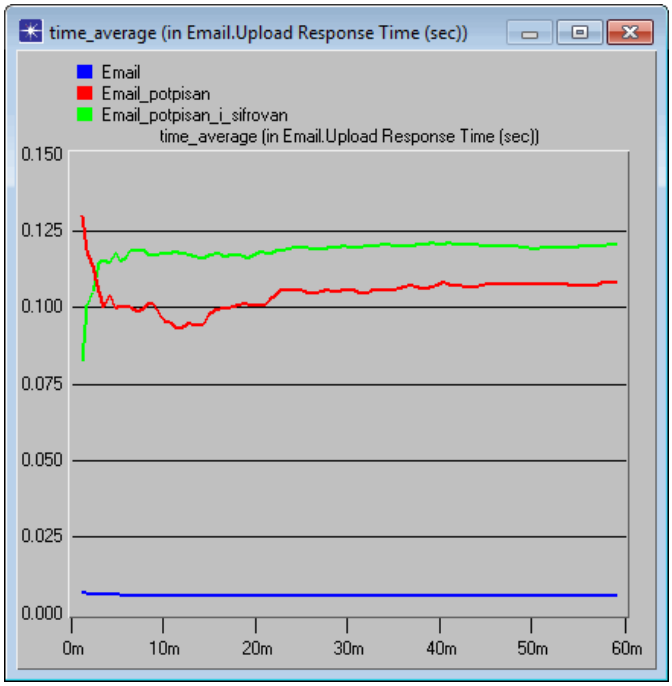
међу корисницима једне мреже. Затим је уведен параметар у виду дигиталног потписа који је послужио за сценарио број два у коме се симулира иста таква комуникација. Након тога се за трећи сценарио, који такође користи исте поставке као и претходна два, додају два параметра који се односе на дигитално потписивање и шифровање у исто време. Резултати симулације су приказани на следећим сликама:



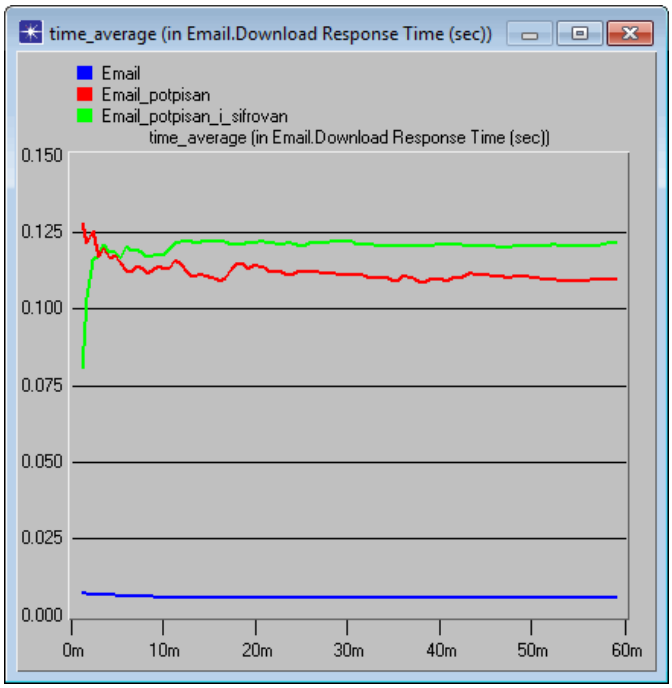

Слика 6.3. Просечна вредност одлазног саобраћаја на мрежи




Слика 6.4. Просечна вредност долазног саобраћаја на мрежи




Слика 6.5. Просечно време одговора сервера на захтев клијената за слање *email* поруке представљен функцијом *time_average*




Слика 6.6. Просечно време одговора сервера на захтев клијената за преузимање *email* поруке представљен функцијом *time_average*

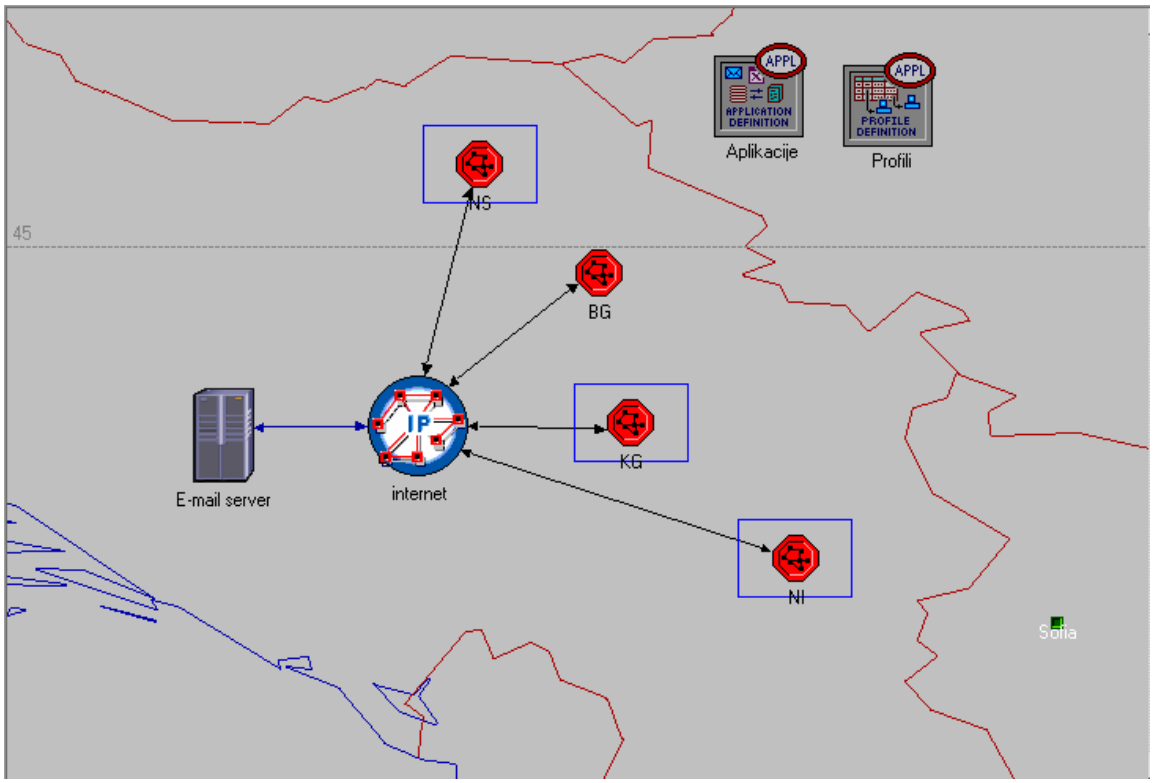
Из приложених резултата се види да је генерисани саобраћај највећи приликом размене порука које су заштићене и аутентификоване од стране корисника. Резултати симулације су очекивани и потврђују чињеницу изнету у уводном излагању да постоји потреба да се податак о неуобичајеном коришћењу размене порука сакрије од потенцијалног нападача.

Сходно изнетим чињеницама и резултатима који су добијени у симулацији, оправданост увођења стеганографских техника у предложени систем за тајну комуникацију, који је приказан у поглављу 5. ове докторске дисертације, је потврђена. Увођење стеганографије у систем за тајну комуникацију додатно повећава безбедност тајне комуникације тиме што скрива информацију да је до некакве неуобичајене комуникације уопште и дошло.

### 6.1.2. Критички осврт на функционалност *PKI* система

У овом симулационом моделу извршена је апроксимација *PKI* система који се користи у предложеном систему за тајну комуникацију, описаном у поглављу 5. За кориснике једног *PKI* система веома је важно да имају увид у листу повучених дигиталних сертификата, а од посебне важности је да та листа буде доступна, ажурна и једноставна за преузимање.

Овим симулационим моделом се врши симулација преузимање *CRL* од стране корисника коришћењем *pull* методе, што корисници *MUPCA* иначе морају и да раде, слика 6.7.




Слика 6.7. Симулациони модела интернета са подмрежама у којима се користи *PKI* систем

Метод преузимања *CRL* од стране корисника са удаљеног сервера се користи у *PKI* систему коме припада сертификационо тело *MUPCA*. Пошто је сертификационо тело *MUPCA* један од битних делова система за тајну комуникацију који се користи у овој дисертацији, било је потребно указати на

недостатке оваквог система који се односе на динамику објављивања и начин дистрибуирања *CRL* крајњим корисницима овог система.

Недостаци који су приказани овом симулацијом могу да утичу и на рад самог система тајне комуникације који је предложен у овој докторској дисертацији. Овај недостатак би био посебно изражен ако би се посматрао кроз рад једног великог *PKI* система који се предлаже на нивоу Европске уније, чији је циљ да опслужује приближно 500 милиона корисника и који је спомињан у поглављу 2 ове дисертације.

Након анализе добијених резултата предложени су начини за унапређење рада сертификационог тела *MUPCA*. Предложена унапређења утичу позитивно на ефикасност рада сертификационог тела *MUPCA*, а самим тим и ефикасност коришћења система за тајну комуникацију предложеног у овој докторској дисертацији. Поред побољшања ефикасности, предлози за унапређење рада сертификационог тела *MUPCA* треба да допринесу већој безбедности њихових корисника, а самим тим и предложеног система за тајну комуникацију.

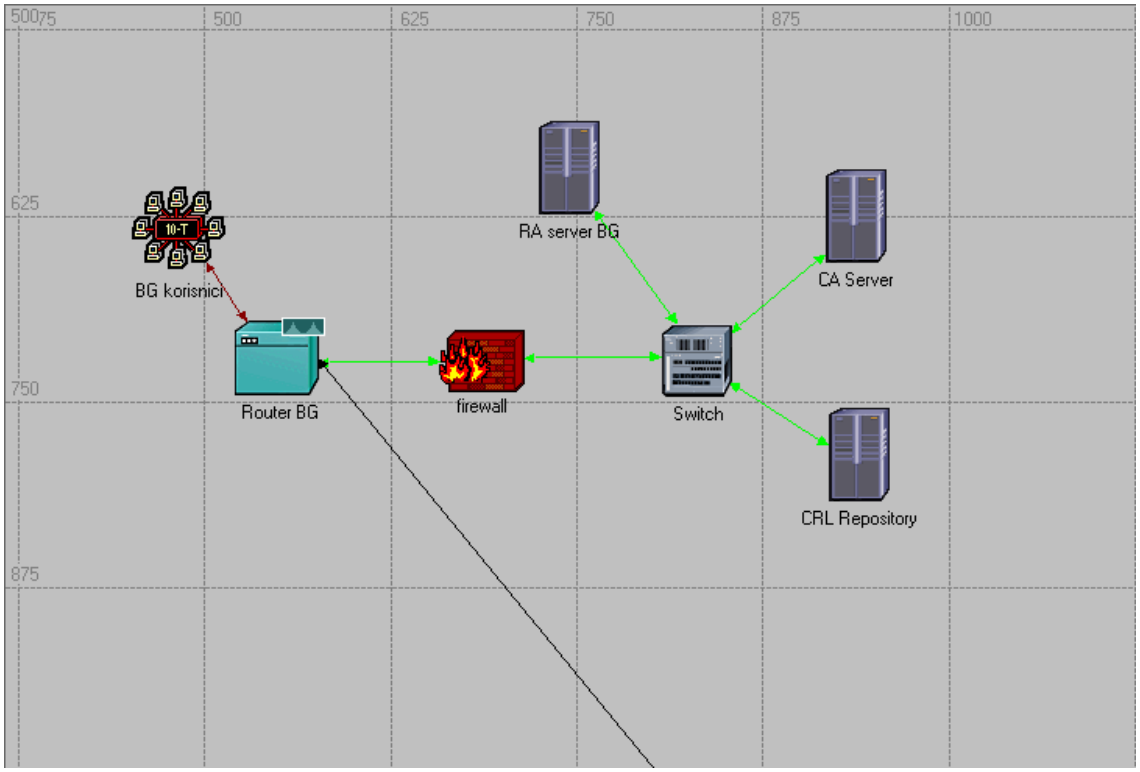
Сервер за слање и примање *email* порука је постављен како би се представила аналогија комуникације између корисника путем интернет мреже и може да се налази било где у свету. У симулационом моделу нису обухваћени сви градови у којима сертификационо тело *MUPCA* има своја регистрациона тела, нити је то био циљ ове симулације.

Објекти који се виде на симулационом моделу који је приказан на претходној слици су објашњени на слици 6.8.

| Име објекта | Модел објекта |
|---|---|
| *E-mail server* | *ppp_server* |
| *internet* | *ip32_cloud* |
| *NS, BG, KG u NI* | *subnet* |
| комуникациони канали | *ppp_DS1 i ppp_DS3* |
| *Aplikacije* | *Application Config* |
| *Profili* | *Profile Config* |

Слика 6.8. Имена и модели објеката коришћени у симулационом моделу

Модели објекта симулационог модела који представљају градове у Републици Србији су заправо подмреже које користе *PKI* систем који се налази у подмрежи *BG* (Београд). Њихова структура се разликује у неколико битних елемената. Објекат симулационог модела који је назван *CA Server* представља сертификационо тело *MUPCA*, слика 6.9.

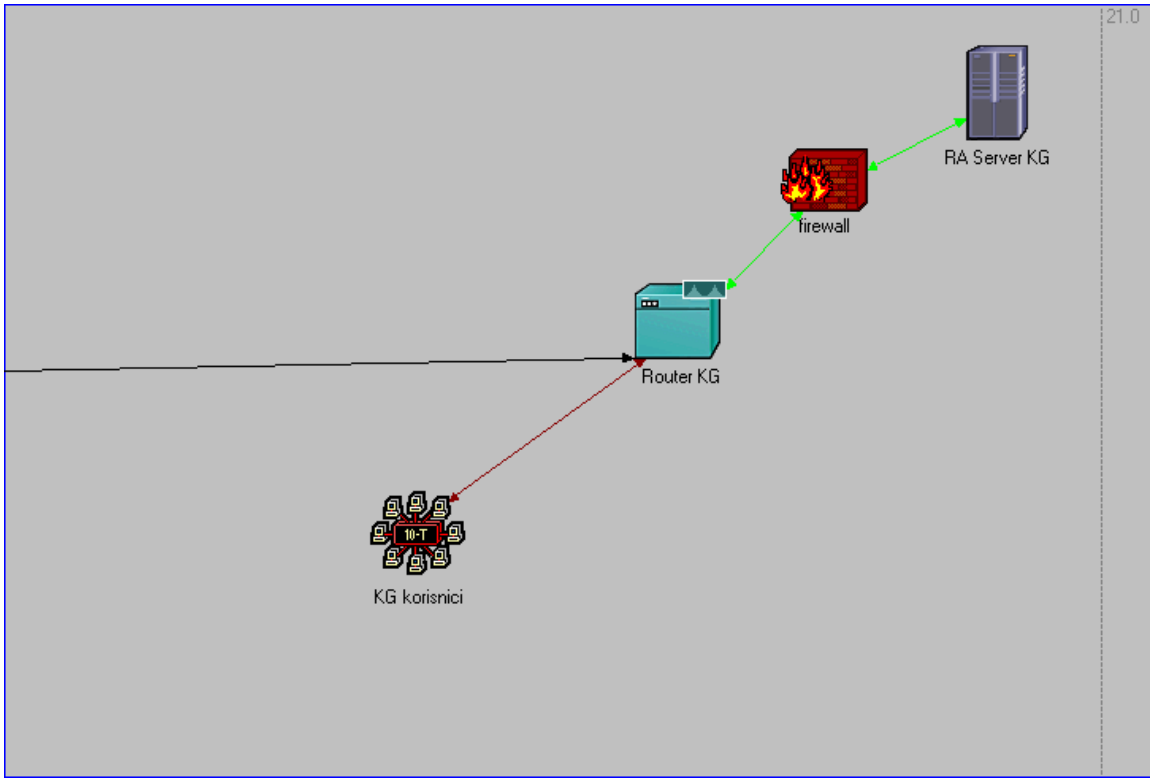



Слика 6.9. Симулациони модел подмреже *BG* (Београд)

*CRL Repository* је база података или директоријум на коме се налази листа опозваних сертификата потписана од стране *MUPCA*. Корисници *PKI* система ће периодично приступати *CRL* серверу и преузимати листу опозваних сертификата. Због ограничења од стране симулационог софтвера, која су већ раније наведена, *CRL* која се преузима од стране корисника у овој симулацији је константне величине. То не осликава рад *PKI* система у стварности, а ни сама *CRL* није константне величине, мерено у *KB*.

Међутим, параметри који се прате у овом симулационом моделу односе се на оптерећење *CRL* сервера и бележе се на два начина. Извршена је симулација преузимања *CRL* када је сервер за преузимање централизован и смештен на једној локацији, а након тога извршена је реконфигурација система тако што је начин преузимања *CRL* децентрализован. Перформансе *CRL* сервера су врло битне за рад оваквог типа мреже и због тога су праћени битни параметри који утичу на њихов рад. Симулациони модел подмреже *KG* (Крагујевац), се пресликава и на остале градове у симулационом моделу, тако да није било неопходно да се прилажу на посебним сликама, слика 6.10.

*RA* сервери који се користе у свим градовима у овом симулационом моделу представљају сервере регистрационих тела и задужени су за креирање захтева за издавање дигиталног сертификата који се након обраде података прослеђује *CA* телу и регистрацију нових корисника. Улога ових *RA* сервера је ограничена на ове две активности и ови сервери немају велики утицај на параметре који се прате.



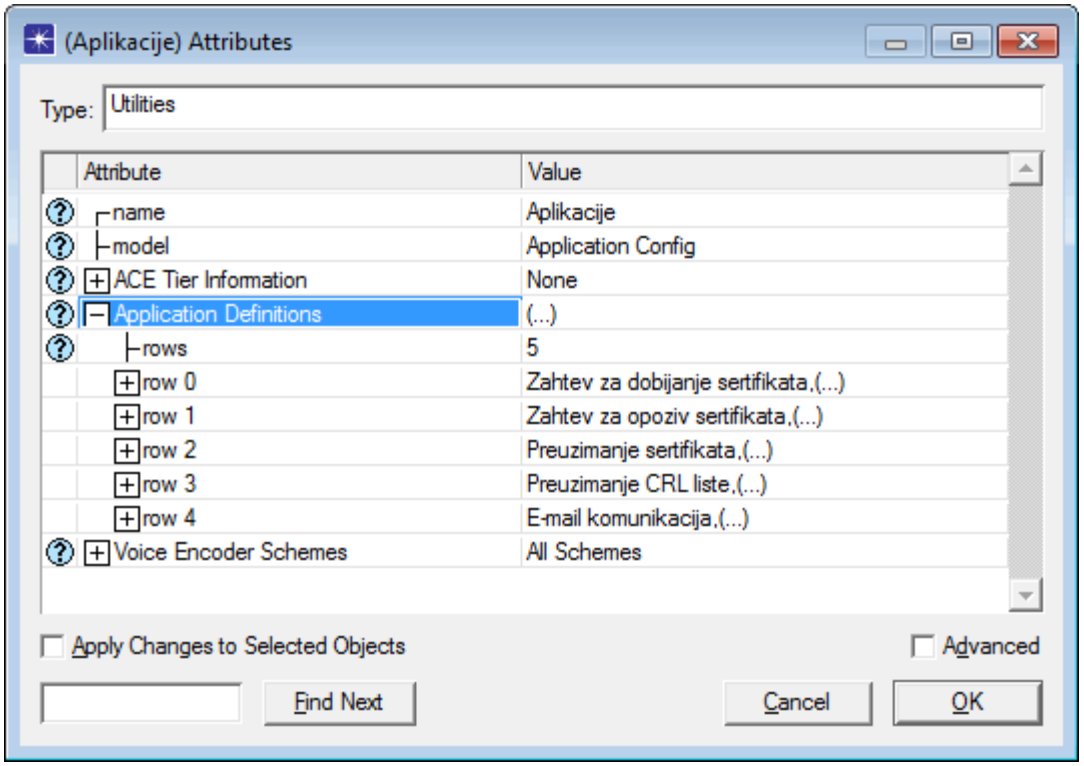

Слика 6.10. Симулациони модел подмреже *KG* (Крагујевац)

Објекти који се виде на симулационом моделу свих подмрежа су објашњени на слици 6.11:

| Име објекта | Модел објекта |
|---|---|
| Сервери | *ethernet_server* |
| Корисници | *10BaseT_LAN* |
| Рутери | *CISCO 7000* |
| Свичеви | *ethernet16_switch* |
| Заштитни зид | *ethernet2_slip8_firewall* |
| комуникациони канали | *10BaseT i 100BaseT* |

Слика 6.11. Имена и модели објеката коришћени у подмрежама симулационог модела

Комуникациони канали који омогућавају комуникацију између групе корисника једне подмреже користе мрежу од 10 *Mbps*. Сервери *PKI* система међусобну комуникацију остварују помоћу мреже од 100 *Mbps*. Дефинисање апликација и протокола који се користе у овом симулационом моделу, који је базиран на поставкама претходно приказаног симулационог модела, приказан је на слици 6.12.



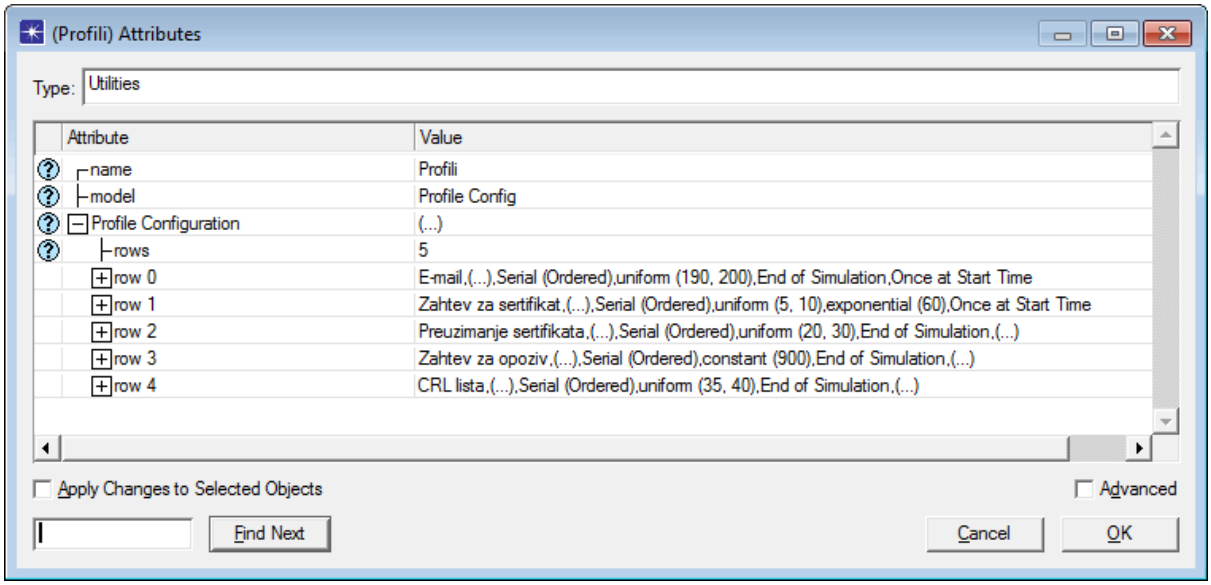

Слика 6.12. Конфигурисање симулационог објекта "Апликације"

Атрибути модела и вредности тих атрибута, који се користе у овом симулираном мрежном окружењу, су приказани на слици 6.13.

| **Име апликације** | **Атрибут модела** | **Вредност атрибута** |
|---|---|---|
| Захтев за добијање сертификата | *HTTP* | *Light Browsing* |
| Захтев за опозив сертификата | *HTTP* | *Light Browsing* |
| Преузимање сертификата | *FTP* | *High load* |
| Преузимање CRL листе | *HTTP* | *1048576 bites* |
| E-mail комуникација | *Email* | *102400 bites* |

Слика 6.13. Параметри апликационих модела

Параметри ових апликација су коришћени за симулацију рада *PKI* система у првом сценарију приказане мрежне конфигурације. У другом сценарију вредности ових параметара нису мењане, већ је извршена реконфигурација мрежног окружења како би се приказао и симулирао децентрализован начин преузимања *CRL*. Активности корисника у оваквом мрежном окружењу дефинисани су на следећи начин, слика 6.14.




Слика 6.14. Конфигурисање симулационог објекта "Профили"

Детаљан опис задатих параметара представља срж рада овог симулационог модела. Називи атрибута и опис активности које ти атрибути реализују у симулационом моделу су прилагођени ограничењима која су дата од стране самог симулационог софтвера, слика 6.15.

| **Назив атрибута** | **Опис активности** |
|---|---|
| E-mail | Апликација се покреће након 190-200 секунди од почетка симулације, што представља време потребно да корисници преузму сертификате и CRL. Извршава се до краја рада симулације. |
| Захтев за сертификат | Апликација се покреће након 5-10 секунди од почетка симулације, извршава се само једном у току симулације у трајању од 10 секунди. |
| Преузимање сертификата | Апликација се покреће након 20-30 секунди од почетка симулације, извршава се два пута током симулације у трајању од 180 секунди. Временски интервал рада је 900 секунди. |
| Захтев за опозив | Апликација се покреће након 900 секунди од почетка симулације у трајању од 60 секунди. |
| CRL листа | Апликација се покреће након 35-40 секунди од почетка симулације, извршава се шест пута у току симулације у трајању од 180 секунди. |

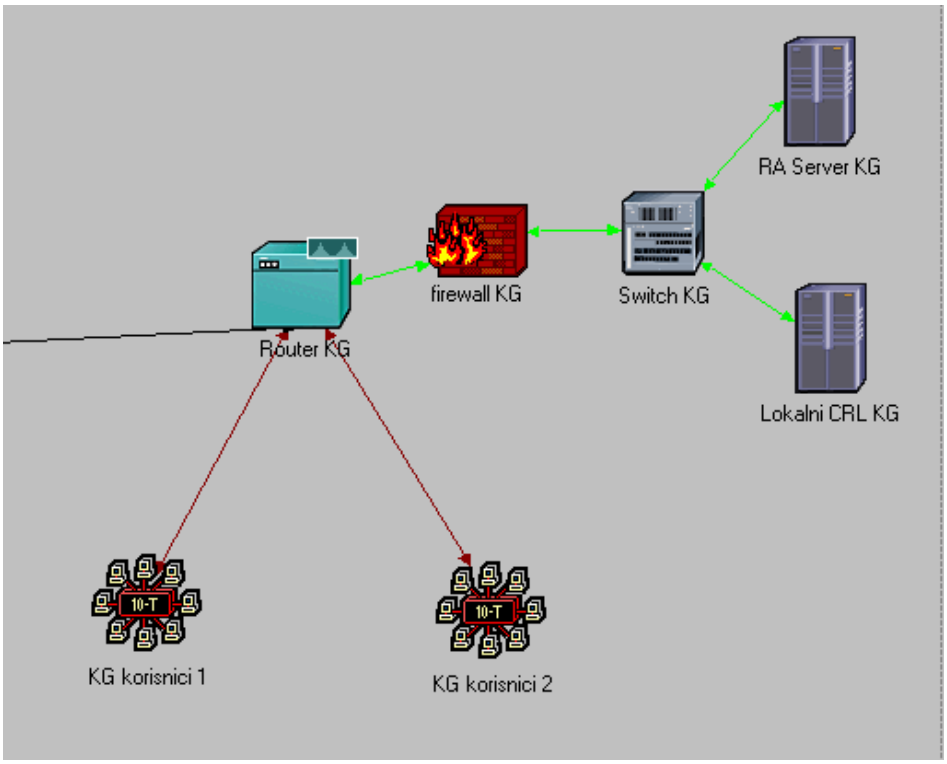
Слика 6.15. Називи атрибута и опис њихових активности

Могућност креирања различитих сценарија у овом експерименту је искоришћена да се комплетан симулациони модел посматра у различитим околностима. Промена одређених параметара објеката, а у одређеним случајевима

и самих објеката симулационог модела, омогућила праћење излазних параметара, евентуалну поновну реконфигурацију симулационог модела и поређење добијених резултата.

За други сценарио овог симулационог модела креирана је још једна апликација, поред постојећих, која је названа "Локално преузимање *CRL* листе" и примењиваће се само на локалне кориснике и *CRL* сервере. Атрибути ове апликације су идентични атрибутима већ представљене апликације првог сценарија под именом "Преузимање *CRL* листе".

Конфигурација подмреже *BG* (Београд) није мењана, а растерећење централног *CRL* сервера је извршено додавањем локалних *CRL* сервера у локалне подмреже. Конфигурација подмреже *KG* (Крагујевац) је измењена, и она је идентична по питању модела објеката који су промењени у подмрежама Нови Сад и Ниш, слика 6.16. Подмрежи Крагујевац је додат један сервер, објекат типа *ethernet_server* који је именован као "Локални *CRL KG*". 80% корисника ове локалне мреже је преусмерено на нови локални сервер. Преусмерени корисници преко рутера су спојени на мрежу линком типа *10BaseT* брзине 10 *Mbps*. Такође, за 80% корисника који ће користити ову апликацију креиран је и нови профил под именом "*CRL* листа локално" који има исте атрибуте као већ представљени профил првог сценарија под именом " *CRL* листа локално".




Слика 6.16. Реконфигурисани симулациони модел подмреже *KG* (Крагујевац)

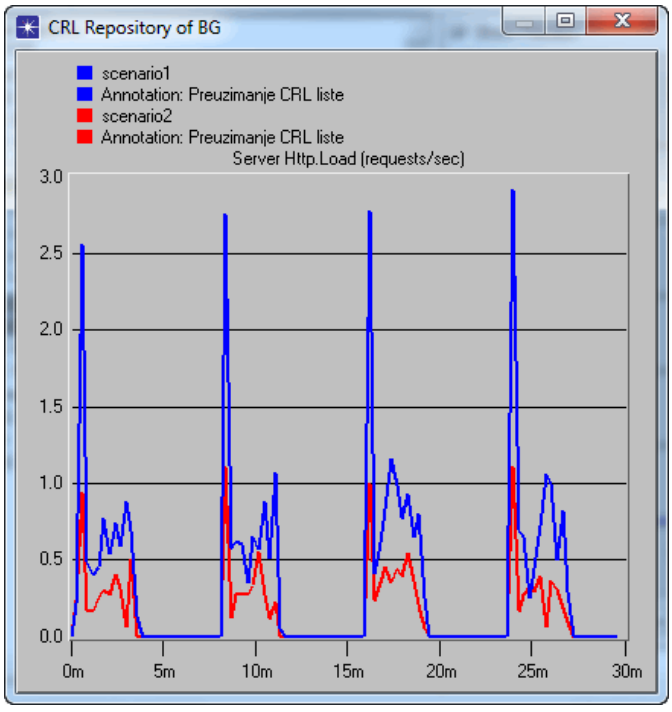
Пре покретања симулације одабрани су статистички параметри који ће да се посматрају и упоређују. Симулациона статистика представља колекцију једне или више вредности којима се описују извесни аспекти процеса понашања током

симулације Статистички подаци који су прикупљани у овој симулацији одабрани су сходно предмету и циљу истраживања постављеног у представљању овог симулационог модела. Праћене су перформансе главног *CRL* сервера у оба сценарија и сходно томе одабрани су следећи статистички параметри за праћење:

- *Load (requests/sec)* - број активних сесија на серверу.
- *Task Processing Time (sec)* - време које је потребно да сервер обради захтев клијента.
- *Traffic Received (bytes/sec)* - просечна стопа долазног саобраћаја.
- *Traffic Sent (bytes/sec)* - просечна стопа одлазног саобраћаја.

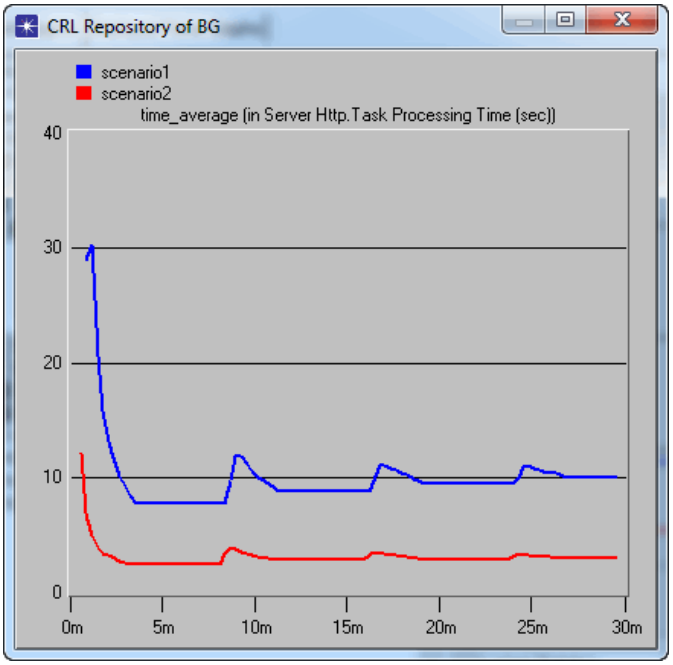
За симулациони модел, у оба сценарија, време трајања симулације је постављено на 30 минута. У оба сценарија симулационог модела приказан је рад 10 корисника сваке подмреже, што у укупном збиру износи 40 корисника, с тим да је у другом сценарију 80% корисника локалних подмрежа преусмерено на локалне сервере.

Подаци за *CRL Repository* сервер који се налази у подмрежи *BG* (Београд) приказани су на сликама 6.17 и 6.18. На слици 6.17 се уочавају задати интервали по којима корисници апликације под именом "*CRL* листа" приступају овом серверу. Са слике се види да је број активних сесија на серверу мањи применом децентрализоване методе за дистрибуирање *CRL*.



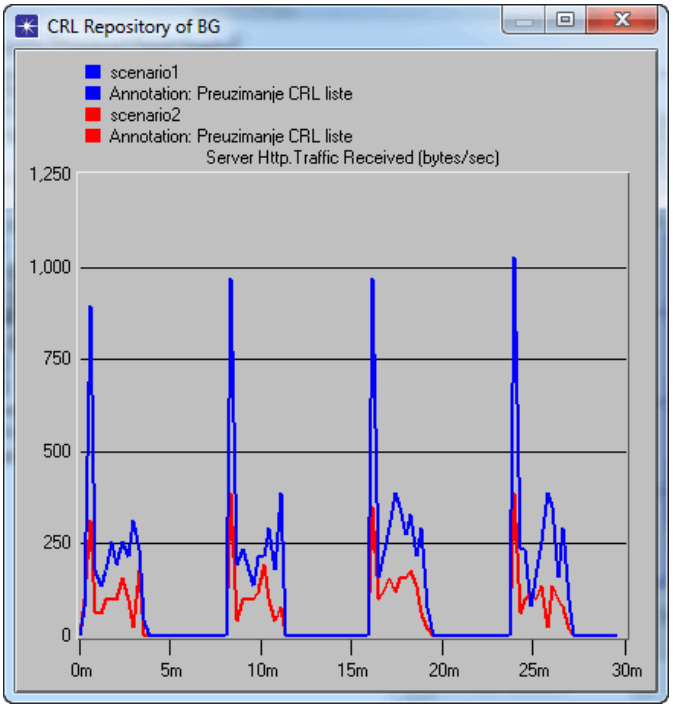

Слика 6.17. Број активних сесија на серверу у подмрежи *BG* (Београд)

Децентрализацијом се *CRL Repository* сервер у подмрежи *BG* (Београд) знатно растерећује, тј. време које је потребно да сервер обради захтеве клијената знатно мање него када је то у питању централизован метод, слика 6.18.

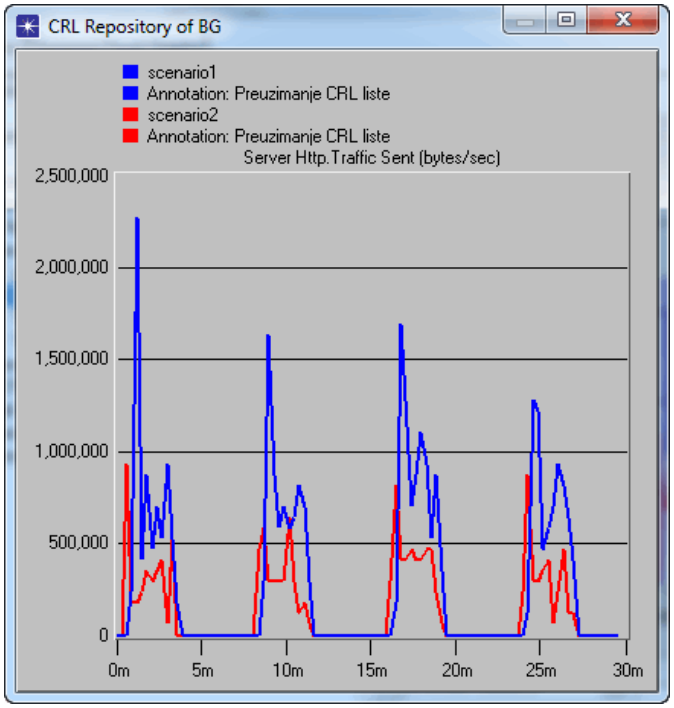



Слика 6.18. Време које је потребно да сервер обради захтев клијента у подмрежи *BG* (Београд)

Просечна стопа долазног и одлазног саобраћаја приказана је на следећим сликама.




Слика 6.19. Просечна стопа долазног саобраћаја у подмрежи *BG* (Београд)




Слика 6.20. Просечна стопа одлазног саобраћаја у подмрежи *BG* (Београд)

Просечна стопа долазног саобраћаја је очекивано мања по вредности јер величина порука које представљају захтеве серверу у подмрежи *BG* (Београд) је мања у односу на *CRL* коју сервер шаље корисницима у супротном смеру.

На овим сликама се такође јасно уочавају задати интервали по којима корисници апликације под именом " *CRL* листа" приступају серверу. Такође се са слика види да је генерисани саобраћај мањи применом децентрализоване методе за дистрибуирање *CRL* и може се закључити да је *CRL Repository* сервер знатно растерећен употребом локалних сервера за дистрибуирање *CRL*.

Информације о коришћеном софтверу у експерименту:

- *OPNET IT Guru Academic Edition 9.1.A PL1(Build 2000)*
- *Microsoft Windows 7 Professional x64, Service Pack 1*

Информације о коришћеном хардверу у експерименту:

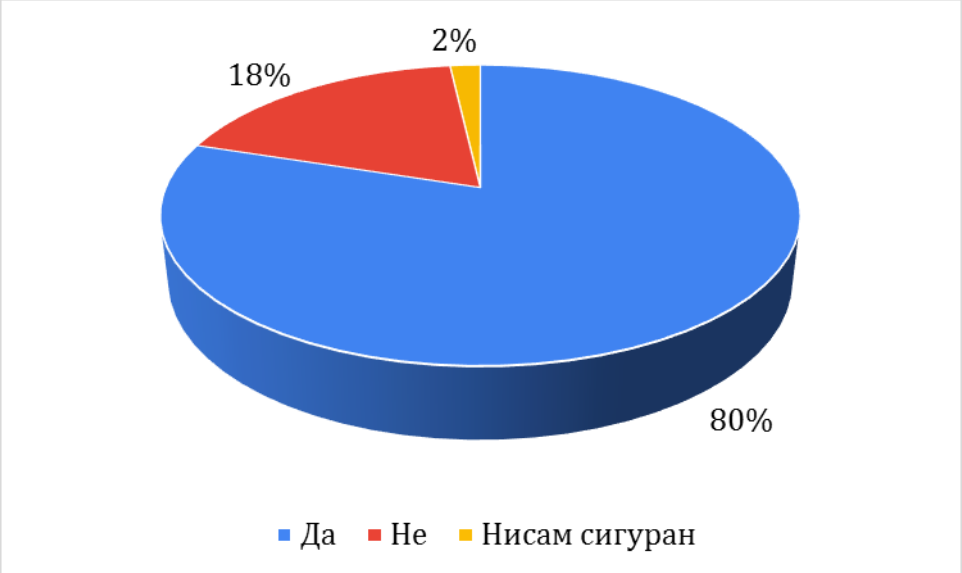
- MB: *Asus H77 P8H77-M*
- CPU: *Intel i5-3470, 3.20 GHz, 4 Core(s)*
- RAM: *8.00 GB DDR3 1600 MHz*
- HDD: *SATA3 7200 2TB*

Резултатима симулације је потврђена претпоставка да размена *CRL* утиче на рад сервера за дистрибуцију исте, самим тим утиче и на перформансе *PKI* система, које посредно утичу и на рад предложеног система за тајну комуникацију. Резултати који су приказани су потврдили да постоје разлике између централизованог и децентрализованог метода за дистрибуирање *CRL* листе.

Уколико би *MUPCA* променио начин који је тренутно у употреби, повлачење *CRL* од стране корисника *PKI* система, увођењем децентрализованих сервера или увођењем *OCSP* протокола безбедносне карактеристике би биле побољшане. Такође се недостатком овог система може сматрати чињеница да се *CRL* објављује једном у току 24 часа. Побољшање ових безбедносних параметара би се директно одразило и на побољшање безбедности корисника предложеног система за тају комуникацију, описаног у глави 5.

## 6.2. Анкета

Анкета о заштити приватности и доприносу исте у друштву спроведена је међу студентима прве године, Високе техничке школе струковних студија у Крагујевцу, на почетку школске 2017. и 2018. године. Питања су била подељена у две групе. Прва група питања односила се на информације о поседовање биометријске личне карте и да ли су упознати са чињеницом да она може садржати квалификовани дигитални сертификат. Друга група питања се односила на заштиту приватности на интернету и да ли су заинтересовани уопште да заштите своју приватност. Анкета је имала за циљ да подстакне испитанике на размишљање о појму приватности на интернету и јачања свести испитаника о важности заштите приватности на интернету.

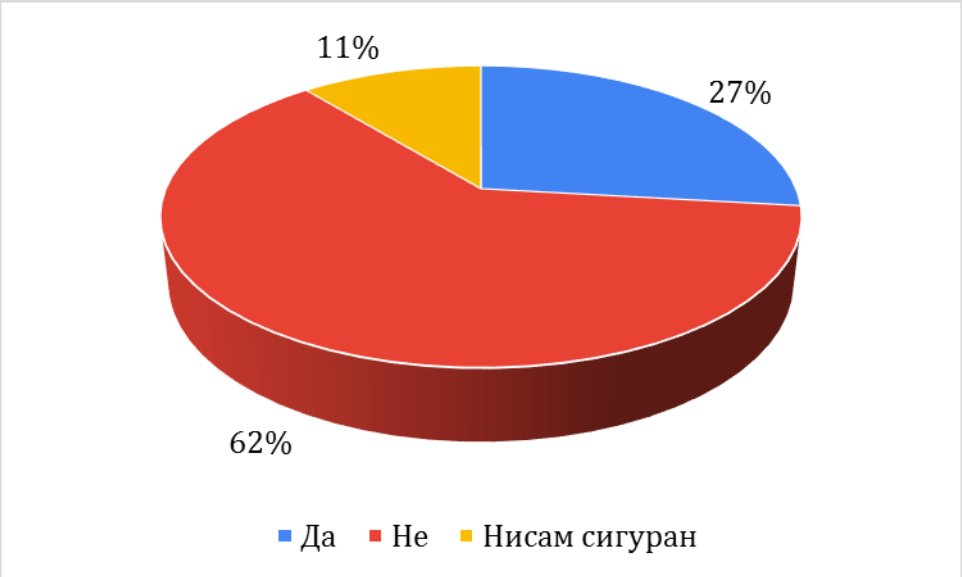



Слика 6.21. Да ли поседујете биометријску личну карту (са чипом)?

Профил анкетираних студената: Од укупног броја испитаника које су одговориле на анкету, више од половине су студенти на одсеку Информатика, старосне доби 18 до 23 година. Овакав профил испитаника одговара појму "дигитално писмена особа".


Слика 6.22. Да ли сте упознати са чињеницом да биометријска лична карта (са чипом) може да садржи квалификовани дигитални сертификат?

80% испитаника поседује биометријску личну карту, 44% испитаника има сазнање да она може садржати квалификовани дигитални сертификат, при чему само трећина од њих је информисана да тиме може заштити своју приватност на интернету.




Слика 6.23. Да ли сте упознати са чињеницом да употребом квалификованог дигиталног сертификата можете да заштитите своју приватност на интернету?

То указује на чињеницу да велики део испитаника није информисан адекватно и не поседује знања везана за могућности заштите, па самим тим и није у могућности да са сигурношћу изрази став да ли би користила биометријску личну карту која садржи квалификовани дигитални сертификат за заштиту своје приватности на интернету.


Слика 6.24. Да ли би сте користили биометријску личну карту (са чипом) која садржи квалификовани дигитални сертификат за заштиту своје приватности на интернету?

Све ово говори у прилог томе да подизање свести испитаника о предностима које им доноси заштита приватности на интернету и сазнање да употребом предложеног система за тајну комуникацију у овој дисертацији могу ту приватност и да остваре. Такође је битно нагласити да је сазнање испитаника о могућностима које им, као крајњим корисницима предложени систем пружа, друштвени допринос овог истраживања у потпуности испуњен.

## 6.3. Поређење с постојећим решењима и правци даљих истраживања

Предложени систем за тајну комуникацију крајњих корисника који унапређује протокол за размену криптографских кључева на бази личних идентификационих докумената доказао је свој "*proof of concept*", тј. да је овај систем, описан у овој докторској дисертацији, доказао изводљивост и показао да су теоретске претпоставке изнете у хипотезама дисертације доказане.

У поређењу са представљеним системима и решењима, описаним у поглављу 4 ове дисертације, предложени систем за тајну комуникацију се показао као комплетно решење које корисницима пружа одговор како да на сигуран и једноставан начин размене тајне кључеве коришћене у стеганографским алатима. Систем који обједињује стеганографске алате, симетричну криптографију и личне идентификационе документе грађана Републике Србије као такав се до сада није користио. Постоје бројни примери употребе личних идентификационих

докумената, који су између осталог наведени у поглављу 2 ове дисертације, међутим, ниједно од њих се није односило на размену криптографских кључева.

Сви алати наведени у поглављу 4 пружају одређени ниво заштите, међутим, у сваком од тих система се поставља питање како и на који начин корисници могу да размене тајне кључеве или лозинке које се користе у тим апликацијама.

Постоје разни системи за размену криптографских кључева који се користе у професионалној пракси и који су доказано сигурни. Предложени систем за тајну комуникацију није препоручљиво користити у сврхе професионалне заштите, првенствено јер се базира на коришћену дигиталних сертификата издатих од "треће стране од поверења". Међутим, иако *MUPCA* представља "трећу страну од поверења" којој корисници њиховог *PKI* система верују, може се тврдити да су тајни кључеви у предложеном протоколу размењени на сигуран начин. Тајни кључеви који се користе у овом решењу првенствено имају за циљ да заштите приватност појединца као индивидуе на интернету, а не великих корпорација и државних служби који би штитили поверљива документа са ознаком "државна тајна". Масовна употреба и лакоћа коришћења предложеног система су две чињенице које би овај предложени систем могао врло лако да оствари.

Даљи развој на предложеном систему тајне комуникације би био развој једне свеобухватне мрежне или *Cloud* апликације која би примену овог система приближила корисницима паметних телефона и апликацијама које они користе. Овај систем је развијен у Јава програмском језику што му гарантује модуларност и примену на готово свим оперативним системима. Такође је потребно развити нови начин за проверу повучених сертификата јер чињенице које су изнете у овој дисертацији указују да је то један од већих недостатака. Међутим, то не зависи директно од предложеног система већ од издавача квалификованих дигиталних сертификата, тј. од сертификационог тела *MUPCA*. Временски период од 24 часа, тј. период који се односи на објављивање *CRL* листе, је предугачак с обзиром на чињеницу да се трансакције било које врсте путем интернет и мобилне мреже извршавају готово тренутно. У таквом једном систему чињеница да корисник нема тренутну информацију о валидности дигиталног сертификата не доприноси безбедности, већ напротив, отвара разне могућности за злоупотребу.

# 7. Закључак

Анализом и систематизацијом постојећих знања, искустава и научних резултата из области истраживања ове докторске дисертације, дефинисан је предмет и циљ истраживања.

Циљ истраживања докторске дисертације је унапређење протокола за размену тајних криптографских кључева који се користе у симетричној криптографији. Извршена је анализа актуелних проблема везаних за безбедну електронску размену тајних кључева који се користе у симетричној криптографији и аутентификацију корисника система за тајну комуникацију, као и анализа постојећих решења у области истраживања.

Развијање система за комуникацију, који се данас већином ослањају на интернет, бежичну комуникацију и комуникацију путем мобилних мрежа у којима брзине преноса података непрестано расту, повећава се и број нових корисника, како и број нових услуга са интуитивним интерфејсима. Анализом изнетих чињеница у докторској дисертацији и доношењем закључка да електронска дистрибуција тајних симетричних кључева постаје све више "уско грло", представљено је унапређено решење које се заснива на симетричним и асиметричним шифарским системима, и на коришћењу јединствених криптолошких параметара који се налазе на личним идентификационим документима грађана Србије.

Практични циљ овог истраживања огледа се у развоју и примени једног новог свеобухватног модела за тајну комуникацију. Ново решење се заснива на коришћењу јединствених параметара који се налазе на идентификационим документима грађана и на примени стеганографских техника за сакривање и утискивање кратких секвенци у различите стандардне медије за комуникацију (слика, текст, говор, видео, електронска пошта и сл.). Развијено решење нема теоријску подлогу за професионалне системе заштите, али је веома употребљиво за комерцијалну употребу и лако се може реализовати и користити у свакодневном раду великог броја стандардних корисника сервиса на интернету.

Спроведена анкета међу студентима прве године Високе техничке школе струковних студија у Крагујевцу, одмах након уписа у прву годину студија, указује на то да развој предложеног модела за тајну комуникацију може да допринесе већој друштвеној прихватљивости и да подстиче кориснике да користе средства за заштиту приватности која су им лако доступна. С подизањем опште свести о једноставности употребе предложеног модела и указивањем на широк спектар могућности који се нуде крајњим корисницима друштвени циљ овог истраживања би био у потпуности задовољен.

Научни допринос овог рада односи се на примени јединствених параметара са личних идентификационих докумената за развој сопственог решења за заштиту тајних симетричних кључева. Поверење у параметре који се користе за сопствено решење почива на поверењу у рад квалификованих сертификационих тела. У овом раду коришћени су квалификовани дигитални сертификати које издаје МУП Републике Србије. Као додатна мера која је усмерена ка побољшању предложеног система за тајну комуникацију предлаже се примена стеганографских техника за сакривање шифрованих кључева симетричне криптографије у одговарајући стего носач.

У дисертацији је извршена детаљна анализа доступних протокола за електронску дистрибуцију тајних симетричних криптографских кључева и указано је на потенцијалне слабости и предности предложеног решења. У раду је показана ефикасност предложеног поступка применом на Веб галерију слика које су дате у тзв. *JPEG* формату. Предложени поступак се ефикасно може применити и код других стандардних носилаца у данашњим комуникација (текст, слика, говор, видео и томе сл.), као и код стандардних комуникационих сервиса (имејл, *Viber, WhatsApp* и сл.). Дат је критички осврт на делове система за тајну комуникацију који могу да утичу на безбедну употребу истог и дате смернице за унапређење недостатака. Када би овај проблем био решен, тј. када би се математички могла потврдити апсолутна тајност у електронској дистрибуцији кључева, то би довело до револуционарних промена у професионалним и комерцијалним системима за заштиту тајности у преносу података.

У складу са до сада наведеним, доприноси докторске дисертације су:

- Развијен је нови протокол за размену тајних симетричних криптографских кључева на бази личних идентификационих докумената пошиљаоца и примаоца. Предложено решење има низ криптолошких предности од којих се издвајају:
  - Не постоји потреба да се смешта и чува велики број тајних кључева код корисника пошто се они могу компромитовати,
  - За сваку нову комуникацијску сесију генерише се нови тајни кључ. Евентуална компромитација једног оваквог кључа не утиче на тајност осталих пренетих порука, пошто су оне шифроване другим кључем.
  - Остварује се потпуна *end-to-end* заштита за сваку комуникацију и за сваки пар учесника у тајној комуникацији.
- Развијено је сопствено решење које не захтева рад тзв. треће стране од поверења. Користе се само параметри који су издати од стране тела које издаје квалификоване дигиталне сертификате.

- Разматрана је примена стеганографских техника за сакривање шифрата у одговарајући тзв. стего носилац. На примеру *JPEG* слика показано је да сакривена информација не утиче на статистичке карактеристике, нити на меморијске карактеристике стего носиоца.
- Нови протокол је отпоран на велики број напада на мрежи.

Резултати рада се могу користити за широки спектар комерцијалних решења за комуникацију. Од корисника таквих решења се не захтева професионално познавање криптографије. Остварена комуникација се тешко може открити и обезбеђује висок степен тајности за апликације које користе тајне симетричне криптографске кључеве. За професионалне системе заштите, остварени резултат се може посматрати као корак више у заштити када се посматрају комбинована решења са надшифровањем и сакривањем шифрованог материјала.

# Литература


[1] Meng, Keju, Fuyou Miao, and Yue Yu. *A secure and efficient on-line/off-line group key distribution protocol. Designs*, Codes and Cryptography 87.7: 1601-1620, 2019.

[2] Vijayakumar, P., et al. *Key management and key distribution for secure group communication in mobile and cloud network*. Future Generation Computer Systems 84: 123-125, 2018.

[3] Al-Qurishi, Muhammad, et al. *An efficient key agreement protocol for Sybil-precaution in online social networks*. Future Generation Computer Systems 84: 139-148, 2018.

[4] Zhou, Yukun, et al. *A similarity-aware encrypted deduplication scheme with flexible access control in the cloud.* Future Generation Computer Systems 84: 177-189, 2018.

[5] Guo, Cheng, et al. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. Future Generation Computer Systems 84: 190-199, 2018.

[6] Shen, Pei-Yuan, Vicky Liu, and William Caelli. *A viable and sustainable key management approach for a national e-health environment*. 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2012.

[7] Kim, Sundeuk, Hyun-Taek Oh, and Young-Gab Kim. *Certificate sharing system for secure certificate distribution in mobile environment*. Expert Systems with Applications 44: 67-77, 2016.

[8] von Maurich, Olga, and Alessandro Golkar. *Data authentication, integrity and confidentiality mechanisms for federated satellite systems*. Acta Astronautica 149 : 61-76. 2018.

[9] John, Saju P., and Philip Samuel. *Self-organized key management with trusted certificate exchange in MANET*. Ain Shams Engineering Journal 6.1: 161-170, 2015.

[10] Yüce, Emre, and Ali Aydn Selçuk. *Server notaries: a complementary approach to the web PKI trust model*. IET Information Security 12.5: 455-461, 2018.

[11] Lozupone, Vincent. *Analyze encryption and public key infrastructure (PKI)*. International Journal of Information Management 38.1: 42-44, 2018.

[12] Nagar, Sami A., and Saad Alshamma. *High speed implementation of RSA algorithm with modified keys exchange*. 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), IEEE, 2012.

[13] Yao, Andrew Chi-Chih, and Yunlei Zhao. *Privacy-preserving authenticated key-exchange over internet*. IEEE Transactions on Information Forensics and Security 9.1: 125-140, 2013.

[14] Zwattendorfer, Bernd, and Daniel Slamanig. *Design strategies for a privacy-friendly Austrian eID system in the public cloud*. Computers & Security 52: 178-193, 2015.

[15] Zwattendorfer, Bernd, and Daniel Slamanig. *The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality*. Journal of information security and applications 27: 35-53, 2016.

[16] Rezaeighaleh, Hossein, Roy Laurens, and Cliff C. Zou. *Secure Smart Card Signing with Time-based Digital Signature*. International Conference on Computing, Networking and Communications (ICNC), IEEE, 2018.

[17] Sánchez-García, Jesús, et al. *On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks*. Future Generation Computer Systems 64: 50-60, 2016.

[18] León-Coca, Jose Maria, et al. *Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe*. Procedia Computer Science 21: 91-98, 2013.

[19] Carretero, Jesus, et al. *Federated identity architecture of the European eID system*. IEEE Access 6: 75302-75326, 2018.

[20] Berbecaru, Diana, Antonio Lioy, and Cesare Cameroni. *Authorize-then-Authenticate: Supporting Authorization Decisions Prior to Authentication in an Electronic Identity Infrastructure*. International Symposium on Intelligent and Distributed Computing. Springer, Cham, 2019.

[21] Lenz, Thomas, and Vesna Krnjic. *Towards Domain-Specific and Privacy-Preserving Qualified eID in a User-Centric Identity Model*. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018.

[22] Slamanig, Daniel, Klaus Stranacher, and Bernd Zwattendorfer. *User-centric identity as a service-architecture for eIDs with selective attribute disclosure*. Proceedings of the 19th ACM symposium on Access control models and technologies, ACM, 2014.

[23] Poller, Andreas, et al. *Electronic identity cards for user authentication-promise and practice*. IEEE Security & Privacy 1: 46-54, 2012.

[24] Lenz, Thomas, and Lukas Alber. *Towards cross-domain eid by using agile mobile authentication*. IEEE Trustcom/BigDataSE/ICESS, IEEE, 2017.

[25] Lips, Silvia, et al. *Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field*. International Conference on Electronic Government and the Information Systems Perspective, Springer, Cham, 2018.

[26] Amin, Muhalim Mohamed, et al. *Information hiding using steganography*. 4th National Conference of Telecommunication Technology, NCTT 2003 Proceedings, IEEE, 2003.

[27] El_Rahman, Sahar A. *A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information*. Computers & Electrical Engineering 70: 380-399. 2018.

[28] Attaby, Abdelhamid Awad, Mona FM Mursi Ahmed, and Abdelwahab K. Alsammak. *Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3*. Ain Shams Engineering Journal, 2017.

[29] Muhammad, Khan, et al. *Image steganography using uncorrelated color space and its application for security of visual contents in online social networks.*" Future Generation Computer Systems 86: 951-960, 2018.

[30] Jain, Mamta, Saroj Kumar Lenka, and Sunil Kumar Vasistha. *Adaptive circular queue image steganography with RSA cryptosystem*." Perspectives in Science 8: 417-420, 2016.

[31] Achuthshankar, Aswathy, et al. *Encryption of Reversible Data Hiding for Better Visibility and High Security*. Procedia Technology 25: 216-223, 2016.

[32] Xiaojian, Luo, and Long Xiang. *AS algorithm: An optimal on-line real-time scheduling algorithm for uniform multiprocessors*. 3rd International Conference on Computational Intelligence & Communication Technology (CICT), IEEE, 2017.

[33] Bharti, Pria, and Roopali Soni. *A new approach of data hiding in images using cryptography and steganography*. International Journal of Computer Applications 58.18, 2012.

[34] Uljarević, Dejan., A. Mišković et al. *An Overview of Steganographic Techniques and Methods Applied on Jpeg Images Using Different Transformational Techniques*. Sinteza 2016 - International Scientific Conference on ICT and E-Business Related Research, Singidunum University Belgrade, pp. 165-172, 2016.

[35] Uljarević, Dejan, et al. *A new way of covert communication by steganography via JPEG images within a Microsoft Word document*. Multimedia Systems 23.3: 333-341. 2017.

[36] Tanenbaum, Andrew S. *Computer networks, 5-th edition*. Prentice Hall, 2011.

[37] Schneier, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 1996.

[38] Veinović, Mladen, and Saša Adamović. *Kriptologija I - 2018*. Univerzitet Singidunum, Beograd, 2018.

[39] Milosavljević, Milan, and Saša Adamović. *Kriptologija 2 - 2017*. Univerzitet Singidunum, Beograd, 2017.

[40] Van Tilborg, Henk CA, and Sushil Jajodia, eds. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[41] Stamp, Mark. *Information security: principles and practice*. New York: Wiley, 2011.

[42] Stamp, Mark, and Richard M. Low. *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons, 2007.

[43] Boneh, Dan, and Victor Shoup. *A graduate course in applied cryptography*. version 0.4, 2017. [Online], https://crypto.stanford.edu/~dabo/cryptobook/ [Cited: 20.10.2019.]

[44] Wagstaff Jr, Samuel S. *Cryptanalysis of number theoretic ciphers*. Chapman and Hall/CRC, 2003.

[45] Gorbenko, Ivan, et al. *The research of modern stream ciphers*. 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), IEEE, 2017.

[46] Jindal, Poonam, and Brahmjit Singh. *A survey on RC4 stream cipher*. Journal of Computer Network and Information Security, 7: 37-45, 2015.

[47] Ellis, Scott R. *A Cryptography Primer.* Computer and Information Security Handbook 2nd Edition: 25-46, Morgan Kaufmann, 2013.

[48] Housley, Russell. *RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)*. Tech. Rep., 2004.

[49] Diffie, Whitfield, and Martin Hellman. *New directions in cryptography*. IEEE transactions on Information Theory: 644-654, 1976.

[50] Kohnfelder, Loren M. *Towards a practical public-key cryptosystem*. PhD Thesis, Massachusetts Institute of Technology, 1978.

[51] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 1978.

[52] Batten, Lynn Margaret. *Public key cryptography: applications and attacks*. John Wiley & Sons, 2013.

[53] Azad, Saiful, and Al-Sakib Khan Pathan. *Practical cryptography: algorithms and implementations using C++*. Auerbach Publications, 2014.

[54] Barker, Elaine, and Allen Roginsky. *Recommendation for cryptographic key generation*. NIST Special Publication (SP) 800-133 Rev. 1, National Institute of Standards and Technology, 2019.

[55] Aryanti, Aryanti, and Ikhthison Mekongga. *Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System*. E3S Web of Conferences, Vol. 31. EDP Sciences, 2018.

[56] Zhou, Xin, and Xiaofei Tang. *Research and implementation of RSA algorithm for encryption and decryption*. Proceedings of 2011 6th International Forum on Strategic Technology, Vol. 2. IEEE, 2011.

[57] Schaefer, Edward. *An introduction to cryptography and cryptanalysis*. California's Silicon Valley: Santa Clara University: 4-5, 2009.

[58] Barker, Elaine, et al. *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*. NIST Special Publication (SP) 800-56B Rev. 2, National Institute of Standards and Technology, 2019.

[59] Mišković, Aleksandar, and Mladen Veinović. *Comparative analysis of the Certification Authority in Serbia*. 19thTelecommunications Forum (TELFOR), Proceedings of Papers, IEEE, 2011. [18]

[60] Kuhn, D. Richard, et al. *SP 800-32. Introduction to Public Key Technology and the Federal PKI Infrastructure*, 2001. [19]

[61] Mrdović, Saša. *Izgradnja infrastrukture javnih ključeva (PKI).* Magistarski rad, Elektrotehnički fakultet u Sarajevu, 2004. [20]

[62] Chokhani, S., et al. *RFC 3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, 2003. [21]

[63] Housley, Russ, et al. *RFC 3280: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile*, IETF, 2002. [22]

[64] Kovinić, Milica et al. *Upotrebom digitalnih sertifikata do sigurnog pristupa servisima*. AMRES BPD 9 106, 2011. [23]

[65] Prodanović, Radomir I., and Ivan B. Vulić. *Model for PKI interoperability in Serbia.* Vojnotehnički glasnik 65.2: 530-549, 2017. [24]

[66] Milosavljević, Milan, and Vladislav Miškovic. *Elektronska trgovina, 5. izdanje*. Univerzitet Singidunum, Beograd, 2019. [25]

[67] Recommendation ITU-T X.509. *Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks*. 2019. [Online], https://www.itu.int/rec/T-REC-X.509-201910-I/en [Cited: 20.11.2019.] [26]

[68] PGP Corporation. *An Introduction to Cryptography*. 2006. [Online], http://eval.symantec.com/mktginfo/downloads/PGP_Intro-to-Crypto_F.pdf [Cited: 15.11.2019.] [27]

[69] Cooper, David, et al. *RFC 5280: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile*. IETF, 2008.

[70] Mišković, Aleksandar, and Srđan Atanasijević. *Analysis of the pull method for CRL list download by PKI simulation model*. Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide, Singidunum University Belgrade, 2014.

[71] Veinović, Mladen, and Aleksandar Mišković. *Metode za proveru statusa i validnosti digitalnih sertifikata*. 10. naučni skup Sinergija, pp.53-58, Bijeljina, 2012. [28]

[72] Santesson, Stefan, et al. *RFC 6960: X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP.* 2013.

[73] Chandramouli, Rajarathnam, Mehdi Kharrazi, and Nasir Memon. *Image steganography and steganalysis: Concepts and practice*. International Workshop on Digital Watermarking, Springer, Berlin, Heidelberg, 2003.

[74] Simmons, Gustavus J. *The prisoners' problem and the subliminal channel*. Advances in Cryptology, Springer, Boston, MA, 1984.

[75] Cox, Ingemar, et al. *Digital watermarking and steganography, second edition*. Morgan Kaufmann, 2007.

[76] Walia, Ekta, Payal Jain, and Navdeep Navdeep. *An analysis of LSB & DCT based steganography*. Global Journal of Computer Science and Technology, 2010.

[77] McAteer, Ian, et al. *Integration of biometrics and steganography: A comprehensive review*. Technologies 7.2: 34, 2019.

[78] Cheddad, Abbas, et al. *Digital image steganography: Survey and analysis of current methods*. Signal processing 90.3: 727-752, 2010.

[79] Sethi, Adarshpal S., and Vasil Y. Hnatyshin. *The practical OPNET user guide for computer network simulation*. Chapman and Hall/CRC, 2012.

[80] Lu, Zheng, and Hongji Yang. *Unlocking the power of OPNET modeler. Cambridge University Press*, 2012.

# Прилог

```java
package org.acme.smartcard;

        import org.acme.smartcard.domain.KeyStoreInfo;
        import org.acme.smartcard.impl.ConfigServiceImpl;
        import org.acme.smartcard.impl.CryptoServiceImpl;
        import org.acme.smartcard.utils.FileIOUtils;

        import java.nio.charset.StandardCharsets;
        import java.security.KeyStore;
        import java.security.PrivateKey;
        import java.security.cert.X509Certificate;
        import java.util.ArrayList;
        import java.util.List;

public class Main {

    public static void main(String[] args) throws Exception {
        final String cfgLocation = "src/main/resources/config/pkcs11.cfg";
        final String keyType = "PKCS11";
        final char[] pin = {'3', '5', '1', '4'};

        // initializing personal ID as java KeyStore
        final ConfigService configService = ConfigServiceImpl.INSTANCE;
        configService.loadPkcsProvider(cfgLocation);
        KeyStore keyStore = configService.createKeyStore(pin, keyType);

        // getting right alias from java KeyStore
        final List<String> aliasList = new ArrayList<>();
        final List<KeyStoreInfo> infos = configService.readKeyStoreInfo(keyStore);
        for (final KeyStoreInfo info : infos) {
            final String alias = info.getAlias();
            aliasList.add(alias);
        }

        String alias = aliasList.get(1);

        // with cryptoService perform encryption and decryption
        CryptoService cryptoService = CryptoServiceImpl.INSTANCE;

        final String text = FileIOUtils.readFileIntoString( filePath: "src/main/resources/files/dummy.txt");

        // encrypting part of the code
        final X509Certificate cert = (X509Certificate) keyStore.getCertificate(alias);

        final byte[] encryptedData = cryptoService.encryptData(cert,  transformation: "RSA", text.getBytes(StandardCharsets.UTF_8));

        // save encrypted file
        FileIOUtils.writeStringIntoFile(new String(encryptedData, StandardCharsets.UTF_8),  filePath: "target/encryptedDummyFile.txt");

        // decrypting part of the code
        final String encryptedText = FileIOUtils.readFileIntoString( filePath: "target/encryptedDummyFile.txt");

        final PrivateKey privateKey = (PrivateKey) keyStore.getKey(alias,  password: null);

        final byte[] decryptedData = cryptoService.decryptData(privateKey,  transformation: "RSA/ECB/PKCS1Padding",
                encryptedText.getBytes());

        final String decryptedText = new String(decryptedData, StandardCharsets.UTF_8);

        // save decrypted data into the file
        FileIOUtils.writeStringIntoFile(decryptedText,  filePath: "target/deryptedDummyFile.txt");

        // unload personal ID card
        configService.unLoadPkcsProvider();
        System.exit( status: 0);
    }
}
```

```java
package org.acme.smartcard.impl;

import org.acme.smartcard.ConfigService;
import org.acme.smartcard.domain.KeyStoreInfo;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import java.security.*;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.Enumeration;
import java.util.List;
import java.util.Objects;

/**
 * Singleton implementation of ConfigService
 *
 * @author Miskovic
 */
public class ConfigServiceImpl implements ConfigService {

    public static final ConfigServiceImpl INSTANCE = new ConfigServiceImpl();

    private static final Logger LOGGER = LoggerFactory.getLogger(ConfigServiceImpl.class);

    private String providerName;

    private ConfigServiceImpl() {

    }

    @Override
    public KeyStore createKeyStore(char[] pin, String keyType) throws Exception {
        LOGGER.info("Creating keystore of keyType {} ", keyType);
        final KeyStore keyStore = KeyStore.getInstance(keyType);
        keyStore.load( stream: null, pin);
        return keyStore;
    }

    @Override
    public void loadPkcsProvider(String config) {
       // final String config = "name = SmartCard\n" + "library = " + configPath;
        // LOGGER.info("Loading provider with config: {}", config);

        //final Provider provider = new SunPKCS11();
        final Provider provider = Security.getProvider( name: "SunPKCS11");
        Provider configuredProvider = provider.configure(config);
        Security.addProvider(configuredProvider);

        this.providerName = provider.getName();
    }

    @Override
    public List<KeyStoreInfo> readKeyStoreInfo(KeyStore keyStore) throws Exception {
        final List<KeyStoreInfo> infos = new ArrayList<>();

        if (Objects.nonNull(keyStore)) {
            final Enumeration<String> aliasesEnum = keyStore.aliases();
            while (aliasesEnum.hasMoreElements()) {
                final KeyStoreInfo info = new KeyStoreInfo();

                final String alias = aliasesEnum.nextElement();
                info.setAlias(alias);
                LOGGER.info("Alias: {}", alias);

                final X509Certificate cert = (X509Certificate) keyStore.getCertificate(alias);
                info.setCert(cert);
                LOGGER.info("Certificate: {}", cert);

                final PrivateKey privateKey = (PrivateKey) keyStore.getKey(alias,  password: null);
                info.setPrivateKey(privateKey);
                LOGGER.info("Private key: {}", privateKey);

                final PublicKey publicKey = cert.getPublicKey();
                info.setPublicKey(publicKey);
                LOGGER.info("Public key: {}", publicKey);

                infos.add(info);
            }
        }

        return infos;
    }

    @Override
    public void unLoadPkcsProvider() {
        LOGGER.info("Unloading provider: {}", providerName);
        Security.removeProvider(providerName);
        this.providerName = null;
    }
}
```

```java
package org.acme.smartcard.impl;

import org.acme.smartcard.CryptoService;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import javax.crypto.Cipher;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.cert.X509Certificate;
import java.util.Base64;
import java.util.Objects;

/**
 * Singleton implementation of CryptoService
 *
 * @author Miskovic
 */
public class CryptoServiceImpl implements CryptoService {

    public static final CryptoService INSTANCE = new CryptoServiceImpl();

    private static final Logger LOGGER = LoggerFactory.getLogger(CryptoServiceImpl.class);

    private CryptoServiceImpl() {

    }

    @Override
    public byte[] decryptData(PrivateKey privateKey, String transformation, byte[] base64Data) throws Exception {
        if (Objects.isNull(privateKey)) {
            throw new RuntimeException("Invalid input parameter. Parameter privateKey can not be null!");
        }

        if (Objects.isNull(base64Data)) {
            throw new RuntimeException("Invalid input parameter. Parameter base64Data can not be null!");
        }

        LOGGER.info("Start decrypting data...");
        final long startTime = System.currentTimeMillis();

        final byte[] decodedData = Base64.getDecoder().decode(base64Data);

        final Cipher cipher = Cipher.getInstance(transformation);
        cipher.init(Cipher.DECRYPT_MODE, privateKey);

        final byte[] decryptedData = cipher.doFinal(decodedData);

        final long totalTime = System.currentTimeMillis() - startTime;

        LOGGER.info("Decryption has finished. Time spent: [{}]", totalTime);

        return decryptedData;
    }

    @Override
    public byte[] encryptData(X509Certificate cert, String transformation, byte[] data) throws Exception {
        if (Objects.isNull(cert)) {
            throw new RuntimeException("Invalid input parameter. Parameter cert can not be null!");
        }

        if (Objects.isNull(data)) {
            throw new RuntimeException("Invalid input parameter. Parameter data can not be null!");
        }

        LOGGER.info("Start encrypting data...");
        final long startTime = System.currentTimeMillis();

        final PublicKey publicKey = cert.getPublicKey();

        final Cipher cipher = Cipher.getInstance(transformation);
        cipher.init(Cipher.ENCRYPT_MODE, publicKey);

        final byte[] encryptedData = cipher.doFinal(data);

        final byte[] encodedData = Base64.getEncoder().encode(encryptedData);

        final long totalTime = System.currentTimeMillis() - startTime;

        LOGGER.info("Encryption has finished. Time spent: [{}]", totalTime);

        return encodedData;
    }
}
```

```java
package org.acme.smartcard.domain;

import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.cert.X509Certificate;

public class KeyStoreInfo {

    private String alias;

    private X509Certificate cert;

    private PrivateKey privateKey;

    private PublicKey publicKey;

    public PublicKey getPublicKey() { return publicKey; }

    public void setPublicKey(PublicKey publicKey) { this.publicKey = publicKey; }

    public String getAlias() { return alias; }

    public void setAlias(String alias) { this.alias = alias; }

    public X509Certificate getCert() { return cert; }

    public void setCert(X509Certificate cert) { this.cert = cert; }

    public PrivateKey getPrivateKey() { return privateKey; }

    public void setPrivateKey(PrivateKey privateKey) { this.privateKey = privateKey; }
}
```

```java
package org.acme.smartcard;

import org.acme.smartcard.domain.KeyStoreInfo;

import java.security.KeyStore;
import java.util.List;

public interface ConfigService {

    KeyStore createKeyStore(char[] pin, String keyType) throws Exception;

    void loadPkcsProvider(String configPath) throws Exception;

    List<KeyStoreInfo> readKeyStoreInfo(KeyStore keyStore) throws Exception;

    void unLoadPkcsProvider();
}
```

```java
package org.acme.smartcard;

import javax.crypto.Cipher;
import java.security.PrivateKey;
import java.security.cert.X509Certificate;

/**
 * Public API for encrypting and decrypting of various data formats.
 *
 * @author Miskovic
 */
public interface CryptoService {

    /**
     * @param privateKey     - Private key that is used when decrypting data.
     * @param transformation - {@link Cipher} transformation (e.g. RSA/ECB/PKCS1Padding)
     * @param base64Data     - The base64 encoded data that will be decrypted.
     * @return - Decrypted byte array
     * @throws Exception
     */
    byte[] decryptData(PrivateKey privateKey, String transformation, byte[] base64Data) throws Exception;

    /**
     * @param cert           - Public certificate that is used for encrypting the data.
     * @param transformation - {@link Cipher} transformation (e.g. RSA)
     * @param data           - Raw data that will be encrypted.
     * @return - Encrypted and base64 encoded byte array.
     * @throws Exception
     */
    byte[] encryptData(X509Certificate cert, String transformation, byte[] data) throws Exception;

}
```