



**УНИВЕРЗИТЕТ СИНГИДУНУМ**  
**ДЕПАРТМАН ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ**  
**-СТУДИЈСКИ ПРОГРАМ-**  
**САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ**

# **Протоколи за установљавање кључа**

**- Мастер рад -**

Ментор:  
Проф. др Младен Веиновић

Студент:  
Немања Менковић  
Бр. индекса:  
410562/2013



Београд, 2014.

## Протоколи за установљавање кључа

**Сажетак:** У раду су приказани протоколи за установљавање кључа, и дистрибуцију кључева, који су засновани на симетричном и асиметричном шифровању. Описани су Needham-Schroder, Керберос и Otway-Rees протоколи, који су засновани на симетричном шифровању, као и Diffie-Hellman, RSA алгоритам и инфраструктура са јавним кључевима, који су базирани на асиметричном шифровању. Упоредјене су обе врсте шифарских система са становишта поверљивости, аутентикације и дужине кључева. У раду је приказан и информационо теоретски протокол за дистрибуцију тајних кључева, који је базиран на сателитском сценарију. Две стране у комуникацији повезане су комуникационим јавним каналом, коме прислушкивач има потпуни приступ. Циљ је успостава тајног низа, односно заједничког симетричног кључа, који познат искључиво странама у комуникацији. У раду је разматран Мауреров протокол, по коме учесници у комуникацији могу да генеришу тајни кључ, упркос чињеници да прислушкивач поседује више информација од легитимних учесника, има неограничене рачунарске ресурсе и комплетно знање о протоколу. Описане су три фазе протокола: дестилација предности, усаглашавање информација и појачавање приватности. Развијен је симулатор протокола за дистрибуцију тајних кључева. У фази дестилације предности, имплементирани су репетитивни протокол, итеративни протокол и *bit-pair* итеративни протокол. За другу фазу коришћен је каскадни протокол, а у трећој фази примењена је универзална класа *hash* функције  $H_1$

**Кључне речи:** установљавање кључева, протокол, комуникациони канал, шифровање

## Key Establishment Protocols

**Abstract:** This paper presents Key Establishment Protocols based on symmetric and asymmetric encryption. The Needham-Schroder, Kerberos and Otway-Rees protocols, which are based on symmetric encryption, are also presented, as well as Diffie-Hellman, RSA algorithm and PKI, which are based on asymmetric encryption. Both encryption systems are compared according to the aspects of confidentiality, authentication, and key rate. This paper also presents information-theoretical approach and the protocol for secret key distribution, which are based on satellite scenario. Two parts in communication are connected through the communication channel, where eavesdropper has a perfect access. The goal is to make a shared string, e.g. symmetric secret key, known to communication parties exclusively. This paper presents Maurer's protocol, according to the communication parties can generate secret key, despite the fact that eavesdropper has much more information than legitimate users, as well as unlimited computational resources and complete knowledge about protocol. Three phases of protocol are presented: advantage distillation, information reconciliation and privacy amplification. A simulator of protocol for secret key generation is developed. In the advantage distillation phase, the repetition code, iteration and bit-pair iteration protocols are implemented. Second phase presents the Cascade protocol, while third phase shows appliance of universal hash function  $H_1$ .

**Keywords:** key establishment, protocol, communication channel, ciphering

## САДРЖАЈ

|                                                                                    |           |
|------------------------------------------------------------------------------------|-----------|
| <b>1. Увод .....</b>                                                               | <b>3</b>  |
| <b>2. Методологија научног истраживања .....</b>                                   | <b>5</b>  |
| 2.1 Предмет истраживања .....                                                      | 5         |
| 2.2 Циљеви истраживања.....                                                        | 5         |
| 2.3 Истраживачке хипотезе.....                                                     | 5         |
| 2.4 Методи истраживања и ток истраживачког процеса .....                           | 5         |
| <b>3. Општа класификација и основни појмови .....</b>                              | <b>7</b>  |
| 3.1 Трећа страна од поверења.....                                                  | 8         |
| 3.2 Аутентикација ентитета, аутентикација кључа и потврда кључа.....               | 8         |
| 3.3 Циљеви и особине протокола.....                                                | 9         |
| 3.4 Разлози за коришћење сесијских кључева .....                                   | 9         |
| 3.5 Тип сигурности и разлике у карактеристикама протокола .....                    | 10        |
| 3.6 Основне претпоставке и противници у протоколима за установљавање кључева ..... | 11        |
| 3.6.1 Противници у протоколима за установљавање кључа.....                         | 11        |
| <b>4. Дистрибуција кључева заснована на симетричном шифровању .....</b>            | <b>13</b> |
| 4.1 Центар за дистрибуцију криптолошких кључева.....                               | 13        |
| 4.2 Протокол за дистрибуцију кључева Needham-Schroder.....                         | 15        |
| 4.3 Керберос протокол за проверу индентитета .....                                 | 17        |
| 4.4 Основна верзија Керберос протокола.....                                        | 18        |
| 4.5 Безбедност Керберос протокола .....                                            | 19        |
| 4.6 Otway-Rees протокол.....                                                       | 20        |
| <b>5. Дистрибуција кључева заснована на асиметричном шифровању .....</b>           | <b>22</b> |
| 5.1 Асиметрични криптографски алгоритми .....                                      | 22        |
| 5.2 Системи са јавним кључевима .....                                              | 22        |
| 5.2.1 Примена система са јавним кључем .....                                       | 26        |

|           |                                                                                                        |           |
|-----------|--------------------------------------------------------------------------------------------------------|-----------|
| 5.2.2     | Захтеви за системе са јавним кључем.....                                                               | 27        |
| 5.3       | Diffie-Hellman протокол.....                                                                           | 28        |
| 5.3.1     | Пример Diffie-Hellman-овог протокола за размену кључева.....                                           | 29        |
| 5.3.2     | Примена Diffie-Hellman-овог протокола.....                                                             | 30        |
| 5.3.3     | Напад на Diffie-Hellman-ов протокол.....                                                               | 30        |
| 5.4       | RSA алгоритам.....                                                                                     | 31        |
| 5.5       | Инфраструктура са јавним кључевима.....                                                                | 33        |
| 5.5.1     | Основне функције и компоненте.....                                                                     | 33        |
|           | Пријављивање крајних корисника .....                                                                   | 33        |
|           | Дигитални сертификат .....                                                                             | 34        |
| 5.5.2     | Формат дигиталног сертификата у систему јавних кључева према<br>стандарду X.509.....                   | 35        |
| 5.6       | Поређење шифарских система са симетричним и асиметричним<br>кључем .....                               | 36        |
| <b>6.</b> | <b>Информационо теоријски приступ криптографији .....</b>                                              | <b>38</b> |
| 6.1       | Информационо теоретски договор тајног кључа .....                                                      | 38        |
| 6.2       | Мауреров протокол (сателитски сценарио).....                                                           | 41        |
| 6.3       | Представљање .....                                                                                     | 42        |
| 6.4       | Протокол дестилација предности .....                                                                   | 43        |
| 6.4.1     | Протокол понављања .....                                                                               | 43        |
| 6.4.2     | Итеративни протокол .....                                                                              | 45        |
| 6.4.3     | Bit pair итеративни протокол.....                                                                      | 47        |
| 6.5       | Каскадни протокол усаглашавања информација.....                                                        | 48        |
| 6.6       | Појачавање приватности.....                                                                            | 50        |
| <b>7.</b> | <b>Симулатор.....</b>                                                                                  | <b>53</b> |
| <b>8.</b> | <b>Закључак .....</b>                                                                                  | <b>59</b> |
|           | <b>Прилог 1: Протоколи за дистрибуцију тајних кључева преко јавних<br/>комуникационих канала .....</b> | <b>61</b> |
|           | <b>Литература.....</b>                                                                                 | <b>64</b> |
|           | <b>Списак слика .....</b>                                                                              | <b>67</b> |
|           | <b>Списак табела.....</b>                                                                              | <b>67</b> |

## 1. Увод

Данашња рачуарска мрежа распрострањена је широм света и користе је милиони корисника помоћу различитих терминала. Због тога област заштите информација које се преносе крој једну такву мрежу добија све више на значају. Захтев за обезбеђивање адекватне заштите информација је уско повезан са једним од главних сервиса криптографије, а то је поверљивост (*confidentiality*, енгл.), која подразумева пренос тајне информације од пошиљаоца (Алисе) до примаоца (Боба) преко несигурног комуникационог канала. Циљ сервиса је да обезбеди да неауторизована страна не дође до поверљивих информација и дефинише до које мере нека информације треба да буде доступна, односно недоступна неовлашћеним корисницима [1][2][3].

Да би смо обезбедили поверљивост, модерна криптографија захтева да пошиљаоц и примаоц унапред размене криптографски кључ. У зависности од природе кључева, криптографију делимо у две класе: криптографија са тајним кључевима (симетрична) и криптографија са јавним кључевима (асиметрична). У првом случају, Алиса и Боб морају да размене кључ који је само њима познат. Главни недостатак оваквог система је како и на који начин дистрибуирати тајни кључ између две легитимне стране на безбедан начин. За разлику од симетричне, у криптографији са јавним кључевима, сваки корисник има два кључа - јавни и тајни. Оваква врста протокола не захтева тајност приликом дистрибуције јавних кључева, али захтева трећу страну од поверења која гарантује да јавни кључеви припадају легитимним учесницима. Основна идеја криптографије са јавним кључевима је да користе одређене математичке функције чија је инверзна функција тешка за израчунавање. На пример, безбедност светски опште познатог RSA шифарског система је заснована на математички сложенем поступку факторизације (растављања) производа два велика проста броја на његове просте чиниоце (факторе). Велики број других шифарских система са јавним кључевима засновани су на сличној претпоставци. Главни недостатак асиметричних система је непостојање чврстог математичког доказа да ли је растављање на факторе једини начин за разбијање RSA [2][3]. Са развојем науке и технологије, рачуарска снага се знатно повећала. Штавише, квантни и ДНК (дезоксирибонуклеинска киселина) рачунари са неограниченом рачунском снагом и способношћу паралелног израчунавања имају могућност за разбијање одређених шифарских система. Алгоритми као што су RSA и DES (*Data Encryption Standard*, енгл.) могу бити разбијени уз помоћ квантног рачунара са одређеним квантним алгоритмом [4][5][6]. Квантни рачунари ће у скорој будућности, ући у наше свакодневне животе. Још већу претњу за шифарске системе представља и све већи развој нових метода и алгоритама напада. На основу досадашњег искуства у области класичне али и модерне криптографије може се закључити да су у већини случајева успешно разбијених шифара коришћене неочекиване методе напада а системи би били разбијени пре него што се то иницијално очекивало. Теорија о доказивој сигурности је развијана и дефинисана, али се у већини случајева заснива на хипотезама и ограниченој рачунарској моћи. За израчунаљиво безбедне шифарске алгоритме који су се у самом почетку показали као доказиво сигурни, постоји могућност да су били рањиви. На пример, када се појавио RSA алгоритам, сматрало се да је граница довољно великог броја чију је факторизацију тешко извршити доста мања (иницијално 129 цифара) него што се касније открило (данас се успешно врши

факторизација броја од 193 цифре). Водећи шифарски стандард AES (*Advanced Encryption Standard*, енгл.) [7] је такође показао да је рањив на алгебарске нападе [8]. Према томе, безусловна сигурност шифарских система ће постајати све значајнија. Али већина садашњих истраживања фокусирана су на израчунљиву безбедност шифарских система. Истраживање безусловне сигурности јесте ограничено на неколико области[9].

## 2. Методологија научног истраживања

### 2.1 Предмет истраживања

Предмет истраживања овог пројектног задатка су протоколи за установљивање кључа. Историја криптологије открива нека решења на овом плану, која су везана за одређене етапе развоја криптологије. С обзиром на ограничену употребу и једноставност шифарских система, који су углавном били намењени за заштиту писаних информација, проблеми везани за генерисање и дистрибуцију кључева били су мање изражени него данас. Брже измене у системима преноса информација, битно су утицале и на измене у системима за шифровање. Заштита тајности информација данас није само привилегија класичних корисника, војске, полиције и других државних структура. Потребе за њом се јављају и у пословној и другим цивилним сферама. Једном речју, свет улази у еру масовне криптозаштите, која мора бити компатибилна са савременим системима електронског комуницирања. Потреба за кључевима енорно расте, што захтева све већу брзину генерисања и отвара проблеме у вези са њиховом доставом, све већем броју и све удаљенијим корисницима.

### 2.2 Циљеви истраживања

У овом раду разматрамо договор тајног кључа (*seacret key agreement*, енгл.) који је заснован на информационо теоријској сигурности. Договор тајног кључа је један од најбитнијих фактора у криптологији и има задатак да реши проблем генерисања кључева и њихове дистрибуције између корисника. Реализација неког шифарског система је практично неостварљива без обезбеђења одговарајућих кључева. Кључеви морају бити произведени и достављени, не једанпут, већ константно. Према томе, обезбеђење ефикасне дистрибуције кључева корисницима је поред тајности, један од најважнијих задатака у изградњи криптолошких комуникационих система.

### 2.3 Истраживачке хипотезе

Проблем дистрибуције тајних кључева је стално присутан у историји криптографије. Без обзира колико је у теорији криптографски алгоритам сигуран, поверљивост његовог механизма може угрозити проблем дистрибуције кључа. Питање дистрибуције кључа може се чинити тривијалним, међутим у криптографском систему то је најслабија карика. Учесници у криптографским системима морају бити способни да генеришу кључеве, односно кључеви морају бити доступни корисницима у комуникацији. Сигурносна метода управљања кључевима је од великог значаја за целокупан безбедносни систем.

### 2.4 Методи истраживања и ток истраживачког процеса

Методологија истраживања заснивала се првенствено на проучавање литературе, која углавном потиче са Интернета али такође и књига из области

заштите информација. У литератури али и на интернету много је мање информација које се баве проблематиком из области дистрибуције тајних кључева преко јавних канала. Због овакве чињенице само истраживање је било доста теже и комплексније. Свака од информација која се налазе у овом раду проверена је на више места у литератури да би де доказало да је релевантна. Циљ овог рада је да помогне свим стручњацима који се баве заштитом информација да добију јаснију слику у овој области као и да им се укаже где могу да пронађу додатне информације које су им потребне.

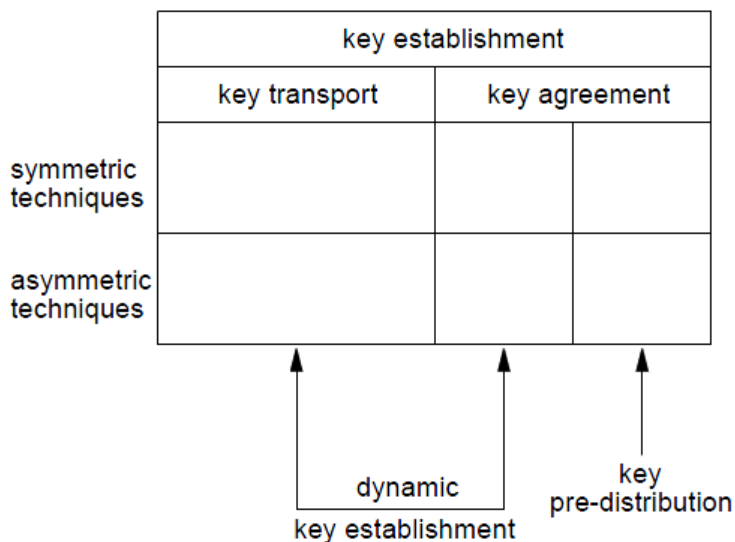
### 3. Општа класификација и основни појмови

Установљивање кључа (*key establishment*, енгл.) је процес или протокол у коме две или више стране у комуникацију могу да одреде заједнички тајни кључ, који се користи за безбедну комуникацију међу учесницима. Установљивање кључа може се поделити у две категорије (Слика 1.):

- Дистрибуција кључа (*key transport*, енгл.) - једна страна креира кључ, и сигурним путем дистрибуира кључ другој страни.
- Договор тајног кључа (*key agreement*, енгл.) - је процедура у којој две или више страна у комуникацију учествују у креирању заједничког тајног кључа.

Шеме за *Key pre-distribution*<sup>1</sup> су протоколи за установљивање кључева при чему су ново оформљени кључеви потпуно одређени априорно, почетним материјалом за кључеве. Супротно од *Key pre-distribution* шема, су шеме за динамично установљивање кључева (*Dynamic key establishment*, енгл.), при чему се кључеви формирају као фиксни пар (или група) корисника, који се разликују у зависности од извршења.

*Dynamic key establishment* се такође назива *Session key establishment* (протокол за установљивање сесијских кључева). У овом случају сесијски кључеви су динамични, па су ти протоколи имуни на познате нападе на кључеве [10].



Слика 1 Општа класификација техника за установљивање кључа

<sup>1</sup> Key pre-distribution (engl.) – размена ново-установљених кључева (a priori), прим.аут.

### 3.1 Трећа страна од поверења

Много протокола за установљивање кључева подразумевају централизацију одн. страну од поверења, у почетном подешавању система. Страна од поверења, у зависности коју улогу игра, има различите називе: трећа страна од поверења (*Trusted third party*, енгл.), сервер од поверења (*Trusted server*, енгл.), сервер за аутентикацију (*Authentication server*, енгл.), центар за дистрибуцију кључева (*Key Distribution Center* (KDC), енгл.), центар за превођење кључева (*Key Translation, Center* (KTC), енгл.) и сертификационо тело (*Certification Authority* (CA), енгл.) [10].

### 3.2 Аутентикација ентитета, аутентикација кључа и потврда кључа

У основи је пожељно да обе стране, у протоколу за установљивање кључа, могу да утврде њихове праве идентитете, одн. који могу да доведу и до приступа резултујућем кључу, спречавајући трећу неовлашћену страну да утврди исти кључ. За ову технику се неформално тврди да пружа сигурно установљивање кључа (*secure key establishment*, енгл.). Ово захтева обострану тајност кључа, и идентификацију страна које имају приступ кључу. Такође, разлике у идентификацији су незнатне, али веома битне, тако да је за аутентикацију ентитета потребно знање о идентитету страна које могу да приступе кључу.

Аутентикацију је могуће дефинисати као процес верификације идентитета ентитета за ког се представља, али постоји пуно аспеката који морају да се узму у обзир, што укључује потврду следећег: *који, какав, када*.

Аутентикација кључа (*key authentication*, енгл.) је процес када се једна страна уверава да ниједна страна осим ње и договорене стране (и могуће и треће сигурно идентификоване стране) имају приступ одређеном тајном кључу.

Аутентикација кључа је независна од тога да ли друга страна поседује тај кључ и да ли прва страна зна за то, никаква акција друге стране није потребна. Из ових разлога, понекад се назива и безусловна (*implicit*, енгл.) аутентикација кључа.

Потврда кључа (*key confirmation*, енгл.) настаје када је једна страна уверена да друга (могуће и не идентификована) има одређени тајни кључ.

Експлицитна аутентикација кључа (*explicit key authentication*, енгл.) настаје када се изврше и аутентикација и потврда кључа.

У случају експлицитне аутентикације, идентификована страна заиста поседује одређени кључ. Апликације за шифровање, које користе протоколе за установљивање кључа и које нуде само имплицитну аутентикацију, кључа почињу шифровање са основним подацима који служе као провера интегритета, тиме померајући терет потврде кључа са механизма установљивања на апликацију.

При аутентикацији кључа, фокус је на идентитету друге стране, а не на вредност кључа, док је код потврде кључа супротно. Потврда кључа углавном подразумева једну страну која добија поруку од друге, поруку која садржи доказ да друга страна има кључ. У пракси, поседовање кључа може бити остварено на различите начине, укључујући и једносмерне хеш (*hash*, енгл.) функције самог кључа, користећи кључ за добијање *hash* вредности, и шифровањем одређеног дела користећи кључ. Ове технике могу да открију део информација о вредности самог кључа. С друге стране, методе које користе технике нултог знања (*zero-knowledge*,

енгл.) дозвољавају демонстрацију поседовања кључа а да при том нису откривене додатне информације о својој вредности.

Аутентикација ентитета није обавезна у свим протоколима. Неки протоколи за установљивање кључа (нпр. као *Diffie-Hellman*-ов протокол за договор тајног кључа, без аутентикације) не пружају аутентикацију ентитета, кључа и потврду кључа. Једнострану потврду кључа је могуће додати, користећи једносмерне хеш функције на добијени (изведени) кључ у финалној поруци.

Протокол за установљивање аутентикационог кључа (*authenticated key establishment*, енгл.) је протокол за установљивање кључа који обезбеђује аутентикацију кључа.

Комбиновање протокола за аутентикацију ентитета и установљивање кључа. У протоколу за установљивање кључа, који подразумева аутентикацију ентитета, важно је да протокол буде изграђен на начин како би гарантовао да је страна чији се идентитет потврђује иста она која је установила кључ. Уколико то није тако, противник може да добије помоћ од ауторизоване стране која тога није свесна, на тај начин да спроведе аспект аутентикације, и тиме изврши лажно представљање приликом установљивања кључа у даљој комуникацији[10].

### 3.3 Циљеви и особине протокола

Криптографски протоколи, који укључују размену порука, захтевају прецизну дефиницију порука које се размењују и акција које свака страна треба да предузме. У зависности од циљева могуће је разликовати следеће типове протокола:

1. Аутентикациони протокол (*authentication protocol*, енгл.) – обезбеђује једној страни одређени ниво сигурности о идентитету друге стране у комуникацији.
2. Протокол за установљивање кључа (*key establishment protocol*, енгл.) – установљивање заједничке тајне, односно кључа.
3. Протокол за установљивање аутентикационог кључа (*authenticated key establishment protocol*, енгл.) – за установљивање заједничког тајног кључа са страном чији је идентитет могуће потврдити [10].

### 3.4 Разлози за коришћење сесијских кључева

Резултат коришћења протокола за установљивање кључа је заједнички тајни кључ, или се они користе за добијање сесијских кључева. Идеално, сесијски кључ је једнократни, односно његово коришћење је ограничено на кратак период код нпр. успоставе једнократне телекомуникационе везе (сесија). Разлози за коришћење једнократних кључева су следећи:

1. Ограничити могући напад на доступни шифрат.
2. Ограничити излагање, уз поштовање временског размака и количине података, у случају компромитације.
3. Избећи дугорочно складиштење појединих тајних кључева, у случају где један терминал комуницира са више других терминала, креирајући кључеве само кад су потребни.

4. Постићи независност током трајања комуникационих сесија или апликација [10].

### 3.5 Тип сигурности и разлике у карактеристикама протокола

Приликом дизајнирања или одабира начина на који се успоставља кључ, важно је узети у обзир карактеристике и гаранције које апликација захтева. Треба направити разлику између функционалности која је пружена кориснику и техничких карактеристика по којима се разликују механизми имплементације. Карактеристике по којима се технике за установљивање кључа разликују:

1. Природа аутентикације. Нека од следећих комбинација може бити пружена: аутентикација ентитета, аутентикација кључа, потврда кључа.
2. Реципроцитет аутентикације. Свака од горе наведених аутентикација и потврда кључа може бити једнострана и заједничка, подједнако.
3. „Свежина“ кључа (*key freshness*, енгл.). Кључ је „свеж“ (из перспективе једне стране) ако се може гарантовати да је нов, за разлику од старијег кључа којег могу да користе ауторизоване стране или противник. Ово је у вези са контролом кључа (*key control*, енгл.).
4. Контрола кључа. У неким протоколима, једна страна бира вредност кључа, док у је другим протоколима кључ изведен из заједничке информације (*key agreement*, енгл.) и можда је пожељно да ниједна страна нема контролу и не може да предвиди вредност кључа.
5. Ефикасност протокола укључује:
  - 1) Број размењених порука између страна.
  - 2) Пропусни опсег који је потребан за размену порука (укупан број битова који се преноси).
  - 3) Сложеност израчунавања сваке стране (која утиче на дужину трајања размене).
  - 4) Могућност ранијег израчунавања да би се смањила комплексност израчунавања на мрежи.
6. Захтеви треће стране:
  - 1) Потреба на мрежи у реалном времену, ван мреже или без треће стране.
  - 2) Ниво поверења у трећу страну (нпр. поверење у сертификат јавних кључева).
7. Врсте сертификата који су коришћени, ако постоје. Уопштено, може се размотрити начин на који је материјал за кључ дистрибуиран, који могу бити повезани са захтевом треће стране, што често није повезано са корисником, обзиром да овај детаљ имплементације нема никакву другу функцију.
8. Непорецивост. Протокол може да обезбеди потврду да је материјал за кључ размењен.

Ефикасност насупрот сигурности, и ефикасност и сигурност као

криптографске технике, су често повезане. На пример, у неким протоколима основни корак се понавља, а сигурност се повећава са бројем понављања. У том случају, ниво сигурности који може да се постигне у одређено време зависи од ефикасности тог, основног корака.

У опису порука протокола, претпоставља се да када идентитет извора или изворне мреже неке поруке није експлицитно укључен у поруку, он се препознаје у контексту или је на други начин познат примаоцу, што је могуће извести у додатним пољима чистог текста [10].

### 3.6 Основне претпоставке и противници у протоколима за установљивање кључева

Да би разјаснили претње којима протоколи могу бити изложени, и да би постојао мотив за коришћење специфичних карактеристика протокола, потребни су општи модел протокола за установљивање кључа и разумевање претпоставки које су везане за тај протокол. Иако се дефиниције и модели могу генерализовати, у тексту је детаљније разматран протокол између две стране (*two-party*, енгл.).

#### 3.6.1 Противници у протоколима за установљивање кључа

Ентитети или стране које комуницирају у протоколу за установљивање кључа имају формални назив “*principals*“ (енгл.), требало би да имају јединствена имена. Претпоставља се да, уз легитимне стране, постоје неауторизоване трећа страна, која може да има много назива, у зависности од околности, као што су: противник (*adversary*, енгл.), улез (*intruder*, енгл.), непријатељ (*enemy*, енгл.), нападач (*attacker*, енгл.), прислушкивач (*eavesdropper*, енгл.) и имитатор (*impersonator*, енгл.).

Код испитивања сигурности протокола, претпоставља се да су криптографски механизми (као што су нпр. алгоритми за шифровање и шеме за дигиталне потписе) безбедни. У супротном, протокол није безбедан. Хипотетички, противник није криптоаналитичар који напада механизме шифровања, већ особа која директно покушава да омета циљ самог протокола, с циљем да порази начин на који су механизми спојени, тј. директно нападајући протокол [1].

Веома популарна и често коришћена класификација безбедносних напада, која је дефинисана стандардима X.800 и у RFC 2828, је она која нападе дели на:

- пасивне нападе, и
- активне нападе.

Пасивни напади уче о систему или користе информације које се преносе системом, али при томе не користе његове ресурсе. Са друге стране, активни напади мењају системске ресурсе (укључујући и информације које се преносе системом) или операције самог система.

Пасивни напади су прислушкивање тј. надгледање преносних канала. Циљ противника је да открије садржај порука које се преносе преко комуникационог канала. Постоје два типа пасивних напада:

1. откривање информационог садржаја поруке, и
2. анализа саобраћаја.

Активни напади су узрок модификације протока података као и креирања њихових лажних протока. Деле се у следеће категорије:

1. лажно представљање,
2. понављање слања послатих порука,
3. генерисање лажних или модификација легалних порука, и
4. неауторизовано коришћење рачунарских ресурса (укидање сервиса) [10].

#### 4. Дистрибуција кључева заснована на симетричном шифровању

Групу симетричних криптографских алгоритама представљају алгоритми код којих је кључ за шифровање идентичан кључу за дешифровање. Алгоритми из ове групе се такође називају и алгоритми са тајним кључем јер је тајност кључа који се користи и за шифровање и за дешифровање основа безбедности порука у систему. Ови системи представљају основу традиционалне криптолошке теорије и развијају се дуги низ година. Обзиром да заштита информација основну примену има у пословима везаним за државне структуре (војска, полиција, дипломатија), ови системи су били искључиво тајни системи, наменски дефинисани и реализовале су их надлежне државне институције [11].

У овом поглављу су описани протоколи за установљивање кључа, који су засновани на дистрибуцији кључа (*key transport*, енгл.) (нпр. пренос тајног кључа који је унапред изабрала једна страна) користећи симетрично шифровање. Описани протоколи укључују трећу страну од поверења, што је приказано Табелом 1. Такође, поједини протоколи користе неке од временских параметара, као што су: (временски печат (*timestamps*, енгл.), секвенца бројева (*sequence numbers*, енгл.) или случајно генерисане бројеве (*random numbers*, енгл.) ). Протоколи за дистрибуцију кључа који су засновани на симетричном шифровању, укључују две стране у комуникацији, *A* и *B*, и трећу страну од поверења са којом априорно деле по пар тајних кључева. Трећа страна од поверења има улогу центра за дистрибуцију кључева (*key distribution center*, KDC, енгл) за снабдевање сесијских кључева или као сервис за преношење кључева (*key translation center*, KTC, енгл.) који обезбеђује да изабрани кључ једне стране буде доступан другој страни [10].

Табела 1 Дистрибуција кључева заснована на симетричном шифровању

| Карактеристике:<br>Протоколи: | Тип сервера | Временски печат<br>( <i>timestamps</i> ) | Број порука |
|-------------------------------|-------------|------------------------------------------|-------------|
| <i>Needham-Schroeder</i>      | KDC         | не                                       | 5           |
| Керберос                      | KDC         | да                                       | 4           |
| <i>Otway-Rees</i>             | KDC         | не                                       | 4           |

##### 4.1 Центар за дистрибуцију криптолошких кључева

Уколико много људи, процеса или система има потребу за међусобну безбедну комуникацију, њихов број чини групу која није статична, односно поједини ентитети се могу придружити или напустити групу у било ком тренутку.

Једноставно решење за овај проблем је да свака страна физичким путем размени кључ за шифровање. Сходно томе, било које две стране могу да успоставе безбедну комуникацију користећи кључ за шифровање који су унапред разменили. Очигледно, овај приступ није практичан за већу групу људи, процеса и система поготово када се чланови често мењају.

Боља решење је да сваки члан групе обезбеди кључ за безбедну комуникацију са центром за дистрибуцију кључева, одн. *мастер* кључ. Када особа  $A$  хоће да успостави сигурну комуникацију са особом  $B$ , онда  $A$  шаље захтев центру за дистрибуцију кључева за сесијски кључ.

Процедура KDC протокола је следећа:

- Особа  $A$  шаље поруку KDC -у са захтевом за комуникацијом са особом  $B$ , а у циљу креирања заједничког кључа сесије  $K_{AB}$ . Порука садржи податке о идентитету особе  $A$  и идентитету особе  $B$ . Треба напоменути да ова порука није шифрована.
- KDC прима поруку и креира такозвани тикет намењен особи  $B$ . Пошто KDC зна тајни кључ особе  $B$ , користи га како би шифровао поменути тикет. Тикет садржи идентитете особа  $A$  и  $B$  и заједнички кључ  $K_{AB}$ . Овако формиран тикет се упакује заједно са заједничким кључем за једну сесију  $K_{AB}$ , шифрује са кључем  $K_A$  и на крају пошаље особи  $A$ , као поруку. Након пријема поруке особа  $A$  је дешифрује, а затим отпакује заједнички кључ,  $K_{AB}$ . Пошто нема кључ  $K_B$  не може да отпакује тикет намењен особи  $B$ .
- У оквиру овог корака особа  $A$  прослеђује тикет намењен особи  $B$ . Особа  $B$  пошто прими тикет, отпакује га и памти кључ  $K_{AB}$  који јој је неопходан ради размене порука са особом  $A$ .
- Поруке протокола:

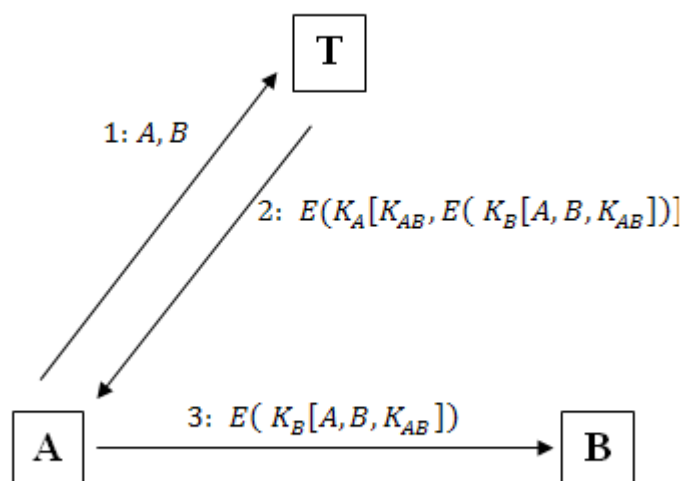
$$A \rightarrow T: A, B \quad (1)$$

$$A \leftarrow T: E(K_A[K_{AB}, E(K_B[A, B, K_{AB}])]) \quad (2)$$

$$A \rightarrow B: E(K_B[A, B, K_{AB}]) \quad (3)$$

- Ову размену порука можемо графички представити Сликаом 2.

После трећег корака, особе  $A$  и  $B$  могу разменити податке коришћењем кључа  $K_{AB}$  као кључа за једнократну сесију. Поред наведеног стандардног начина размене кључева са KDC-ом постоје и други протоколи, тј. протоколи за размену кључева [12].



Слика 2 Графички приказ KDC протокола

## 4.2 Протокол за дистрибуцију кључева Needham-Schroder

Када особа  $A$  жели да успостави сигурну комуникацију са особом  $B$ , потребно је да обе стране поседују мастер кључеве  $K_A$  и  $K_B$  за комуникацију са KDC. Процедура је следећа :

- Страна  $A$  користи кључ  $K_A$  како би послала захтев KDC-у за сесијски кључ у намери да започне комуникацију са страном  $B$ .
- Порука послата од стране  $A$  према KDC-у, укључује и мрежну адресу ( $ID_A$ ), стране  $B$  као и јединствени сесијски идентификатор (*unique session identifier*, енгл.). Сесијски идентификатор (познат као *nonce*, енгл. број за једнократну употребу) означава се као  $N_1$ . Примарни услов за *nonce* је да мора бити случајно генерисани број и мора бити јединствен за сваки нови захтев послат од  $A$  према KDC-у. Порука послата од  $A$  према KDC, може се представити као:

$$E(K_A, [ID_A, ID_B, N_1]).$$

- KDC одговара страни  $A$  шифрованом поруком користећи кључ  $K_A$ .

Компоненте поруке су:

- Сесијски кључ  $K_S$  за комуникацију између страна  $A$  и  $B$ .
- Оригинална порука примљена од стране  $A$ , укључујући и *nonce* који је коришћен за дату поруку. И он омогућује страни  $A$  да упореди примљену поруку од KDC са послатим захтевом. Након тога страна  $A$  може да успостави више једновремених сесија са страном  $B$ .
- Пакет информација послатих од стране  $A$  према страни  $B$ . Овај пакет информација је шифрован користећи мастер кључ стране  $B$ ,

$K_B$  који укључује поново кључ сесије  $K_S$  и идентификатор  $ID_A$  (страна  $A$  нема приступ пакету јер не познаје кључ  $K_B$ ).

- Поруку коју је KDC послао страни  $A$  можемо представити као:

$$E(K_A, [K_S, ID_A, ID_B, N_1, E(K_B, [K_S, ID_A])]).$$

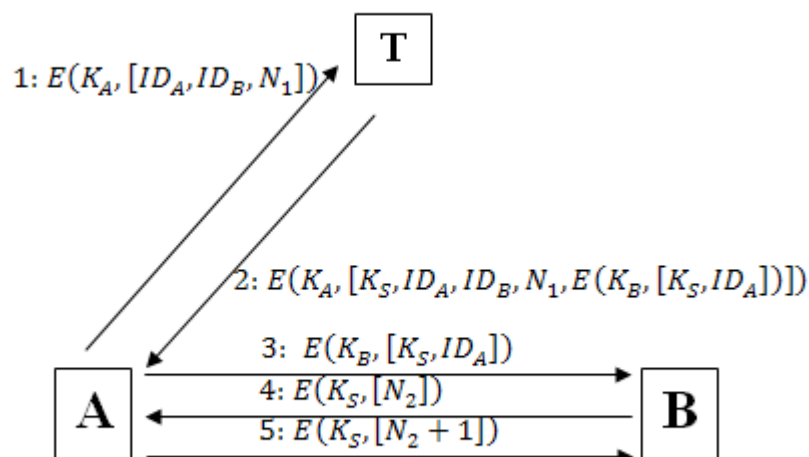
- Користећи свој мастер кључ  $K_A$ , страна  $A$  дешифрује примљене поруке од KDC. Само страна  $A$  и KDC имају приступ мастер кључу  $K_A$ , тако да је страна  $A$  сигурна да је примљена порука послата од стране KDC.
- Страна  $A$  задржава сесијски кључ  $K_S$  и шаље пакет страни  $B$ . Ова порука се шаље отворено од стране  $A$ , али га претходно шифрује KDC, користећи мастер кључ (стране  $B$ )  $K_B$ . Одавде следи да је ово први контакт стране  $A$  и стране  $B$  који је заштићен од прислушкивача.
- Страна  $B$  дешифрује примљену поруку од стране  $A$  користећи свој мастер кључ  $K_B$ ,  $ID_A$  у дешифрованој поруци са идентификатором у примљеној поруци од стране  $A$ . Након упоређивања, страна  $B$  је сигуран да комуницира са страном  $A$ .
- Страна  $B$  сада поседује сесијски кључ за сигурну комуникацију са страном  $A$ .
- Користећи сесијски кључ  $K_S$ , страна  $B$  шаље страни  $A$  поруку  $N_2$ . Страна  $A$  одговара страни  $B$  са  $N_2 + 1$ , користећи исти сесијски кључ  $K_S$ . Ово служи као потврда да кључ важи за тренутну сесију, што захтева да се оно што страна  $A$  шифрује кључем  $K_S$  разликује од онога што страна  $B$  шифрује кључем  $K_S$ . Овај део договора такође обезбеђује да страна  $B$  зна да га није контактирала страна  $A$ , тако да  $A$  не жели да комуницира с њим. Додатна корист овог корака је да је обезбеђена заштита од напада понављањем. Порука послата од стране  $B$  према страни  $A$  може се представити изразом:

$$E(K_S, [N_2]),$$

Страна  $A$  одговара страни  $B$  поруком:

$$E(K_S, [N_2 + 1]).$$

- Ова размену порука графички је представљена Сликом 3. Најбитнији елемент ове размене порука је то што KDC шаље назад повратну информацију страни  $A$  за страну  $B$ , тако да искључиво страна  $B$  може да је разуме [12].

Слика 3 Графички приказ *Needham-Schroder* протокола

### 4.3 Керберос протокол за проверу идентитета

Керберос је протокол који трећем лице од поверења служи за проверу идентитет, који је пројектован за TCP/IP мреже. Сервис Керберос има улогу треће стране од поверења, која обезбеђује сигурну проверу идентитета у мрежи, омогућавајући једној особи да приступи различитим серверима у тој мрежи. Керберос је заснован на симетричној криптографији, и користи тајни кључ са сваким ентитетом у мрежи, а познавање тог тајног кључа једнако је доказу идентитета.

Керберос је развијен на институту MIT, у оквиру пројекта Атена. Модел Кербероса је заснован на *Needham-Schroderovom* протоколу треће стране од поверења [1].

Основни протокол Керберос подразумева: клијента *A*, сервера и верификатора *B*, и страну од поверења *T* (сервер за аутентикацију Керберос). На самом почетку протокола *A* и *B* не деле тајне податке, док *T* дели тајне податке са сваким (нпр. лозинка корисника, трансформисана у криптолошки кључ одговарајућом функцијом). Примарни циљ за *B* је да верификује идентитет *A*, а установљивање тајног кључа је бочни ефекат. Опционо, обухвата финалну поруку која обезбеђује заједничку аутентикацију учесника и установљивање додатног тајног параметра *A* и *B* (*subsession key*, енгл. под-сесијски кључ који није изабрала страна *T*).

Процедура протокола је следећа: *A* захтева од *T* одговарајуће гаранције (поједине податке) да изврши своју аутентикацију код *B*. *T* има улогу KDC-а, враћајући *A*, сесијски кључ шифрован за *A* и шифровани *ticket* за *B*. Тикет, који *A* прослеђује до *B*, садржи сесијски кључ и индентитет учесника *A*, што омогућава њену аутентикацију страни *B*, придруживањем одређене поруке (*authenticator*, енгл.) коју је креирала од страна *A* и која садржи временски печат шифрован одговарајућим сесијским кључем [10].

#### 4.4 Основна верзија Керберос протокола

Резиме:  $A$  у интерактивној комуникацији са сервером од поверења  $T$  и страном  $B$ .

Резултат: аутентикација  $A$  страни  $B$  (могућност међусобне аутентикације), са установљивањем кључа.

1. Систем обележавања. Подаци по избору су означени звездом (\*).  
 $E$  је симетрични алгоритам за шифровање.  
 $N_A$  је *nonce* изабран од стране  $A$ ,  $T_A$  је *timestamp* стране  $A$ .  
 $k$  је сесијски кључ изабран од  $T$ , за комуникацију  $A$  и  $B$ .  
 $L$  је период важења (*lifetime*, енгл).
2. Почетно подешавање:  $A$  и  $T$  деле кључ  $K_{AT}$ , такође  $B$  и  $T$  деле кључ  $K_{BT}$ .  
 Дефинишемо  $ticket_B = EK_{BT}(k, A, L)$  и  $authenticator = E_k(A, T_A, A_{subkey}^*)$ .
3. Поруке протокола:

$$A \rightarrow T: A, B, N_A \quad (1)$$

$$A \leftarrow T: ticket_B, EK_{AT}(k, N_A, L, B) \quad (2)$$

$$A \rightarrow B: ticket_B, authenticator \quad (3)$$

$$A \leftarrow B: E_k(T_A, B_{subkey}^*) \quad (4)$$

4. Процедура протокола. Алгоритам  $E$  има уграђени механизам за интегритет, и уколико није реализована провера интегритета, протокол не успева.
  - I.  $A$  генерише  $N_A$  и шаље серверу  $T$  (порука (1)).
  - II.  $T$  генерише нови сесијски кључ  $k$ , и дефинише период валидности  $L$  за *ticket*, који садржи почетак и крај валидности.  $T$  шифрује  $k$ , примљени *nonce*,  $L$ , и примљени идентификатор стране  $B$ , користећи кључ стране  $A$ .  $T$  такође креира безбедни *ticket* користећи кључ стране  $B$  који садржи  $k$ , примљени идентификатор  $A$  и  $L$ .  $T$  све то шаље страни  $A$  (порука(2)).
  - III.  $A$  дешифрује део поруке (2) али не и део који садржи *ticket*, користећи кључ  $K_{AT}$  да би добила:  $k$ ,  $N_A$ ,  $L$ , и идентификатор стране за који је *ticket* креиран.  $A$  изврши верификацију да се идентификатор и  $N_A$  подударају са идентификатором и  $N_A$  послатим у поруци (1), и сачува  $L$  као референцу.  $A$  узима свој идентификатор и нови *timestamp*  $T_A$ , по избору генерише тајни  $A_{subkey}$ , и све шифрује користећи кључ  $k$  како би формирала *authenticator*.  $A$  шаље  $B$  поруку (3).
  - IV.  $B$  за примљену поруку (3) дешифрује *ticket* користећи кључ  $K_{BT}$  да добије кључ  $k$  и с њим дешифрује *authenticator*, па проверава следеће:
    - 1) да ли се поље идентификатора  $A$  у *ticket*-у и *authenticator*

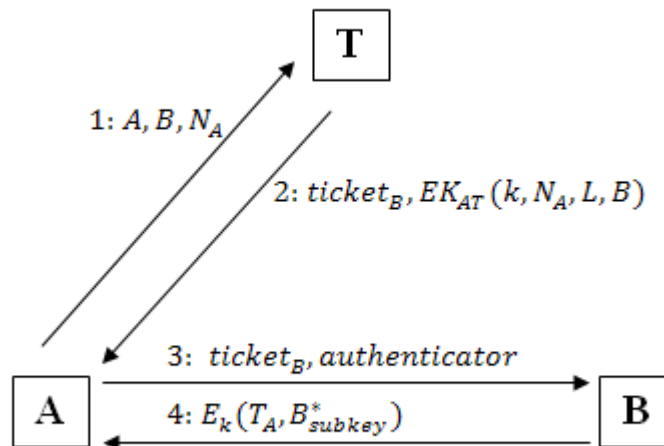
подударају,

- 2) да ли је *timestamp*  $T_A$  у *authenticator*-у валидан, и
- 3) да ли је локално време стране  $B$  у оквиру  $L$  спецификован у *ticket*-у.

Ако су сви кораци провере исправни,  $B$  декларише аутентикацију стране  $A$  успешном и сачува тражени  $A_{subkey}$ .

- V. (Опционо за обострану аутентикацију ентитета:)  $B$  саставља и шаље поруку (4) страни  $A$  која садржи *timestamp* стране  $A$  добијен из *authenticator*-а, шифровано кључем  $k$ ,  $B$  може опционо да укључи *subkey* да омогући договор око *subsession key*.
- VI. (Опционо за обострану аутентикацију ентитета:)  $A$  дешифрује поруку (4). Ако се *timestamp* поклапа са оним који је послат у поруци (3),  $A$  декларише аутентикацију стране  $B$  успешном и сачува тражени  $B_{subkey}$ .

Ову размену порука графички је представљена Сликаом 4 [10].



Слика 4 Графички приказ Керберос протокола

## 4.5 Безбедност Керберос протокола

Постоји могућност кеширања и понављања старих аутентификатора. Иако би временске ознаке требало да то спрече, понављања се могу извршити за време рока важења карте. Сервери треба да складиште све важеће карте како би се спречила понављања, што то није увек могуће. Осим тога, рок важења карте може да буде дугачак али, уобичајено, траје осам сати.

Аутентификатори се ослањају на чињеницу да су сви часовници у мрежи синхронизовани. Ако је могуће преварити сервер у погледу тачног времена, онда се стари аутентификатор може поновити. Већина мрежних временских протокола је несигурна, па ово може да буде озбиљан проблем.

Керберос је рањив и на напад погађањем лозинке. Нападач може да скупља карте и да затим покуша да их дешифрује. Треба имати на уму да просечан корисник обично не бира добре лозинке. Ако нападач прикупи довољно карата, постоји велика вероватноћа да открије лозинку.

Један од најозбиљнијих напада укључује злонамерне програме. Протокол Керберос се ослања на чињеницу да су програми поуздани, али ништа не може спречити нападача да кришом замени све клијентске Керберос програме верзијом која записује лозинке, поред тога што извршава протокол. Тај проблем постоји у сваком криптографском програмском пакету на недовољно заштићеном рачунару, али је Керберос, због тога што се масовно користи у овим окружењима посебно погодна мета.

Побољшања Кербероса односе се на реализацију криптографије са јавним кључевима и примену смарт-картице за управљање кључевима [1].

## 4.6 Otway-Rees протокол

*Otway-Rees* протокол ослања се на трећу страну од поверења, која обезбеђује аутентиковану дистрибуцију кључева у четири корака, односно четири поруке као и код протокола Керберос, с тим што не захтева временски печат.

Резиме:  $B$  је у интерактивној комуникацији са сервером од поверења  $T$  и страном  $A$ .

Резултат: установљивање новог заједничког тајног кључа  $K$  између  $A$  и  $B$ .

1. Систем обележавања.

$E$  је симетрични алгоритам за шифровање.

$k$  је сесијски кључ изабран од  $T$ , за комуникацију  $A$  и  $B$ .  $N_A$  и  $N_B$  су *nonces* изабрани од стране  $A$  и  $B$ , респективно, који омогућавају контролу валидности кључа.  $M$  је помоћни *nonce* изабран од стране  $A$  као сервисни идентификатор трансакције.

2. Почетно подешавање:  $T$  дели симетричне кључеве  $K_{AT}$  и  $K_{BT}$  са странама  $A$  и  $B$ , респективно.

3. Поруке протокола:

$$A \rightarrow B: M, A, B, E_{K_{AT}}(N_A, M, A, B) \quad (1)$$

$$B \rightarrow T: M, A, B, E_{K_{AT}}(N_A, M, A, B), E_{K_{BT}}(N_B, M, A, B) \quad (2)$$

$$B \leftarrow T: E_{K_{AT}}(N_A, k), E_{K_{BT}}(N_B, k) \quad (3)$$

$$A \leftarrow B: E_{K_{AT}}(N_A, k) \quad (4)$$

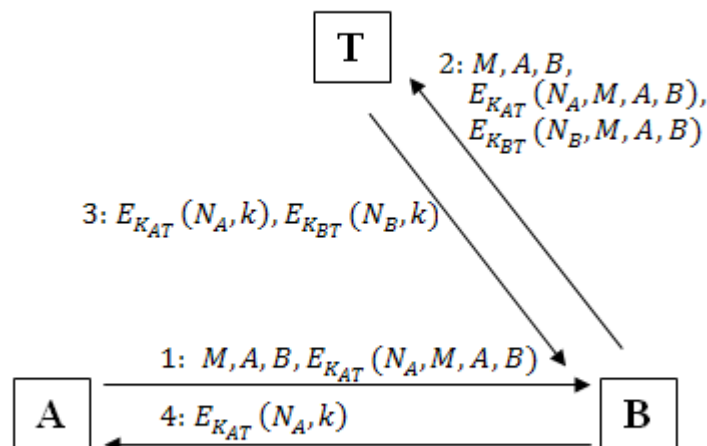
4. Рад протокола: Заједнички кључ захтева испуњење следећих корака.

- I.  $A$  шифрује податке за сервер који садржи два *nonces*  $N_A$  и  $M$ , свој идентитет и идентитет стране  $B$ , који захтева од сервера да им

дистрибуира кључ.  $A$  шаље шифрат заједно са отвореним текстом страни  $B$  у поруци (1).

- II.  $B$  креира свој *nonce*  $N_B$  и поруку која је слична шифрованој поруци која је примљена од стране  $A$ , и шаље је заједно са примљеном поруком од стране  $A$  серверу  $T$  у поруци (2).
- III.  $T$  упоређује идентификаторе ( $M, A, B$ ) из отвореног дела поруке (2) са идентификаторима из шифрованог дела поруке (2). Уколико је верификација успешна  $T$  креира поруке респективно, које садрже нови кључ  $k$  и *nonces* страна  $A$  и  $B$  шифроване кључевима  $K_{AT}$  и  $K_{BT}$  и обе поруке шаље страни  $B$ , порука (3).
- IV.  $B$  дешифрује део своје поруке, из поруке (3) и проверава  $N_B$  да ли се поклапа са оним који је послат у поруци (2) и, уколико је провера тачна, прослеђује први део поруке који је намењен страни  $A$ , порука (4).
- V.  $A$  дешифрује поруку (4) и проверава да ли се  $N_A$  поклапа са оним што је послато у поруци (1).

Ова размена порука графички је приказана Сликаом 5 [10].



Слика 5 Графички приказ Otway-Rees протокола

## 5. Дистрибуција кључева заснована на асиметричном шифровању

### 5.1 Асиметрични криптографски алгоритми

Асиметрични криптографски алгоритми су највећа достигнућа криптологије друге половине двадесетог века. Откривени су у процесу решавања два озбиљна проблема везана за примену симетричних криптографских алгоритама. Први проблем је заштита тајности и дистрибуција кључева у поступцима заштите података симетричним криптографским системима. Други проблем односи се на употребу симетричних криптографских алгоритама, односно на то како постићи потписивање дигиталне поруке. Питање је како обезбедити механизам који ће бити еквивалент потпису поруке на папиру, који мора да гарантује да у току преноса није промењен интегритет поруке, и да омогући механизам провере аутентичности пошиљаоца [11].

### 5.2 Системи са јавним кључевима

Године 1976. *Whitfield Diffie* и *Martin Hellman* са Стенфорд универзитета остварили су запањујући продор на пољу криптографије. Они су увели појам система са јавним кључевима, технологију која се драстично разликовала од свих поступака коришћених у последњих 400 година. Њихово откриће је решавало оба проблема везана за симетричне криптографске системе а, убрзо после открића, ови системи су добили назив асиметрични шифарски системи.

Наиме, у асиметричним шифарским системима се користе различити кључеви за шифровање и дешифровање, јавни и тајни кључ, тако да кључ за шифровање може бити познат свима, а само онај који поседује кључ за дешифровање може дешифровати поруку. Међутим, захтев за великим капацитетом рачунарских ресурса код ових алгоритама утиче на карактеристике система у којима се примењују, тако да се не препоручује њихова примена за заштиту тајности информација у системима са великим протоком информација. Ово правило не оспорава, по аутоматизму, ове алгоритме, јер начин на који је уз коришћење оваквих алгоритама могуће остварити функције интегритета, аутентичности и непорецивости има несумњиву предност над традиционалним техникама. У раду су описани алгоритмима са јавним кључевима али са становишта квалитета, отпорности на различите нападе, ефикасност и лакоћу имплементације, као и распрострањеност, нису сви подједнако добри. У том смислу се као изузетно робустан, већ више од двадесет година, намеће RSA (*Rivest, Shamir, Adleman*), јер одолева готово свим теоријским и технолошким нападима. Опис и начин употребе овог алгоритма прописани су у стандарду PKCS#1 верзија 2. Поред RSA у примени су и друга два алгоритма, DSA (*Digital Signature Algorithm*, енгл.) и ECDSA (*Elliptic Curve DSA*, енгл.), који припадају стандардима дигиталног потписа – NIST стандард DSS (*Digital Signature Standard*, енгл.).

Поменути алгоритми имају две веома важне карактеристике:

1. Рачунарски је готово немогуће одредити кључ за дешифровање уколико су познати само алгоритам и кључ за шифровање.
2. Оба кључа, и јавни и тајни, могу да се користе за шифровање односно дешифровање. Порука која је шифрована тајним кључем може се

дешифровати само његовим криптографским паром – јавним кључем, и обрнуто.

Системи са јавним кључевима састоје се од шест елемената:

- Отворени текст - порука коју је потребно шифровати
- Алгоритам шифровања - поступак трансформације отвореног текста у заштићени облик
- Јавни и тајни кључ - криптографски пар кључева који је одабран тако да се један користи за шифровање а други за дешифровање. Тачан начин трансформације је одређен примењеним алгоритмом и употребљеним кључем.
- Шифрат - резултат трансформације поруке отвореног текста
- Алгоритам дешифровања - овај алгоритам за улазне вредности добија шифрат и одговарајући кључ, и производи отворени текст.

У тексту који следи коришћен је следећи систем обележавања:

- $KUa$  - јавни кључ корисника  $A$ ,
- $KRa$  - тајни кључ корисника  $A$ ,
- $EKUa$  - поступак шифровања јавним кључем корисника  $A$ ,
- $EKR a$  - поступак шифровања тајним кључем корисника  $A$ ,
- $DKUa$  - поступак дешифровања јавним кључем корисника  $A$ ,
- $DKRa$  - поступак дешифровања тајним кључем корисника  $A$ .

При чему важе следеће релације:

$$DKRa(EKUa(X)) = EKUa(DKR a(X)) = X$$

$$DKUa(EKR a(X)) = EKR b(DKU b(X)) = X$$

Шифровање порука криптографским системима са јавним кључевима обухвата следеће кораке:

1. Сваки корисник генерише пар кључева који ће бити коришћени за шифровање или дешифровање порука.
2. Сваки корисник поставља један од та два кључа у јавни регистар кључева или други фајл који је јавно доступан. Овај кључ представља његов јавни кључ. Његовог криптографског пара, други генерисани кључ, корисник држи у тајности и он представља његов тајни кључ. На овај начин сваком кориснику је доступна колекција јавних кључева свих учесника у комуникацији.
3. Уколико Боб жели да пошаље поруку Алиси, Боб шифрује дату поруку Алисиним јавним кључем
4. Када Алиса прими такву поруку, она је дешифрује својим тајним кључем. Други учесници не могу да дешифрују дату поруку јер само Алиса зна свој тајни кључ.

Овакав приступ омогућује да сви учесници у комуникацији имају приступ јавним кључевима, док се тајни кључеви генеришу локално, за сваког учесника понаособ, и никада се не врши њихова дистрибуција. Све док се корисников тајни

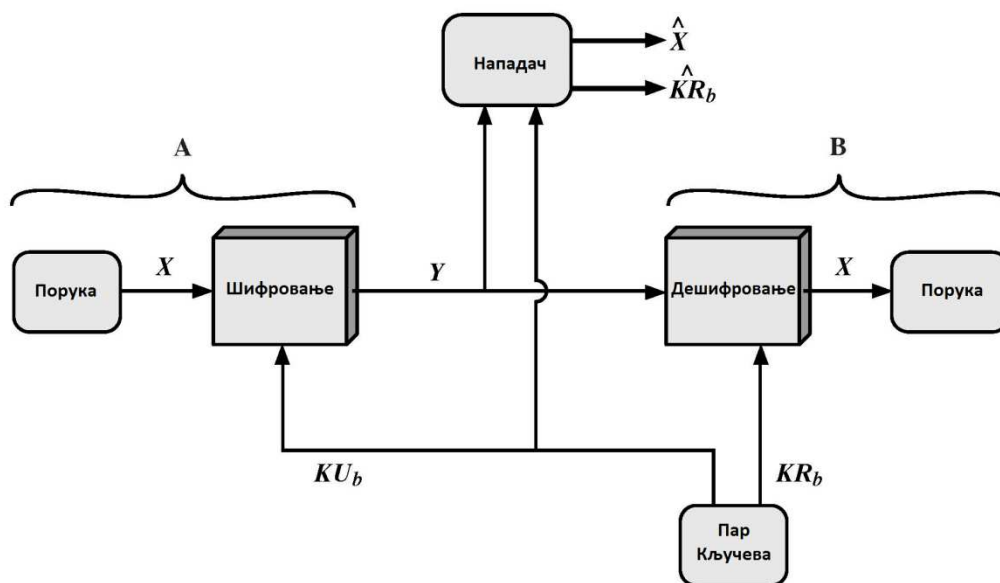
кључ држи заштићен и у тајности то гарантује да је комуникација безбедна.

На Слици 6 приказана је шема шифровања порука применом система са јавним кључем. Приказани су основни елементи система. Нека  $A$  представља извор порука и нека он производи текст отворене поруке  $X = [X_1, X_2, X_3, \dots, X_M]$ .  $M$  елемената поруке  $X$  су слова унапред дефинисаног алфавета. Порука је намењена одредишту  $B$ . Страна  $B$  генерише међусобно зависни пар кључева: јавни кључ,  $KU_b$ , и тајни кључ,  $KR_b$ .  $KR_b$  је познат само страни  $B$ , док је  $KU_b$  јавно доступан, и страна  $A$  може да му приступи. Са поруком отвореног текста  $X$  и кључем шифровања  $KU_b$ , страна  $A$  формира шифрат  $Y = [Y_1, Y_2, Y_3, \dots, Y_N]$ . Математички, према претходно усвојеној нотацији, ово се може представити следећом релацијом:

$$Y = E_{KU_b}(X)$$

Прималац коме је намењена порука, уколико располаже одговарајућим паром кључева – његов тајни кључ, у могућности је да изврши инверзну трансформацију. На пријемној страни, страна  $B$  алгоритмом дешифровања поруке и применом свог тајног кључа, дешифрује добијену поруку и добија отворени текст који је послала страна  $A$ . Поступак дешифровања је еквивалентан следећој релацији:

$$X = D_{KR_b}(Y) = D_{KR_b}(E_{KU_b}(X))$$

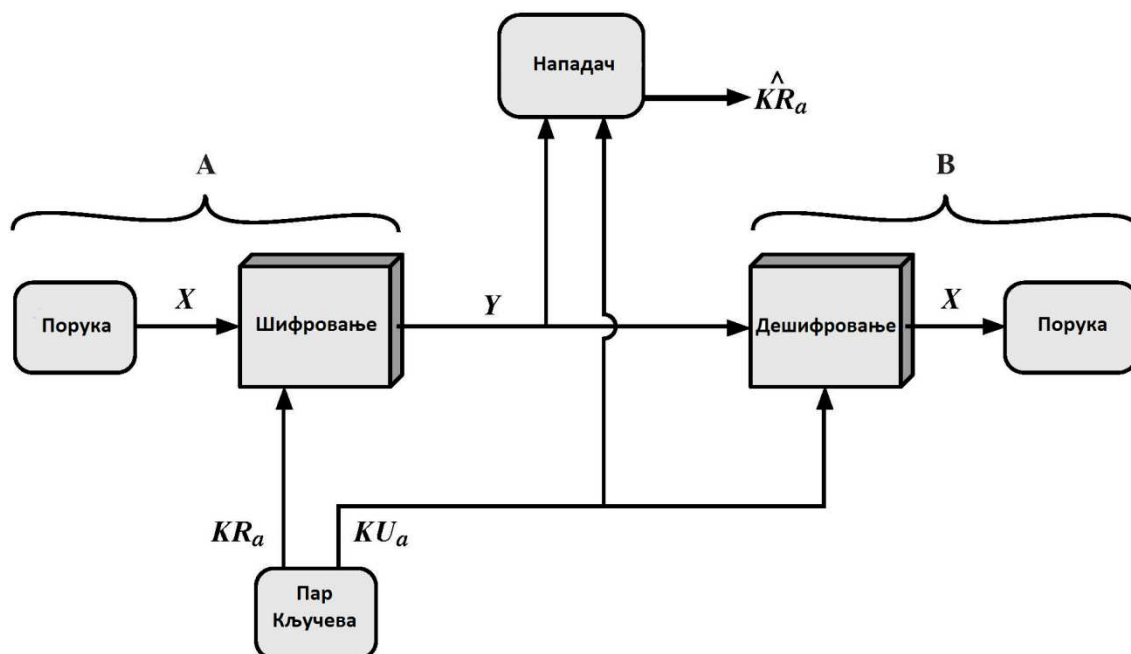


Слика 6 Системи са јавним кључем – очување тајности

У овом случају, криптоаналитичару су доступни јавни кључ примаоца и шифрат. Опционо, криптоаналитичар познаје и криптографски поступак који је употребљен за шифровање поруке. Међутим, да би могао да открије садржај шифроване поруке, криптоаналитичар мора да открије тајни кључ примаоца поруке. У томе лежи криптолошка вредност асиметричних криптографских система. Ради се о постулату по ком је рачунарски немогуће, у реалном времену, одредити  $KR_a$  на основу познавања  $KU_a$  – тј. не постоји детерминистичка веза између криптолошког пара кључева.

У системима са јавним кључевима се прави разлика између поступака

применом којих се реализује аутентичност и поступака за очување тајности. Слика 7 приказује употребу асиметричних система за реализацију аутентичности пошиљаоца.



Слика 7 Системи са јавним кључем – аутентичност

У овом случају страна  $A$  припрема поруку коју ће да пошаље страни  $B$  и шифрује је употребом алгорита шифровања и својим тајним кључем. Овај поступак се може описати следећом релацијом:

$$Y = E_{KR_a}(X)$$

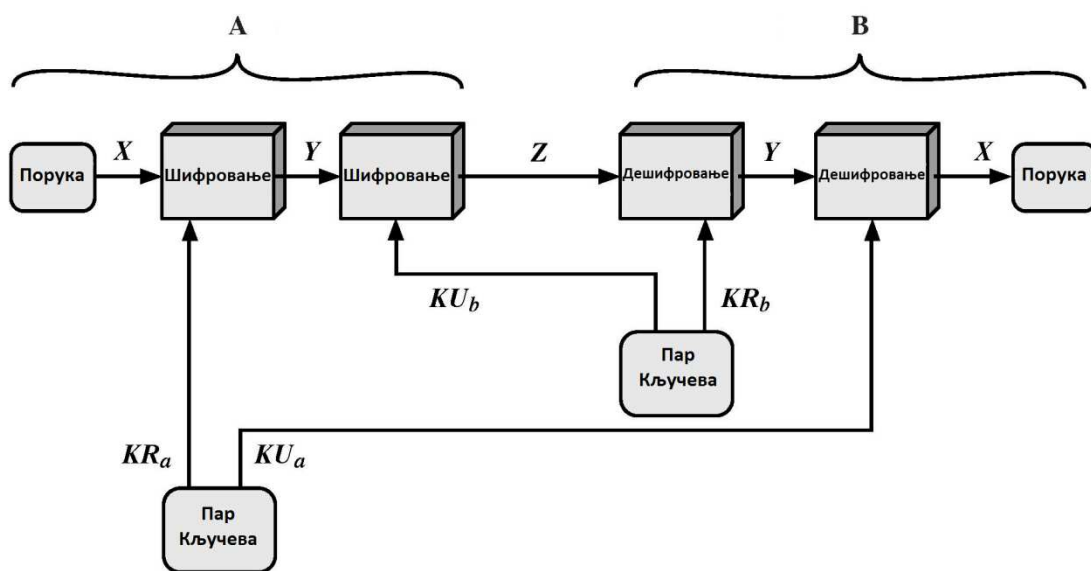
Пошто је порука шифрована тајним кључем  $A$  учесника у комуникацији, искључиво страна  $A$  је могла да ту поруку генерише на тај начин. Такође, немогуће је извршити модификацију поруке уколико не располажемо тајним кључем  $KR_a$ . На тај начин, оваквом поруком се постиже аутентичност стране која је послала поруку као и то да интегритет поруке није нарушен при њеном преносу. На пријемној страни, страна  $B$  врши дешифровање поруке применом алгорита дешифровања и јавног кључа пошиљаоца  $KU_a$ . Представљено релацијом то изгледа овако:

$$X = D_{KU_a}(Y) = D_{KU_a}(E_{KR_a}(X))$$

У претходном случају, улазна порука је шифрована и тим поступком је постигнуто очување аутентичности стране која је послала поруку као и очување интегритета поруке. Међутим, овај поступак има један недостатак. Овакав поступак очувања аутентичности захтева велики меморијски простор. Потребно је обезбедити простор да се сваки документ чува као отворени текст (за потребе коришћења у том облику). Такође је потребно чувати копију отвореног текста у облику шифрата за потребе верификације садржаја поруке, у случају потребе. Много ефикаснији начин архивирања, који даје подједнако добре резултате, је да се врши шифровање малог блока података (неколико стотина бита) који представљају одређену функцију отвореног текста. Такав блок, који представља један аутентикатор, мора да има

механизам који онемогућава промене на документу тако да се та промена не манифестује на идентификатор. Уколико је аутентикатор шифрован тајним кључем пошиљаоца обезбеђују се поменути захтеви аутентикације. Овај поступак је познат као дигитално потписивање поруке.

Важно је напоменути да овакав поступак аутентикације не обезбеђује очување тајности података, па криптоаналитичар може познавајући јавни кључ пошиљаоца и алгоритам шифровања да дође до отвореног садржаја поруке. Дакле, овако послате поруке су имуне на промену садржаја али ниси имуне на могућност увида у садржај. Поставља се питање да ли је применом система са јавним кључем могуће истовремено обезбедити и аутентичност и очување тајности. Одговор је, наравно, потврдан. Ово се постиже применом двостроког шифровања применом парова јавних и тајних кључева. Слика 8 приказана је шема којом се постиже оваква заштита.



Слика 8 Системи са јавним кључем – аутентичност и очување тајности

Обрада поруке  $X$  почиње шифровањем поруке тајним кључем пошиљаоца (страна  $A$ )  $KR_a$ . Након тога, тако добијену поруку ( $Y$ ) шифрујемо алгоритмом шифровања и јавним кључем примаоца (страна  $B$ )  $KU_b$ . Тако добијени шифровани текст  $Z$  може интерпретирати само онај коме је порука намењена, тј. онај ко има одговарајући пар кључа. Првим шифровањем обезбеђује се аутентичност док друго шифровање постиже заштиту тајности. На пријемној страни прво се врши дешифровање тајним кључем примаоца  $KR_b$ , а затим и јавним кључем пошиљаоца  $KU_a$ . Поменути поступак је еквивалентан следећим релацијама:

предајна страна:  $Y = E_{KR_a}(X), Z = E_{KU_b}(Y)$ , тј.  $Z = E_{KU_b}(E_{KR_a}(X))$

пријемна страна:  $Y = D_{KR_b}(Z), X = D_{KU_a}(Y)$ , тј.  $X = D_{KU_a}(D_{KR_b}(Z))$

### 5.2.1 Примена система са јавним кључем

Системи са јавним кључем су они који користе криптографске алгоритме са

два кључа, један који се држи у тајности и други који је јавно доступан. У зависности од примене, пошиљалац користи свој приватни кључ, јавни кључ примаоца, или оба, и на тај начин реализује одређени тип криптографске функције. Под таквим условима, системе са јавним кључевима могуће је класификовати у три категорије:

- Системи за шифровање/дешифровање поруке - пошиљалац шифрује поруку јавним кључем примаоца.
- Системи за дигитално потписивање поруке - пошиљалац потписује поруку својим тајним кључем. Потписивање се може остварити на два начина, потписивањем целе поруке или потписивање малог блока података (неколико стотина бита) који представљају одређену функцију поруке.
- Системи за размену кључева - два корисника размењују сесијски кључ. Код ових система могућ је већи број приступа, па и онај који укључује приватне кључеве обе стране.

Одређени број криптографских алгоритама је погодно за све три примене, док су други погодни за једну или две поменуте примене. Табелом 2 приказане су примене најпознатијих асиметричних криптографских алгоритама.

Табела 2 Примена система са јавним кључем

| Алгоритам           | Систем за шифровање/дешифровање поруке | Систем за дигитално потписивање поруке | Систем за размену кључева |
|---------------------|----------------------------------------|----------------------------------------|---------------------------|
| RSA                 | ДА                                     | ДА                                     | ДА                        |
| EC – Elliptic Curve | ДА                                     | ДА                                     | ДА                        |
| Diffie – Hellman    | НЕ                                     | НЕ                                     | ДА                        |
| DSS                 | НЕ                                     | ДА                                     | НЕ                        |

### 5.2.2 Захтеви за системе са јавним кључем

Криптографски системи приказани на Сликама 6, 7 и 8 примењују криптографске алгоритме који се базирају на употреби два међусобно зависна кључа. *Diffie* и *Hellman* су поставили основне постулате ових система без демонстрације на већ постојећем алгоритму. Јавно су публиковали основне захтеве које један такав алгоритам треба да задовољи:

1. Страна *B* лако и једноставно генерише пар кључева (јавни кључ, *K<sub>Ub</sub>*, и тајни кључ, *K<sub>Rb</sub>*)
2. Предајна страна (страна *A*) лако, уколико познаје јавни кључ примаоца (страна *B*) *K<sub>Ub</sub>* и отворени текст поруке *M* коју треба да шифрује, генерише шифровани текст *C*:

$$C = E_{KU_b}(M)$$

3. Пријемна страна (страна  $B$ ) лако дешифрује добијени шифровани текст применом свог тајног кључа,  $KR_b$ , да би генерисала оригинални текст поруке:

$$M = D_{KR_b}(C) = D_{KR_b}(E_{KU_b}(M))$$

4. Рачунарски је готово немогуће, у реалном времену, на основу познавања јавног кључа  $KU_a$  одредити одговарајући тајни кључ  $KR_a$ .
5. Рачунарски готово је немогуће, у реалном времену, на основу познавања јавног кључа којим је извршено шифровање одређене поруке,  $KU_a$ , и познавања шифрата  $C$ , одредити текст оригиналне поруке  $M$

Шести захтев је такође користан али није и неопходан у примени система са јавним кључевима.

6. Два кључа могу бити примењена и било ком поретку

$$M = E_{KU_a}(D_{KR_a}(M)) = D_{KR_a}(E_{KU_a}(M))$$

Ово су веома сложени захтеви, што потврђује и чињеница да је свега неколико алгоритама (RSA, EC – *Elliptic Curve*, *Diffie–Hellman*, DSS) задовољило поменуте захтеве. Ови алгоритми имају веома широку примену [11].

### 5.3 Diffie-Hellman протокол

*Diffie-Hellmanov* поступак размене кључа је криптографски протокол који омогућује особама које се не познају да размене симетрични тајни кључ преко небезбедног комуникационог канала. Размењени кључ се касније може користити за шифровање порука употребом симетричног шифарског система. Симетрични шифарски систем се користи због уштеде времена за шифровање и дешифровање.

*Diffie* и *Hellman* су 1976. године понудили решење проблема размене кључева, засновано на дискретном логаритамском проблему, односно на тежини рачунања дискретних логаритама у коначном пољу. Они су објавили поступак за размену тајног кључа потребног за шифровање употребом симетричног шифарског система.

*Diffie-Hellmanov* протокол за размену кључева обухвата следеће кораке:

- Два учесника се унапред договоре о два велика броја,  $n$  и  $g$ . Број  $g$  је прост у односу на  $n$ , а највећи заједнички делилац им је број 1. Најпрактичније је одабрати за  $n$  велики прост број  $p$ . Бројеви  $p$  и  $g$  су јавно доступни.
- Алиса бира своју тајну вредност  $a$ . Боб бира своју тајну вредност  $b$ . Ове вредности представљају велике случајне просте бројеве.
- Алиса, када жели да успостави комуникацију са Бобом, шаље му резултат израчунавања операције:

$$A = g^a \pmod{p}.$$

- Боб шаље Алиси свој резултат израчунавања операције:

$$B = g^b \pmod{p}.$$

- Алиса на основу примљене вредности од Боба рачуна:

$$K = B^a(\text{mod } p) = (g^b)^a(\text{mod } p) = g^{ab}(\text{mod } p).$$

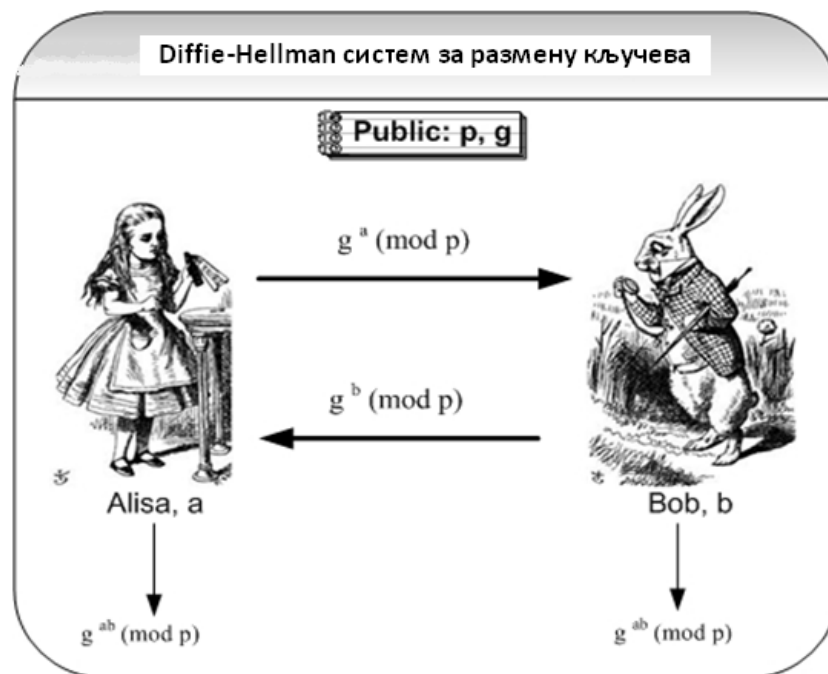
- Боб на основу примљене вредности од Алисе рачуна:

$$K = A^b(\text{mod } p) = (g^a)^b(\text{mod } p) = g^{ab}(\text{mod } p).$$

- Добијена заједничка вредност се користи као симетрични кључ.

Из ових корака протокола, евидентно је да, за размену симетричног кључа, нису потребни тајни канали. Добијена вредност  $K$  је симетрични кључ који Алиса и Боб могу користити за даљу безбедну комуникацију. Нападач може да сазна вредности  $g$ ,  $p$ ,  $A$ ,  $B$  јер су послате јавно, каналом везе али не може, на основу ових вредности, да одреди вредности  $a$  и  $b$ , а уколико би то могао да уради, систем би био небезбедан, што би значило да је решен проблем дискретног логаритма.

Пример *Diffie-Hellman*-овог алгоритма, који се користи за размену заједничког симетричног кључа приказан је Сликаом 9. Овај алгоритам није намењен за шифровање или дигитално потписивање.



Слика 9 *Diffie-Hellman* систем за размену кључева

### 5.3.1 Пример *Diffie-Hellman*-овог протокола за размену кључева

Због лакшег рачунања у примеру који следи биће коришћени мали бројеви. У пракси се за  $p$  вредност користи број који је већи од 1024 бита.

Алиса и Боб прихватају да су  $p = 33$  и  $g = 3$ . Алиса рачуна  $a = 11$  и шаље Бобу:

$$A = 3^{11}(\text{mod } 33) = 3.$$

Боб рачуна  $b = 9$  и шаље Алиси:

$$B = 3^9(\text{mod } 33) = 15.$$

Након што су разменили вредности, Алиса и Боб израчунају заједнички кључ. Алиса рачуна свој кључ:

$$K_A = 15^{11}(\text{mod } 33) = 15.$$

Боб рачуна свој кључ на исти начин као и Алиса:

$$K_B = 3^9(\text{mod } 33) = 15.$$

Одакле следи да је  $K_{AB}$ :

$$K_A == K_B = 15.$$

### 5.3.2 Примена Diffie-Hellman-овог протокола

*Diffie-Hellman*-ов протокол обезбеђује размену тајног кључа путем небезбедног комуникационог канала. Примењује се у мрежним протоколима који омогућују безбедну комуникацију. Користи се:

- у IPsec (*IP security*, енгл.) протоколу,
- унутар IKE (*Internet Key Exchange*, енгл.) структуре,
- у SSH и TLS протоколима и
- у поступку стварања дигиталних потписа и дигиталних сертификата.

Овај протокол означио је прекретницу у комуникацији шифрованим порукама. Сигурност протокола се темељи на експоненцијалној сложености израчунавања дискретног логаритма за велике бројеве. Основа сигурности протокола лежи у теорији великих бројева. Због тежине рачунања дискретног логаритма уколико се користе довољно велики прости бројеви није могуће, уз постојећу технологију, у разумном времену, грубом силом (*brute force*, енгл.) извести успешан напад на *Diffie-Hellman*-ов протокол. *Diffie-Hellman*-ов протокол има једну рањивост, а то је недостатак аутентикације учесника. Због тога је могуће извести напад „човек у средини“ (*man-in-the-middle attack*, енгл.). За спречавање овог напада потребно је извршити аутентикацију учесника који размењују кључеве. Протокол има раширену примену и чини темељ заштите комуникације путем небезбедних комуникационих канала, као што је Интернет. Користи се за успостављање безбедне комуникације и размену кључева у рачунарским мрежама.

*Diffie-Hellman*-ов протокол је ушао у историју као један од најзначајнијих открића јер је омогућио размену тајног кључа симетричних шифарских система. И, поред сталних истраживања у подручју размене кључева, *Diffie-Hellman*-ов протокол се још увек употребљава као једино решење за размену тајних кључева у криптографским системима.

### 5.3.3 Напад на Diffie-Hellman-ов протокол

Озбиљан проблем код имплементације *Diffie-Hellman*-овог алгоритма, је осетљивост на напад типа „човек у средини“. Овај напад може бити активан и пасиван. Уколико је напад активан, он може да пресретне поруку, измени је и проследи даље, док је код пасивног напада могуће искључиво прислушкивање комуникационог канала. Претпоставља се да нападач може да има улогу активног

нападача у сценарију човека у средини. У том случају *Diffie-Hellman*-ов протокол је небезбедан јер нападач дели један симетрични кључ  $K_{AE}$  са Алисом и један симетрични кључ  $K_{BE}$  са Бобом, чиме постаје посредник у комуникацији.

Пример напада „човек у средини“: Када Алиса пошаље вредност  $A$ , нападач пресреће поруку и уместо Алисине вредности шаље своју вредност  $E = g^e \pmod{p}$  коју је претходно израчунао, познавајући јавно објављене бројеве  $p$  и  $g$ . Нападач рачуна кључеве  $K_A$  и  $K_B$ :

$$K_{EA} = A^e \pmod{p} = (g^a)^e \pmod{p} = g^{ae} \pmod{p}$$

$$K_{EB} = B^z \pmod{p} = (g^b)^z \pmod{p} = g^{bz} \pmod{p}$$

Алиса рачуна кључ:

$$K_{AE} = E^a \pmod{p} = (g^e)^a \pmod{p} = g^{ae} \pmod{p}$$

Боб рачуна кључ:

$$K_{BE} = E^b \pmod{p} = (g^e)^b \pmod{p} = g^{be} \pmod{p}$$

Ако након размене кључева Алиса и Боб наставе комуникацију користећи израчунате кључеве, па нападач може да наруши тајност и интегритет комуникације.

После овакве размене кључева, када Алиса шаље шифровану поруку  $C_1 = E(P, K_{AE})$ , где је  $P$  отворени текст, нападач пресреће и дешифрује поруку, а самим тим долази до садржаја поруке  $P = D(C_1, K_{AE}) = D(E(P, K_{AE}), K_{EA})$ . Нападач тада може да шифрује отворени текст  $P$  или да убади неки други текст  $P'$  и тако шифровано пошаље Бобу  $C_2 = E(P', K_{EB})$ . Боб мисли да је добио поруку од Алисе и својим кључем дешифрује поруку  $P' = D(C_2, K_{EB}) = D(E(P', K_{EB}), K_{BE})$ .

На исти начин је могуће остварити комуникацију у супротном смеру. Алиса и Боб не могу да открију да је њихову комуникацију надгледао нападач. Према томе, овакве и сличне размене кључева потребно је додатно обезбедити поступком аутентикације учесника у комуникацији [1][2][13].

## 5.4 RSA алгоритам

RSA је алгоритам за асиметричну криптографију, првенствено намењен шифровању података али се данас користи и у системима електронског потписа. RSA је индустријски стандард у области асиметричне криптографије и заштити података, па је широко примењен у различитим типовима сигурносних протокола и системима електронског пословања. Алгоритам је настао је 1977. године универзитету МИТ, у САД.

Безбедност RSA заснована је на сложености факторизације великих бројева. Јавни и приватни кључ су функције једног пара великих бројева који садрже од 100 до 200 цифара, или више простих бројева. Сматра се да је одређивање оригиналне поруке на основу шифрата и кључа за шифровање еквивалентно факторизацији производа два велика проста броја. За шифровање код асиметричних система се користи једносмерна функција са замком.

Суштина алгоритма је у проналажењу функције  $E$  која мења отворен текст  $M$  у шифрат  $C$ , односно  $C = E(M, K_e)$ . Параметар  $K_e$  је јавни кључ и служи искључиво за шифровање. Не може се употребити за дешифровање  $M \neq D(C, K_e)$  због тога што је  $E$  једносмерна функција. Уколико је порука намењена за Боба, свако може

шифровати поруку за њега коришћењем његовог јавног кључа  $K_e$ . За дешифровање Боб мора да употреби тајну вредност  $K_d$  (приватни кључ) и да примени инверзну функцију  $M = D(C, K_d)$  како би из шифрата  $C$  добио отворен текст  $M$ . Услов за успешно шифровање и дешифровање је да буде:  $M = D(E(M, K_e)K_d)$ . Неопходно је познавање одговарајуће математичке функције која има наведена својства, а припада класи једносмерних функција са замком. У наведеном примеру приватни кључ  $K_d$  је замка. Познавањем замке процес дешифровања је једноставан. Без замке, дешифровање је практично немогуће. Функција која задовољава наведене претпоставке је облика:

$$f(x) = x^e \bmod N.$$

Уз одговарајући избор вредности  $e$  и  $N$  ова функција је једносмерна. Уз познавање тајне вредности (замке) може да се нађе њена инверзна функција. Без познавања замке, она је практично готово нерешива.

Да се генеришу два кључа, насумично се изабере два велика проста броја,  $p$  и  $q$  и формира се њихов производ  $N = p \cdot q$ . Затим се насумично изабере кључ за шифровање  $e$ , узајамно прост са производом  $\varphi(N) = (p-1)(q-1)$  и уз услов  $e < \varphi(N)$ . Коначно, потребно је одредити  $d$  на основу следећег  $d = e^{-1}(\bmod \varphi(N))$ , тако да важи  $ed = 1(\bmod \varphi(N))$ . Прости бројеви  $p$  и  $q$  више нису потребни.

Број  $N$  је модул,  $e$  је експонент за шифровање, а  $d$  је експонент за дешифровање. RSA пар кључева садржи јавни кључ  $(N, e)$  и приватни кључ  $(d)$ .

За операције шифровања и дешифровања примењује се функција модуларног експонента на следећи начин:

Формула за шифровање:

$$C = M^e \bmod N$$

Формула за дешифровање:

$$M = C^d \bmod N.$$

Тајност асиметричног шифарског система са RSA алгоритмом заснива се на сложености факторизације броја  $N$  (који је јаван) на чиниоце  $p$  и  $q$ . Било би једноставно, коришћењем јавно доступне вредности  $e$  одредити приватну вредност  $d$  из услова  $ed = 1(\bmod \varphi(N))$ . За довољно велике бројеве  $p$  и  $q$  процес факторизације је дуготрајан. Уз доступне рачунарске ресурсе могуће га је упоредити са процесом тоталне претраге по простору свих кључева код симетричних шифарских система. Проблем који се јавља код асиметричних шифарских система је непостојање чврстог математичког доказа да је растављање на факторе једини начин за разбијање RSA.

С обзиром да је  $C = M^e \bmod N$ , потребно је показати да је :

$$M = C^d \bmod N = M^{ed} \bmod N.$$

Генерисање тајног кључа:

$$p = 47$$

$$q = 71$$

Одредити вредност  $N$ :

$$N = pq = 47 * 71 = 3337$$

$$\varphi(N) = (p-1)(q-1) = 46 * 70 = 3220$$

Изабрати број  $e$  (узајамно прост):

$$e = 79$$

У том случају је:

$$d = 79^{-1} \bmod 3220 = 1019$$

Резултат за јавни ( $N, e$ ) и приватни кључ  $d$ :

$$(N, e) = (3220, 79)$$

$$d = 1019$$

Након израчунатог кључа  $d$ , параметри  $p$  и  $q$  се уништавају на сигуран начин, јер сигурност зависи баш од свих параметара [2].

## 5.5 Инфраструктура са јавним кључевима

Инфраструктуру са јавним кључевима, PKI (*Public Key Infrastructure*, енгл.) чине хардвер, софтвер, полисе и процедуре које су неопходне за управљање, генерисање, складиштење и дистрибуцију криптографских кључева и дигиталних сертификата. Она дефинише модел за свеобухватну сигурносну инфраструктуру чије су услуге имплементиране уз помоћ концепата система за шифровање који користе асиметричне алгоритме.

### 5.5.1 Основне функције и компоненте

Управљање, генерисање, складиштење и дистрибуција криптографских кључева и дигиталних сертификата се одвија кроз Сертификационо тело (*Certification Authority*, CA, енгл.) и Регистрационо тело (*Registration Authority*, RA, енгл.).

Улога СА је да представља страну од поверења за све учеснике у комуникацији. СА функционише на следећи начин: крајњи корисници, који међусобно немају успостављени ланац поверења, му верују, па он прво врши аутентикацију крајњих корисника (директно или посредством RA). После успешне аутентикације, СА издаје дигитални сертификат крајњем кориснику. Издати сертификат гарантује идентитет корисника и потписан је дигиталним сертификатом самог СА. Крајњи корисници сад користе своје дигиталне сертификате, које је издало СА, како би доказали свој идентитет један другом и успоставили сигурну комуникацију.

#### Пријављивање крајњих корисника

Да би користили услуге инфраструктуре јавних кључева, крајњи корисници прво морају да прођу процес пријављивања који обухвата проверу идентитета и размену информација са за то задуженом компонентом инфраструктуре јавних кључева Регистрационим телом.

Први корак у процесу пријављивања је регистрација при којој се провера идентитет крајњег корисника који подноси захтев за сертификатом. Ниво провере идентитета зависи од типа сертификата за који се подноси захтев (нпр. сертификата

који се користе при електронској куповини има строжи ниво провере од осталих типова сертификата) и за сваки тип сертификата је дефинисан одговарајућим документом 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: како ће се одвијати сама комуникација, како ће се дистрибуирати сертификати, на које начине се успоставља сигурна комуникација између крајњих корисника и СА, како се генерише и доставља пар асиметричних кључева.

### Дигитални сертификат

Дигитални сертификати омогућавају потврду идентитета при електронским трансакцијама, слично као што су личне карте у међуљудским интеракцијама.

Он повезује податке о идентитету корисника са паром асиметричних кључева који се користе за шифровање и потписивање дигиталне информације чиме потврђује нечије право на коришћење криптографских кључева.

Дигитални сертификат је издат и дигитално потписан од стране СА. 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.

Најчешће коришћени формат дигиталног сертификата је дефинисан ITU-T X.509 стандардом. Додатне спецификације и финесе су дефинисане PKCS и PEM стандардима.

При слању поруке пошиљалац дигитално потписује поруку и уз њу шаље и свој дигитални сертификат како би прималац могао да провери идентитет пошиљача. Уз поруку може да буде послато и више дигиталних сертификата који формирају хијерархијски ланац поверења, где један дигитални сертификат потврђује аутентичност претходног дигиталног сертификата. На самом врху у хијерархији поверења налази се *root* (највиши ниво) СА коме верују сва остала сертификациона тела. Јавни кључ *root* СА мора да буде јавно познат и доступан.

**Сертификација** обухвата процес издавања и достављања сертификата крајним корисницима и обавља је СА.

**Опозив сертификата.** Иако је период важења дигиталног сертификата дефинисан датумима у одговарајућим пољима сертификата, дешава се да дође до компромитовања тајног кључа или промене неког од основних личних података који се налазе у сертификату, што има за последицу опозивање сертификата, односно његово повлачење из употребе. Опозвани сертификати се објављују преко листа опозваних сертификата (*Certificate Revocation List* – CRL, енгл.) које објављује СА које је издало сертификат. У неким случајевима, уместо листе опозваних сертификата, се користе протоколи за проверу стања сертификата у реалном времену

који дају позитиван или негативан одговор о статусу сертификата. Пример таквог протокола је OSCP (*Online Certificate Status Protocol*, енгл.).

**Провера валидности сертификата.** Као што је претходно поменуто, неважећи (опозвани) сертификати се објављују преко листа опозваних сертификата или се користе протоколи за проверу стања сертификата. Трећа страна је дужна да пре него што прихвати сертификат провери његову валидност. Сваки сертификат садржи поље.

Инфраструктура са јавним кључевима користи асиметричну криптографију и дигиталне сертификате како би обезбедила аутентикацију корисника, интегритет и тајност података и немогућност порицања послате информације [14].

### 5.5.2 Формат дигиталног сертификата у систему јавних кључева према стандарду X.509

Формат X.509 одређује запис и дефинише поља у сертификатима. Овај стандард такође предвиђа начине опозива сертификата, као и алгоритме за шифровање. Први PKI пројекат је подразумевао употребу X.509 стандарда. Многе компаније у свету своје пословање темеље на овом стандарду, као што су VISA и MasterCard. У тексту који следи дат је преглед структуре сертификата, по стандарду X.509, верзија 3.

- Верзија сертификата – верзија сертификата који се употребљава.
- Серијски број – серијски број сертификата је јединствени идентификатор сертификата издатог од СА.
- Идентификатор алгоритма – идентификује алгоритам којим је СА потписао сертификат.
- Издавач сертификата – потписник сертификата.
- Валидност сертификата – сваки сертификат је валидан у одређеном временском периоду. Временски период је одређен датумом почетка и краја валидности сертификата.
- Назив ентитета – повезује приватни кључ са јавним кључем из сертификата.
- Подаци о јавном кључу ентитета – садржи јавни кључ ентитета и идентификатор криптографског алгоритма.
- Идентификатор издавача – јединствено поље које садржи име издавача према X.500 стандарду
- Идентификатор ентитета – јединствено поље за идентификацију ентитета.
- Проширења – прописана у верзији 3 дигиталних сертификата. Дефинише стандарде проширења верзије 2.
- Дигитални потпис сертификата – идентификује потпис сертификата приватним кључем сертификационог центра [15].

## 5.6 Поређење шифарских система са симетричним и асиметричним кључем

Стално се поставља питање шта је боље криптографија са јавним кључем или симетрична криптографија. Навешћемо неколико предности криптографије са јавним кључем, нпр. поверљивост која је обезбеђена без дељења тајни, врло је битно и корисно у данашњем, комерцијалном свету. Не постоји проблем са разменом кључева као код симетричних шифарских система. Аутентикација се обавља без дељења тајни. Дигитални потпис се користи као доказ о пореклу поруке. Јавни кључ није потребно штитити, потребно је само да се са сигурношћу зна да је јавни кључ заиста кључ особе за коју се представља.

Предности симетричне криптографије у односу на асиметричне:

1. Брзина шифровања и дешифровања, практична имплементација.
2. Није хардверски захтевна.
3. Употреба релативно кратких кључева.

Недостаци симетричних система:

1. Кључеви морају бити тајни.
2. Потреба за сигурним каналом приликом размене кључева.
3. Пракса налаже промену кључа за сваку сесију.

Предности асиметричне криптографије у односу на симетричне:

1. Није потребан сигуран канал за размену јавних кључева.
2. Само један кључ мора бити тајан.
3. Кључеви могу остати непромењени дуже времена.

Недостаци асиметричних система:

1. Брзина шифровања и дешифровања је неколико стотина пута мања.
2. Кључеви су знатно дужи.

**Табела 3** Однос дужина симетричних и асиметричних кључева

| Дужина кључа DES алгоритма | Одговарајућа дужина кључа RSA алгоритма |
|----------------------------|-----------------------------------------|
| 56 бита                    | 512 бита                                |
| 80 бита                    | 1024 бита                               |
| 112 бита                   | 2048 бита                               |
| 128 бита                   | 3072 бита                               |
| 192 бита                   | 7680 бита                               |
| 256 бита                   | 15360 бита                              |

Односи дужине кључева симетричних и асиметричних шифарских система

приказани су у Табели 3. који обезбеђују сличан степен сигурности приликом грубих напада.

Асиметрични алгоритми су доста спорији из разлога што је модуларан аритметика рачунски захтевна. Брзина шифарских система са јавним кључевима није једини проблем, постоји проблем и код дужине кључа.

Безбедност се заснива на претпоставкама које нису доказане, и даље остаје могућност за решавање проблема факторизације у будућности.

Проблем ове врсте се решава изградњом хибридних система, под којим се подразумева, криптографски систем у коме се систем са јавним кључем користи за размену симетричног или сесијског кључа, а за шифровање података користи се систем са симетричним кључем (нпр. IPsec и SSL) [2][16] .

## 6. Информационо теоријски приступ криптографији

Криптографија и теорија информација су уско повезане иако је, историјски гледано криптографија доста старија дисциплина. Шенон је разрадио и поставио прве научне основе теорије информација и добио далекосежне резултате, које је објавио 1948. године у делу под називом „Математичка теорија комуникација“ [17].

Постоје два типа криптографске сигурности: израчунљиво безбедна (рачунски сигурна) и информационо теоријска (безусловно сигурна) криптографска сигурност. Израчунљиво безбедна сигурност подразумева да је сигурност криптографског система заснована на тешко израчунљивим методама напада, док је информационо теоријска сигурност заснована на немогуће израчунљивим методама напада (и поред огромне рачунарске моћи).

Рачунска сигурност за сваки практичан шифарски систем, заснована је на претпоставци о разумно тешком израчунљивом моделу сигурности. Супротно рачунарској сигурности, информационо теоријски систем сигурности се не ослања на такве претпоставке, али се ослања на пробабилистичкој претпоставци понашања свемира, на пример канали са шумом или квантни канали. Међутим, и поред те претпоставке рачунски безбедни системи могу да генеришу случајне кључеве који су независни у односу на противничково знање.

Иако је информационо теоријска сигурност јача од рачунске сигурности, она је мање практична. Шеноновим доказом да апсолутна тајност захтева да криптолошки кључ буде исте дужине као и отворени текст показало се да је безусловна сигурност непрактична. Ипак о овом закључку треба поново размислити. За разлику од Шеноновог модела чије резултате задржавамо, криптографија заузима своје место у физичком свету (сваки комуникациони канал је заснован на физичком процесу) у коме нико не може имати комплетну информацију у систему, на пример услед шума.

Теорија информација има неколико примена у криптографији. Прво можемо доказати безусловну сигурност у криптографским системима. Друго можемо доказати немогућност и доњу границу резултата за постизање безусловне сигурности. Треће то је главни алат за смањивање доказа који се односе да је разбијање криптографских система једнако тешко као разбијање основних криптографских функција на којима је тај систем заснован (нпр. једносмерне функције или псеудо случајне функције) [18].

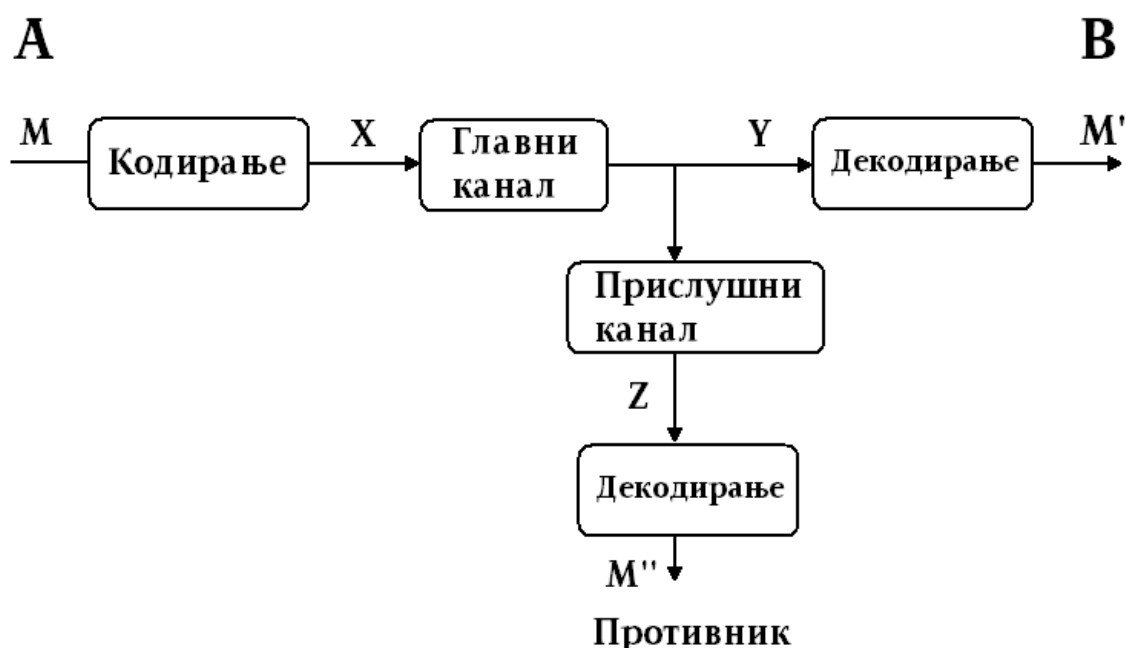
### 6.1 Информационо теоретски договор тајног кључа

Шенонова претпоставка да непријатељ прими потпуно исту поруку као и легитимни учесник узима се у обзир уколико се користи комуникациони канал у којем нема грешака. Међутим, у комуникационим каналима јавља се шум, па се у малом броју случајева ови канали претварају у канале у којима готово и да не постоји грешка преноса података (са смањеном брзином информација), што се изводи коришћењем кодова за исправљање грешке. Ова наизглед небитна обсервација указује на чињеницу да је Шеноново нагађање непотребно рестриктивно ако основним каналима у којима постоји шум може да се приступи криптографском

апликацијом, облика тајне комуникације кроз канале емитовања (*secret communication using broadcast channels*, енгл.).

Мотивисан оваквим размишљањима Вејнер је сматрао да је сценарио комуникације у којем Алиса може да пошаље информације Бобу преко дискретног канала тако да прислушкивач Ева може да прими Бобов канал (сигнал) само кроз додатне каскадне независне канале који смањују капацитет канала који користи Ева. Вејнер је доказао да у таквом (у општем случају нереалном) окружењу Алиса може да шаље информације Бобу у готово потпуној тајности, без потребе да пре тога размене кључ.

Вејнеров прислушни канал приказан је на Слици 10.



Слика 10 Вејнеров прислушни канал

Вејнеров модел и резултате, генерализовали су Сизар и Корнер који сматрају да дискретни канал за емитовање који користи прислушкивач Ева није обавезно деградирана верзија поруке, коју је примио легитимни учесник Боб. Заједнички унос главном каналу и каналу који користи Ева је случајна променљива  $X$  коју је одабрала Алиса према дистрибуцији вероватноће  $P_X$ , и случајне променљиве које су примили Боб и Ева су  $Y$  и  $Z$ .  $X$ ,  $Y$  и  $Z$  узимају вредности или бројеве одређене алфабетом  $\mathcal{X}$ ,  $\mathcal{Y}$  и  $\mathcal{Z}$ . Карактеристике канала су потпуно одређене условном дистрибуцијом вероватноће  $P_{YZ|X}$ . Вејнерово почетно подешавање  $X$ ,  $Y$  и  $Z$  праве Марковљев низ  $P_{Z|XY} = P_{Z|Y}$  који указује на  $I(X; Z|Y) = 0$ .

Капацитет тајности  $C_s(P_{YZ|X})$  описаног канала емитовања са транзицијом дистрибуције вероватноће  $P_{YZ|X}$  је дефинисана као максимална брзина којом Алиса може поуздано да шаље информације Бобу тако да је брзина којом Ева користи ову информацију произвољно мала, тј. капацитет тајности је максималан број бита који користи канал, тако да Алиса може тајно да шаље податке Бобу [19].

У односу на претходно описани модел, Маурер је унапредио модел, додајући му јавни канал између Алисе и Боба, тако да је између њих омогућена интерактивна комуникација. Ако је јавни канал аутентичан, тј. емитовање преко јавног канала не може да модификује Ева, могуће је постићи тајну комуникацију, и у случајевима када је канал који користи Ева бољи од оног који користи Боб. У тексту који следи приказан је Мауреров модел тајног система (*secrecy system*, енгл.):

1. Алиса, Боб и Ева имају приступ
  - а) комуникационим каналима са шумом
  - б) јавном, небезбедном каналу без грешке.
2. Уколико је  $C'$  информација у вези отвореног текста  $M$ , која је доступна Еви извесна корелација између  $C'$  и  $M$  је дозвољена.

Било која порука емитована кроз комуникациони канал садржи одређен ниво шума, што имплицира да ни Боб ни Ева не добијају увек идентичну копију поруке коју је послала Алиса. Из тог разлога  $C'$  означава Евину информацију у вези  $M$ . Ова претпоставка у вези јавног канала је такође прихватљива јер се лако постиже кроз овакав канал. У супротном, користећи технику за исправљање грешака, свака порука путем јавног канала се прихвата као тачна, тј. без грешке.

У Шеноновом моделу постигнута је информационо теоретска сигурност условом  $I(C; M) = 0$ . У Мауреровом моделу дозвољена је мала корелација између  $C'$  и  $M$ , и описује се као  $I(C; M) < \epsilon, m.j. H(M|C') = H(M) - \epsilon$ , за  $\epsilon > 0$ . Када  $\epsilon$  тежи нули,  $M$  поседује велики степен тајности (*highly secret*, енгл.).

На основу претходно наведеног модификованог модела, идеја информационог теоретског договора тајног кључа предложена је у [19]. Након успешног договора тајног кључа између Алисе и Боба, ОТР могу да буду коришћене за емитовање отвореног текста са савршеном тајношћу.

Информационо теоретски договор тајног кључа садржи три фазе:

1. Фаза иницијализације (*initialization phase*, енгл.): преко комуникационог канала са шумом, Алиса, Боб и Ева добијају случајне вредности променљивих  $X$ ,  $Y$  и  $Z$ , респективно, дистрибуиране са неком вероватноћом  $P_{XYZ}$ .
2. Фаза комуникације (*communication phase*, енгл.): Алиса и Боб размењују информације путем јавног канала. Ова фаза је познатија као јавна дискусија (расправа), и даље се дели у три фазе:
  - а) За време фазе дестилације предности (*advantage distillation*, енгл.), Алиса и Боб размењују информације, означене случајном променљивом  $U$ . Алиса добија нову случајну променљиву  $A$  од  $X$  и  $U$ . Слично, Боб добија нову случајну променљиву  $B$  од  $Y$  и  $U$ . Овим би требало добити резултат, у ситуацији да Боб има више информација Алисине случајне променљиве  $A$  него што Ева има, или да Алиса има више информација у вези Бобове случајне променљиве  $B$  него што их има Ева, тј.  $H(A|X, U) = 0, H(B|Y, U) = 0, H(A|B) < H(A|Z, U)$  или  $H(B|A) < H(B|Z, U)$ .
  - б) Алиса и Боб, размене неке сувишне информације да би исправили неслагање између њихових случајних променљива у току фазе усаглашавања информација (*information reconciliation*, енгл.). Уколико је сувишна информација  $V$  тада, користећи  $V$ , Алиса и Боб долазе до

заједничког низа  $S$ , а Ева и даље има одређену неизвесност везану за  $S$ . У формули,  $H(S|A, V) = 0$ ,  $H(S|B, V) = 0$ , и  $H(S|Z, U < V) > 0$ .

в) Фаза појачања приватности (*Privacy amplification* (PA), енгл.) обезбеђује Алиси и Бобу да генеришу тајан низ  $S'$  од заједничког али делом тајног низа  $S$ . Пут до комплетирања PA је да Алиса изабере одговарајућу *hash* функцију која је означена са  $G$ , и да је пошаље Бобу. Онда они рачунају *hash* вредност  $S' = G(S)$ , и очекују да буде  $H(S'|G, Z, U, V) = H(S') - \epsilon$  за мало  $\epsilon$ .

3. Фаза одлучивања (*decision phase*, енгл.): Алиса и Боб заједнички прихватају или одбацују извршење протокола, у зависности од тога да ли верују да низ  $S' = G(S)$  може служити као тајни кључ [19].

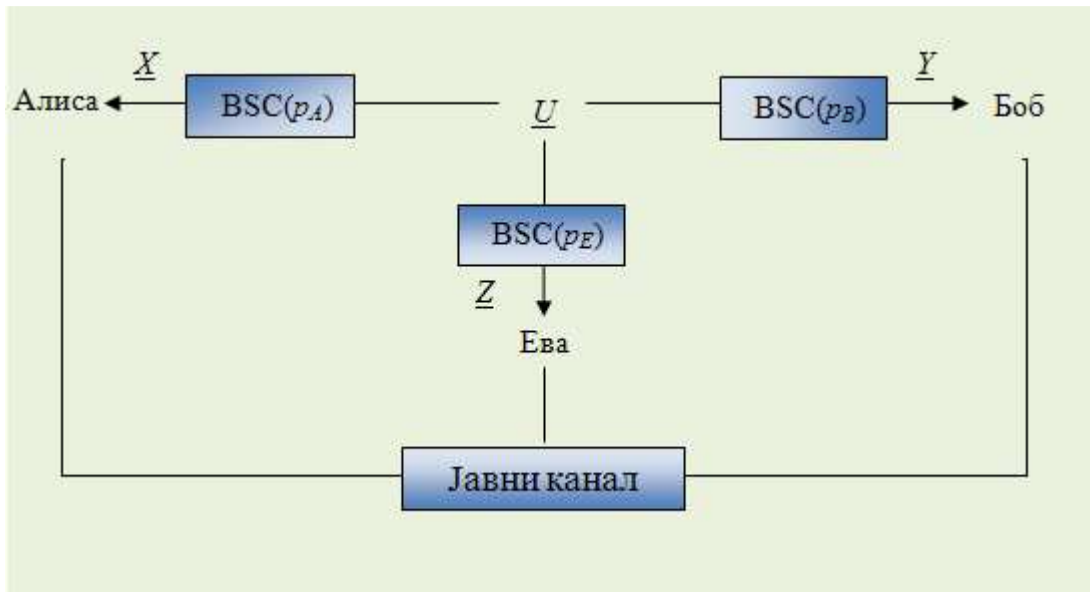
## 6.2 Мауреров протокол (сателитски сценарио)

Маурер је 1993. године предложио протокол у ком Алиса и Боб могу имати два мање корелисана низа него што га поседује Ева, а да ипак успеју да успоставе заједнички кључ. Циљ протокола је да Алиса и Боб успоставе тајни низ који ће бити само њима познат или заједнички симетрични кључ. Тај низ се користи као једнократни кључ за шифровање (*one-time-pad*). Сателитски сценарио (Слика 11.) је могућ чак и када је грешка Евиног канала  $\epsilon$  мања од грешака Алисиног и Бобовог канала. Сценарио није могућ у случајевима у којима је Евина грешка  $\epsilon = 0$  (идеалан приступ сателиту), или уколико Алиса и Боб не могу да приме емитоване низове.

Сателитски сценарио састоји се од четири фазе. У првој (иницијалној) фази Алиса, Боб и Ева примају почетне низове са сателита путем бинарног симетричног канала (BSK). Сви низови примљени са сателита су различити, али постоји одређен степен корелације међу њима [20]. Низови су дужине  $N$ , али нису истоветни и представљају несавршене копије неког оригинала који никоме није познат. Одавде следи да је:

$$\begin{aligned} p(A_i \neq U_i) &= \epsilon_A \\ p(B_i \neq U_i) &= \epsilon_B \\ p(E_i \neq U_i) &= \epsilon_E \end{aligned}$$

Уколико је Евина грешка мања од Алисине и Бобове, Алиса и Боб немају предност над Евом и не могу да уђу у трећу и четврту фазу протокола.



Слика 11 Сателитски сценарио

Друга фаза је дестилација предности. Ово је процес генерисања предности у односу на Еву захваљујући аутентичности јавног канала.

Трећа фаза протокола је усаглашавање информација или исправљање грешака. Након  $n$  итерација протокола за дестилацију предности Алисин и Бобов низ су и даље различити. Циљ протокола за усаглашавање информација је да вероватноћа  $p(A \neq B)$  буде мања од одређене, унапред задане вредности.

Четврта фаза протокола је појачавање приватности у којој се елиминише Евина информација универзалним хеширањем.

У даљем раду дат је детаљан опис фаза протокола.

### 6.3 Представљање

У раду је разматран сателитски сценарио у почетној фази информационо теоретског протокола за размену тајног кључа. Сателит емитује случајне бинарне низове  $\underline{U} = (U_1, U_2, \dots, U_N)$  са ослабљеном снагом сигнала. Алиса, Боб и Ева примају  $\underline{A} = (A_1, A_2, \dots, A_N)$ ,  $\underline{B} = (B_1, B_2, \dots, B_N)$  и  $\underline{E} = (E_1, E_2, \dots, E_N)$  кроз три независна бинарно симетрична канала са одговарајућим вероватноћама грешке над битовима  $p_A$ ,  $p_B$ , и  $p_E$ . Након тога, Алиса и Боб почињу јавну комуникацију путем јавног канала. У овом раду претпостављено је да је јавни канал на који су Алиса и Боб повезани аутентичан (*autentic*, енгл.). Ева може видети било коју поруку између Алисе и Боба, али не може да неприметно модификује или убаци лажну поруку. Јавна комуникација има три фазе: дестилација предности (*advantage distillation* (AD), енгл.), усаглашавање информација (*information reconciliation* (IR), енгл.), и појачавање приватности (*privacy amplification* (PA), енгл.).

Фокус овог рада усмерен је ка практичном протоколу дестилације предности (AD), усаглашавању информација (IR) и појачавању приватности (PA) за овај специфичан, реалистичан сателитски сценарио. За разматрање дестилације предности, неопходна је претпоставка да Ева има бољу опрему него легитимни учесници, из чега следи да је  $p_A > p_E$  и  $p_B > p_E$  (у супротном Алиса и Боб имају

предност).

Дефинишемо максималну дужину тајног кључа (*secret-key rate*, енгл.) од  $A$  и  $B$ , респективно, према  $E$  и означавамо са  $S(A;B|E)$  – то је максимална дужина са којом Алиса и Боб могу да генеришу најдужи кључ у комуникацији преко несигурног јавног канала.

Важи следеће:

$$S(A;B|E) \geq \{I(A;B) - I(A;E), I(B;A) - I(B;E)\}. \quad (6.1)$$

Доња граница није уска, што представља довољан услов за постојање информационо теоретског протокола за размену кључа. У следећем параграфу приказано је на који начин Алиса и Боб могу појачати аутентичност јавног канала како би стекли предност над Евом тј. на који начин они полазе из  $I(A;B) \leq I(A;E)$  и  $I(A;B) \leq I(B;E)$ , да би се после одређене комуникације путем јавног канала, дошло до  $I(A;B|C) > I(A;E|C)$  или  $I(A;B|C) > I(B;E|C)$ , где  $C$  представља случајну променљиву [21].

## 6.4 Протокол дестилација предности

У овом поглављу описани су познати протоколи дестилације предности који су засновани на претходно описаном сценарију.

### 6.4.1 Протокол понављања

Протокол понављања (*repetition code protocol*, енгл.) приказан је у [19]. Сваки пут када Алиса хоће да пошаље информациони бит  $R$  Бобу, она генерише  $N$ -битску репетитивну кодну реч  $\underline{R} = (R, R, \dots, R)$ , и шаље  $\underline{R} + \underline{A} = (R + A_1, R + A_2, \dots, R + A_N)$  путем јавног канала Бобу. Боб рачуна  $\underline{R} + \underline{A} + \underline{B} = (R + A_1 + B_1, R + A_2 + B_2, \dots, R + A_N + B_N)$ , и прихвата  $R$  ако и само ако је кодна реч једнака, све нуле (0) у овом случају је  $R=0$ , или су све јединице (1) у том случају претпостављамо да је  $R=1$ . Боб јавља Алиси кроз јавни канал да ли је прихватио  $R$ .

Почетна узајамна вероватноћа грешке између Алисе и Боба у примљеном низу са сателита  $\underline{A}$  и  $\underline{B}$  је:  $\epsilon_0 = p_A + p_B - 2p_A p_B$ . Сагласно са протоколом, Алиса и Боб прихватају бит само када је  $\underline{A} \oplus \underline{B} = \underline{0}$  или  $\underline{1}$ , са вероватноћом грешке  $\epsilon_0^N + (1 - \epsilon_0)^N$ . Са вероватноћом  $1 - \epsilon_0^N - (1 - \epsilon_0)^N$ , не добијају ништа. Другим речима, са вероватноћом  $\epsilon_0^N + (1 - \epsilon_0)^N$  они филтрирају један бит са  $N$ -иницијалног низа. Апостериори битска вероватноћа грешке између филтрираних битова дата је:

$$\beta = \frac{\epsilon_0^N}{\epsilon_0^N + (1 - \epsilon_0)^N}. \quad (6.2)$$

Да би смо израчунали Евину очекивану вероватноћу грешке користимо следеће формуле:

$$q_A = 1 - p_A;$$

$$\begin{aligned}
q_B &= 1 - p_B; \\
q_E &= 1 - p_E; \\
\alpha_{00} &= q_A q_B q_E + p_A p_B p_E; \\
\alpha_{01} &= q_A q_B p_E + p_A p_B q_E; \\
\alpha_{10} &= q_A p_B q_E + p_A q_B p_E; \\
\alpha_{11} &= q_A p_B p_E + p_A q_B q_E;
\end{aligned} \tag{6.3}$$

Када Алиса шаље  $\underline{R} + \underline{A}$  Бобу преко јавног канала, Ева прислушкује пренос и може да рачуна  $\underline{R} + \underline{A} + \underline{E}$  користећи свој низ  $\underline{E}$ . Уколико  $p_\omega$  означава вероватноћу да је примљени вектор (кодна реч) одређене Хамингове тежине  $\omega$ ,  $0 \leq \omega \leq N$ , након што је Боб прихватио кодну реч, онда је  $p_\omega = \alpha_{00}^{N-\omega} \alpha_{01}^\omega + \alpha_{10}^{N-\omega} \alpha_{11}^\omega$ . Евина најбоља стратегија је да погађа,  $R = 0$  када је тежина од  $\underline{R} + \underline{A} + \underline{B}$  (стриктно) мања од  $\lfloor N/2 \rfloor$  и  $R = 1$  у супротном. Следи да је Евина вероватноћа грешке у односу на Алисин дестилован низ дата формулом:

$$\gamma = \frac{1}{\epsilon_0^N + (1 - \epsilon_0)^N} \sum_{\omega=\lfloor \frac{N}{2} \rfloor}^N \binom{N}{\omega} p_\omega \tag{6.4}$$

Доњу границу *secret-key rate* одређујемо протоколом понављања. После извршења протокола, заједничка информација између Алисе и Боба је  $I_B = 1 - h(\beta)$  док је заједничка информација између Алисе и Еве дата формулом:

$$I_E = \sum_{\omega=0}^N \binom{N}{\omega} \frac{p_\omega}{\epsilon_0^N + (1 - \epsilon_0)^N} \left[ 1 - h\left(\frac{p_\omega}{p_\omega + p_{N-\omega}}\right) \right]. \tag{6.5}$$

Из формуле 5.1 следи да *secret-key rate* задовољава услов:

$$S(A;B||E) \geq r \cdot (I_B - I_E), \tag{6.6}$$

где кофицијент  $r = [(1 - q_A q_B - p_A p_B)^N + (q_A q_B - p_A p_B)^N] / N$  рефлектује умањење бита за Алису и Боба (од  $N$ -бита прихвата се само 1 ако је кодна реч примљена). За  $N$  довољно велико,  $I_B$  биће веће од  $I_E$ , па ће  $\beta$  бити мања од  $\gamma$  и *secret-key rate*  $S(A;B||E)$  је строго позитиван за свако  $p_E > 0$ .

Обзиром да је  $r$  важан параметар у процени извршења појединости протокола дестилације предности и усаглашавања информација, дата је формална **дефиниција**:

Уколико је  $n$  дужина Алисиног и Бобовог оригиналног низа, где је Бобов низ добијен емитовањем Алисиног низа кроз BSC са вероватноћом грешке  $p$ , и уколико је  $Q$  бочна информација коју Алиса и Боб размењују кроз јавни комуникациони канал за време AD/IR протокола. Протокол се завршава тако што Алиса добија низ  $\underline{A}'$  и Боб  $\underline{B}'$  [21].

Уколико је  $\beta$  апостериори вероватноћа грешака између  $\underline{A}'$  и  $\underline{B}'$  и уколико  $I(\underline{A}'|Q)$  означава информацију коју има Ева у вези  $\underline{A}'$  знајући  $Q$ , онда је брзина информација (*information rate*, енгл.) у протоколу одређена формулом:

$$R_\beta(p) = 1 - I(\underline{A}'|Q)/n.$$

Ако Алиса и Боб одбацују бите из њихових низова, да би надокнадили одлив информација према Еви због њихове комуникације путем јавног канала, њихови низови се скраћују после IR протокола. Према томе, информацијска брзина (*information rate*, енгл.) је дужина крајњег исправљеног низа подељена са дужином оригиналног низа.

Уопштеност се не губи уколико се претпостави да је Боб онај који увек исправља различитост (грешке) између свог и Алисиног низа.

Циљ AD/IR протокола је да  $p$  тежи 0 а да, истовремено важи да је  $R_o(p)$  максимално. За веће  $R_o(p)$  протокол је квалитетнији. За количину размењених информација путем јавног канала AD/IR доња граница је  $H(\underline{A}|\underline{B}) = n \cdot h(p)$ , при чему је  $h(p) = -p\log(p) - (1-p)\log(1-p)$ , што означава ентропију бинарне функције. Из наведеног следи да је горња граница за  $R_o(p)$   $1-h(p)$ .

Вероватноћа да је  $A_i \neq B_i$ ,  $1 \leq i \leq n$ , описује се изразом  $\epsilon_0$ , па је информацијска брзина репетитивног протокола одређена формулом:

$$R_\beta(\epsilon_0) = r = \frac{\epsilon_0^N + (1-\epsilon_0)^N}{N} \quad (6.7)$$

при чему је  $N$  дужина репетитивног кодовања, а  $\beta$  узајамна грешка након извршене размене бита [21].

#### 6.4.2 Итеративни протокол

Репетитивни код протокол има особину да, када се  $N$  повећава,  $\beta$  се смањује брже од  $\gamma$ . Из наведеног следи да постоји такво  $N_0$  да је  $\beta < \gamma$  када је  $N \geq N_0$ . Односно, кад  $N$  расте,  $R_\beta(\epsilon_0)$  опада експоненцијално у односу на  $N$ . Репетитивно кодирање се показало као неефикасан протокол за размену бита (или најмању брзину протока информација). Овај случај настаје када је  $p_E$  много мање од  $p_A$  и  $p_B$ , јер кодна реч веће дужине омогућава да Алиса и Боб добију већу предност над Евом. За побољшање перформанси протокола Маурер предлаже итеративни протокол [13]. Сваки итеративни протокол садржи неколико рунди, а свака рунда користи репетитивни код протокол са крајом дужином кодне речи  $b$ . Алисин и Бобов низ се скраћује после сваке рунде и њихови низови постају све сигурнији. Показано је у [13] да  $k$ -рунда итеративног протокола са дужином кодне речи  $b$  одговара  $N=b^k$  репетитивном код протоколу, прихватањем овог итеративног протокола долазимо до веће *information rate* од репетитивног протокола. Формална дефиниција итеративног протокола приказана је у тексту који следи.

Дефиниција:  $k$ -рунда итеративни протокол са кодном речи дужине  $b$  за

дестилацију предности, тј.  $[b,k]$  итеративни протокол је протокол који:

- се састоји од  $k$ -рунди,
- у свакој рунди се користи репетитивни-код протокол, при чему се крајњи резултат (добити бити) користе за следећу рунду.

Према дефиницији, репетитивни код протокол дужине  $N$  је  $[N,1]$  итеративни протокол.

Теорема која следи описује опште особине итеративног протокола  $[b,k]$ .

Теорема: За претходно наведени сценарио, уколико је  $\epsilon_0 = p_A + p_B - 2p_A p_B$  која означава почетну вероватноћу грешке, тада  $[b,k]$  итеративни протокол задовољава следеће:

1. Боб добија нови дестиловани низ са вероватноћом грешке

$$\beta = \frac{\epsilon_0^{b^k}}{\epsilon_0^{b^k} + (1 - \epsilon_0)^{b^k}} \quad (6.8)$$

заједничка информација између сваког бита Алисиног новог низа и Бобовог низа одговара вредности  $I_B = 1 - h(\beta)$ ;

2. користећи најбољу стратегију Ева добија нови низ са вероватноћом грешке

$$\gamma = \frac{1}{\epsilon_0^{b^k} + (1 - \epsilon_0)^{b^k}} \sum_{\omega=\lfloor \frac{b^k}{2} \rfloor}^{b^k} \binom{b^k}{\omega} p_\omega \quad (6.9)$$

са  $p_\omega = \alpha_{00}^{b^k - \omega} \alpha_{01}^\omega + \alpha_{10}^{b^k - \omega} \alpha_{11}^\omega$ , где су  $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$  дефинисане у поглављу 5.2.1. Заједничка информација између сваког бита Алисиног новог низа и Евиног новог низа добијамо

$$I_E = \sum_{\omega=0}^{b^k} \binom{b^k}{\omega} \frac{p_\omega}{\epsilon_0^{b^k} + (1 - \epsilon_0)^{b^k}} \left[ 1 - h\left(\frac{p_\omega}{p_\omega + p_{b^k - \omega}}\right) \right] \quad (6.10)$$

3. *information rate* протокола одређујемо по формули

$$R_\beta(\epsilon_0) = \frac{1}{b^k} \frac{\epsilon_0^{b^k} + (1 - \epsilon_0)^{b^k}}{\prod_{i=1}^{k-1} (\epsilon_0^{b^i} + (1 - \epsilon_0)^{b^i})^{b-1}} \quad (6.11)$$

при чему *secret-key rate* између Алисе и Боба у односу на Еву задовољава

$$S(A; B || E) \geq R_\beta(\epsilon_0) \cdot (I_B - I_E). \quad (6.12)$$

### 6.4.3 Bit pair итеративни протокол

*Bit pair iteration* протокол је предложио Гендер. Састоји се од неколико рунди које се извршавају на бинарни низ Алисе и Боба. У свакој рунди Алиса и Боб користе следеће кораке:

1. Препроцесирање: Алиса и Боб деле низове на парове битова.
2. Рунда  $i$ : Алиса шаље Бобу *parity* бит (бит парности) за сваки пар битова преко јавног канала. Боб рачуна *parity* бит за сваки пар битова свог низа и упоређује их са *parity* битом Алисиног низа. Ако се *parity* битови поклапају, Боб шаље обавештење ОК преко јавног канала. Први бит пара се одбацује да се надокнаде „процуреле“ информације према Еви са *parity* битом. Преостали бит од пара се враћа за следећу рунду. Ако се парности разликују, пар битова се одбацује у потпуности.
3. Враћени битови (који нису одбачени) формирају улазни низ за следећу рунду.

У свакој рунди протокола, Алиса и Боб прихватају бит само ако им се парност за пар битова подудара. У том случају, шаблон грешке може бити (0,0) или (1,1). Једноставно се увиђа да након рунде  $i$ , Алиса и Боб прихватају један бит са вероватноћом  $\epsilon_{i-1}^2 + (1 - \epsilon_{i-1})^2$ . Бобова вероватноћа грешке опада са  $\epsilon_{i-1}$  на  $\epsilon_i = \frac{\epsilon_{i-1}^2}{\epsilon_{i-1}^2 + (1 - \epsilon_{i-1})^2}$ , па  $k$ -round *bit pair iteration* протокол постаје  $[2, k]$  *iteration* протокол са *information rate*  $R_\beta(\epsilon_0)[2, k]$ . Има исти ефекат као репетитивни код протокол, међутим са већом продуктивношћу у односу на *information rate*. У свакој следећој рунди Евина предност је смањена иако у почетној фази има више информација од Боба које су везане за Алисин низ.

Доња граница *secret-key rate* је изведена у [19]

$$S(X; Y|Z) \geq R_\beta(\epsilon_0)[2, k] \cdot (I_B - I_E), \quad (6.13)$$

где је *information rate*

$$R_\beta(\epsilon_0)[2, k] = \frac{1}{2^k} \frac{\epsilon_0^{2^k} + (1 - \epsilon_0)^{2^k}}{\prod_{i=1}^{k-1} (\epsilon_0^{2^i} + (1 - \epsilon_0)^{2^i})^{2^i}} \approx \frac{\epsilon_0^2 + (1 - \epsilon_0)^2}{2^k}. \quad (6.14)$$

Обзиром да је *information rate* репетитивног код протокола дужине  $2^k$ , и износи  $R_\beta(\epsilon_0)[2^k, 1] = \frac{\epsilon_0^{2^k} + (1 - \epsilon_0)^{2^k}}{2^k}$  закључује се да је  $R_\beta(\epsilon_0)[2, k] \gg R_\beta(\epsilon_0)[2^k, 1]$ . Као што је описано у претходном параграфу,  $[2, k]$  итеративни протокол, тј. *Bit pair iteration* протокол показао се као најпродуктивнији протокол [21].

## 6.5 Каскадни протокол усаглашавања информација

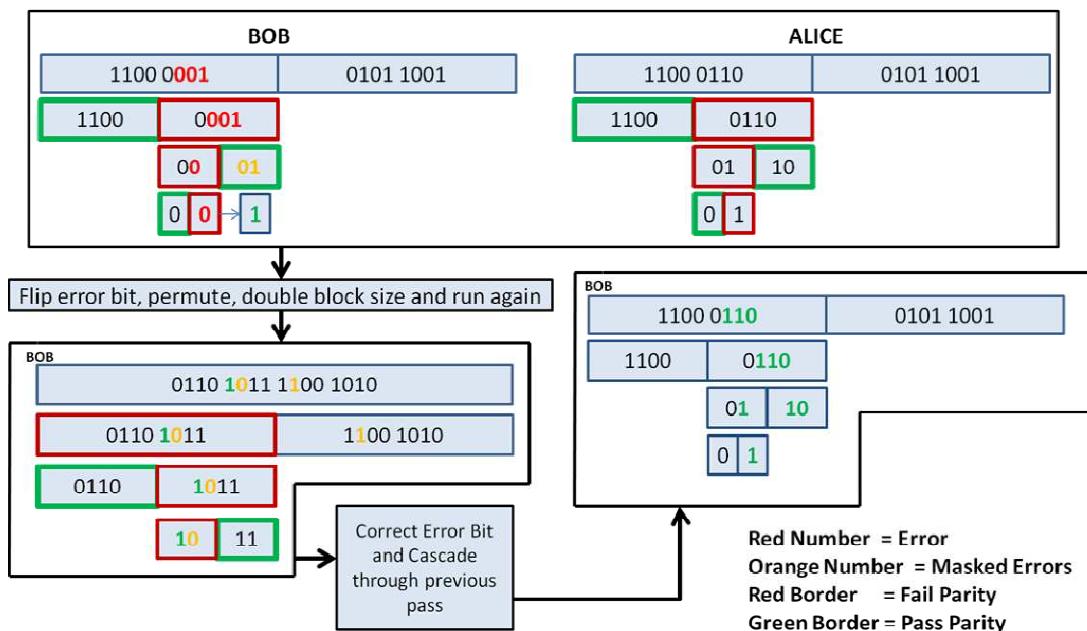
Протокол каскадног решавања грешака је модификација протокола који су објавили Бенет, Бесет, Бресард, Салваил и Смолин (BBBSS), а предложио Бенет 1991. године. BBBSS је коришћен као протокол за интерактивну детекцију и корекцију грешака који су аутори назвали Бинарни. BBBSS је користио модификовани BB84 QKD протокол користећи базу кружне поларизације уместо дијагоналне базе. Осим замене база, BBBSS је функционисао као имплементација BB84.

*The Binary reconciliation protocol* (протокол бинарне претраге за исправљање грешака) је коришћен током корака решавања грешака за исправљање грешке које су унете у квантни канал преко шума и прислушљивача. Након што Алиса и Боб добију процену грешке која је заснована на делу просејаног кључа (*sifted key*, енгл.) и утврђују да ли је праг грешке прескочен. Када стопа грешке превазиђе праг неуспеха, Алиса и Боб започињу прве размене и користе раније одређене случајне пермутације, примењујући их на шифтоване битове кључа (*row key* корак). Сврха пермутације је раздвојити погрешне случајне битове и одвојити узастопне грешке. У следећем кораку Алиса и Боб поделе све шифтоване битове кључа на блокове од  $N/2$  бита који зависе од процењене стопе грешака, са циљем да број грешака по блоку буде што мањи. Након тога Алиса и Боб користе класичне канале да упореде парове блокова. За блокове у којима се парови не слажу, мора да постоји непаран број грешака како се паран број грешака не би међусобно маскирао. Блок је онда подељен на пола у два мања блока дужине  $N/4$ , након чега се изводи још једна провера парова на првом подблоку. Пошто сигурно постоји бар једна грешка у једном од подблокова, паритет једног подблока открива где је грешка настала. Ако постоји паритет у првом подблоку, онда је грешка настала у другом подблоку. Подблок са грешком се даље дели у мање подблокове и поново се проверава паритет док се не утврди грешка у биту, затим се грешка исправља.

Потпуни број размењених упарених бита одређује се као  $\log_2(N/2)$ , при чему је  $N$  број бита у првом блоку. Пошто се размена упарених бита одвија на класичном каналу, где Ева може да пасивно прислушкује, претпоставља се да упарени битови дају Еви информације о тајном кључу. Одбацујући задњи бит у сваком блоку и подблоку који је укључен у проверу парова, информација коју Ева добија о кључу је смањена. Обзиром да број парних грешака не може бити детектован, кључ се поново пермутује и протокол бинарне провере се поново пушта у рад. Да би се смањио број одбачених бита после провере парова, бинарни протокол користи додатни процес током наредних пролазака, и искористи мањи број бита. Паритет случајног дела шифтованог кључа је калкулисан и упоређен. Делови који не прођу проверу паритета су даље подељени и проверени коришћењем бинарне претраге. Аутори BBBSS-а су препоручили 20 случајних провера паритета, после чега Алиса и Боб претпостављају да су њихови добијени кључеви идентични.

Бресард и Салваил су 1994. године направили каскадни протокол као побољшање протокола бинарне претраге за исправљање грешака, у односу на битове који процуре кроз део *reconciliation* (помирење низова). Повећањем корака процесуирања протокола аутори су тврдили да су унапредили проблем одлива информација и смањење „цурења“ бита на теоретски минимум који је потребан да се оствари помирење. Операција каскаде је готово идентична Бинарном протоколу осим тога што су локације и вредности грешака у биту задржане за коришћење у наредним пролазима. Информација о грешкама у биту је коришћена у наредним

пролазима тако да алгоритми могу да исправе све непарне грешке и онда изведу каскаду уназад кроз претходне пролазе, како би нашли парне грешке које су у претходним корацима биле маскиране. Детаљни опис каскаде приказан је у тексту који следи. На Слици 12. приказан је каскадни модел исправљања грешака.



Слика 12 Каскадни модел исправљања грешака

Протокол каскадног исправљања грешака започиње проценом стопе грешака анализе шифтованих кључева. Анализа је направљена као у BBSS, са делом шифтованог кључа који се упоређује кроз класичне канале између Алисе и Боба. Алиса и Боб након тога поделе своје шифтоване кључеве у блокове величине која зависи од стопе грешака. Аутори су емпиријски одредили почетну величину блока  $N_1$  која износи  $0.73/p$  при чему је  $p$  процењена грешка. Уколико је стопа грешака 0.01, онда је  $N_1=73$  или приближно 1 грешка по блоку. Тада паритете блокова упоређују Алиса и Боб путем јавног канала, а Бинарни протокол је коришћен за исправљање грешака. Последњи бит сваког блока се у том делу комуникације не одбацује. Такође, све информације о локацији грешака се чувају. Након изведене пермутације шифтованог кључа, почиње нови пролаз. Међутим, за разлику од BBSS-а, величина блока је повећана на  $N_2=2N_1$ , и изводи се још једна Бинарна претрага. Све грешке пронађене у овом пролазу настају као резултат две или више парних грешака, које су биле маскиране у претходном пролазу. Користећи информацију о локацији грешке из претходног пролаза алгоритам Каскаде подразумева враћање на најкраћи блок, који је садржао исправљену грешку при првом пролазу и дели је да би нашао скривену грешку. Протокол наставља рад на исти начин са свим нађеним грешкама, изводећи каскаде за раније пролазе, како би били пронађени исправљени маскирани битови. Након одређеног броја пролаза, пермутација и каскада, протокол завршава са ниском вероватноћом и резултујућом малом грешком.

После представљања Каскаде, објављено је и неколико радова са покушајима унапређивања алгоритма и смањења одлива информација преко јавног канала.

Сугимото и Јамазаки објавили су напредну верзију са циљем смањења броја битова који „цури“, приметивши да је каскада јако ефикасна у исправљању грешака у прва два пролаза, али са великим смањењем ефикасности наспрам информације која „исцури“ са осталим пролазима. У суштини, аутори су успели да емпиријски одреде да је, у просеку, у првом пролазу исправљено око 50% преосталих грешака. Каскада из грешке у пролазу број 2 исправља око 25% преосталих грешака. Уместо да настави високо интерактивне пролазе Каскаде, аутори су предложили да се трећи пролаз пребаци на потврђену бисектовну методу која се користи у BBBSS за исправку преостале грешке. Ова оптимизација је омогућила модификованом Каскадном алгоритму да буде остварен ближе теоретском од оригиналног протокола Каскада зато што мањи број битова „цури“ у јавни канал за време каснијих пролаза.

Друге модификације Каскаде укључују корак пермутације протокола. Пермутација пре сваког пролаза је намењена да рашири грешке не би ли смањила могућност да те грешке остану прикривене током провере парности. Чен је 2000. године препоручио да се случајне пермутације замене *interleaving* техником која је специјализована за смањење или елиминацију групе грешака из *burst error*. Чен је емпиријски показао да се одлив информација може смањити тако да је упоредив са стандардном Каскадом. У току 2002. године, Нгујен је предложио још једну модификацију метода пермутације која се користи у Каскади. Предложио је да се створи нови блок који садржи први бит из сваког претходног блока, а други блок са другим битом из сваког претходног блока итд., све док сваки бит не буде пребачен у нове блокове. Након тога се Каскада даље одвија по устаљеном режиму. Овај метод се показао као побољшање операције Каскаде.

Накасис је предложио потпуну модификацију и алгоритма Каскаде и корака *reconciliation* грешака. У тој модификацији предложен је нови метод који укључује корак процењивања грешака који се најчешће изводи на почетку *reconciliation* грешака. Уместо постојећег, шифтован кључ је подељен, и паритети су проверавани док одређени број подблокова не покаже грешке у паритету. Користећи више различитих калкулација и емпиријске примере података, аутори су направили табелу могућег броја измењених битова користећи Бернулијеву вероватноћу дистрибуције грешака. Упоредјујући вероватноће са грешкама у паритету, аутори су успели да одреде могуће преостале грешке после сваког пролаза и да искористе 7-битне *Hamming* кодове да исправе грешке, након што се процени да је остао мали број грешака. У 2006. години показано је да је теоретску горњу границу за одлив информација могуће прекорачити при експериментисању. Рас и Колмитзер су покушали да унапреде ефикасност и одлив информација Каскаде 2009. године, заменивши Каскадну дуплирану величину блока динамичном методом која користи Бајезинску статистику и информације из претходних извршења да би алгоритму дали „способност да учи“. Капраро и Окипинти су 2007. године покушали да унапреде перформансе учења каскаде направивши паралелну имплементацију за прераду која је фокусирана на максимизирање стопе кључа у хардверском подешавању. Боугатас, Ијед и Резиг су се фокусирали на интеграцију појачавања приватности унутар протокола Каскаде изучавањем методе „интерактивног одбацивања“ да максимизирају и ефикасност *reconciliation* и робусност против прислушкивања [22].

## 6.6 Појачавање приватности

Појачавање приватности (*privacy amplification*, енгл.) је неопходно када две стране желе да филтрирају тајни кључ из великог заједничког али делимично тајног

низа. Идеју је први пут представио Бенет [23]. Она служи као темељ у информационо теоријском тајном договору кључа и квантном протоколу договора тајног кључа.

Уколико се претпостави да Алиса и Боб деле  $n$ -битски низ  $S$ , при чему непријатељ Ева има неке од информација, које означавамо са  $Z=z$ . Онда је стандардни начин за реализацију појачавања приватности да Алиса насумице изабере функцију из одређене класе хеш функција и пошаље опис одабране функције Бобу преко јавног канала. Алиса и Боб рачунају хеш њиховог делимично тајног низа  $S$  док се Евина делимична неизвесност у вези низа  $S$  развија у готово потпуну неизвесност око коначног тајног кључа.

Као *information reconciliation* и *privacy amplification* такође укључује јавну расправу између Алисе и Боба. Значајан део метода које су предложене користи савршени аутентичан јавни канал (нпр. савршенство омогућено техником кодова за исправљање грешака). Као резултат сви, укључујући и Еву, могу да сазнају цео садржај тих преноса преко јавног канала. С друге стране, пренос преко јавног канала не може бити измењен или потиснут од стране Еве, без да буде детектован. Са таквим каналом, Ева може да спроведе искључиво пасиван напад. Дужина  $r$  коначног дестилованог тајног кључа је горња граница Евине (Ренијева) ентропије  $S$  тј.  $r \leq H_2(S|Z = z)$ .

Аутентичност је могуће осигурати физичким карактеристикама појединих канала. Нпр. новине су често предложене у шифарским системима са јавним кључем и системима за дигитално потписивање, за откривање јавних кључева. Међутим, користећи новине за јавну расправу је недовољно ефикасан да би био практичан.

Разумљивија претпоставка је да јавни канал није аутентичан, тј. Ева такође може да примени активан напад. Проблем који се у овом случају јавља је како постићи аутентичност преко неаутентичног јавног канала. Предложена су два примера како реализовати *privacy amplification* преко неаутентичног канала.

Пример 1: Алиса и Боб деле додатни (али краћи) тајни кључ поред делимичног тајног низа  $S$ . Алиса и Боб користе тајни кључ за безусловну сигурну аутентикацију током *privacy amplification* процеса.

Пример 2: Само је делимично тајан низ  $S$  доступан Алиси и Бобу. Користе један део низа  $S$  за безусловно сигурну аутентикацију и други део за дестилацију тајни.

Први пример се заснива на теорији безусловне аутентикације. Алиса и Боб користе краћи тајни кључ поред делимично тајног низа. Краћи тајни кључ може да се користи једном (као *one-time pad*, енгл.) да осигура безусловну аутентичност за појачавање приватности. Овим примером појачавања приватности као резултат може да се постигне најдужи тајни кључ, део добијеног кључа, који се затим може користити као замена за кратки тајни кључ, током наредне аутентикације. Постоји могућност да противник активно учествује у јавну комуникацију између Алисе и Боба тако да Алиса и Боб могу да исцрпе целу своју понуду провере идентитета, без добијања новог тајног кључа. Са оваквим приступом противника, да активно учествује, у првом примеру не може се извршити адекватна аутентикација.

У другом примеру, аутентикација се постиже тако што се жртвује део тајног низа који поседују Алиса и Боб. Резултати показују да је једносмерни протокол преноса за појачавање приватности против активног напада могућ ако је Евина мин-ентропија  $H_\infty(S|Z = z)$ , од  $S$  да је већи од  $2n/3$ .

Пример 3: Алиса и Боб деле два независна низа која су делом тајна  $S_1$  и  $S_2$ . Нпр.  $S_1$  користимо за аутентикацију а  $S_2$  за појачавање приватности [21].

За потребе овог рада претпоставиће се да Алиса и Боб комуницирају преко аутентичног канала, за појачавање приватности користи се универзална класа функција  $H_1$  (*universal hash functions*, енгл.) [24].

Дефиницијом: претпоставимо да је  $A = \{0, 1, \dots, a - 1\}$  и  $B = \{0, 1, \dots, b - 1\}$ . Узмимо да је  $p$  прост број  $p \geq a$ . Узмимо да је  $g$  било која функција из  $Z_p$  за  $B$ , која треба да што приближније преслика исти број елемената од  $Z_p$  у сваки елемент  $B$ . Формално захтевамо  $|\{y \in Z_p \mid g(y) = i\}| \leq \lceil p/b \rceil$  за свако  $i \in B$ . Природан избор за  $g$  је остатак по модулу  $b$ . Када је  $b = 2^k$  за неко  $k$ , то износи узимање последњих  $k$  битоа у бинарном представљању од  $y$ .

Узмимо да су  $m$  и  $n$  елементи од  $Z_p$  са  $m \neq 0$ . Дефинишемо  $h_{m,n}: A \rightarrow Z_p$  од  $h_{m,n}(x) = (mx + n) \bmod p$ . Онда дефинишемо  $f_{m,n}(x) = g(h_{m,n}(x))$ . Класа  $H_1$  је скуп  $\{f_{m,n} \mid m, n \in Z_p \text{ и } m \neq 0\}$ .

## 7. Симулатор

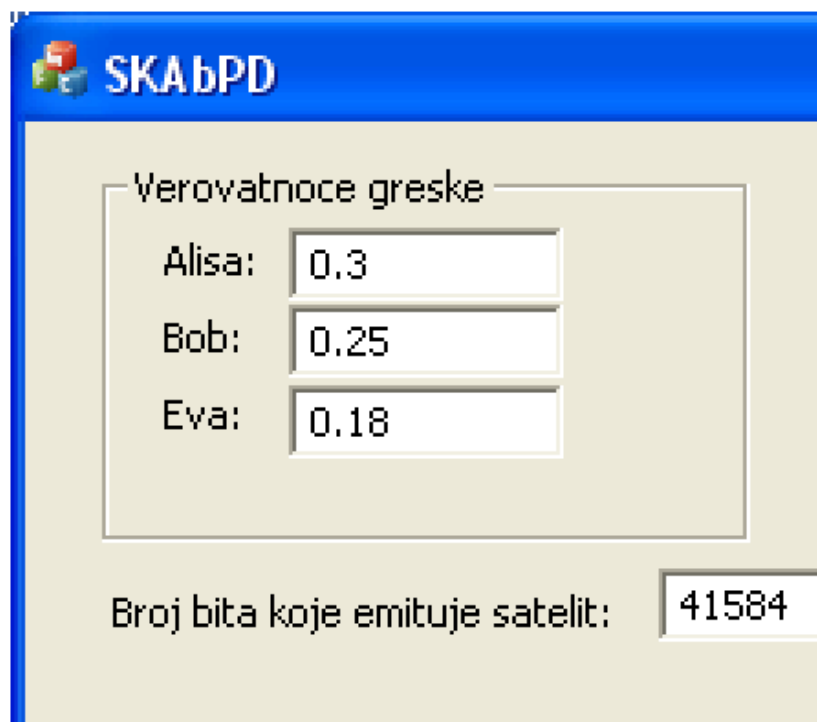
За потребе овог рада је израђен симулатор протокола за дистрибуцију криптолошких кључева преко јавних комуникационих канала. У симулатору су имплементиране све фазе протокола.

На Слици 13. дат је графички приказ интерфејса.

Слика 13 Графички приказ интерфејса

Симулатор је развијен у програмску језику C++, коришћењем *Microsoft Visual Studio 2010* платформе и применом MFC библиотеке за графички приказ интерфејса. У даљем раду је објашњен сваки блок симулатора.

На почетку симулације потребно је поставити почетне параметре (Слика 14). Прво се дефинишу вероватноће грешке за сва три канала односно учесника (Алиса, Боб и Ева). То представља грешке у низовима бита примљених са сателита. Потом се уноси параметар за дужину низа који се прима са сателита, односно број бита који емитује сателит износи 41584.



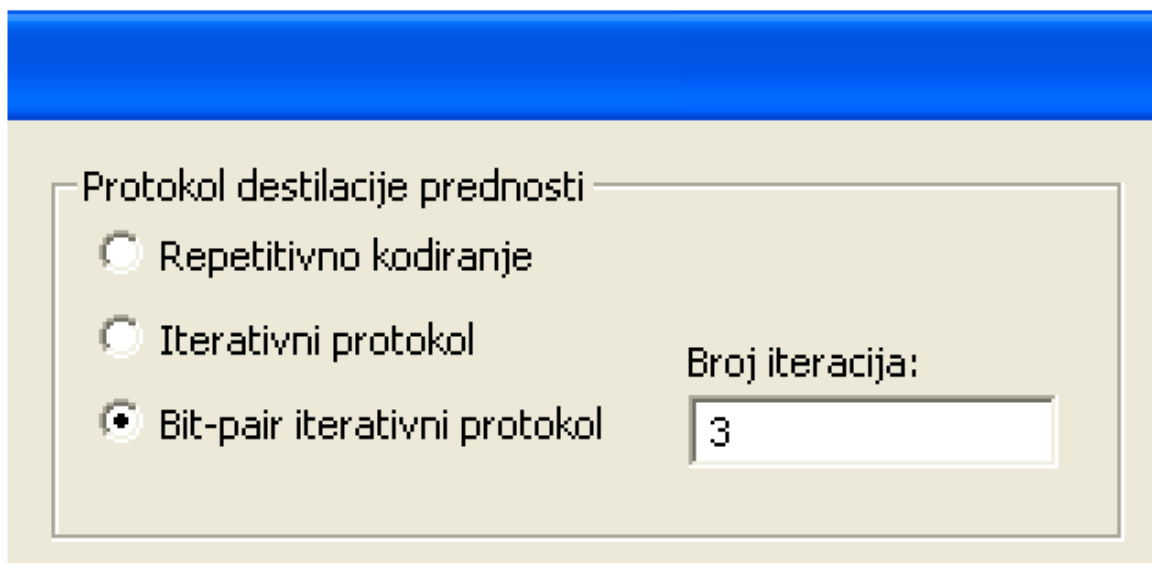
The screenshot shows a software window titled "SKAБPD" with a blue header bar. Inside the window, there is a section titled "Verovatnoce greske" (Probability of error) containing three input fields: "Alisa:" with the value "0.3", "Bob:" with the value "0.25", and "Eva:" with the value "0.18". Below this section, there is a label "Broj bita koje emituje satelit:" (Number of bits emitted by the satellite) followed by an input field containing the value "41584".

Слика 14 Иницијална (почетна) фаза

Прва фаза протокола је протокол дестилације предности. За извршење прве фазе дестилације предности на располагању су три могућности (Слика 15):

- Протокол репетитивног кодирања
- Итеративни протокол
- *Bit-pair* итеративни протокол.

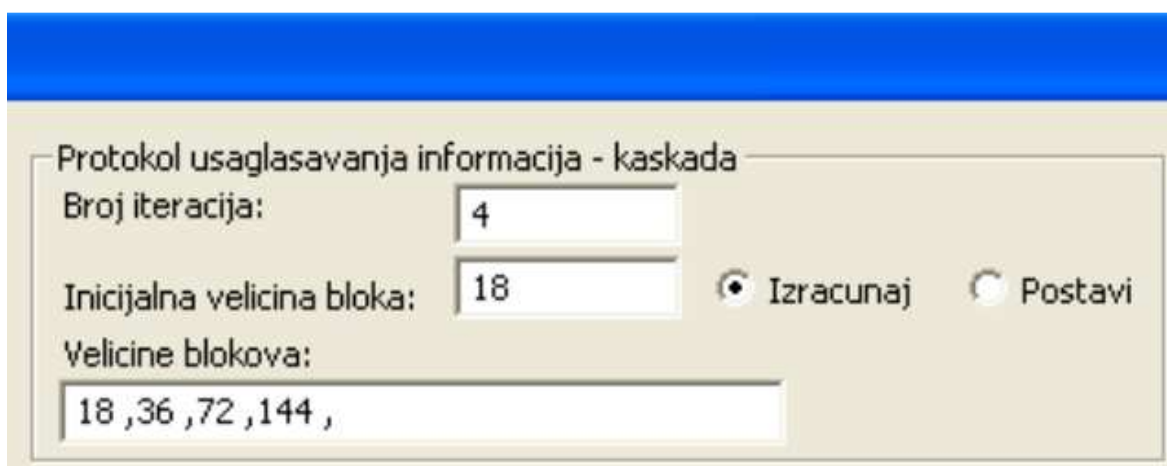
За сваки протокол потребно је поставити почетне параметре, тј. број итерација. При избору Репетитивног кодирања дефинише се једна итерација. Дужина кодне речи се поставља произвољно. Итеративни протокол такође захтева постављање броја итерација и дужине кодне речи, при чему су обе вредности произвољне. Код *Bit-pair* итеративног протокола број итерација је произвољан, док је кодна реч фиксне дужине.



Слика 15 Протокол дестилације предности

У другој фази протокола имплементиран је каскадни протокол за исправљање грешака, односно протокол за усаглашавање информација (Слика 16). Потребно је поставити параметар за број итерација, односно рунди. Препоручен број рунди је 4. Након извршења све четири рунде велика је вероватноћа да су низови усаглашени, што је објашњено у поглављу 5.4.

Иницијална величина блока се може дефинисати произвољно или сам симулатор може поставити ову вредност. Након сваке извршене рунде величина блока се удвостручава. Нпр. ако је почетна вредност величине блока 18, у другој рунди ће износити 36, а у трећој и четвртој рунди 72 и 144, респективно.



Слика 16 Протокол усаглашавања информација

На Слици 17. приказане су очекиване вредности (прва колона) добијене применом наведених формула, као и вредности истих параметара добијене

симулацијом (друга колона).

| Očekivane vrednosti - dobijene iz formula      |                    | Vrednosti dobijene simulacijom |
|------------------------------------------------|--------------------|--------------------------------|
| Alisa - greska u prijemu:                      | 0.3                | 0.297325894574836              |
| Bob - greska u prijemu:                        | 0.25               | 0.252765486725664              |
| Eva - greska u prijemu:                        | 0.18               | 0.184734513274336              |
| Uzajamna greska Alisa - Bob ( $\beta$ ):       | 0.0375531758838199 | 0.0389140271493213             |
| Uzajamna greska Alisa - Eva ( $\gamma$ ):      | 0.15035118609705   | 0.266968325791855              |
| Uzajamna informacija po bitu $I_B$ :           | 0.769041140663824  | 0.76270930445985               |
| Uzajamna informacija po bitu $I_E$ :           | 0.664299072816627  | 0.162919342778966              |
| $I_B - I_E$ :                                  | 0.104742067847197  | 0.599789961680884              |
| Brzina informacija ( Information rate - $r$ ): | 0.02703013481364   | 0.0265727202770296             |
| Brzina ključa ( Secret key rate ):             | 0.0028311922145691 | 0.0159380508767164             |
| Velicina deljenog niza:                        | 1124.0211260904    | 1105                           |
| Broj pogresnih bita Alisa-Bob:                 | 42.2105630452023   | 43                             |
| Broj pogresnih bita Alisa-Eva:                 | 168.997909505834   | 295                            |
| Potencijalna velicina tajnog ključa:           | 117.732297050644   | 662.767907657377               |

Слика 17 Очекиване вредности и вредности добијене симулацијом

У наставку је дато објашњење за сваки параметар приказан на симулатору:

1. Алиса - грешка у пријему: иницијално постављена вредност је 0.3, док се симулацијом добија вредност тако што се упореди добијени Алисин низ са оригиналним низом примљеним са сателита. За Бобову и Евину грешку у пријему користимо исту методу.
2. Узајамна грешка Алиса - Боб ( $\beta$ ): вредност из прве колоне се израчунава на основу формуле 6.8, док се вредност из друге колоне добија поређењем Алисиног и Бобовог низа добијених симулацијом.
3. Узајамна грешка Алиса - Ева ( $\gamma$ ): прва вредност следи из формуле 6.9, а вредност добијена симулацијом се постиже тако што се упореди Алисин низ са Евиним низом.
4. Узајамна информација по биту  $I_B$ : за прву вредност примени се формула  $I_B = 1 - h(\beta)$ , док се вредност из друге колоне добија убацивањем вредности из тачке 2 ( $\beta$  добијена симулацијом) у наведену формулу.

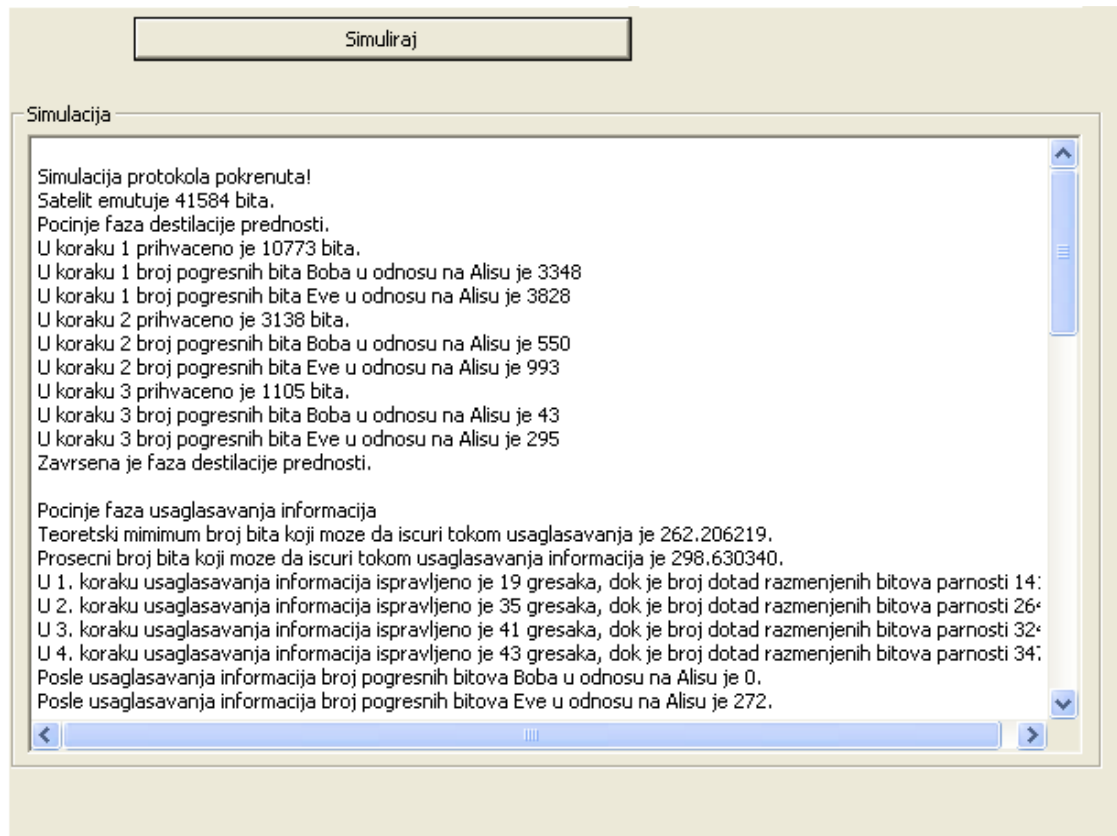
5. Узајамна информација по биту  $I_E$ : помоћу формуле 6.10 израчунава се прва вредност, док се вредност из друге колоне израчунава коришћењем добијене вредности  $\gamma$  (тачка 3.) у формули  $I_E = 1 - h(\gamma)$ .
6. Наредни параметар у табели се добија одузимањем вредности добијених у претходне две тачке ( $I_B - I_E$ ).
7. Брзина информација (*Information rate*): применом формуле 6.11 израчунава се брзина информација, док се друга вредност добија дељењем величине дељеног низа (тачка 9) са бројем бита емитованих са сателита.
8. Брзина кључа (*Secret key rate*): параметар из прве колоне се израчунава помоћу формуле 6.12, док се друга вредност израчунава коришћењем добијених вредности из симулације (брзина информација,  $I_B$  и  $I_E$ ).
9. Величина дељеног низа: добија се множењем параметра *information rate* са бројем примљених бита са сателита у иницијалној фази.
10. Број погрешних бита Алиса – Боб: узајамна грешка ( $\beta$ ) се множи са величином дељеног низа.
11. Број погрешних бита Алиса – Ева: узајамна грешка ( $\gamma$ ) се множи са величином дељеног низа.
12. Потенцијална величина тајног кључа: израчунава се множењем брзине кључа (тачка 8) са бројем бита емитованих са сателита.

Након извршења симулације добија се текстуални извештај приказан на Слици 18. који укључује све фазе протокола. За иницијалну фазу добија се обавештење да је симулација покренута и приказ броја емитованих бита са сателита.

У фази дестилације предности за сваки корак се исписују вредности за следеће параметре: број укупно прихваћених бита, број погрешних бита Боба у односу на Алису и број погрешних бита Еве у односу на Алису.

После фазе усаглашавања информација приказује се број погрешних бита Боба у односу на Алису, односно Еве у односу на Алису. Може се приметити да Ева увек има знатно већи број погрешних бита у односу на Алису, него што има Боб.

Последња фаза је појачавање приватности у којој се смањује Евина информација по биту о кључу. Бинарно је приказан тајни кључ договорен између Алисе и Боба, као и кључ који има Ева.



Слика 18 Симулација

## 8. Закључак

Први део рада приказује протоколе за установљивање кључа, који су засновани на дистрибуцији кључа, коришћењем симетричног шифровања. Описани протоколи укључују трећу страну од поверења. Такође, поједини протоколи користе неке од временских параметара, као што су: временски печат, секвенца бројева или случајно генерисане бројеве. Протоколи за дистрибуцију кључа који су засновани на симетричном шифровању, укључују две стране у комуникацији, и трећу страну од поверења са којом априорно деле по пар тајних кључева. Трећа страна од поверења има улогу центра за дистрибуцију кључева, за снабдевање сесијских кључева или као сервис за преношење кључева, који обезбеђује да изабрани кључ једне стране буде доступан другој страни.

У другом делу рада описани су системи јавних кључева. У асиметричним шифарским системима се користе различити кључеви за шифровање и дешифровање, јавни и тајни кључ, тако да кључ за шифровање може бити познат свима, а само онај који поседује кључ за дешифровање може дешифровати поруку. Међутим, захтев за великим капацитетом рачунарских ресурса код ових алгоритама утиче на карактеристике система у којима се примењују, тако да се не препоручује њихова примена за заштиту тајности информација у системима са великим протоком информација. Ово правило не оспорава, по аутоматизму, ове алгоритме, јер начин на који је уз коришћење оваквих алгоритама могуће остварити функције интегритета, аутентикације и непорецивости има предност над традиционалним техникама. У раду је описан RSA алгоритам. Приказан је Diffie-Hellmanov поступак размене кључа који омогућује учесницима, који нису познати једни другима, да размене симетрични тајни кључ преко небезбедног комуникационог канала. Размењени кључ се касније може користити за шифровање порука употребом симетричног шифарског система. Симетрични шифарски систем се користи ради уштеде времена за шифровање и дешифровање. Такође је описана инфраструктура са јавним кључевима и дато је поређење шифарских система са симетричним и асиметричним кључем.

Постоје два типа криптографске сигурности: рачунски сигурна и безусловно сигурна. Рачунски сигурна подразумева да је сигурност криптографског система заснована на тешко израчунљивим методама напада, док је безусловно сигурна заснована на немогуће израчунљивим методама напада. У овом раду дат је приказ различитих приступа размени тајних кључева за потребе сигурне комуникације између две стране са посебним освртом на информационо теоретски приступ.

Информационо теоретски приступ размени кључева показује како да се од делимично познатог дељеног низа битова дође до значајног краћег дељеног тајног кључа. Обрађен је Мауреров сателитски модел информационо теоретске размене кључева који се састоји из следећих фаза: дестилација предности, усаглашавање информација и појачавање приватности. Коришћена су три приступа дестилације предности: репетитивни протокол, итеративни протокол и *bit-pair* итеративни протокол. Развијен је симулатор протокола за дистрибуцију тајних кључева путем јавних комуникационих канала. Симулатор имплементира све фазе информационо теоретског протокола, односно Мауреровог протокола.

Проблем дистрибуције кључева је стално присутан у историји криптографије. Без обзира колико је у теорији криптографски алгоритам сигуран, поверљивост

његовог механизма може угрозити проблем дистрибуције кључа. На први поглед, питање дистрибуције кључа се чини тривијалним, међутим у криптографском систему је једна од најслабијих карика. Ако две стране размењују податке у безбедном окружењу, неопходно је да верују трећој страни од поверења, која дистрибуира кључеве што, у овом случају, постаје слаба карика у ланцу безбедности у односу на наведене. И поред тврдњи да је проблем дистрибуције криптолошких кључева нерешив, средином седамдесетих година прошлог века откривено је поуздано решење. Обзиром да је рачунарска техника преобразила примену криптографских алгоритама, чињеница је да је највећу промену у криптографији двадесетог века изазвао развој силицијумске технологије и техника за дистрибуцију кључева. Ово откриће сматра се највећим криптографским остварењем од изума моноалфabetске методе криптозаштите, која је једна од најраније откривених метода заштите порука, настала пре око две хиљаде година.

## Прилог 1: Протоколи за дистрибуцију тајних кључева преко јавних комуникационих канала

Главни проблем криптографије је пренос поруке  $M$  од пошиљаоца Алисе до примаоца Боба преко небезбедног комуникационог канала, тако да непријатељ Ева која има приступ овом каналу је у немогућности да добије било какву корисну информацију у вези поруке  $M$ .

Ово је класичан модел шифарског система који је представио Клод Шенон [25]. Ева има савршен приступ небезбедном каналу, према томе сматра се да је примила идентичну копију шифрата  $C$  као и што је примио легитимни учесник Боб, где је  $C$  добијен као функција отвореног текста  $M$  и заједничког тајног кључа  $K$ , Алисе и Боба.

Према Шенону шифарски систем је перфектан ако је шифрат статистички независан од отвореног текста, односно у информационо теоријском смислу шифрат не даје никакву информацију о отвореном тексту:

$$I(M; C) = 0.$$

Када се користи овакав систем за шифровање поруке  $M$ , нападач може само да погађа отворени текст без обзира што поседује шифрат  $C$ . На тај начин постављени услов апсолутне тајности имплицира да нападач не може ништа научити односно сазнати у вези отвореног текста на основу познатог шифрата.

Шенон је дао једноставан пример апсолутне тајне шифре познате као ОТР (*one-time-pad*, енгл.) која је потпуно непрактична за већину шифарских система у којима само краћи кључеви могу да се користе. Шенон је доказао песимистички резултат да апсолутна тајност може бити постигнута само уколико је кључ за шифровање исте дужине као и отворени текст  $M$  или већи:

$$H(K) \geq H(M). \quad (1)$$

Углавном сви постојећи шифарски системи који се користе базирани су на Шеноновом моделу, али са коришћењем краћих кључева, који се теоријски могу разбити, нпр. потпуном претрагом кључева. Да би дизајнирали шифарске системе који се могу користити у пракси, потребно је обезбедити сигурност такву да је немогуће њено разбијање у реалном времену. Међутим за криптолошке системе који се не примењују у пракси сигурност може бити доказана без коришћења недоказивих и неразумљивих хипотеза.

Апсолутна тајност је често унапред осуђивана као непрактична због Шеноновог песимистичког резултата (1). Један од циљева овог рада је да релативизујемо Шенонов песимизам додатном претпоставком да изузев тајног кључа непријатељ има потпун приступ информацији као и легитимни учесник, је доста ограничавајућа да би уопште била реализована [26].

Постизање апсолутне тајности без унапред дељеног кључа  $K$ , подразумева модификацију Шеноновог модела тако да нападач не може да прими тачно исту информацију као и легитимни учесник. Претходна два приступа базирана на овој идеји су представљена од стране Вижнера у раду под називом „Квантна криптографија“ (коју су даље обрађивали Бенет, Брасард и други [27]) и Маурера у раду под називом „Случајне Шифре“ [28] које користе јавни случајни низ који је предуг да би се реализовао у реалном времену. Ова два приступа су непрактична за

коришћење [26].

Вејнер је представио канал са шумом у криптографији [29]. У његовом моделу непријатељ слуша на прислушном каналу (*wiretap channel*, енгл.), и он је доказао да је могуће послати поруку са безусловном сигурношћу без дељеног кључа. Сизар и Корнер [30], генерализовали су Вејнеров модел прислушног канала у модел канала за емитовање (*broadcast channel*, енгл.), који су подразумевали сценарио у којем непријатељ Ева прихвата поруке послате од стране Алисе преко канала који је доста некавалитетнији (шум) од канала легитимног учесника. Ова претпоставка да је Евин канал доста лошији од главног канала је нереална. Ова нереална претпоставка није неопходна ако Алиса и Боб могу да комуницирају преко небезбедног јавног канала. Базиран на моделу Сизара и Корнера, Маурер је представио нови модел коме је додао додатни канал између Алисе и Боба. Модел је касније генерализовао у ефективнији модел [26][19]. Његов модел се може имплементирати у сателитском каналу за емитовање. Алиса, Боб и Ева примају три случајне променљиве  $X$ ,  $Y$  и  $Z$ , које су емитоване сигналом са сателита са одређеним нивом шума са заједничком вероватноћом расподеле  $P_{XYZ}$ , где се  $X$ ,  $Y$  и  $Z$  променљиве најчешће разликују једна од других. Након тога Алиса и Боб започињу договор тајног кључа преко јавног канала. Циљ је да се отклоне грешке између  $X$  и  $Y$  и да се добију усаглашени низова између Алисе и Боба који представља дељени кључ и смање Евино знање о низу. Овакав договор тајног кључа преко јавног канала углавном се састоји из три фазе: прва фаза је дестилација предности (*advantage distillation*, енгл.) [26][31][19] у којој се заједничка информација легитимних учесника пречишћава и стиче предност у односу на непријатеља (*advantage degeneration*, енгл.) [32], друга фаза је исправљање грешака (*information reconciliation*, енгл.) која има за циљ да отклони све грешке током размене порука преко аутентификованог јавног канала [27], трећа фаза јесте појачавање приватности (*privacy amplification*, енгл.) која је неопходна када две стране желе да филтрирају тајни кључ из великог заједничког али делимично тајног низа, односно да елиминишу Евину информацију о тајном низу [33][34][35][9].

Уели Маурер и Стефан Волф су доказали да горе поменути договор кључа се може унапредити и појачати [36]. Ефекат бочних информација је представљен у комуникацији преко јавних канала преко Евине Рени ентропије и веза између исправљања грешака и појачавања приватности је приказана [37] и побољшана у јачи протокол којег су предложили [36].

За јавни канал не постоје значајне последице у практичном криптографском смислу, зато што канал не обезбеђује тајност података. Самим тим претпоставимо да све поруке које су емитоване на јавни канал Ева може примити без грешке, али не може да модификује или да убаци лажну поруку, а да при том не буде детектована.

Аутентификација и интегритет података може се осигурати коришћењем, безусловно сигурном аутентификационом шемом [38], базираном на универзалном хеширању, које захтева да Алиса и Боб деле заједнички краћи кључ на почетку. У овом случају наш предлог је искористити део кључа за безусловну сигурност, који би био коришћен за аутентификацију касније у протоколу.

Искористити јавни кључ да би две стране добиле тајни кључ од иницијалног заједничког делом тајног низа претходно је разматрао Леунг Јоу Чхеонг [39] и независно од њега Бенет, Брасард и Роберт [33].

На традиционалне начине, кључеви се углавном дистрибуирају тајним каналима или преко криптосистема са јавним кључевима. Тајни канали су скупи и тешки за одбрану, док су шифарски системи са јавним кључевима само израчунљиво

безбедни. И један и други систем обезбеђују методе за дистрибуцију кључева преко небезбедних канала.

Овај рад подразумева дистрибуцију кључева као и шифровање. Безусловно сигуран заједнички кључ изгенерисан од стране једног од ових протокола могао би се искористити као кључна секвенца у *one-time-pad*, како би достигли перфектну тајност за пренете поруке[9][26].

## Литература

- [1] Schneier, B., **Applied Cryptography**, John Wiley & Sons Inc., Second Edition, 1996.
- [2] Веиновић, М., Адамовић, С., **Основе за анализу и синтезу шифарских система**, [Књига].- Београд: Универзитет Сингидунум, 2013. - 1 : Т. 1 : стр. 247. - 978-86-7912-469-2.
- [3] Alonso, M., „*Cryptographic Protocols in Optical Communication*“, Ph.D Thesis, Universitet Erlangen, Numberg 2006.
- [4] Shor, P., „*Algorithms for quantum computation diskretelog and factoring*“, Proceeding of the 35th IEEE Symposium on the Foundations of Computer Science, Nov. 20-22, Santa Fe, NM, USA., pp.124-134, 1994.
- [5] Grover, L., „*A fast quantum mechanical algorithm for database search*“, Proceeding of the 28th Annual ACM Symposium on the Theory of Computation, May 22-24, ACM Press, New York, pp.212-219, 1996.
- [6] Grover, L., „*Quantum mechanics helps in searching for a needle in a haystack*“, Phys. Rev. Lett., 79:325-328, 1997.
- [7] Daemen, J., Rijmen, V., „*The Design of Rijandel: AES-the Advanced Encryption Standard*“, Springer-Verlag, Berlin 2002.
- [8] Courtois, N., Pieprzyk, J., „*Cryptanalysis of blok ciphers with over-defined sytems of equations*“, Proceeding of the 8th International Conference on the Theory and Aplication of Cryptology and Information Security: Advances in Cryptology, Dec.1-5, Springer-Verlag, London, UK., pp.267-287, 2002.
- [9] Wang, Y., „*Unconditional Security of Cryptosystem: A Review and Outlook*“, Trends in Applied Sciences Research, Academic Journals Inc., 2011.
- [10] Menezes, A., Paul C., Scott, V., **Handbook of applied cryptography**, CRC press, 1996.
- [11] Stallings, W., **Cryptography and network security, principles and practices**, Fifth Edition, Practice Hall, 2011.
- [12] Kak, A., „*Lecture and Notes on Computer and Network Security*“, Purdue University, 2014.  
<https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf>
- [13] Diffie-Hellman protokol (NCERT, 2009),  
<http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2009-12-284.pdf>
- [14] Kovinić, M., „*Uvod u kriptografiju i infrastrukturu javnih ključeva (PKI)*“, Akademska mreža Srbije – AMRES, 2010.
- [15] Milenković, M., Adamović, S., Šarac, M., Radovanović, D., „*Upravljanje X. 509 sertifikatima u PKI sistemu*“, Acta facultatis medicae Naissensis, 2010.
- [16] Kurdulija, N., „*Analiza osetljivosti digitalnog potpisa*“, Univerzitet u Beogradu, Matematički fakultet, 2009.
- [17] Shannon, C., „*A mathematical theory of communication*“, Bell System Techncl Joural, Vol. 27, pp.379-423 and 623-656, 1948.

- [18] Maurer, U., „*Information-Theoretic Cryptography*“, CRYPTO'99, LNCS 1666, Springer - Verlag, pp.47-65, Berlin Heidelberg 1999.
- [19] Maurer, U., „*Secret key agreement by public discussion from common information*“, IEEE Trans. Inform. Theory, Vol. 39, pp. 733–742, May 1993.
- [20] Milosavljević, M., Adamović, S., Milenković, M., „*Mogućnosti distribucije kriptoloških ključeva javnim kanalima*“, Sinergija 2010., Beograd., 2010.
- [21] Liung, S., „*Information-theoretic secret key agreement*“, Eindhoven: Technische Universiteit Eindhoven, 2002.
- [22] Calver, T., „*An Empirical Analysis Of The Cascade Secret Key Reconciliation Protocol For Quantum Key Distribution*“, Department of the Air Force Air University, Air Force Institute of Technology, 2011.
- [23] Bennett, C., Brassard, G., Robert, J., „*How to reduce your enemy's information*“, In: Adv. in Cryptology – Proceedings of CRYPTO '85, Lecture Notes in Comput. Sci., Vol. 218, Berlin. Germany: springer-Verlag, pp. 468-476, 1986.
- [24] Carter, J., Wegman, M., „*Universal Classes of Hash Functions*“, Journal of computer and system sciences 18, pp 143-154, 1979.
- [25] Shannon, C., „*Communication theory of secret systems*“, Bell System Technical Journal, Vol. 28, pp. 656-715, 1949.
- [26] Maurer, U., „*Protocols for Secret Key Agreement by Public Discussion Based on Common Information*“, Advances in Cryptology – CRYPTO'92, LNCS 740, Springer – Verlag, pp.461-470, Berlin Heidelberg 1993.
- [27] Bennett, C., Bessette, F., Brassard, G., Salvail, L., Smolin, J., „*Experimental quantum cryptography*“, J. Cryptol., Vol. 5, pp.3-28, 1992.
- [28] Maurer, U., „*Conditionally-Perfect secrecy and a provably-secure randomized cipher*“, Journal of Cryptology, Vol. 5, No. 1, pp.53-66, 1992.
- [29] Wyner, A., „*The wire-tap channel*“, Bell System Technical Journal, Vol.54, pp.1355-1387, 1975.
- [30] Csiszar, I., Korner, J., „*Broadcast channels with confidential messages*“, IEEE Trans. Inform. Theory, Vol. 22, pp.339-348, 1978.
- [31] Gander, M., Maurer, U., „*On the secret key rate of binary random variables*“, Proceedings of the IEEE International Symposium on Information Theory, June 27- July 1, Trondheim, Norway, p.351, 1994.
- [32] Yupu, H., Bo, Y., Yuqing, Z., „*An advantage degeneration protocol in complete security scheme*“, Acta Electronica Sinica, Vol. 30, pp.533-535, 2002.
- [33] Bennett, C., Brassard, G., Robert, J., „*Privacy amplification by public discussion*“, SIAM J. Comput., Vol. 17, pp.210-229, 1988.
- [34] Bennett, C., Brassard, G., Crkpeau, C., Maurer, U., „*Generalized privacy amplification*“, IEEE Trans. Inform. Theory, Vol. 41, pp.1915-1923, 1995.
- [35] Maurer, U., Wolf, S., „*Privacy amplification secure against active adversary*“, In: Adv. in Cryptology – Proceedings of CRYPTO '91, Vol. 1294, pp.307-321, 1996.

- [36] Maurer, U., Wolf, S., „*From weak to strong information-theoretic key agreement*“, Proceedings of the IEEE International Symposium on Information Theory, June 25-30, Sorrento, Italy, p.18, 2000.
- [37] Shengli, L., „*Research on information-theoretic security in cryptography*“, Ph.D. Thesis, Xidian University, China, 1999.
- [38] Wegman, M., Carter, J., „*New hash functions and their use in authentication and set equality*“, Journal of Computer and System Sciences, Vol. 22, pp.265-279, 1981.
- [39] Leung-Yan-Cheong, S., „*Multi-user and wiretap channels including feedback*“, Tech. Rep. No. 6603-2, Stanford University, Information Systems Lab., July 1976.

## Списак слика

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Слика 1 Општа класификација техника за установљавање кључа .....         | 7  |
| Слика 2 Графички приказ KDC протокола .....                              | 15 |
| Слика 3 Графички приказ <i>Needham-Schroder</i> протокола .....          | 17 |
| Слика 4 Графички приказ Керберос протокола .....                         | 19 |
| Слика 5 Графички приказ <i>Otway-Ress</i> протокола .....                | 21 |
| Слика 6 Системи са јавним кључем – очување тајности .....                | 24 |
| Слика 7 Системи са јавним кључем – аутентичност .....                    | 25 |
| Слика 8 Системи са јавним кључем – аутентичност и очување тајности ..... | 26 |
| Слика 9 <i>Diffie-Hellman</i> систем за размену кључева .....            | 29 |
| Слика 10 Вејнеров прислушни канал .....                                  | 39 |
| Слика 11 Сателитски сценарио .....                                       | 42 |
| Слика 12 Каскадни модел исправљања грешака .....                         | 49 |
| Слика 13 Графички приказ интерфејса .....                                | 53 |
| Слика 14 Иницијална (почетна) фаза .....                                 | 54 |
| Слика 15 Протокол дестилације предности .....                            | 55 |
| Слика 16 Протокол усаглашавања информација .....                         | 55 |
| Слика 17 Очекиване вредности и вредности добијене симулацијом .....      | 56 |
| Слика 18 Симулација .....                                                | 58 |

## Списак табела

|                                                                        |    |
|------------------------------------------------------------------------|----|
| Табела 1 Дистрибуција кључева заснована на симетричном шифровању ..... | 13 |
| Табела 2 Примена система са јавним кључем .....                        | 27 |
| Табела 3 Однос дужина симетричних и асиметричних кључева .....         | 36 |