МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета математика

Основи криптографије и шифарски системи са јавним кључем

УЧЕНИК:
Ленка Стаматовић, 4ц

МЕНТОР:
Милица Мисојчић

Београд, јун 2020.

Садржај

1 Увод **1**

2 Основни појмови **2**

3 Историја криптографије **3**

4 Основи теорије бројева **6**
4.1 Дељивост целих бројева 6
4.2 Конгруентност по модулу 7

5 Системи са јавним кључем **10**
5.1 RSA шифарски систем 10
5.1.1 Генерисање кључа 10
5.1.2 Размена кључева 11
5.1.3 Шифровање поруке 11
5.1.4 Дешифровање поруке 11
5.1.5 Пример 11
5.1.6 Предности и мане алгоритма 12
5.2 Проблем дискретног логаритма у коначном пољу (ПДЛКП) 12
5.3 Протокол усаглашавања кључа Дифи-Хелман (ПУКДХ) 13
5.3.1 Пример 13
5.4 ЕлГамалов алгоритам за шифровање 13
5.4.1 Принцип рада алгоритма (генерисање кључа, шифровање и дешифровање) 14
5.4.2 Пример 14
5.5 Размена кључева Меси-Омура 14
5.5.1 Принцип рада алгоритма 15
5.5.2 Пример 15

6 Потписи и аутентикација **16**
6.1 Потписи помоћу RSA 16
6.1.1 Пример проблема са RSA 16
6.1.2 Пример 17
6.1.3 Пример потписа помоћу RSA: 17
6.2 ЕлГамалов потпис 17
6.2.1 Пример 18
6.3 Шноров поступак аутентикације 18

1 Увод

Криптографија је наука која се бави састављањем и анализирањем протокола сигурне комуникације, како би се спречило да одређена приватна порука доспе у јавност или погрешне руке. Шифровањем оригиналне поруке добија се шифрована која је безбедна за транспорт и коју ће само прималац моћи да дешифрује. Сама реч криптографија настала је од две грчке речи $\kappa\rho\upsilon\pi\tau\sigma\varsigma$ (kryptos) и $\gamma\rho\alpha\varphi\varepsilon\iota\nu$ (graphein) што значи "скривено" или "тајно" и "написати".

Данас се модерна криптографија заснива на коришћењу знања различитих наука као што су математика, електротехника, информатика, физика и комуникацијске науке. Криптографија је у прошлости примењивана углавном за сигурну комуникацију док данас она има много већу примену у електронској трговини, чипованим платним картицама, дигиталним валутама тј. новцу, компјутерским шифрама, војној комуникацији, итд.

Циљ сваког криптографског система је исти без обзира на то ко намерава да користи систем или алгоритам по којем систем функционише. Сваки творац криптографског система води рачуна да корисницима обезбеди следеће: **поверљивост (енгл. Confidentiality)** (информација која се преноси не сме бити разумљива неком коме није намењена), **интегритет (енгл. Data integrity)** (информација не сме бити измењена пре самог преношења, а да пошиљалац или прималац не буду обавештени о томе), **немогућност избегавања одговорности (енгл: Non-repudiation)** (пошиљалац поруке не може у каснијим стадијумима комуникације да ускрати или порекне своје намере за пренос порука и договорен начин комуникације), **аутентикација (енгл. Autentification)** (пошиљалац и прималац поруке морају међусобно да потврде своје идентитете пре слања односно примања поруке).

У овом раду су прво наведени основни појмови везани за криптографију ради лакшег праћења остатка рада, наведени су неки примери из историје криптографије, обрађене су основе криптографије, које чини математичка грана теорија бројева, и у даљем раду су обрађени неки шифарски системи са јавним кључем. За сваки систем је објашњен принцип рада самог алгоритма (шифровање и дешифровање порука), дат је по један пример са конкретним вредностима бројева које користи алгоритам и понегде су наведене предности и мане. Највише пажње је посвећено најпознатијем систему са јавним кључем, RSA систему. Свака литература користи имена која се односе на пошиљаоца, примаоца и противника при објашњавању принципа по којем ради алгоритам. У овом раду Алиса је неко ко шаље поруку, Бобан је онај који је прима, а Цица је пресреће и покушава да је дешифрује.

2 Основни појмови

Отворени текст(ОТ) је оригинални текст који треба послати, нпр. "ZDRAVO".

Шифрат(ST) је шифрована порука, нпр. XQABER.

Шифровање је трансформација отвореног текста у шифрат.

Дешифровање је (инверзна) трансформација шифрата у отворени текст.

Кодирањем се ОТ трансформише у низ цифара или бита.

Декодирање трансформише низ цифара или бита у отворени, полазни текст.

За кодирање се често користи ASCII код где се свако слово представља низом од 8 бита (A -> 01000001, B -> 01000010, a -> 01100001, 0 -> 00110000, ? -> 00111111, ...). Због тога у кодирању и декодирању нема ничег тајног.

Проточна шифра је тип шифровања код кога се ОТ трансформише најчешће бит по бит или симбол по симбол.

Блоковска шифра групише симболе ОТ у блокове, након чега их трансформише у ST.

Неки од примера блоковске шифре су биграми (парови слова) и триграми (тројке слова). Advanced Encryption Standard (скраћено AES) ради са блоковима од по 128 бита тј. 16 знакова.

Шифра премештања премешта место словима (знаковима, битовима,...) ОТ да би добила ST.

Шифра замене мења слова (знакове, бите) неким другим, не мењајући им редослед.

Комбинована шифра уједно примењује и замену и премештање слова (знакова, бита).

Шифарски систем је пар кога чини алгоритам шифровања и дешифровања.

Кључ представља параметар којим се бира конкретна шифарска трансформација у једном шифарском систему.

Симетрични систем подразумева коришћење истог тајног кључа за алгоритам шифровања и дешифровања.

Асиметрични систем подразумева чување кључа за дешифровање у строгој тајности, док је кључ за шифровање јавно познат.

Криптоанализа је процес у ком одређена особа покушава да из шифрата добије оригинални текст, не знајући кључ за дешифровање.

Декриптирање представља успешну криптоанализу, некад и само делимичну.

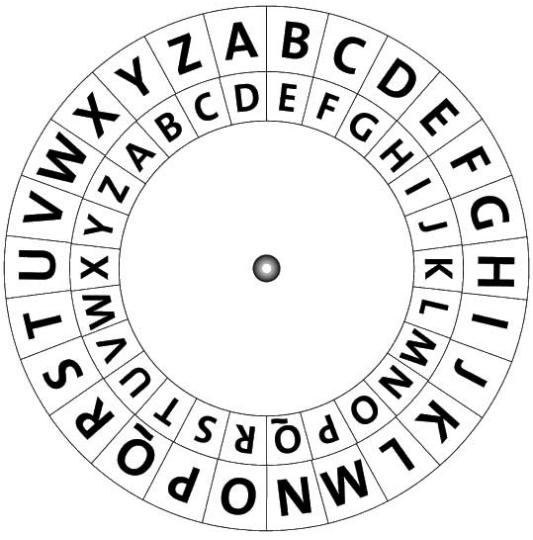
3 Историја криптографије

Први облици криптографије, који су били далеко простији од данашњих, сежу далеко у прошлост (до чак 400 год. п. н. е.). Пре модерне и компјутеризоване ере криптографијом је требало да се обезбеди само поверљивост поруке, док се у данашње време фокусира на више фактора током процеса криптографије (интегритет поруке, потврда идентитета пошиљаоца и примаоца поруке, дигитални потписи, итд.). У даљем тексту овог поглавља ће бити наведени и кратко објашњени неки од познатијих коришћених система кроз историју.

Спартанска шифра Скитале је пример шифарског система који користи метод шифре премештања. Претпоставља се да су Спартанци користили овај начин шифровања током војних кампања. Предност овог система је била у брзини дешифровања и малој вероватноћи за добијање погрешне поруке. Наиме, прималац добија поруку на дугачкој папирној траци коју треба да обмота око штапа довољне дужине и одређеног полупречника. У овом систему полупречник штапа представља кључ за дешифровање.
Пример: "Кључ је дијаметар штапа" ће након одмотавања гласити "кемшљдетуитачјапјара".

к	љ	у	ч	ј
е	д	и	ј	а
м	е	т	а	р
ш	т	а	п	а

Цезарова шифра је пример симетричног шифарског система који користи замену шифре. Свако слово абецеде је замењивано са словом на трећем месту после њега у абецеди. Тако би на пример порука *Caesar* постала *Fdhvdu*. Цезаровом шифром се такође може назвати било који систем који користи исти алгоритам, али различит број померених места (у лево или у десно). Ова шифра добила је име по Јулију Цезару који је користио систем слова померених у десно за 3 места да би комуницирао са својим генералима. За дешифровање се користио Цезаров точак ради бржег и лакшег читања порука.



Плејферова шифра је једна од првих која је обрађивала биграме, а уједно и примењивала метод замене. Коришћена је током десетих година XX века за време Бурског рата. Ако се за кључ изабере реч PALMERSTON помоћу ње се формира следећа табела:

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	IJ	K	Q	U
V	W	X	Y	Z

Табела је увек величине 5×5 и формира се тако што се редом попуне поља словима која чине кључ, а затим се остатак табеле попуни редом преосталим словима абецеде. Након тога се посматрају биграми слова који се шифрују помоћу табеле. Ако се на пример шифрује биграм SF, посматра се правоугаоник у табели чија су два темена слова S и F. Шифрат чине преостала два темена тог правоугаоника OC. Редослед је одређен чињеницом да су S и O у истој врсти, као и F и C. Ако су два слова у истој врсти њихов шифрат се формира тако што се она замене словима десно од њих у истој врсти (CG постаје DB). Даље, ако су два слова у истој колони она се замењују словима испод њих (PR постаје RB). Двострука слова се прво трансформишу у пар датог слова и слова X након чега се тај пар шифрује помоћу датих правила. Реч BALLON се прво трансформише у облик BA LX ON, након чега се шифрује у CPTXNR. Слова I и J се налазе на истом месту у табели због броја различитих слова.

ADFGVX шифра је шифра која користи метод замене и премештања. Њу су користили Немци у I светском рату. Прво се отворени текст трансформише методом замене помоћу фиксиране табеле:

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Свако слово које је на реду за шифровање се замењује паром ознака (врста, колона). Узмимо за пример OT PRODUCTCIPHERS. Помоћу дате табеле OT се прво трансформише у FG AG VD VF XA DG XV DG XF FG VG GA AG XG. Након тога следи фаза премештања, која се изводи на основу кључа без поновљених слова. Нека кључ у овом случају гласи DEUTCH. Формира се нова табела где се у прву врсту уписују редом слова кључа, у следећој врсти се та слова нумеришу по положају у абецеди, а у даљим врстама се редом уписују слова трансформисаног текста:

D	E	U	T	S	C	H
2	3	7	6	5	1	4
F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

Затим се слова исписују по колонама при чему се прати редослед бројева од 1 до 7 у другој врсти. У овом примеру шифрат који се очитава је DXGX FFDG GXGG VVVG VGFG GDFA AAXA.

За време II светског рата је показано да наизменично коришћење замене и премештања даје добре шифарске системе. Међутим, систем ADFGVX је лош јер се користи само по једна замена и премештање, при чему је замена фиксна и не зависи уопште од кључа. PURPLE и ENIGMA су компликовани комбиновани шифарски системи који су коришћени у II светском рату, а такође су направљени и рачунари (COLOSSUS) за разбијање тих шифри. После 1970. године озбиљан проблем је представљала угроженост безбедности рачунара. Појавила се потреба за сигурнијим шифрама за комерцијалну употребу. 1974. године се појавила шифра LUCIFER, а одмах следеће се појавила шифра DES (скраћено од Data Encryption Standard) и обе су биле комбиноване шифре.

4 Основи теорије бројева

Теорија бројева се бави проучавањем особина целих бројева. Сабирање, одузимање и множење су бинарне операције скупа $\mathbb{Z}$, тј. скуп $\mathbb{Z}$ је затворен у односу на њих. Са дељењем то није случај и због тога се појављује питање дељивости целих бројева.

4.1 Дељивост целих бројева

Дефиниција 4.1. *Нека је скуп $\mathbb{Z}$ скуп целих бројева ($\mathbb{Z} = \{0, \pm1, \pm2, \pm3, ...\}$). За целе бројеве a,$b \in \mathbb{Z}$ кажемо да a дели b или да је b дељив бројем a (ознака $a|b$), при чему број a мора бити различит од 0, ако постоји цео број n такав да је $b = a \cdot n$ за неко $n \in \mathbb{Z}$.*

Теорема 4.1. ***О Еуклидском дељењу целих бројева:***
Сваки цео број a може се на јединствен начин помоћу датог природног броја b приказати у облику

$$a = b \cdot q + r,$$

*при чему је $0 \leq r < b$ и $q, r \in \mathbb{Z}$. Број q се назива **количником**, а број r **остатком** при дељењу броја a бројем b.*

Доказ. Посматрајмо скуп целих бројева $\{..., a-2b, a-b, a, a+b, a+2b, ...\}$ и изаберимо у њему најмањи број који је природан или једнак 0 (постојање таквог броја следи из једне од основних особина скупа природних бројева). Обележићемо изабрани број са r и нека је он једнак $a - q \cdot b$. Тада је

$$a = b \cdot q + r, \ 0 \leq r < b, \tag{1}$$

јер би у случају $r \geq b$ и број $a - (q+1) \cdot b$, који је мањи од $a - q \cdot b$, био природан или једнак нули. Тиме је доказана егзистенција бројева q и r. Докажимо сада јединственост тих бројева. Претпоставимо да постоји још један пар бројева (q_1, r_1), такав да је $a = b \cdot q_1 + r_1$ и $0 \leq r_1 < b$. Одузимањем ове једнакости од једнакости (1) добијамо

$$0 = b \cdot (q - q_1) + (r - r_1),$$

односно да $b|(r - r_1)$. Због $|r - r_1| < b$ имамо да је $r - r_1 = 0$, тј. да је $r = r_1$, а због тога и $q = q_1$. ■

Дељивост можемо посматрати као релацију (два броја x и y су у релацији ако $x|y$). Посматрајући ову релацију у скупу природних и целих бројева долазимо до закључка да је релација дељивости рефлексивна и транзитивна у скупу целих бројева, док је у скупу природних бројева то **релација поретка** (антисиметрична је, транзитивна и рефлексивна):

- $a|a,\ a \in \mathbb{Z} \vee a \in \mathbb{N}$
- $a|b \wedge b|a \Rightarrow a = b,\ a, b \in \mathbb{N}$
- $a|b \wedge b|c \Rightarrow a|c,\ a, b, c \in \mathbb{Z} \vee a, b, c \in \mathbb{N}$

Особине релације дељивости:
Нека су бројеви $a, b, c \in \mathbb{Z}$

- $a|b \Rightarrow a|b \cdot c$
- $a|b \wedge a|c \Rightarrow a|b \cdot x + c \cdot y, \forall x, y \in \mathbb{Z}$
- $a|b \wedge b|a \Rightarrow a = b \vee a = -b$
- $a, b > 0 \wedge a|b \Rightarrow a \leq b$

Теорема 4.2. ***Основни став аритметке:***
Сваки природан број ($n \in \mathbb{N} \wedge n > 1$) *може се представити на следећи начин:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_k^{\alpha_k}$$

где су $p_1, p_2, p_3, ..., p_k$ *прости бројеви, а* $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k$ *природни. Такав облик природног броја назива се канонски облик тј.* ***канонска факторизација****.*

Дефиниција 4.2. *Укупан број позитивних делилаца природног броја* a *означавамо са* $\tau(a)$*.*

Лако се може закључити да је $\tau(a) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdot ... \cdot (\alpha_k + 1)$ где је $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_k^{\alpha_k}$ канонска факторизација броја a.

Дефиниција 4.3. *Највећи међу заједнички делиоцима бројева* a *и* b *је* ***највећи заједнички делилац*** *тих бројева. Обележава се* $NZD(a, b)$ *или једноставније само* (a, b)*. За целе бројеве* a *и* b *кажемо да су* ***узајамно прости*** *ако важи* $(a, b) = 1$*.*

Дефиниција 4.4. *Цео број* $p > 1$ *је* ***прост*** *ако нема ниједан делилац* $d, 1 < d < p$*. Цео број* $m > 1$ *који није прост је* ***сложен****.*

4.2 Конгруентност по модулу

Дефиниција 4.5. *Два дата цела броја* a *и* b *су* ***конгруентна по модулу*** m ($m \in \mathbb{N} \wedge m > 1$) *ако дају исти остатак при дељењу са* m*. Пишемо*

$$a \equiv b \pmod{m}.$$

Из дате дефиниције се лако могу извести следеће особине конгруенције по модулу m:

- $a \equiv b \pmod{m} \iff m|a-b$
- $a \equiv b \pmod{m} \iff a = m \cdot t + b, t \in \mathbb{Z}$

Даље, конгруентност по модулу је **релација еквиваленције** (рефлексивна је, симетрична и транзитивна):

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Због тога се скуп целих бројва релацијом $\bmod m$ разбија на m дисјунктних подскупова (класе еквиваленције). Сваки подскуп садржи по једног представника из скупа $[0, m-1]$. Скуп ових подскупова означава се са $\mathbb{Z}/_m\mathbb{Z}$ или $\mathbb{Z}_m$. $\mathbb{Z}_m$ има m елемената, а бројеви $0, 1, ..., m-1$ су представници m елемената скупа $\mathbb{Z}_m$.

Особине конгруенције:

- Сабирање и множење у $\mathbb{Z}_m$:

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$$

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$$

- Промена модула конгруенције:

$$a \equiv b \pmod{m} \quad \wedge \quad d|m \Rightarrow a \equiv b \pmod{d}$$

- Инверз у $\mathbb{Z}_m$:
  за $x \in \mathbb{Z}_m$ инверз постоји ако је $(x, m) = 1$ и тада важи

$$x \cdot x^{-1} \equiv 1 \pmod{m}$$

- Дељење у $\mathbb{Z}_m^*$(скуп бројева $x \in \mathbb{Z}_m$ за које постоји инверз):

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \quad \wedge \quad (c, m) = 1$$
$$\Rightarrow a \cdot c^{-1} \equiv b \cdot d^{-1} \pmod{m}$$

- Решавање конгруенције $a \cdot x \equiv b \pmod{m}$:
  1. $(a, m) = 1 \Rightarrow x = a^{-1} \cdot b$;
  2. $(a, m) = g > 1 \quad \wedge \quad g|b \Rightarrow x \equiv (\frac{a}{g})^{-1} \cdot \frac{b}{g} \pmod{m}$;
  3. $(a, m) = g > 1 \quad \wedge \quad g \nmid b \Rightarrow \nexists x$.

Дефиниција 4.6. ***Ојлерова*** [1] ***функција*** *датог природног броја m представља број природних бројева који нису већи од датог броја и узајамно су прости са њим. Означава се са $\varphi(m)$.*

Другачије се Ојлерова функција дефинише као број елемената произвољног сведеног система остатака по модулу m ($\varphi(m) = |\mathbb{Z}_m^*|$). Ако је p прост број Ојлерова функција за тај број износи $\varphi(p) = p - 1$. Ојлерова функција се лако може израчунати и за степен датог простог броја p: $\varphi(p^r) = p^r \left(1 - \frac{1}{p}\right) = p^{r-1}(p-1)$. За сваки други природан број Ојлерова функција се може израчунати коришћењем мултипликативног својства $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ ако важи $(m, n) = 1$. Дакле, да би се израчунала Ојлерова функција за произвољан природан број, он се прво мора раставити на просте чиниоце. Тако је на пример $\varphi(720) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5) = 2^3 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot 4 = 192$.

Теорема 4.3. ***Ојлерова теорема:***
Ако је $(a, m) = 1$ онда је $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Теорема 4.4. ***Мала Фермаова*** [2] ***теорема:***
Ако је p прост број и ако $p \nmid a$, онда је $a^{p-1} \equiv 1 \pmod{p}$.

Мала Фермаова теорема је само специјалан случај Ојлерове теореме.

[1] Леонард Ојлер (нем. Leonhard Euler, 1707-1783), швајцарски математичар и физичар
[2] Пјер де Ферма (франц. Pierre de Fermat, 1601-1665), француски математичар

5 Системи са јавним кључем

Шифарски систем са јавним кључем је онај систем у коме је јавно познат алгоритам шифровања, али је полиномијални алгоритам за налажење кључа за дешифровање, полазећи од кључа за шифровање, непознат. Појам система са јавним кључем су први пут увели Дифи [3] и Хелман [4] 1976. године. Први такав систем који су они дефинисали био је протокол и назвали су га "размена кључева Дифи-Хелман". 1977. године објављен је најпознатији систем за асиметричну криптографију, RSA систем. Предност асиметричне криптографије је у томе што се не води брига о томе да ли ће неко пресрести јавни кључ. Најважније примене шифарских система са јавним кључем су размена кључа за симетрични шифарски систем и дигитални потпис, док се за шифровање порука овакви системи ретко користе јер су спорији од симетричних система шифровања.

5.1 RSA шифарски систем

RSA шифарски систем је првенствено био намењен шифровању података, а данас се такође користи и у системима електронског потписа. Овај систем данас представља индустријски стандард у области асиметричне криптографије и заштити података, тако да је широко примењен у многим сигурносним протоколима и системима електронског пословања. Његови оснивачи су Рон Ривест [5], Ади Шамир [6] и Леонард Ејдламн [7] по чијим презименима је и добио назив.
Пре преласка на само објашњење алгоритма подсетимо се да ако је $(n, m) = 1$ и $a \equiv 1 \pmod{\varphi(n)}$, онда је $m^a \equiv m \pmod{n}$.

У овом раду, објашњење принципа по коме ради RSA алгоритам ће бити подељен у 4 дела: генерисање кључа, размена кључева, шифровање и дешифровање поруке.

5.1.1 Генерисање кључа

1. Бирају се два проста броја p и q са око 150 декадних цифара. Ради боље заштите бројеви се бирају насумично.

2. Израчунава се број $n = p \cdot q \approx 10^{300}$.

3. Израчунава се Ојлерова функција броја n, $\varphi(n) = (p-1)(q-1)$.

4. Бира се цео број e при чему мора да важи да је $(e, \varphi(n)) = 1$ и $1 < e < \varphi(n)$.

5. Израчунава се број d преко одабраног броја e: $d \equiv e^{-1} \pmod{\varphi(n)}$.

[3] Бејли Витфилд Дифи (енгл. Bailey Whitfield Diffie, 1944.), амерички криптограф
[4] Мартин Едвард Хелман (енгл. Martin Edward Hellman, 1945.), амерички криптограф
[5] Роналд Лин Ривест (енгл. Ronald Linn Rivest, 1947.), криптограф и професор на МИТ Универзитету
[6] Ади Шамир (енгл. Adi Shamir, 1952.), израелски криптограф
[7] Леонард Макс Ејдлман (енгл. Leonard Max Adleman, 1945.), научник теоријске информатике и професор рачунарства и молекуларне биологије на Универзитету Јужне Калифорније

5.1.2 Размена кључева

Власник кључа јавно објављује пар (n, e) и тај пар се назива јавним делом кључа, док бројеве d, p, q чува у тајности и они представљају тајни (приватни) део кључа. На тај начин свако може да шифрује поруку и пошаље је било коме, али ће само власник кључа моћи да је дешифрује и разуме. Претпоставимо да Алиса жели да пошаље поруку Бобану. У том случају она ће користити Бобанов јавни део кључа који је он објавио да би шифровала поруку, а затим му је послала.

5.1.3 Шифровање поруке

Да би Алиса послала Бобану поруку M (која може да буде кључ за AES кодиран систем), знајући пар бројева (n, e), она израчунава $C \equiv M^e \pmod{n}, (0 \leq C \leq n)$ и затим Бобану шаље број C.

5.1.4 Дешифровање поруке

Када Бобан добије поруку од Алисе он ће, знајући приватни део свог кључа доћи до отвореног текста тако што ће израчунати $C^d \pmod{n}$ и тако добити M ($C^d \equiv (M^e)^d \equiv M^{e \cdot d} \equiv M^1 \equiv M \pmod{n}$). Ако Цица пресретне Алисину поруку C она је не може дешифровати без Бобановог параметра d.

5.1.5 Пример

1. Бобан бира два проста броја $p = 17$ и $q = 41$.
2. Израчунава број $n = p \cdot q = 697$.
3. Израчунава Ојлерову функцију броја n, $\varphi(n) = (p-1)(q-1) = 640$.
4. За број e узима број 33 (узајамно је прост са 640).
5. Израчунава број d преко одабраног броја e: $d \equiv 33^{-1} \equiv 97 \pmod{640}$.

Бобан објављује бројеве 697 и 33 на свој сајт. Алиса жели да користи афину шифру $C \equiv aP + b \pmod{26}$ са кључем $(a, b) = (7, 25)$. Она прво кодира дати кључ бројем 207 ($7 \cdot 26 + 25 = 207$), а затим израчунава шифрат 156 ($207^2 \equiv 332 \pmod{697}, 207^4 \equiv 332^2 \equiv 98 \pmod{697}, 207^8 \equiv 98^2 \equiv 543 \pmod{697}, 207^{16} \equiv 543^2 \equiv 18 \pmod{697}, 207^{32} \equiv 18^2 \equiv 324 \pmod{697}, 207^{33} \equiv 324 \cdot 207 \equiv 156 \pmod{697}$). Алиса шаље Бобану број 156 помоћу кога ће он добити број 207 ($156^d = 156^{97} \equiv 207 \pmod{697}$). Ако Цица пресретне Алисину поруку њој ће бити тешко да од броја 156 добије 207 не знајући број 97. Када је Бобан дошао до броја 207, тиме се завршава део RSA алгоритма. Он ће даље број 207 јединствено представити преко броја 26 ($207 = 26 \cdot 7 + 25$, теорема 4.1) и тиме добити кључ афине шифре (7,25) где ће број 7 бити количник, а број 25 остатак при дељењу броја 207 бројем 26. Дошавши до кључа афине шифре Бобан ће лако дешифровати дугачку поруку коју му је послала Алиса.

5.1.6 Предности и мане алгоритма

Да би се одредио параметар d само помоћу јавног дела кључа потребно је израчунати $\varphi(n)$ што представља врло комплексан проблем и готово је немогуће израчунати га само на основу броја n. Да би се одредила Ојлерова функција неког броја, њега је потребно раставити на чиниоце. За тај посао познати су само субекспоненцијални, али не и полиномијални алгоритми. Због тога је RSA алгоритам прилично поуздан и сигуран. Када би се користио симетричан систем за шифровање, особе које комуницирају би користиле заједнички кључ око кога би претходно морале да се договоре, што може бити непрактичнно и несигурно. Коришћењем RSA алгоритма се може решити тај проблем тако што би се преко њега разменио кључ за симетричан систем. Са друге стране, с обзиром на то да овај алгоритам користи просте бројеве са неколико стотина цифара, за множење таква два броја су потребни специјални алгоритми за множење. Такође, то множење некад може и да потраје и због тога је овај алгоритам доста спорији од симетричних алгоритама шифровања.

Постоје правила којих се треба држати приликом бирања параметара за RSA алгоритам:

- Бројеве p и q треба изабрати тако да $(p-1, q-1)$ буде мали број.
- Оба броја треба да имају велики прост чинилац.
- Бројеви не би требало да буду превише близу један другом, док однос већег и мањег обично није већи од 4.
- Углавном је e релативно мало, да би се смањило време шифровања (често се узима да је e=3 или $e = 65537 = 2^{16} + 1$).

Постоје специјални алгоритми који се користе за разбијање RSA алгоритма уколико није испоштовано неко од прва три правила.

RSA се може (али ређе) користити за шифровање саме поруке, уместо за шифровање кључа за AES систем. Алиса тада кодира одређену поруку M бројем n_B $(0 \leq M < n_B)$, а затим шаље Бобану остатак $M^{e_B} \pmod{n_B}$. Уколико је порука предугачка она се разбија на блокове $M_1, M_2, M_3, ..., M_i < n_B$.

5.2 Проблем дискретног логаритма у коначном пољу (ПДЛКП)

Нека је p прост број. Са $\mathbb{F}_p = \mathbb{Z}_p$ ћемо означити коначно поље са p елемената $\{0, 1, 2, ..., p-1\}$ са операцијама $+, -, \cdot$. За све елементе $\alpha \neq 0$ може се одредити њихов инверз, те се може и делити свим елементима различитим од нуле. Скуп $\mathbb{F}_p^* = \{1, 2, 3, ..., p-1\} = \mathbb{F}_p$ је цикличан што значи да садржи бар један елемент g такав да је $\{1, g, g^2, g^3, ...\} = \mathbb{F}_p^*$. Тај елемент g се назива *генератор* или *примитивни корен* по модулу p. Изаберимо неки број $b \in \mathbb{F}_p^*$. Тада знамо да је $g^i = b$ за неки позитиван цео број $i \leq q-1$. Одређивање броја i за унапред задате $\mathbb{F}_p, g, b$ се назива *проблем дискретног логаритма у коначном пољу (Finite Field Discrete Logarithm*

Problem). Чињеницу да је $g^i = b$ можемо написати и у облику $log_g b = i$. Најбољи алгоритми за решавање ПДЛКП имају сложеност сличну факторизацији, тј. субекспоненцијални су.

5.3 Протокол усаглашавања кључа Дифи-Хелман (ПУКДХ)

Протокол усаглашавања кључа над коначним пољем Дифи-Хелман омогућава Алиси и Бобану да размене кључеве без непосредног сусрета. За више корисника A, B, C,... фиксирају се параметри: прост број q, одговарајуће поље $\mathbb{F}_q^*$ и његов генератор g. Бројеви q и g се користе у целом систему и јавни су. Сваки корисник има свој приватни кључ $a_A, a_B, a_C, ...$ који је већи од 1 а мањи од $q-1$ и јавни кључ $g^{a_A}, g^{a_B}, g^{a_C}, ...$ који објављује. Након креирања појединачних кључева Алиса шаље Бобану g^{a_A} на почетку поруке. Да би њих двоје усагласили кључ за AES, они користе остатак $g^{a_A a_B}$. Алиса ће тај остатак добити степеновањем g^{a_B} на a_A, док ће Бобан тај исти број добити степеновањем g^{a_A} на a_B. Цица од параметара поседује q, g, g^{a_A}, g^{a_B}, али од њих не може да израчуна $g^{a_A a_B}$ без решавања ПДЛКП. Да би добила $g^{a_A a_B}$ Цица мора да степенује g^{a_A} на a_B. Да би дошла до броја a_B, она мора да искористи бројеве g и g^{a_B}, а то се своди на ПДЛКП, за шта се не зна ефикасан алгоритам. Да Цица не би дешифровала Алисину поруку, Алиса и Бобан морају да испоштују неколико правила при бирању параметара: број $q-1$ треба да има велик прост чинилац (иначе ће Цица искористити алгоритам за решавање ПДЛКП). Остатак $g^{a_A a_B}$ је отприлике исте величине као и $q \geq 10^{200}$. Да би се од овога добио кључ за AES, они се могу договорити да издвоје најнижих 128 бита бинарне репрезентације броја $g^{a_A a_B}$. Често Алиса и Бобан генеришу своје приватне кључеве a_A, a_B у тренутку контакта и користе их само за ту размену порука.

5.3.1 Пример

Нека је $q = 97$, а генератор датог поља $g = 5$. Алисин приватни кључ је $a_A = 36$, па је $g^{a_A} = 5^{36} \equiv 50 \pmod{97}$ њен јавни кључ. Што се тиче Бобана, његов приватни кључ је $a_B = 58$, а јавни $g^{a_B} = 5^{58} \equiv 44 \pmod{97}$. Алиса и Бобан редом израчунавају $(g^{a_B})^{a_A} = 44^{36} \equiv 75 \pmod{97}$ и $(g^{a_A})^{a_B} = 50^{58} \equiv 75 \pmod{97}$. Полазећи од бројева 97, 5, 50, 44 Цица не може лако да дође до броја 75.

5.4 ЕлГамалов алгоритам за шифровање

ЕлГамалов систем за шифровање се базира на систему Дифи-Хелман јер је поступак припреме (генерисања кључа) сличан као код ПУКДХ. Представљен је 1985. године од стране Тахера Елгамала [8]. Може се користити за слање порука, али и за слање кључа за AES систем. Међутим, овај систем се више користи у варијанти заснованој на примени елиптичких кривих, него кад се користе коначна поља.

Алгоритам се може дефинисати над коначним пољем G величине q. Ако је величина поља велики прост број p, онда ће Алиса поруку M да кодира бројем између 0 и $p-1$. Уколико је пак $q = 2^d$ онда се порука M пребацује у ASCII код

[8] Тахер Елгамал (енгл. Taher Elgamal, 1955), египатски криптограф

(нпр. 101110...), па се низ бита кодира полиномом (нпр. $1 \cdot x^{d-1} + 0 \cdot x^{d-2} + 1 \cdot x^{d-3} + ...$). Ако је порука превелика, разбија се на блокове.

5.4.1 Принцип рада алгоритма (генерисање кључа, шифровање и дешифровање)

- При генерисању кључа Алиса користи јавне податке: генератор поља g и број g^{a_B}.
- Затим бира случајни број k који мења за сваку нову поруку ($1 < k < q$).
- Знајући све потребне параметре израчунава бројеве g^k и $M \cdot g^{a_B k} (= (g^{a_B})^k)$, а затим тај пар шаље Бобану.
- Бобан не зна Алисин изабран број k, али му он није ни потребан јер поседује свој приватни део кључа a_B. Он израчунава $g^{a_B k} = (g^k)^{a_B}$.
- Затим израчунава $(g^{a_B k})^{-1}$ (у пољу G).
- Поруку M добија множењем $(Mg^{a_B k}) \cdot (g^{a_B k})^{-1} = M$.

Уколико Цица пресретне Алисин пар који она шаље Бобану, она ће поседовати бројеве g и g^k, за шта јој треба решавање ПДЛКП да би дошла до броја k. Када би решила тај проблем и дошла до траженог броја Цица би могла лако да израчуна $g^{a_B k}$, па $(g^{a_B k})^{-1}$, а затим и саму поруку.

5.4.2 Пример

Нека је величина поља G, $q = 97$, а његов генератор $g = 5$. Бобан чува у тајности свој приватни кључ $a_B = 58$, а јавни објављује, $g^{a_B} = 44$. Алиса жели да пошаље поруку $M = 30$ Бобану. Она за случајни број k бира број 17. Алиса онда израчунава $g^k = 5^{17} = 83$ и $(g^{a_B})^k = 44^{17} = 65$ знајући Бобанов јавни кључ. Шифрована порука $M \cdot g^{a_B k} = 10$ и $g^k = 83$ се шаљу Бобану. Када Бобан добије бројеве 83 и 10 и знајући $a_B = 58$, израчунава $(g^k)^{a_B} = 83^{58} = 65$ и $(g^{a^B k})^{-1} = 65^{-1} = 3$. Након тога лако долази до поруке M: $Mg^{a_B k}(g^{a_B k})^{-1} = 10 \cdot 3 = 30 = M$.
Напомена: Сва израчунавања се врше у пољу G тј. применом правила конгруенције (по модулу 97).

5.5 Размена кључева Меси-Омура

Овај протокол су 1982. године представили Џејмс Меси [9] и Џим К. Омура [10] као побољшање Шамировог протокола. Овај алгоритам се не сврстава ни у асиметричне, ни у симетричне шифарске системе. Може се користити за размену кључева или порука, а највише се примењивао код мобилних телефона. Алгоритам ради над коначним пољем $\mathbb{F}_q^*$ где је q велики број, али нису потребни ни генератор поља ни јавни кључеви.

[9] Џејмс Меси (енгл. James Lee Massey, 1934–2013), теоретичар информација и криптограф

[10] Џим К. Омура (енгл. Jimmy K. Omura, 1940.), инжењер електротехнике и теоретичар информација

5.5.1 Принцип рада алгоритма

- Пре слања поруке Алиса бира случајни кључ e_A који ће користити за шифровање: $(e_A, q-1) = 1$
- На исти начин Бобан бира свој кључ e_B: $(e_B, q-1) = 1$. Та два кључа њих двоје ће користити за само једну размену порука.
- Свако од њих даље израчунава $d_A \equiv e_A^{-1} \pmod{q-1}$(Алиса) и $d_B \equiv e_B^{-1} \pmod{q-1}$(Бобан) које чувају за себе.
- Алиса кодира поруку бројем из поља $M \in \mathbb{F}_q^*$ (ако је предугачка разбија је на блокове).
- Алиса шаље Бобану остатак M^{e_A} из поља.
- Бобан израчунава $(M^{e_A})^{e_B} = M^{e_A e_B}$ и враћа дати број Алиси.
- Алиса израчунава $(M^{e_A e_B})^{d_A} = M^{e_A d_A e_B} = M^{e_B}$ и то поново шаље Бобану.
- Бобан израчунава $(M^{e_B})^{d_B} = M$ и добија поруку.

Принцип рада се може објаснити и на сликовит начин: Алиса жели да пошаље поруку Бобану, али једино што поседује је кутија са катанцем за који само она има кључ. Она тако закључану кутију са поруком шаље Бобану иако он за тај катанац нема кључ. Бобан добија закључану поруку, ставља још један катанац за који само он има кључ и враћа кутију Алиси. Алиса откључава свој катанац и скида га, након чега порука остаје закључана само Бобановим катанцем. Тако закључану поруку шаље Бобану коју он сада може да откључа.

5.5.2 Пример

За величину поља се узима број $q = 677$. Алиса жели да пошаље Бобану биграм SC. Биграм прво кодира бројем $18 \cdot 26 + 2 = 470 = M(S = 18, C = 2)$. За приватне кључеве бирају $e_A = 255$ и $e_B = 421$. Израчунавају бројеве $d_A = 255^{-1} \pmod{676} = 395$ и $d_B = 421^{-1} \pmod{676} = 281$. Алиса израчунава $470^{255} \equiv 292 \pmod{677}$ и број 292 шаље Бобану. Бобан израчунава $292^{421} \equiv 156 \pmod{677}$ и број 156 враћа Алиси. Алиса израчунава $156^{395} \equiv 313 \pmod{677}$ и број 313 шаље Бобану. Бобан долази до полазног броја 470 израчунавајући $313^{281} \equiv 470 \pmod{677}$ након чега лако долази до биграма SC дељењем бројем 26 са остатком.

6 Потписи и аутентикација

Када би Цица послала поруку Бобану, али се представила као Алиса, то се не би могло назвати подметањем лажне поруке, већ лажним представљањем. Како Бобан и Алиса могу да се заштите? Потребно је да уведу систем дигиталног потписивања да би били сигурни ко им шаље поруке. Поступак који обезбеђује да будете сигурни да је поруку послао прави пошиљалац зове се *аутентикација*. Аутентикација повезује јавни кључ са особом или институцијом. Користе се потписи и сертификати. Најчешће се за потписе користе системи са јавним кључем.

6.1 Потписи помоћу RSA

Претпоставићемо да Алиса(=A) и Бобан(=B) користе RSA систем. Како у датом систему не постоји заједнички кључ који знају само њих двоје, Цица(=C) може да пошаље поруку Бобану потписујући се као Алиса.
Нека је f_B шифарска трансформација која се користи за слање порука Бобану (у систему RSA, $C \equiv f_B(P) = P^{e_B} \pmod{n_G}$), а f_A за слање порука Алиси. Тада се функција f_B^{-1} користи за дешифровање које врши Бобан (у систему RSA, $P \equiv f_B^{-1}(C) = C^{d_B} \pmod{n_G}$). Исто тако важи и за Алису која користи f_A^{-1}. Функције f_B и f_A су познате свима, док функцију f_B^{-1} зна само Бобан, а f_A^{-1} само Алиса.

Случај 1: Алиса жели да пошаље поруку P Бобану, без шифровања. На крају поруке она ће се потписати користећи своју функцију $f_A^{-1}(\text{"}Alisa\text{"})$. Овај потпис изгледа као шифрат док Бобан не искористи јавну функцију $f_A(f_A^{-1}(\text{"}Alisa\text{"})) = \text{"}Alisa\text{"}$. Иако само Алиса зна функцију f_A^{-1} коју користи за шифровање свог имена, Цица може да пресретне целу поруку и копира само крајњи део који изгледа као шифрат, који ће после користити за потписивање у својим порукама.

Случај 2: Уколико Алиса жели да шифрује целу поруку са потписом она прво Бобану мора послати поруку "*Poruka od Alise*" или ако не жели да непријатељ сазна ко шаље поруку послаће $f_B(\text{"}Poruka\ od\ Alise\text{"})$. Након тога шаље $f_B(f_A^{-1}(P))$. Бобан зна f_B^{-1} па ће лако израчунати $f_B^{-1}(f_B(f_A^{-1}(P))) = f_A^{-1}(P)$. Даље може да израчуна $f_A(f_A^{-1}(P)) = P$ и тиме добија Алисину поруку.

Случај 3: Алиса шифрује отворени текст P алгоритмом AES. Након тога она израчунава MAC(Message Authentication Code) за отворени текст, па га шифрује и потписује помоћу AES. Претходно је Алиса Бобану послала кључеве за AES и MAC користећи RSA.

6.1.1 Пример проблема са RSA

Претоставићемо да је $n_A < n_B$. Нека је $P_1 = \text{"}Poruka\ od\ Alise\text{"}$, а P_2 стварна порука. Алиса израчунава $P_1^{e_B} \pmod{n_B}$ и шаље Бобану. Знамо да је $0 \leq P_1^{e_B} < n_B \pmod{n_B}$. Алиса даље израчунава $P_2^{d_A} \pmod{n_A}$, где је $0 \leq P_2^{d_A} < n_A \pmod{n_A}$. Затим израчунава $(P_2^{d_A})^{d_B} \pmod{n_B} < n_B$ и то шаље Бобану. У даљем тексту ће се подразумевати да је $P_2^{d_A}$ резултат свођења степена по одговарајућем модулу n_A. Бобан редом израчунава $(P_1^{e_B})^{d_B} = P_1 \pmod{n_B}$, $((P_2^{d_A})^{e_B})^{d_B} \doteq P_2^{d_A} \pmod{n_A}$ и $(P_2^{d_A})^{e_A} = P_2 \pmod{n_A}$. Проблем настаје због тога што Бобан не може да уради

исту ствар када шаље Алиси поруку јер је $n_A < n_B$. На месту са изразом обележеним са $\doteq$ Алиса би имала израз $P_2^{d_B} \pmod{n_A}$. При томе је могуће да се деси да је $n_A < P_2^{d_B} < n_B$. Ако је n_B за две цифре дуже од n_A, онда $P_2^{d_B} \pmod{n_A}$ може да буде конгруентан са ≈ 100 различитих бројева по модулу n_B.

6.1.2 Пример

Нека су дате следеће вредности: $n_A = 1000, n_B = 100000$ и $P_2^{d_B} = 10008$. Број 10008 име јединствен остатак по модулу n_B, али тај број по модулу n_A даје остатак 8. Због тога је немогуће одредити да ли је тај остатак 8, 1008, 2008, ..., 99008. Ових 100 вредности имају различите остатке по модулу n_B, али један исти остатак по модулу n_A.

Овај проблем се може решити на следећи начин: Пошто је $n_A < n_B$, Бобан треба да шаље $f_B^{-1}(f_A(P_2))$. Алиса зна да је порука од Бобана захваљујући делу P_1 и зна да је $n_A < n_B$, па израчунава $f_B(f_B^{-1}(f_A(P_2))) = f_A(P_2)$. После тога примењује f_A^{-1}. Закључак је да кад се порука шифрује да се увек прво користи мало n, па велико n.

6.1.3 Пример потписа помоћу RSA:

Нека су $n_B = 221, e_B = 187, d_B = 115, n_A = 209, e_A = 191, d_A = 131$. Алиса жели да потпише и шифрује поруку 97 за Бобана. Како она то ради? Прво користи мало n, па велико n. Прво потпис: $97^{d_A} \pmod{n_A} = 97^{131} \pmod{209} = 108$, па онда шифровање: $108^{e_B} \pmod{n_B} = 108^{187} \pmod{221} = 56$. Бобан добија шифрат 56, а то је једино што види непријатељ. Када Бобан добије поруку, он ће најпре да примени велико n, па мало n: $56^{d_B} \pmod{n_B} = 56^{115} \pmod{221} = 108$, $108^{e_A} \pmod{n_A} = 108^{191} \pmod{209} = 97$. Сада Бобан жели да потпише и шифрује поруку 101 за Алису. Кад шаље поруку, најпре примењује мало n, па велико n: $101^{e_A} \pmod{n_A} = 101^{191} \pmod{209} = 112$ (шифровање), $112^{d_B} \pmod{n_B} = 112^{115} \pmod{221} = 31$ (потпис). Бобан шаље потпис 31. Алиса прво примењује велико n, па мало n: $31^{e_B} \pmod{n_B} = 31^{187} \pmod{221} = 112$, $112^{d_A} \pmod{n_A} 112^{131} \pmod{209} = 101$.

6.2 ЕлГамалов потпис

ЕлГамалов потпис послужио је као основа нешто сложенијем стандарду дигиталног потписа, DSS, скраћено од Digital Signature Standard. Иако је и овај алгоритам представио египатски криптограф Тахер Елгамал, 1985. године, не треба га мешати са ЕлГамаловим системом за шифровање.

У овом алгоритму се полази од великог простог броја p, генератора g за $\mathbb{F}_p^*$, јавних кључева $g^{a_A}, g^{a_B}, ...$ и тајних кључева $a_A, a_B, ...$ Претпоставимо опет да Алиса жели да пошаље поруку Бобану. Нека је та порука S, при чему је S број за који важи $1 < S < p$. Алиса бира случајни број k тако да је $1 < k < p, (k, p-1) = 1$, и израчунава $g^k \equiv r \pmod{p}$. Затим она решава конгруенцију по x: $S \equiv a_A \cdot r + k \cdot x \pmod{p-1}$. Тако добија $x \equiv k^{-1} \cdot (S - a_A \cdot r) \pmod{p-1}$. Приметимо сада да је $g^S \equiv g^{a_A \cdot r + k \cdot x} \equiv g^{a_A \cdot r} \cdot g^{k \cdot x} \equiv (g^{a_A})^r \cdot (g^k)^x \equiv (g^{a_A})^r \cdot r^x \pmod{p}$. Алиса шаље Бобану бројеве r, x, S као потпис. Бобан утврђује да је порука од Алисе упоређивањем

бројева $(g^{a_A})^r \cdot r^x \pmod p$ и $g^S \pmod p$. Зашто је Бобан сигуран да је порука од Алисе? Зато што Бобан зна да је само она могла да реши $x \equiv k^{-1}(S - a_A r) \pmod{p-1}$ знајући a_A.

6.2.1 Пример

Нека су $p = 677$ и $g = 2$. За MAC поруке узмимо број $S = 316$. Алиса за свој тајни кључ бира $a_A = 307$, па је дати јавни кључ $g^{a_A} = 498 (2^{307} \equiv 498 \pmod{677})$. Она бира кључ поруке који задовољава горе наведене услове $k = 401$. Даље израчунава $r = g^k = 2^{401} \equiv 616 \pmod{667}$. Затим решава конгруенцију $S \equiv a_A \cdot r + k \cdot x \pmod{p-1}$, тј. $316 = 307 \cdot 616 + 401 \cdot x \pmod{676}$. За x добија вредност 512. Алиса Бобану шаље бројеве $(r, x, S) = (616, 512, 316)$. Када Бобан добије поруку израчунава $g^S = 2^{316} \equiv 424 \pmod{677}$. $(g^{a_A})^r = 498^{616} \equiv 625 \pmod{677}$, $r^x = 616^{512} \equiv 96 \pmod{677}$. Како је $g^{a_A r} g^{kx} \equiv 625 \cdot 96 \equiv 424 \pmod{677}$ исто што и $g^S \equiv 424 \pmod{6777}$ Бобан утврђује да је порука стигла од Алисе.

6.3 Шноров поступак аутентикације

Шноров алгоритам је представљен од стране Клауса Шнора[11] који се међу првима базирао на нерешивости проблема дискретног логаритма. Параметри који се користе у систему бирају се на следећи начин: Нека су p и q прости бројеви такви да важи $q|p-1$. Број a бирамо тако да буде $a^q \equiv 1 \pmod p$. Бројеве a, p, q користе сви учесници система. Сваки учесник поседује и свој приватни кључ s и јавни кључ $v \equiv a^{-s} \pmod p$.

Аутентикација особе A којој се проверава идентитет се врши на следећи начин: Особа A бира случајни број r који је мањи од q и израчунава $x \equiv a^r \pmod p$. Она шаље број x особи B коју треба да увери у свој идентитет. Затим особа B шаље особи A случајни број $e, 0 \leq e \leq 2^t - 1$.A израчунава $y = r + s_A \cdot e \pmod q$ и то шаље назад особи B. B израчунава $a^y \cdot v_A^e \pmod p$ и упоређује добијену вредност са бројем x. На овај начин је установљено да је особа која је послала број y управо особа чији је јавни кључ v_A.

[11] Клаус Питер Шнор (енгл. Claus-Peter Schnorr,1943.), немачки математичар и криптограф

Литература

[1] М. Живковић, *Криптографија* (PDF), 2009

[2] З. Каделбург, В. Мићић, С. Огњановић, *Анализа са алгебром 2*, Круг, Београд, 2017

[3] E. Schaefer, *An introduction to cryptography*(PDF), Santa Clara University

[4] С. Вујошевић, *Теорија бројева и криптографија* (PDF), 2010

[5] В. Мићић, З. Каделбург, Д. Ђукић, *Увод у теорију бројева*, Друштво математичара Србије, 2013