УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРИРОДНО-МАТЕМАТИЧКИ
ФАКУЛТЕТ
ДЕПАРТМАН ЗА МАТЕМАТИКУ И
ИНФОРМАТИКУ

# Примена теорије бројева у криптографији

**Мастер рад**

**Ментор:**
**Др Бојан Башић**

**Студент:**
**Бранка Милаковић M5 632/20**

"*Mathematics is the queen of the sciences and number theory is the queen of mathematics.*"
*Gauss*

"*Number theorists are like lotus − eaters −having tasted this food, they can never give it up.*"
*Kronecker*

"*A little bit of math can accomplish what all the guns and barbed wire can't : a little bit of math can keep a secret.*"
*Snowden*

"*A secret between two is a secret of God; a secret among three is everybody's secret.*"
*French proverb*

# Садржај

## Предговор

У овом раду упознаћемо се са појмом криптографије, неким њеним методама и применама, као и елементима математике који су потребни за разумевање и рад са криптографијом. Поред појма криптографија упознаћемо се и са значењем појма стеганографија који се често доводи у везу са појмом криптографија јер се циљеви ове две вештине донекле поклапају. Циљ и једне и друге вештине је тајно преношење порука, али су алати који се користе другачији. Управо да би се боље увидела разлика између ова два појма биће дато неколико примера стеганографије.

# 1 Увод

## 1.1 Шта је теорија бројева

Теорија бројева је математичка дисциплина која се бави проучавањем особина бројева, претежно целих и природних бројева. Када говоримо о природним бројевима мислимо на скуп чији су елементи бројеви: 1, 2, 3, 4... и означавамо га са $N$, док када говоримо о целим бројевима мислимо на скуп чији су елементи: 0, $\pm$ 1,$\pm$ 2, $\pm$ 3, $\pm$ 4... и означавамо га са $Z$.

С обзиром на то да се човек од најранијих времена сусретао са овим бројевима, закључујемо да теорија бројева представља једну од најстаријих математичких дисциплина. Појмови који се и данас уче у основним и средњим школама познати су још од античког доба. Пример тога је Питагорина теорема, која се и данас учи у седмом разреду основне школе. Осим тога, постоје алгоритми који су још тад откривени, али се, због своје ефикасности, и даље примењују. У то доба коришћен је израз аритметика, који је синоним за теорију бројева, тачније, теорија бројева је била називана вишом аритметиком. Иако је израз аритметика застарео и данас се више не користи када се говори о теорији бројева, и даље се може наћи у именима неких математичких области и теорема, примери тога су: аритметичке функције, основна теорема аритметике, аритметика елиптичних кривих...

Теорија бројева састоји се од неколико подобласти:

1. Елементарна теорија бројева
2. Аналитичка теорија бројева
3. Алгебарска теорија бројева
4. Геометријска теорија бројева
5. Комбинаторна теорија бројева
6. Рачунарска теорија бројева

Елементарна теорија бројева проучава целе бројеве, али при том не користи технике из других математичких области. Ова област бави се питањима дељивости, факторизације, остацима и разним својствима простих и савршених бројева и конгруенција (о њима ће после бити речи).

Аналитичка теорија бројева такође проучава целе бројеве, али при том користи технике које се примењују у анализи и комплексној анализи.

Алгебарска теорија бројева представља теорију бројева примењену на скуп бројева који је проширен елементима који се називају алгебарски бројеви. Алгебарски бројеви су нуле полинома са рационалним коефицијентима, али они сами нису рационални. Геометријска теорија бројева, позната и као геометрија бројева, уводи основне геометријске појмове у теорију бројева.

Рачунарска теорија бројева проучава алгоритме који су важни за теорију бројева. Неки од њих, попут алгоритама за проверу да ли је број прост и алгоритма за факторизацију целих бројева, примењују се у криптографији и о њима ће касније бити више речено.

## 1.2 Шта је криптографија

Криптографија је наука која се бави шифровањем и дешифровањем информација ради њиховог очувања или скривања. Назив криптографија настао је од грчких речи, *kryptos* што значи тајан или скривен, и *graphein* што значи писати, дакле у директном преводу криптографија значи скривено писање.

Поред појма криптографије имамо и појам стеганографија који се такође односи на преношење порука у тајности. Главна одлика стеганографије је сакривање постојања поруке. Пример стеганографије је постојање невидљивог мастила, на пример сок од лимуна се помеша са водом и њиме се напише порука која се, кад се папир осуши, не види али постаје видљива када се папир приближи извору топлоте, на пример пламену свеће.
Код криптографије постојање поруке није тајност, али сама порука јесте. Она омогућава да две стране комуницирају преко „небезбедног" канала тако да нико други не разуме шта је речено.

Циљеви криптографије су:

1. Очување тајности информација (нико не сме да открије садржај информација)

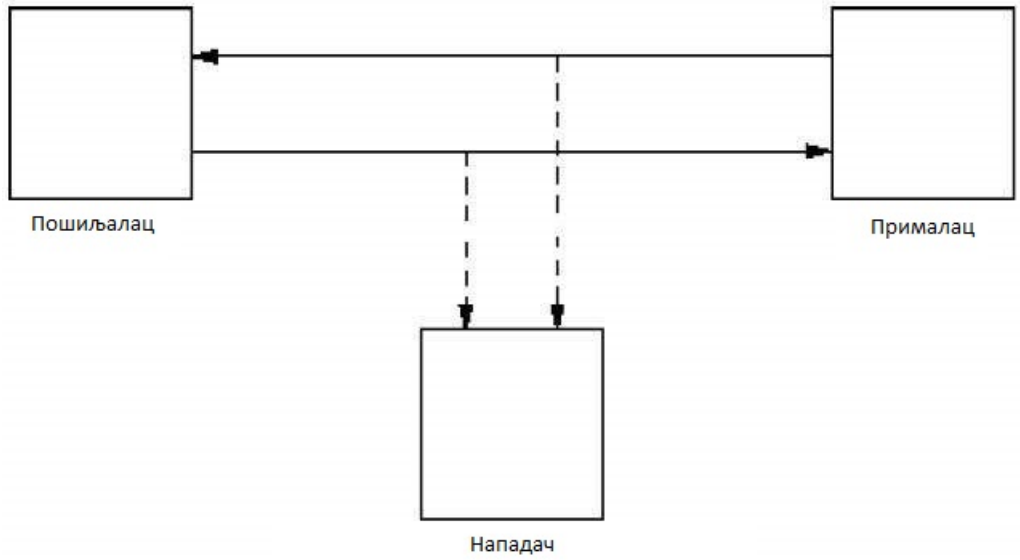
2. Очување интегритета информација (неовлашћена особа не сме да измени информације)

3. Очување аутентичности информација (провера идентитета пошиљаоца)

Елементи криптографије су:

1. шифровање – поступак којим се читљив текст преводи у нечитљив
2. дешифровање – поступак којим се шифрован текст преводи у читљив текст
3. кључ – почетна вредност алгоритма који се користи за шифровање

Поред криптографије сусрећемо се са појмом криптоанализа. Криптоанализа је наука која проучава дешифровање шифрованог текста приликом чега није познат алгоритам за дешифровање. Криптоанализу углавном користи трећа страна која жели да сазна садржај текста који јој није намењен, али користе је и дизајнери алгоритама да би утврдили сигурност алгоритма.




Приказ пошиљаоца и примаоца поруке и нападача који покушава да сазна поруку

Криптоанализа је област која је почела да се развија нешто касније него криптогафија. Са њеним развојем настаје и нова математичка област, под називом криптологија, коју чине криптографија и

криптоанализа. Управо због тога, данашњи криптолози су претежно математичари.

С обзиром на то да је криптографија област која се већ дуго развија, временом је направљено више модела шифара које се разликују у појединим аспектима. У даљем тексту биће наведене врсте шифара и начин на који их класификујемо.

Ако гледамо шифре у односу на то какав алфабет користе, имамо:

1. Полиалфабетне шифре – за свако слово алфабета постоје два или више слова која га могу заменити;

2. Моноалфабетне шифре – свако слово алфабета се замењује тачно једним словом алфабета.

Ако гледамо кључ који шифре користе, онда их можемо поделити на:

1. Симетричне шифре – то су оне шифре за које, ако знамо функцију која је коришћена за шифровање, можемо лако да одредимо функцију помоћу које можемо дешифровати текст;

2. Асиметричне шифре – шифре за које, иако знамо функцију која је коришћена за шифровање, ипак нисмо у стању да одредимо функцију помоћу које можемо дешифровати поруку (овим шифрама ће бити посвећена посебна пажња у овом раду);

3. Хибридне шифре – као што се може претпоставити на основу имена, ове шифре користе и симетричне и асиметричне кључеве.

Следећа подела је према врсти операција које се користе при шифровању, и ту имамо:

1. Супституционе шифре – шифре у којима се слова замењују неким другим словима тако да се оригинална слова и не морају јављати у тексту који се шифрује;

2. Транспозиционе шифре – шифре у којима слова оригиналног текста остају иста, али се мења њихов редослед;

3. Хибридне шифре – слично као и у претходној подели, овде хибридне шифре представљају комбинацију супституционих и транспозиционих шифри.

Следећа подела је према начину на који се обрађује текст који се шифрује:

1. Блоковне шифре – код њих се текст дели на блокове који се посебно шифрују;

2. Проточне шифре – текст који се шифрује се гледа као низ знакова без прекида, тј. нема блокова који се посебно шифрују.

За крај, имамо још поделу према начину који трећа страна користи да би открила шифровану поруку:

1. Компромитовани алгоритми – чине је алгоритни које су нападачи већ детаљно анализирали због чега су им познати начини за декрипцију. У ову групу спада већина алгоритама који су нам познати;

2. Некомпромитовани алгоритми – су они алгоритми за које су покушаји за декрипцију за сада безуспешни. Пример таквог алгоритма је RCA алгоритам на који ћемо посебно обратити пажњу у овом раду;

3. Неанализирани алгоритми – веома мала група у којој се налазе алгоритми за које још није било покушаја дешифровања без унапред познате шифре.

# 2 Историја

## 2.1 Ране шифре и стенографија

Криптографија, односно шифровање или кодирање, користи се хиљадама година. Спартанци су први који су користили криптографију у војне сврхе. Они су користили направу која се назива скитал и која је уствари била дрвени штап са намотаном траком на коју се онда хоризонтално писала порука, која самим тим не би могла бити прочитана ако би се трака одмотала са штапа. Исто тако, порука не би била читљива ако би се намотала на штап друге дебљине. Једини начин да се порука прочита јесте да се трака на којој је порука намота на штап који је исте дебљине као онај на ком је трака била када је порука написана.

Скитал

Колико је познато, Спартанци су и први који су користили стенографију. У прилог томе говори анегдота из седме књиге Херодотовог дела „Историја“ која говори о намери персијског краља Ксеркса да освоји Грчку, тадашњу Хеладу. Наиме, Демератос, који је некада био краљ Спарте и који је из исте протеран, сазнао је за Ксерксове намере и решио је да обавести Спартанце. Да не би био ухваћен, то је урадио на следећи начин: узео је дрвену плочу преливену воском (такве плоче су се у то доба користиле за писање) и скинуо восак и написао поруку директно на дрвету, затим је дрво поново прелио воском тако да се ништа није видело. На тај начин је порука могла да буде пренесена а да нико не помисли да она постоји. Међутим, неприлика се јавила када је порука дошла у Спарту јер тадашњи краљ Спарте, Леонида, и његови људи нису знали шта да раде са њом. Проблем је решила Леонидина супруга, Горга, која је предложила да се восак скине са плоче. Након што су је послушали били су у могућности да прочитају писмо и да га затим проследе осталим полисима. Управо

због ове поруке Грчка је успела да се одбрани од Ксерксовог напада и да спречи ширење Персије ка Европи.

Још један занимљив пример примене стенографије имамо у петој Херодотовој књизи у делу који говори о опсади Накса. Хистијеј, који је невољно био лоциран у Сузи, хтео је да поручи Аристагори, који је владао у Милету, да је време да се подигне устанак. Да би то урадио, обријао је главу свог највернијег роба и на њој истетовирао писмо за Аристагору. Чим је коса порасла довољно да се писмо не види Хистијеј је послао роба Аристагори уз наредбу да каже Аристагори да му обрије главу и погледа је. Исто као и у примеру са дрветом и воском, ни овде нико није ни претпоставио да постоји порука која је сакривена на глави и испод косе једног роба.

Следећи пример, долази нам из, да кажемо, новије историје, јесте начин плетења косе робова у Америци и њихов начин плесања. Вероватно смо сви имали прилике да, бар на телевизији, видимо занимљиве шаре које Афроамериканци стварају уплићући своју косу, али мало ко зна да тај начин плетења води порекло из робовласничких времена. У то време, робовима на плантажама није било дозвољено да читају и пишу и временом већина робовласника је успела да научи њихов језик довољно да их разуме па су морали да нађу други начин за преношење информација. Тај начин је био плетење косе. Како су углавном сви радили на великим пантажама, они који су планирали да побегну на главама су плели плетенице које су уствари биле мапе пута којим је требало ићи. На пример, плетенице које су ишле уз главу су представљале пут којим је требало ићи да би се побегло, ако би нека плетеница била умотана тако да изгледа као пужић, представљала је планину или брдо поред којег је требало проћи и тако даље... Осим тога, плетенице су им служиле да у њима сакрију делиће злата и семена која би, кад би се нашли на слободи, засадили и узгајали. Нажалост, за ово нема писаних доказа већ само усмених предања, али упркос томе, сматрала сам да је важно поменути.

Примери плетеница које су се плеле

Осим плетеница, занимљиво је споменути плес капуеру који је настао међу колонијама робова у Бразилу које су тежиле да вежбају своје борилачке вештине. Како то није било дозвољено, развили су врсту плеса који у себи садржи доста акробатике и удараца који њиховим власницима нису деловали сумњиво, а њима је омогућавало да вежбају и да успут преносе културу и традицију.

Капуера

Ово су били примери где је стенографија успешно примењена али, нажалост, има и примера где није. Такав је пример Марије Стјуарт, која је током заробљеништва код сер Волсингема, уз помоћ племића Ентонија Бабингтона, ковала план да се ослободи. Њихова писма су преношена у тајној прегради у буради са пивом, али оно што нису знали је да је Маријин стражар сазнао за писма и слао их Волсингему, који их је читао без Маријиног и Бабингтоновог знања и чекао повољну прилику која је дошла када је Бабингтон Марији написао детаље плана и имена свих укључених.

Може се приметити да је у овим примерима порука коју је требало пренети била изложена јавности и било ко је могао да дође до ње, само да је знао да она постоји. Ту се крије кључна разлика између криптографије и стенографије, јер код криптографије супротна страна зна да порука постоји, можда ће чак и успети да дође до ње, али ако не буде знала да је дешифрује, све је то узалудно. Док, са друге стране, ако би друга страна сазнала за стенографски сакривену поруку и дошла до ње, одмах би је знала, управо због тога је код стенографије кључно то да друга страна не зна за постојање поруке.

Сада када је разлика између криптографије и стенографије јасна, можемо се вратити појму криптографија и видети још неке историјске примере где се она примењивала.
Познато је и да је Цезар користио криптографију када је слао поруке. Наиме он је замењивао сва слова у поруци на унапред одређен начин. Рецимо да порука коју је хтео да пошаље гласи: „Напад”. Тада би сва слова заменио словима која су три слова испред њих. У табели су наведена сва слова азбучним редом, ту видимо да су слова н, а, п, д редом 16, 1, 19 и 5. слово, даље њих замењујемо словима која су на 19, 4, 22 и 8. месту.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Д | Ђ | Е | Ж | З | И | Ј | К | Л | Љ | М |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| Н | Њ | О | П | Р | С | Т | Ћ | У | Ф | Х | Ц | Ч | Џ | Ш |

Дакле шифрована порука гласи: „пгтгж”.

Прималац поруке, да би дешифровао поруку, треба свако слово да замени словом које се налази три слова пре написаног слова. Управо

због тога овај начин шифровања припада врсти шифри које називамо супституционе шифре.

Примећујемо да се већ у овом, најстаријем познатом начину шифровања, примењује теорија бројева. Наиме, нека је $m$ број који смо доделили слову у оригиналној поруци и нека је $c$ број који одговара слову којим мењамо почетно слово приликом шифровања. Број 3, односно број места за колико померамо слова називамо кључ и обележићемо га са $k$. Сада важи да је

$$c \equiv m + k \pmod{29}, k \in Z_{29} \tag{1}$$

Или можемо посматрати на следећи начин: $f(m) = m+3 \pmod{29}$, тада је инверзна функција $f^{-1}(c) = c-3 \pmod{29}$. Функцију $f$ користимо приликом шифровања, а функцију $f^{-1}$ користимо приликом дешифровања поруке.

Наравно, да би овај начин шифровања радио, потребно је да особа која прима поруку зна на који је начин порука шифрована, односно потребно је да зна кључ да би могао да је дешифрује.

Ако би порука доспела до погрешне особе, та особа не би могла лако да прочита поруку без кључа, али постојали су начини за то. Један од начина је било испробавање свих могућих бројева који могу бити кључ. У нашем примеру тих бројева очигледно има 29 што нам говори да би се порука на крају успела дешифровати и без кључа, али то захтева велику количину времена. Други начин назива се анализа учесталости и захтева познавање учесталости слова у језику. Односно, да би се применила ова метода потребно је знати којом учесталошћу се примењује које слово у језику на ком је написана шифра, а затим погледати које слово се највише пута појављује у шифрованом тексту и на основу тога претпоставити који је кључ, ако тако направљени кључ није одговарајући може се покушати са другим словом и тако док се не успе.

Како се људско знање развијало, а самим тим и могућност лакшег дешифровања, тако се и криптографија развијала. Први који су дешифровали поруке без кључа, односно примењивали криптоанализу, били су Арапи. Њихова предност била су висока математичка, статистичка и лингвистичка достигнућа. Захваљујући њима уочили су слова која се појављују чешће од других, слова која се најчешће појављују заједно, и на тај начин су успели да примене прву анализу учесталости.

## 2.2 Виженерова шифра

Цезарова шифра је била пример моноалфабетне шифре, тј. шифре која користи само једну азбуку. Након ње настаје вишеазбучна, односно полиалфабетна, шифра која, као што само име каже, користи више азбука. Један од најпознатијих примера полиалфабетне шифре је Виженерова шифра.

Виженерова шифра је добила име по француском криптографу Блезу де Виженеру[1], коме су, у 19. веку, погрешно приписане заслуге за њено откриће. Данас нам је познато да је ту шифру први спомињао Италијан Ђован Батиста Беласо[2].

Виженеров шифарник за шифровање користи реч или фразу, коју називамо кључ, у којој се свако слово замени његовом нумеричком вредности. Притом исто слово не мора, сваки пут кад се појави, бити замењено истом вредношћу. Постоје два начина да се примени Виженерова шифра, али најпре се порука која се шифрује дели на блокове оне дужине колика је дужина речи или фразе која се користи за шифровање. После овога имамо две могућности.

Прва могућност је да се свако слово замени својом нумеричком вредношћу у таблици (може се користити таблица попут оне у Цезаровој шифри). Исто се уради и са кључем. Нека су у том случају $k_1, \ldots, k_n$ нумеричке вредности слова која чине кључ, а $m_1, \ldots, m_n$ нумеричке вредности слова у блоковима поруке. Сада сваку нумеричку вредност слова у поруци замењујемо нумеричком вредношћу коју добијамо на следећи начин:

$$c_i \equiv m_i + k_i \pmod{29} \tag{2}$$

Сада добијене бројеве заменимо словима која им одговарају и добили смо шифровану поруку.
Очигледно, да би се ово дешифровало потребно је применити сличну функцију:

$$m_i \equiv c_i - k_i \pmod{29}. \tag{3}$$

Дакле, први блок цифара, односно њихову нумеричку вредност сабирамо са бројем који одговара првом слову кључа и гледамо њихов остатак при дељењу са бројем цифара које користимо. Бројеве из другог блока сабирамо са бројем који одговара другом слову кључа

[1] Blaise de Vigenère (1523 - 1596) - француски дипломата, криптограф, преводилац и хемичар

[2] Giovan Battista Bellaso (1505 - непознато) - италијански криптолог

и исто гледамо остатак при дељењу. Овај поступак наставимо све док шифрујемо целу поруку, а ако у неком моменту искористимо сва слова кључа, онда крећемо опет од почетног слова. Ако се деси да кључ има више слова него што је блокова, онда само станемо кад шифрујемо сва слова. Такође се може десити да је последњи блок краћи од осталих али то не представља проблем, у том случају слова која су нам остала у последњем блоку шифрујемо у складу са правилима.

На пример, нека је порука коју хоћемо да пошаљемо: Непријатељ долази, и нека је кључ: Столица. Тада су блокови које добијамо и њихове нумеричке вредности (преузете из таблице која је стављена код Цезарове шифре):
Неприја - 15, 6, 18,19, 9, 10, 0
тељдола - 21, 6, 13, 4, 17, 12, 0
зи - 8, 9
Кључ је столица, односно 20, 21, 17, 12, 9, 26, 0, па бројеве у првом реду треба сабрати са 20, бројеве у другом реду са 21 и у трећем реду 9 и гледати њихов остатак при дељењу са 29. Тада добијамо: 6, 26, 9, 10, 0, 1, 20, 13, 27, 5, 25, 9, 4, 21, 25, 26 што је шифрован текст који се шаље. Ако желимо, можемо те бројеве претворити у слова при чему добијамо: ецијабсльчђхидтхц, па тако послати поруку.

Други начин је примена Виженерове таблице (која се налази на следећој страни), која је позната и као Виженеров квадрат, који се састоји од алфабета изнова написаног у новом реду тако да је свако слово сваки пут померено за једно место. Сваки ред заправо одговара некој од могућих комбинација Цезарове шифре. Разлика је у томе што се у неком моменту шифровања прелази у други ред и слова се замењују по правилу које је у том реду. Који ће се ред користити зависи управо од кључа. Рецимо да хоћемо да пошаљемо поруку: Напад здесна. Нека је кључ: Брзо. Пошто реч брзо има четири слова, први блок су прва четири слова: напа, а пошто је прво слово кључа Б у таблици гледамо врсту која је код слова Б и на тај начин мењамо слова. Следећа четири слова мењамо у складу са променом која је код слова Р јер је то друго слово кључа. Са овим поступком наставимо док не шифрујемо цео текст.

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

Виженерова таблица за абецеду

Све ово су били примери шифровања у којима је потребно скривати кључ који је претходно утврђен, међутим са развојем математике откривени су модели шифровања који своје кључеве јавно објављују. О њима ће више речи бити у следећем поглављу.

## 2.3 Енигма

Реч енигма (на грчком *ainigma* - загонетка) означава нешто што нам је непознато, што не можемо да решимо. Почетком 20. века немац Артур Шербијус[3] је конструисао машину за шифровање радиотелеграфских порука којој је дао назив Енигма. Шербијус је покушао да заинтересује јавност за Енигму, међутим ова машина је привукла пажњу немачке војске која ју је користила током Другог светског рата.

[3]Arthur Scherbius (1878 - 1929) - немачки инжењер

Као што видимо на слици на следећој страни, ова справа подсећа на писаћу машину. Са предње стране има тастатуру са 26 слова абецеде и 26 сијалица од којих свака представаља по једно слово. Састојала се од тастатуре и ваљака који су имали струјне контакте који су преносили струју од тастера који је притиснут кроз ваљак па све до сијалице која означава одређено слово и која потом засветли. Након што се један тастер притисне, ваљци се окрену тако да, кад бисмо сад притиснули исти тастер, засветлела би сијалица код другог слова. На тај начин се добијала шифра која се није могла разбити јер је једно исто слово сваки пут било другачије шифровано. Овако су се шифровале и дешифровале поруке помоћу Енигме. Порука се уносила помоћу тастатуре, а шифрована порука би излазила, тј. читала се помоћу сијалица.

Стандардна машина Енигма је имала 3 ваљка што на први поглед не делује пуно, али то је давало чак 17576 почетних положаја ваљака (од чега је и зависило шифровање).

Дакле, пошто имамо три ваљка, број начина да се они распореде је $3 \cdot 2 \cdot 1 = 6$. Сваки ваљак можемо довести у почетни положај који приказује једно од 26 слова абецеде, а пошто имамо 3 ваљка, они нам дају $26 \cdot 26 \cdot 26 = 17576$ почетних положаја који се разликују. Када то помножимо са 6 могућих распореда ваљака, добијамо 105456 различитих комбијација шифре. Када погледамо ове бројеве, постаје много јасније зашто шифре није било могуће дешифровати без Енигме. Поред тога, постојао је начин да се шифровање додатно „закомпликује“ тако што су се струјна кола која су повезивала слова могла заменити, што је додатно повећавало број могућих комбинација. На основу свега овде реченог, да се закључити да је поруку шифровану помоћу Енигме било могуће дешифровати само помоћу друге Енигме, и то ако се зна како је прва Енигма „подешена“.

Примерак Енигме

За Енигму се заинтересовала немачка војска која је убрзо направила своју верзију овог уређаја који је, пред почетак Другог светског рата, имао чак 5 ротора. Иако је француска и британска војска већ 1931. године знала да постоји ова машина и чему служи, нису успели да разоткрију њену шифру. То је успело тек пољском тиму који је предводио математичар Марјан Рајевски. Захваљујући овом тиму Пољска је од 1933. до 1938. године пратила поруке немачке армије,

а када су 1939. сазнали да се припрема инвазија на Пољску, своја открића су проследили британској војсци. Тада су Немци повећали сигурност шифровања тако што су број ротора са 3 повећали на поменутих 5 ротора и тако што су сваки дан мењали начин шифровања, што је додатно отежало разбијање шифре.

Занимљив је начин на који су Британска и Француска војска дошле до машине, наиме, Немац Ханс Тило Шмит, који је из финансијских разлога и освете због бешчасног отпуштања из војске током Првог светског рата, француској обавештајној служби дозволио да фотографише упуства за употребу Енигме, као и дневне шифре које су се користиле у септембру и октобру 1932. Касније га је управо француска обавештајна служба одала Немцима због чега је завршио у затвору у Берлину где се убио тровањем.

Након што је Пољска поделила своја сазнања, дешифровање порука које су послате путем Енигме је настављено у Еглеској. Ту се истиче математичар Алан Тјуринг, који је пронашао начин да у потпуности дешифрује поруке које су Немци слали. Верује се да ово скратило трајање рата за можда чак и годину дана, што је спасило велики број живота.

После рата Енигма машине које су припадале Немачкој и њеним савезницима су Енглеска, Француска и САД конфисковале и продале у блискоисточне и афричке земље, чиме су, како се претпоставља, себи омогућили да дешифрују и прате поруке тих земаља.

# 3 Шифровање помоћу јавног кључа

Множење бројева и растављање резултата множења на просте факторе, иако су међусобно инверзне операције, изузетно се разликују у тежини. Множење је поприлично једноставно и даје се основцима за вежбу, док растављање броја, поготово већег броја, на просте факторе представља много тежи проблем, шта више, сматра се скоро немогућим раставити велики број на просте факторе. Управо на овој чињеници заснивају се алгоритми за шифровање помоћу јавног кључа.

Ови алгоритми објављују кључ за шифровање поруке тако да му свако може приступити и послати шифровану поруку, али кључ за дешифровање, који се не може извести из кључа за шифровање, остаје скривен.

Шифровање се може посматрати као функција $f$ која деловима поруке која се шифрује задаје одређене вредности. Дакле, ако је $P$ порука коју треба послати и $S$ иста та порука када се шифрује, можемо записати:

$$S = f(P). \tag{4}$$

Тада се дешифровање ради помоћу инверзне функције:

$$P = f^{-1}(S). \tag{5}$$

Међутим, налажење инверзне функције $f^{-1}$ представља проблем тј. немогуће је наћи ту функцију у разумном времену.


Скица шифровања јавним кључем

## 3.1 Основни појмови

Да бисмо разумели о чему се ради у наставку рада потребно је подсетити се математичких појмова који ће се користити.

**Дефиниција 3.1.** Група $(G, *)$ је циклична ако је генерисана једним елементом тј. ако постоји $g \in G$ тако да је сваки елемент из G степен елемента $g$:

$$G = \langle g \rangle = \{g^n : n \in Z\}. \tag{6}$$

Елемент $g$ се тада назива генератор групе.

**Дефиниција 3.2.** Ако неутрални елемент групе $(G, *)$ обележимо са $e$, ред елемента $a$ групе $(G, *)$ је најмањи природан број $n$ такав да је $a^n = e$. Ако такав број не постоји, онда кажемо да је елеменат $a$ бесконачног реда.

**Дефиниција 3.3.** Ако је група $(G, *)$ коначна, онда број њених елемената зовемо редом групе. Ако је бесконачна, онда кажемо да је група $(G, *)$ бесконачног реда.

**Дефиниција 3.4.** Група $(G, *)$ је комутативна ако за све $x, y \in G$ важи

$$x * y = y * x. \tag{7}$$

**Дефиниција 3.5.** Нека је $G$ непразан скуп и нека су $*$ и $\cdot$ бинарне операције на том скупу. Алгебарска структура $(G, *, \cdot)$ је поље ако важе следећи услови:

1. $(G, *)$ је комутативна група
2. $(G \backslash \{e\}, \cdot)$ је комутативна група, а $e$ је неутрални елемент у групи $(G, *)$
3. За свако $x, y, z \in G$ важи закон дистрибутивности тј. $x \cdot (y * z) = (x \cdot y) * (x \cdot z)$.

**Дефиниција 3.6.** Нека је $G$ непразан скуп и нека су $*$ и $\cdot$ бинарне операције на том скупу. Алгебарска структура $(G, *, \cdot)$ је прстен ако важе следећи услови:

1. $(G, *)$ је комутативна група
2. $\cdot$ је асоцијативна операција

3. За свако $x, y, z \in G$ важи закон дистрибутивности тј. $x \cdot (y * z) = (x \cdot y) * (x \cdot z)$ и $(y * z) \cdot x = (y \cdot x) * (z \cdot x)$

**Дефиниција 3.7.** Нека је $(G, *, \cdot)$ прстен. Карактеристика прстена $G$ је најмањи позитиван цео број $n$ такав да је $n * a = 0$. Ако такав број не постоји, онда кажемо да је прстен карактеристике 0.

**Тврђење 3.8.** Карактеристика поља је увек 0 или прост број $p$.

**Дефиниција 3.9.** Инвертибилни елементи прстена $(G, *, \cdot)$ су $x \in G$ такви да постоји $y \in G$ за које је $x \cdot y = y \cdot x = 1$. Скуп свих инвертибилних елемената се обележава са $G^*$

**Напомена.** Нула не припада скупу $G^*$.

**Дефиниција 3.10.** За цео број $b$ кажемо да је делилац целог броја $a$, односно да дели $a$ (у ознаци $b \mid a$ ), ако постоји цео број $q$ тако да је $a = bq$.

**Дефиниција 3.11.** Цео број $v$ који дели сваки цео број зовемо јединичним елементом прстена $Z$.

**Теорема 3.12.** *Прстен $Z$ има тачно два јединична елемента:* 1 *и* $-1$.

**Теорема 3.13.** *За све целе бројеве $a$, $b$ и $c$ важи*

1. $a \mid a$;
2. *Ако* $a \mid b$ *и* $b \mid c$, *тада и* $a \mid c$;
3. *Ако* $a \mid b$ *и* $b \mid a$, *тада постоји јединични елемент* $v$ *тако да је* $a = bv$;
4. *Ако* $c \mid a$ *и* $c \mid b$, *тада* $c \mid a + b$, $c \mid a - b$ *и* $c \mid ka$ *за сваки цео број* $k$. *Штавише, тада за све целе бројеве* $\alpha$, $\beta$ *важи* $c \mid \alpha a + \beta b$.

**Теорема 3.14.** *За све целе бројеве $a$ и $b$, $b \neq 0$ , постоје јединствени цели бројеви $q$,$r$ тако да је*

$$a = qb + r \tag{8}$$

*и*

$$0 \leq r < |b|. \tag{9}$$

Поступак наведен у претходној теореми назива се дељење са остатком. Том приликом добијају се цели бројеви $q$ и $r$ који се, редом, називају целобројни количник и остатак. Можемо приметити да број $b$ дели број $a$ акко је остатак при дељењу $a$ са $b$ једнак 0.

**Теорема 3.15.** *Нека је $B$ цео број већи од 1. Тада се сваки позитиван цео број $A$ на јединствен начин може записати у облику*

$$A = a_n B^n + a_{n-1} B^{n-1} + ... + a_1 B^1 + a_0 \tag{10}$$

*где је $a_n \neq 0$ и $0 \leq a_i < B$ за све $0 \leq i < n$.*

**Дефиниција 3.16.** Нека су $a$ и $b$ два цела броја. За цео број $d$ кажемо да је највећи заједнички делилац бројева $a$ и $b$ ако важи

1. $d \mid a, d \mid b$;
2. За сваки цео број $c$ такав да $c \mid a$ и $c \mid b$ важи $|c| \leq |d|$.

Можемо приметити да ако број $d$ задовољава дате услове, онда исте услове задовољава и број $-d$, због тога ћемо, ако није другачије наведено, за највећи заједнички делилац увек узимати позитиван број $d$. У наставку ће највећи заједнички делилац за бројеве $a$ и $b$ бити означен са $(a, b)$.

**Дефиниција 3.17.** Цели бројеви $a$ и $b$ су узајамно прости ако је њихов највећи заједнички делилац 1.

На моменат ћемо се вратити на дељење са остатком које смо раније спомињали. Разлог томе је чињеница да за сваки број $m$ имамо $m$ могућих остатака, што доводи до поделе скупа целих бројева на класе бројева који дају исти остатак при дељењу са бројем $m$. Ову поделу остварујемо коришћењем бинарне операције која се назива конгруенција по модулу $m$ и дефинише се на следећи начин:

**Дефиниција 3.18.** Нека су $a, b$ и $m$ цели бројеви. $a$ је конгруентно са $b$ по модулу $m$, у ознаци $a \equiv b \pmod{m}$ ако и само ако $m \mid a - b$.

**Теорема 3.19.** *(Основна теорема аритметике)*
*Сваки природан број $a > 1$ може се приказати као производ (позитивних) простих бројева и при томе је та факторизација јединствена до на поредак фактора тј. ако важи $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, где су $p_i, q_j$ прости бројеви за све $1 \leq i \leq r, 1 \leq j \leq s$, тада је $r = s$ и постоји пермутација $\pi$ скупа $\{1, 2, \dots, r\}$ тако да је $p_i = q_{\pi(i)}$ за све $1 \leq i \leq r$.*

У разлагању $a = p_1 p_2 \dots p_r$ се један дати прост број може појавити више пута као прост фактор. Због тога је уобичајено да се у разлагању броја на просте факторе, они који се понављају више пута окупе у степене различитих простих бројева: $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} ... {p_k}^{\alpha_k}$. Ово разлагање назива се канонички облик броја $a$.

**Дефиниција 3.20.** Нека је $m \geq 1$, означимо са $\varphi(m)$ број свих елемената стандардног потпуног система остатака по модулу $m$ (тј. низа $0, 1, \dots, m$) који су узајамно прости са $m$. На овај начин добија се Ојлерова функција $\varphi : Z^+ \to Z^+$.

**Теорема 3.21.** *Нека је $n > 1$ природан број дат у каноничком облику. Тада је*

$$\varphi(n) = \prod_{i=1}^{k} ({p_i}^{\alpha_i} - {p_{i-1}}^{\alpha_{i-1}}) = n \cdot \prod_{p|n} (1 - \frac{1}{p}), \tag{11}$$

*где је број $p$ прост број.*

**Теорема 3.22.** *(Ојлерова теорема)*
*Нека је $a \in Z$ и $m > 0$ тако да је $(a, m) = 1$. Тада је $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

**Дефиниција 3.23.** Нека је $k \geq 2$, $p$ прост број и $a \in Z$ тако да је $(a, p) = 1$. Конгруенције облика $x^k \equiv a \pmod{p}$ се називају биномне конгруенције. Када је $k = 2$, кажемо да је $a$ квадратни остатак по модулу $p$.

**Дефиниција 3.24.** Како би се лакше изразило својство „бити квадратни остатак“, уводи се Лежандров симбол $\left(\frac{a}{p}\right) = \pm 1$ тако да је:

- $\left(\frac{a}{p}\right) = 1$ ако је $a$ квадратни остатак по модулу $p$,
- $\left(\frac{a}{p}\right) = -1$ ако $a$ није квадратни остатак по модулу $p$.

**Дефиниција 3.25.** Јакобијев симбол $\left(\frac{a}{m}\right)$ дефинише се као проширење Лежандровог симбола када је доњи аргумент произвољан непаран број $m > 1$. Нека је $m = p_1 p_2 \dots p_r$ разлагање броја $m$ на просте факторе (не морају бити различити) и нека је $(a, m) = 1$. Тада је вредност Јакобијевог симбола на следећи начин дефинисана производу вредности Лежандрових симбола:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right) \tag{12}$$

Ако је број $m$ прост, онда се Лежандров и Јакобијев симбол поклапају.

## 3.2 Појам дискретног логаритма

**Дефиниција 3.26.** Нека је $G$ коначна циклична група реда $n$ и нека је $g$ генератор те групе, а $b$ произвољан елемент те групе. Дискретни логаритам, у ознаци $\log_g b$, је јединствени цео број $x$ мањи од $n$ такав да је $b = g^x$.

Ако имамо коначну мултипликативну групу $G$ реда $n$ онда за сваки елеменат $b$ из те групе можемо израчунати $b^x$. Са друге стране, наћи број $x$ којим треба степеновати $b$ да би се добио $g$ представља проблем који се назива *проблем дискретног логаритма.*

**Дефиниција 3.27.** Нека је $g$ генератор за ${Z_p}^*$, где је $p$ прост број, и нека је $b$ произвољан елемент те групе. Проблем дискретног логаритма представља проналажење целог броја $x$ таквог да важи $0 \leq x \leq p-2$ и $b = g^x \pmod{p}$.

**Дефиниција 3.28.** Нека је $g$ генератор коначне цикличне групе $G$ реда $n$ и нека је $b$ произвољан елемент те групе. Генерализовани проблем дискретног логаритма је наћи цео број $x$ такав да важи $0 \leq x \leq n-1$ и $b = g^x$.

## 3.3 Алгоритам и сложеност алгоритма

Реч алгоритам потиче од имена чувеног арапског научника, које је гласило Абу Џафар Мухамед ибн-Муса ал-Хорезми[4]. Једна од његових чувених књига за коју се претпоставља да се оригинално звала „Al kitab aldzam val-tafrik bi hisab al-Hind“ односно „Књига о сабирању и одузимању у индијском рачуну“, је током прве половине 7. века преведена на латински (и захваљујући томе делимично сачувана) и тада је названа „Algorismi de numero Indorum“[5], у преводу „Ал-Хорезми о индијској вештини рачунања". Одавде се јасно види како је настао појам алгоритма, међутим, за разлику од данашњег појма, тада (док су се још користили римски бројеви) се реч алгоритам односила на вештину сабирања са арапским цифрама (које су, заправо, потекле из Персије и из тог разлога су их Арапи звали персијским цифрама, али с обзиром на то да су их у Европу донели Арапи, овде су оне остале упамћене као арапске цифре).

Данас реч алгоритам има сасвим друго значење тј. односи се на поступак решавања одређеног проблема корак по корак. Тачније, он представља конкретан низ корака које треба направити да би се дошло до решења проблема. Наравно, што је проблем компликованији потребно је више корака да би се он решио, а ако је број корака превелик поставља се питање колико је алгоритам практичан.

**Дефиниција 3.29.** Нека су $f$ и $g$ две реалне функције. Пишемо да је $f = O(g)$ ако постоје константа $C > 0$ и реалан број $x_0$ такви да за све $x \geq x_0$ важи неједнакост

$$f(x) \leq Cg(x). \tag{13}$$

У том случају, кажемо да функција $g$ асимптотски ограничава функцију $f$.

Знак $O$ се назива Ландауов симбол и говори о брзини раста функција и редова. Следе правила за рачунање $O$:

- $c \cdot f = O(f)$ за свако $c > 0$
- $O(c \cdot f) = O(f)$ за свако $c > 0$
- $c \cdot O(f) = O(f)$ за свако $c > 0$

[4] Abu Dzafar Muhamed ibn-Musa al-Horezmi (иако је персијског порекла знатно је допринео развоју читаве арапске културе)

[5] Латински и арапски назив књиге су преузети из књиге Кратак увод у анализу алгоритама - Игор Долинка

- $O(O(f)) = O(f)$
- $O(f_1) + O(f_2) + O(f_3) + ... + O(f_n) = \max\{O(f_1), O(f_2), ..., O(f_n)\}$ за природан број $n$
- $O(f) \cdot O(g) = O(f \cdot g)$
- $g = O(f) \implies O(f + g) = O(f)$
- $log_a n = O(log_b n)$ за $a, b > 1$, односно база логаритма није битна све док је већа од 1 и сви такви алгоритми су исте сложености.

За нас је битан појам полиномне сложености алгоритма, који означава да је број корака који је потребан да се изврши алгоритам асимптотски ограничен са $n_k$, где је $k$ неки позитиван цео број, а $n$ број улазних фактора. Иако делују компликовано, алгоритми полиномне сложености су, заправо, јако брзи и међу њима се налазе алгоритми који решавају сабирање, множење, кореновање, степеновање, логаритмовање... Занимљиво је да ту спадају алгоритми који израчунавају константе попут $\pi$ и $e$.

## 3.4 Дифи–Хелман шифровање

1976. године Витфилд Дифи[6] и Мартин Хелман[7] објавили су чланак у ком су представили идеју за решење дугогодишњег проблема о преношењу кључа за шифровање. Њихова идеја је била да кључ за шифровање јавно објаве, тако да му свако може приступити, али да кључ за дешифровање остане тајан. Због тога што постоје два различита кључа, и један се не може извести на основу другог, овај начин шифровања се зове шифровање асиметричним кључем.

Дифи и Хелман су користили чињеницу да је степеновање елемента поља $F_p$, где је $p$ прост број, позитивним целим бројем $x$, по модулу $p$ операција сложености $O(lnx)$, док је налажење инверзне операције поприлично тешко. Налажење броја $x$ представља проблем дискретног логаритма, који би се теоретски могао решити у полиномном времену, али у пракси нам није позната ни једна метода која је толико ефикасна.

**Алгоритам 3.30.** [8] Ако две особе, Боб и Алис, желе да размене информације за које не желе да их ико сазна, они одаберу прост број

[6] Whitfield Diffie (рођен 1944.) - амерички криптограф и математичар

[7] Martin Hellman (рођен 1945.) - амерички криптограф

[8] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition, страна 388

$p$ и $g \in F_p$. Након тога, обоје праве кључеве (који су мањи од $p$) такве да ниједна особа не може да их открије.

1. **Алис прави јавни кључ**
   Алис бира број $a$ из интервала $[2, p-2]$ и потом степенује унапред договорени број $g$ са бројем који је одабрала. Затим одређује број $x$ који је по модулу $p$ конгруентан добијеном производу.

   $$x \equiv g^a \pmod{p} \tag{14}$$

   Управо тај број $x$ је Алисин кључ.

2. **Боб прави јавни кључ**
   Исто као и Алис, Боб бира број $b$ из интервала $[2, p-2]$, тим бројем степенује унапред одабрани број $g$ и тражи његов остатак при дељењу са $p$. Тај остатак, обележимо га са $y$, је Бобов јавни кључ.

   $$y \equiv g^b \pmod{p} \tag{15}$$

   Следећи корак је да Алис и Боб направе заједнички кључ који ће само њих двоје знати.

3. **Алис и Боб праве заједнички кључ**
   Боб рачуна:

   $$k \equiv x^b \pmod{p} \tag{16}$$

   Алис рачуна:

   $$k \equiv y^a \pmod{p} \tag{17}$$

Видимо да заједнички кључ праве тако што јавни кључ оног другог степенују са бројем који су одабрали из интервала $[2, p-2]$. Тако добијене вредности су идентичне јер важи

$$(g^a)^b = (g^b)^a = g^{ab} \tag{18}$$

То јест, ако број, у нашем случају $g$, степенујемо бројем који није прост, тај степен можемо факторисати и степеновати једним фактором, а потом добијени резултат степеновати другим фактором. Наравно, све то наставља да важи и након што применимо конгруенције.

Укратко, овај алгоритам се ослања на чињеницу да је скоро немогуће израчунати $g^{ab}$ чак и ако знамо $g^a$ и $g^b$.

У теорији, горенаведени алгоритам делује једноставно, али поставља се питање како се он примењује?

Након што су Алис и Боб направили своје кључеве требају послати поруку. Рецимо да Алис шаље поруку Бобу, она ће онда потражити Бобов јавни кључ и искористити га да шифрује поруку коју затим шаље Бобу. Када Боб прими шифровану поруку користи свој приватни кључ да је дешифрује.

На пример[9], Алис и Боб могу да се договоре за јавни кључ док причају телефоном (који представља несигуран начин комуникације):

1. Алис и Боб се договоре да одаберу прост број $p = 13$ и $g = 2$ као генератор групе ${Z_{13}}^*$.

2. Алис бира $a = 11$ и рачуна $x = 2^{11} \pmod{13} = 7$ и шаље Бобу резултат 7. То може урадити тако што ће, на пример, рећи Бобу у телефонском разговору.

3. Боб бира $b = 9$ и рачуна $y = 2^9 \pmod{13} = 5$ и шаље Алис резултат 5 што се, такође, може урадити путем телефонског позива.

4. Сада Алис рачуна $k = y^a = 5^{11} \pmod{13} = 8$, а Боб рачуна $k = x^b = 7^9 \pmod{13} = 8$. Видимо да се добијају исти резултати па је тајни кључ управо број 8.

У случају да је неко прислушкивао Алисин и Бобов позив могао је да сазна прост број $p$ и генератор који су одабрали, а потом и вредности $g^a$ и $g^b$, међутим није могао да чује вредност $g^{ab}$ па му је циљ да то сам израчуна.

Проблем израчунавања $g^{ab}$ када су познати $g^a$ и $g^b$ назива се Дифи–Хелманов проблем ($DHP$).

Ако особа која слуша разговор успе да реши проблем дискретног логаритма ($DLP$), и из $g^a$ нађе $a$, онда лако може да нађе $g^{ab}$. Самим тим, верује се да су $DHP$ и $DLP$ у већини група у криптографији еквиваленти.

У датом примеру због малог $p$ није тешко пронаћи $a$ и $b$, и на основу њих наћи $g^{ab}$. Управо због тога се у пракси за $p$ узимају велики бројеви.

[9] Сви бројеви у овом примеру преузети су из чланка: Бернадин Ибрахимпашић, Драгана Ковачевић, Дискретни логаритам, страна 52

Кевин Макерли[10] је 1989. године поставио проблем тако што је дефинисао бројеве:

$q = \frac{7^{149}-1}{6}$ и
$p = 2 \cdot 739 \cdot q + 1$

и потом је рекао да стране А и Б (у овом примеру Алис и Боб) рачунају:

- Алис рачуна $b_A \equiv 7^{x_A} \pmod{p}$ (користећи тајни кључ $x_A$)
- Боб рачуна $b_B \equiv 7^{x_B} \pmod{p}$ (користећи тајни кључ $x_B$)

и добијају бројеве:
$b_A$ = 1274021801199739468242692443343228497493820425869316216545577352903229146790959986818609788130465951664554581442805880767660337781

$b_B$ = 1801622852874531024447828348367998950159670466953466973130251217340599537720584759581769106253806921016518486623621379340268030 49.

Затим је тражио да се нађе заједнички тајни кључ $K \equiv 7^{x_A \cdot x_B} \pmod{p}$.
Такође, понудио је 100 долара ономе ко успе да израчуна $K \equiv 7^{x_A \cdot x_B}$.

Овај проблем успели су да реше тек 1998. Вебер и Дени[11]. Они су прво израчунали Алисин тајни кључ
$x_A$ = 6185869085965188327359333165203790426798764306952171345914622218495259981561448778207574921829097774083387918504579467497 34,
а затим и
$K$ = 3812728041119001413807839150792963419399864355101867028505637561504552396692940392210217251405327092887263942637006353279774 0808.

Иако је овај проблем решен, видимо да је, да би се дошло до решења, било потребно 9 година, што је превише дуг временски период јер се у међувремену кључеви могу лако променити и онда цео процес креће из почетка, тако да је ипак исплативо користити овај алгоритам. Из овог примера такође видимо да нам није толико битно да ли се може наћи инверзна функција, већ да је битно да је процес налажења те функције дуготрајан, и да је то оно што нам гарантује сигурност података.

[10] Kevin S. McCurley (рођен 1954.) - амерички математичар и криптограф
[11] Damian Weber, Thomas Denny

## 3.5 Одабир простих бројева

Прости бројеви су позитивни цели бројеви који се могу поделити само са 1 и са самим собом и, као што смо видели, да би Дифи-Хелманов алгоритам радио потребно је наћи такав број. Проблем настаје због тога што је њихово појављивање у скупу целих бројева тешко предвидиво и то је довело до развоја начина за проверу да ли је неки број прост.

Метод који се често користи за бирање простих бројева је да се узме неки број одговарајуће дужине и да се затим провери да ли је он прост. Први начин за проверу да ли је број који се тад узме прост јесте да се број проба поделити са свим простим бројевима који су мањи од њега. Иако би нам овај поступак дао исправан одговор, ипак није захвалан за примену јер изискује превише времена. Управо због тога су се развили тестови који дају одговор на питање да ли је неки број прост или није.

Ти тестови су подељени у две групе:

- тестове који дају конкретан одговор на питање да ли је број прост и притом обезбеђују математички доказ (стварни тестови)
- тестове који говоре да је број „вероватно прост" или „вероватно сложен" (пробабилистички тестови)

Предност пробабилстичких тестова над стварним тестовима је у томе што захтевају мање рачунарских ресурса и мање времена. Приликом ових тестова, прост број никада неће бити препознат као сложен, али мана је у томе што некада сложен број може бити препознат као прост. Ови тестови, поред броја који се испитује, користе и случајно изабран број $a$, па се грешке могу редуковати понављањем теста са другачије одабраним вредностима броја $a$.

У наставку је изложено неколико тестова који се користе у ту сврху.

**Фермаов тест** - Овај тест користи Фермаову теорему која каже да, ако је $n$ прост број, онда за сваки позитиван цео број $a$ мањи од $n$ који је узајамно прост са $n$, важи

$$a^{n-1} \equiv 1 \pmod{n} \text{ тј. } a^{n-1} - 1 \equiv 0 \pmod{n}.$$

Ако би се нашао бар један позитиван цео број $a$ мањи од $n$, узајамно прост са $n$, за који не важи $a^{n-1} - 1 \equiv 0 \pmod{n}$ то би значило да

је број $n$ сложен. У овом случају број $a$ се назива „Фермаов сведок сложености“ броја $n$. Са друге стране, ако би дате једнакости важиле за сваки одабран број $a$, то не би било довољно да тврдимо да је број $n$ прост. У случају да је $a$ такав да важи $a^{n-1} - 1 \equiv 0 \pmod{n}$ за сложен број $n$, кажемо да је $a$ „Фермаов лажов“ и да је број $n$ псеудопрост за базу $a$. Очигледно, псеудопрости бројеви пролазе Фермаов тест.

**Соловеј–Штрасенов тест** - Овај тест се заснива на строжим критеријумима него Фермаов тест па самим тим отклања неефикасност Фермаовог теста. Постао је популаран кад су се појавили асиметрични шифарски системи, поготово RCA систем.

Заснива се на Ојлеровом критеријуму, који каже да, ако је $n$ прост број, онда за сваки позитиван цео број $a$ који је мањи од $n$ и узајамно прост са $n$ важи:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

где је $\left(\frac{a}{n}\right)$ Јакобијев симбол. Ако је $n$ сложен број и $a$ такав да су они узајамно прости и важи $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, кажемо да је $n$ „Ојлеров псеудопрост број за базу $a$“ и да је $a$ „Ојлеров лажов“. У супротном тј. ако не важи $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ кажемо да је $a$ „сведок“ за сложеност броја $n$. Вероватноћа да случајно изабран број $a$ буде сведок је бар 50%, а ако тест поновимо $m$ пута, са различитим вредностима броја $a$, вероватноћа да број $n$ који је сложен прође те тестове је мања или једнака $\frac{1}{2^m}$.

**Леманов тест** - Разликује се од претходног теста по томе што не мора да се рачуна Јакобијан. Вероватноћа да $a$ буде сведок сложености је бар 50%. Овај тест треба поновити бар $m$ пута, сваки пут са другом вредношћу броја $a$. Ако сваки пут за вредност израза $a^{\frac{n-1}{2}}$ добијемо 1 или -1, али не увек 1, $n$ је вероватно прост број, а могућност грешке је $\frac{1}{2^m}$.

**Милер–Рабинов тест** - Због своје ефиксаности и тачности у потпуности је заменио Соловеј–Штрасенов тест. Уједно је и најзаступљенији пробабилистички тест. Заснива се на особинама јаких псеудопростих бројева, због чега се назива и „јак псеудопрост тест“. Јак псеудопрост број за базу $a$ је непаран сложен број $n$, такав да је

$$a^r \equiv 1 \pmod{n} \tag{19}$$

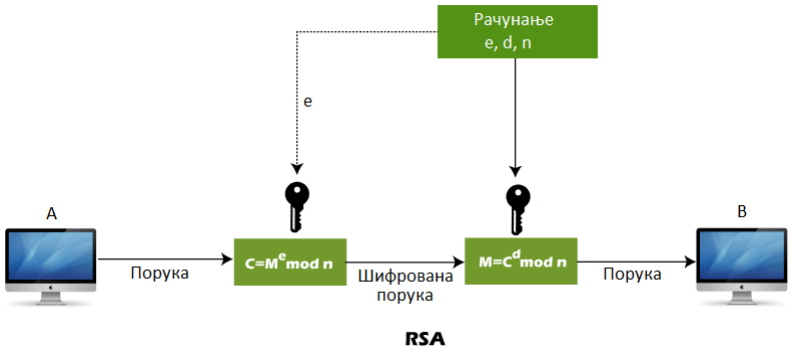
или

$$a^{2^j \cdot r} \equiv n - 1 \pmod{n}, \tag{20}$$

притом $r$ и $j$ су такви да је $n - 1 = 2^s \cdot r$, где је $s$ највећи степен двојке који дели $n - 1$ и $0 \leq j \leq s - 1$, ако такво $j$ постоји. Ако је $a^r \neq 1 \pmod{n}$ за све $j$ мање од $s$, кажемо да је $a$ „јак сведок“ да је $n$ сложен. Ако тест поновимо $m$ пута, вероватноћа да ће сложен број $n$ проћи тест је $\frac{1}{4^m}$. Дакле, вероватноћа да ће тест показати погрешно овде знатно опада.

## 3.6 РСА шифровање

Убрзо након што су Дифи и Хелман објавили своју идеју, Ривест, Шамир и Адлеман [12] су дошли до РСА шифровања које се данас више користи. Овај алгоритам заснива се на растављању производа два велика проста броја на чиниоце.




Скица РСА алгоритма

На интуитивном нивоу идеја РСА алгоритма изгледа овако:
Рецимо да Алис жели да пошаље Бобу поруку. Она ће је ставити у кутијицу на коју ће потом ставити катанац за који само она има кључ и тако је послати Бобу. Када прими поруку, Боб не може да је откључа, али ставља на њу катанац за који само он има кључ

[12] Rivest, Shamir и Adleman

и шаље назад Алис. Када добије кутијицу назад, Алис откључава катанац који је ставила и враћа Бобу кутијицу на којој је само његов катанац. Када добије кутијицу, Боб може да је отвори. На овај начин је порука сигурно пренета и нико други није могао да је откључа. Алгоритам који бисмо том приликом користили изгледа овако:

**Алгоритам 3.31.** Алгоритам за прављење приватног и јавног кључа[13]

1. **Бирање простих бројева**
   Бирају се два различита проста броја $p$ и $q$

2. **Прављење јавног кључа**
   $N = p \cdot q$
   $\phi = (p-1) \cdot (q-1)$ је вредност Ојлерове функције за $N$.
   Бира се цео број $E \in [3, N-2]$ такав да су $E$ и $\phi$ узајамно прости;
   На овај начин је направљен јавни кључ $(N, E)$ који се објављује.

3. **Прављење приватног (тајног) кључа**
   $D = E - 1 \pmod{\phi}$;
   На овај начин је направљен тајни кључ $D$ који се чува.

Сада смо креирали приватни и јавни кључ за РСА шифровање. С обзиром на то да се $\phi$ не објављује, не постоји начин да се са сигурношћу сазна $D$. Ова метода ослања се на претпоставку да је $N$ тешко факторисати. Када то не би био случај, било ко би на основу јавног кључа могао да нађе $\phi$ (само факторише $N$), узме $E$ и онда нађе $D$.

Након што су кључеви направљени, потребно их је искористити. Начин да се то уради приказан је у следећем алгоритму.

**Алгоритам 3.32.** Алгоритам за РСА шифровање и дешифровање [14]

Нека су $D_A$, ($N_A$, $E_A$) Алисин приватни и јавни кључ, који су направљени у претходном алгоритму. Сада ћемо видети како Боб може да шифрује поруку и како је Алис може дешифровати.

1. **Боб шифрује поруку користећи Алисин јавни кључ**
   Нека је $x$ порука коју Боб хоће да пошаље. Он је шифрује тако

[13] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 389

[14] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 389

што $x$ степенује бројем $E_A$ и узима број који му је конгруентан по модулу $N_A$.
$y = x^{E_A} \pmod{N_A}$
$y$ је шифрована порука коју Боб шаље Алис.

2. **Алис дешифрује поруку**
Алис је примила шифровану поруку $y$ и открива оригиналну поруку $x$ користећи свој тајни кључ $D_A$. То ради тако што примљену поруку степенује са $D_A$, а потом број који добије дели са $N_A$ и узима остатак при дељењу.
$x = y^{D_A} \pmod{N_A}$

Очигледно, треба да важи $x^{D_A E_A} \equiv x \pmod{N}$, али ово свакако важи јер смо $D$ конструисали тако да је $x^{D_A E_A} = x(x^{\phi})^k \equiv x \cdot 1^k = x \pmod{N}$ када су $x$ и $N$ узајамно прости.

На овај начин доста људи може да има објављене своје јавне кључеве и свако може да им пошаље поруку али поставља се питање како да се зна од кога је порука стигла? Овај проблем је решен увођењем дигиталног потписа. Прављење потписа на једноставан начин је приказано у следећем алгоритму.

**Алгоритам 3.33.** [15] Претпоставимо да су $D_A$, ($N_A$, $E_A$) Алисини кључеви, а $D_B$, ($N_B$, $E_B$) Бобови кључеви. Сада ћемо видети како Боб може потписати поруку $x$ користећи цео број $s$ који припада интервалу $[0, min\{N_A, N_B\}]$.

1. **Боб шифрује поруку и потписује се**
Боб прави потпис $s$ тако што $x$ степенује својим јавним кључем, а затим добијени број дели са $N_A$ и узима остатак при дељењу. Укратко: $s = x^{D_B} \pmod{N_B}$ .
Потом Боб користи Алисин јавни кључ да би шифровао свој потпис: $y = s^{E_A} \pmod{N_A}$.

2. **Алис је примила шифровану и потписану поруку**
Алис користи свој приватни кључ да би дешифровала потпис: $s = y^{D_A} \pmod{N_A}$.
А потом дешифрује поруку користећи Бобов јавни кључ: $x = s^{E_B} \pmod{N_B}$.

Занимљиво је да овде шифровање иде у супротном смеру, тј. када је Боб шифровао поруку користио је Алисин јавни кључ, а потом

[15] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 390

је она користила свој приватни да дешифрује поруку, међутим, код потписивања Боб прво користи свој приватни кључ да би шифровао свој потпис, а затим Алис користи Бобов јавни кључ да прочита потпис. Приметимо да, с обзиром на то да се потпис може прочитати помоћу јавног кључа, било ко може да зна да је Боб послао поруку, али то нам није битно јер је циљ свакако да порука стигне где треба а да притом нико са стране не уме да је протумачи, што је овим путем успешно урађено. Такође, нико не може да се потпише као Боб јер, као што је већ речено, да би се потписао он користи свој тајни кључ који није могуће открити на основу његовог јавног кључа.

Проблем код оваквог начина потписивања је што има превише симетричности. Ако неко састави поруку $x = x_1x_2$ и некако убеди Боба да пошаље Алис потписе $y_1$ и $y_2$ који одговарају компонентама $x_1$ и $x_2$, онда он може да се претвара да је Боб и пошаље Алис поруку. Ово се може решити увођењем хеш функције која ће онемогућити одређене методе за разбијање потписа.

## 3.7 Хеш функција

Хеш функција је једносмерна функција која представља суму поруке и користи се за проверу интегритета поруке. Проблем са овом функцијом је што се исти хеш може добити од другачије комбинације садржаја и циљ криптографије је да нађе начин да један хеш одговара само једној функцији. Ова функција поруку дужине $n$, где је $n$ број битова, компресује у поруку дужине $k$. Очигледно, приликом компресије долази до одређених губитака.

Хеш функција која се примењује у криптографији мора да има следеће особине:

1. Дужина добијене излазне поруке је коначна и углавном мања од оригиналне поруке

2. Лако се израчунава и не зависи много од дужине оригиналне поруке

3. Једносмерна је тј. на основу ње је скоро немогуће конструисати оригинални текст

4. Једнозначност - тешко је наћи другу поруку која има исту хеш функцију као оригинална порука

5. Промена једног бита узрокује промену бар половине битова добијене хеш функције.

Хеш функције се најчешће примењују код дигиталног потписивања. Један пример примене хеш фунције је дат у следећем алгоритму. Овај алгоритам приказује како се хеш функција користи приликом дигиталног потписивања.

**Алгоритам 3.34.** PCA шифровање са потписом, сигурнија верзија [16]

Претпоставимо да су $D_A$, ($N_A$, $E_A$) Алисини кључеви, а $D_B$, ($N_B$, $E_B$) Бобови кључеви. Овај алгоритам показује како Алис може дешифровати добијену поруку и потврдити Бобов потпис. Такође претпостављамо и да постоји хеш функција $H$.

1. **Боб шифрује поруку и додаје потпис**
   Боб прво шифрује поруку користећи Алисин јавни кључ: $y = y^{E_A} \pmod{N_A}$.
   Нека је са $y_1$ означен хеш текста $x$: $y_1 = H(x)$.
   Затим Боб прави потпис $s$ користећи хеш текста: $s = {y_1}^{D_B} \pmod{N_B}$.
   Сада Боб шаље Алис поруку са потписом: $(y, s)$.

2. **Алис дешифрује**
   Након што је примила поруку $(y, s)$ Алис је дешифрује користећи свој тајни кључ.
   $x = y^{D_A} \pmod{N_A}$ Наравно свој кључ примењује само на текст, односно на $y$, јер је то део који је Боб шифровао користећи њен јавни кључ.

3. **Алис проверава потпис**
   Након што је открила текст, Алис проверава да ли порука стигла од Боба тако што користи његов јавни кључ и потом проверава да ли се добијени резултат поклапа са хеш функцијом: $y_2 = s^{E_B} \pmod{N_B}$.
   Ако је $y_2 = H(x)$ онда је Боб послао поруку и Алис ће прихватити потпис.
   Ако је $y_2 \neq H(x)$ онда је порука стигла од неког другог и Алис ће је одбити.

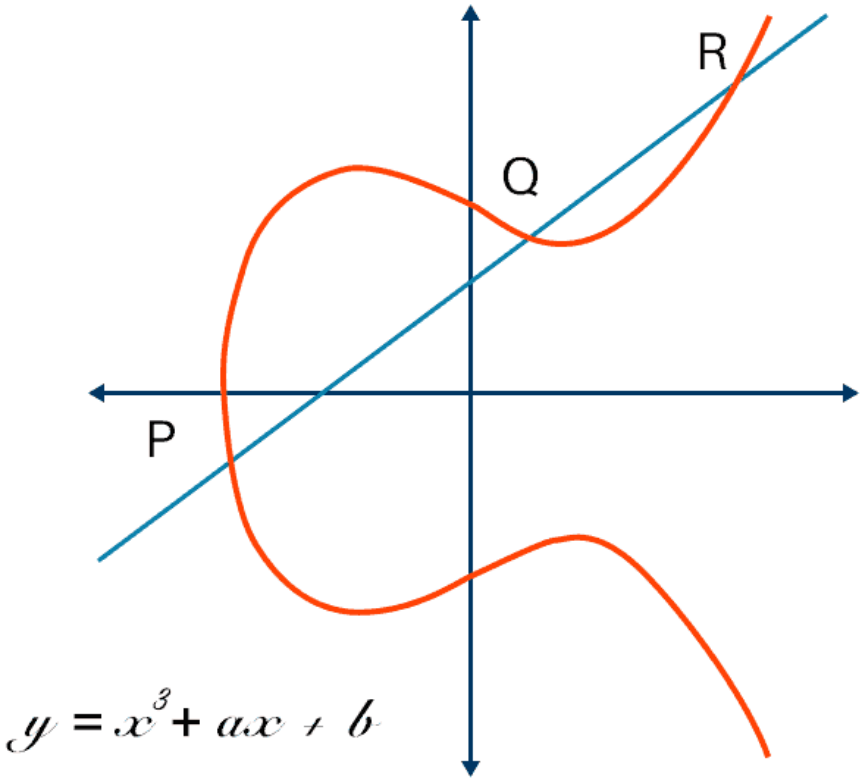
Занимљиво је приметити да у случају када није битно да се сакрије садржај поруке толико колико је битно да се зна од кога је порука стигла, сама порука се и не мора шифровати већ се може једноставно послати, али је зато јако битно потписати се и потом проверити валидност потписа.

[16] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 391

## 3.8 Шифровање помоћу елиптичне криве (ECC)

Шифровање помоћу елиптичне криве је врста шифровања које се ради над коначним пољем $F$ помоћу криве $E(F)$ која је јавна. Заснива се на проблему дискретног логаритма и представља један од најважнијих начина шифровања у криптографији. Крива $E$ је углавном кубна крива која има једначину облика

$$E(F) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j \quad (21)$$




Пример елиптичне криве

**Дефиниција 3.35.** Кубна крива $E$ која је несингуларна (тј. кубна крива чији график нема самопресечних и сингуларних тачака) и чији су коефицијенти из поља $F$ (који нису сви нула), назива се елиптична кубна крива над пољем $F$. Заједно са њом је дата тачка O која се налази у бесконачности (замишљена тачка на крају криве).

**Напомена.** Сингуларне тачке су тачке чији су парцијални изводи по обе координате једнаки нули.

**Дефиниција 3.36.** Нека је крива $E$ дата формулом $y^2 = x^3 + a \cdot x^2 + b \cdot x + c$. За тачке $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ на елиптичној кривој $E$ дефинишемо операцију $+$ на следећи начин:

$$P + Q = R = (x_3, y_3) \tag{22}$$

$$x_3 = k^2 - a - x_1 - x_2, \tag{23}$$

$$-y_3 = k \cdot (x_3 - x_1) + y_1, \tag{24}$$

где је $k$ дефинисано на следећи начин:

$$k = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3 \cdot {x_1}^2 + 2a \cdot x_1 + b}{2 \cdot y_1}, & x_1 = x_2 \end{cases} \tag{25}$$

Шифровање елиптичном кривом се заснива на налажењу целог броја $n$ за који важи: $Q = n \cdot P$, где су $P$ и $Q$ тачке на кривој $E$. У изразу $Q = n \cdot P$, $\cdot$ представља операцију коју примењујемо на скалар и на тачку и дефинишемо је на следећи начин:

$$n \cdot P = \underbrace{P + P + ... + P}_{n}. \tag{26}$$

С обзиром на то да се ова операција дефинише на исти начин као операција множења реалних бројева, обе операције ће бити обележене са $\cdot$.

**Дефиниција 3.37.** Ред тачке $P$ на кривој $E$ је најмањи природан број $n$ за који важи $n \cdot P = O$. Ако такав број не постоји кажемо да је тачка $P$ бесконачног реда.

**Дефиниција 3.38.** Ред елиптичне криве $E$ једнак је броју тачака на кривој који је повећан за 1 (због тачке у бесконачности).

За почетак ћемо видети како се шифровање помоћу елиптичне криве примењује на Дифи–Хелманов алгоритам:

**Алгоритам 3.39.** ECC објављивање кључева [17]

1. **Алис прави јавни кључ**
   Алис бира $K_A \in [2, n-2]$ што представља њен тајни кључ.
   Затим прави свој јавни кључ $Q$ на следећи начин: $Q = K_A \cdot P$.

[17] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 392

2. **Боб прави јавни кључ**
   Боб бира произвољно $K_B \in [2, n-2]$, ово ће бити његов тајни кључ.
   Затим прави свој јавни кључ на исти начин као и Алис: $R = K_B \cdot P$.

3. **Боб и Алис праве заједнички кључ**
   Боб рачуна тачку: $K = K_B \cdot Q$.
   Алис рачуна тачку: $K = K_A \cdot R$.

Тачке које су добили Алис и Боб се поклапају јер, очигледно, важи следеће:

$$K_B \cdot (K_A \cdot P) = K_B \cdot K_A \cdot P = K_A \cdot K_B \cdot P = K_A \cdot (K_B \cdot P). \qquad (27)$$

**Напомена.** Пре почетка је потребно одредити јавну елиптичну криву $E$ и тачку $P$ на тој кривој која је такође јавна и реда је $r$, где је $r$ најчешће неки прост број.

**Напомена.** Приватни кључеви су цели бројеви.

**Напомена.** Занимљиво је да су у овом шифровању јавни кључеви, као и заједнички кључ, тачке на кривој $E$.

Сада се поставља питање како да знамо да се тачка $P$ коју смо одабрали налази на кривој $E$? Алгоритам који нам одговара на то питање је дат у наставку.

**Алгоритам 3.40.** Тражење тачке на елиптичној кривој[18]
Нека је $p$ прост број већи од 3, претпоставимо да је елиптична крива $E$ одређена једначином $y^2 = x^3 + ax + b$.
Прво бирамо $x \in [0, p-1]$.
Потом дефинишемо $t = (x(x^2 + a) + b) \pmod{p}$.
Ако је

$$\left(\frac{t}{p}\right) = -1 \pmod{p},$$

крећемо од почетка. Ако не, узимамо координате

$$(x, \pm\sqrt{t}\ mod\ p).$$

[18]Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 323

Следећи алгоритам показаће како да нађемо тачку $P \in E$ реда $r$.

**Алгоритам 3.41.** Тражење тачака простог реда [19]
Нека је дата елиптична крива $E(F_p)$ реда $f \cdot r$, где је $r$ прост број.

1. **Налажење почетне тачке**
   Први корак је да помоћу претходног алгоритма изаберемо тачку $P \in E$.

2. **Проверавамо да ли је тачка $P$ реда $r$**
   $Q = f \cdot P$
   Ако је $Q = O$, онда се враћамо на први корак.
   Иначе, узимамо тачку $Q$ која је реда $r$.

Једна од битних примена овог алгоритма је у конструисању дигиталних потписа. Начин да се то уради дат је у следећем алгоритму који нам одједном даје функције за прављење кључа, потписивање и проверу потписа. Претпоставља се да је $M$ порука коју треба послати и да нам је позната одговарајућа хеш функција $H$.

**Алгоритам 3.42.** Алгоритам за дигитални потпис[20]

1. **Алис прави кључ**
   Алис бира криву $E$, реда $f \cdot r$ где је $r$ „велики“ прост број.
   Потом Алис тражи тачку $P \in E$ која је реда $r$ помоћу претходног алгоритма.
   Затим бира произвољно $d \in [2, r-2]$.
   $Q = d \cdot P$
   Алис објављује јавни кључ: $(E, P, r, Q)$ , а $d$ чува као тајни кључ.

2. **Алис потписује поруку**
   Да би се потписала Алис бира произвољно $k \in [2, r-2]$ и рачуна:
   $(x_1, y_1) = k \cdot P$;
   $R = x_1 \pmod r$;
   $s = k^{-1}(H(M) + Rd) \pmod r$.
   Ако је $s = 0$ враћамо се на почетак овог корака.
   Алисин потпис је уређени пар $(R, s)$ који се преноси са поруком $M$.

[19] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 393
[20] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 393

3. **Боб потврђује да је Алис послала поруку**
   Боб узима Алисин јавни кључ $(E, P, r, Q)$ и рачуна:
   $w = s^{-1} \pmod{r}$;
   $u_1 = H(M)w \pmod{r}$;
   $u_2 = Rw \pmod{r}$;
   $(x_0, y_0) = u_1 \cdot P + u_2 \cdot Q$;
   $v = x_0 \pmod{r}$.
   Ако је $v = R$, Боб потврђује да је Алисин потпис у питању.
   Иначе, није Алисин потпис у питању.

Претпоставља се да је шифровање елиптичном кривом сигурније од RSA шифровања јер је развојем рачунара постало могуће разбити неке RSA шифре. Насупрот томе, доказано је да би, да се дешифрује оно што је шифровано елиптичном кривом, коришћењем данашње технологије било потребно више времена него што је наш универзум стар. Још једна предност шифровања елиптичном кривом је то што је кључ доста краћи него кључ код RSA шифровања (које је сигурније када је кључ дужи) и због тога га је лакше складиштити и радити са њим.

Још једна занимљивост у вези шифровања помоћу елиптичне криве је то да се у њу, тачније у њене тачке, може директно уградити текст. О овоме нам говори следећа теорема.

**Теорема 3.43.** *За прост број $p > 3$ нека је $E$ елиптична крива над пољем $F_p$, облика*

$$y^2 = x^3 + ax + b.$$

*Нека је $X$ позитиван цео број мањи од $p$. Тада је $X$ или $x$-координата неке тачке на $E$, или на кривој $E'$, која има облик*

$$gy^2 = x^3 + ax + b,$$

*за неко $g$ које није квадратни остатак по модулу $p$. Даље, ако је $p \equiv 3 \pmod{4}$, и одредимо*

$$s = X^3 + aX + b \pmod{p}$$

$$Y = s^{\frac{(p+1)}{4}} \pmod{p},$$

*онда су $(X, Y)$ координате тачке на или $E$ или $E'$ редом, јер је*

$$Y^2 \equiv s, -s \pmod{p}$$

*где у другом случају узимамо да је $E'$ устварии*

$$-y^2 = x^3 + ax + b.$$

Следи алгоритам који показује како се текст директно убацује у криву, а потом и како се чита са ње.

**Алгоритам 3.44.** Директно примењивање ECC енкрипције[21]

Претпоставимо да је Боб формирао кључ као у алгоритму 3.39 и да су одређене криве $E$ и $E'$ и на њима тачке $P$ и $P'$ редом.

1. **Алис уграђује текст**
   Алис на основу претходне теореме одређује криву $E$ или $E'$ на којој је број $X$ вредност $x$-координате (и ако је $y$-координата битна можемо израчунати број $Y$ који би био вредност $y$ координате), с тим да ћемо, ако се $X$ налази на обе криве $E$ и $E'$, за криву узети $E$.
   У зависности од тога коју криву користи, $E$ или $E'$, Алис ради следеће:
   $d = 0$ или 1 - ово одређује која је крива узета;
   $Q = P$ или $P'$;
   $Q_B = P_B$ или $P'_B$.
   Алис бира произвољно $r \in [2, p-2]$.
   Сада Алис прави „елиптични додатак“ $U = r \cdot Q_B + (X, Y)$ којем је задатак да замаскира текст.
   На крају прави „траг“ помоћу ког ће моћи да се открије замаскирани текст: $C = r \cdot Q$.
   Све ово заједно се шаље у облику: $(U, C, d)$.

2. **Боб дешифрује да би открио скривени текст**
   Боб прво треба да открије на којој кривој је скривен текст, због тога гледа шта је $d$.
   Након тога примењује приватни кључ $(X, Y) = U - K_B \cdot C$.
   Сада Боб открива оригинални текст $X$ у облику $x$-координата.

Овај начин шифровања се назива још и Ел Гамалова[22] шема.

[21] Преузето их књиге Richard Crandall, Carl Pomerance, Prime Numbers A Computational Perspective, Second Edition страна 395

[22] Taher Elgamal (рођен 1955.) - египатски криптограф

# 4 Протокол бацања новчића

У криптографији протокол је алгоритам који одређује кораке које треба предузети.

До сада смо видели како се теорија бројева примењује у протоколима везаним за размену кључева. Сада ћемо видети како се теорија бројева може применити у мало више свакидашњим ситуацијама.

Протокол бацања новчића[23] настао је као одговор на питање како обезбедити поштену размену информација међу више неповерљивих страна. На пример, ако Боб и Алис желе да бацају новчић али нису на истом месту па не могу обоје да виде резултат. Договор је да, ако Боб погоди како је новчић пао, онда је он победио, а ако не, онда је Алис победила. Како ће Боб знати да га Алис није слагала за резултат?

За почетак, Алис ће одабрати два велика проста броја $p$ и $q$ и њиховим множењем добиће број $n$. Након тога ће изабрати произвољан прост број $r$ такав да $n$ није квадратни остатак по модулу $r$, и послати оба броја Бобу.

Боб бира један од два исказа: „мањи прост фактор броја $n$ је квадратни остатак по модулу $r$“ или „ већи прост фактор броја $n$ је квадратни остатак по модулу $r$“ и шаље Алис свој одговор.

Сада Алис говори Бобу да ли је погодио и шаље му бројеве $p$ и $q$ да се увери да она није варала.

[23] Coin toss; Coin-flip protocol

# 5 Блокчејн технологија

Блокчејн[24] је јавна база података која је подељена на више делова који су међусобно повезани, али се налазе на различитим местима. Сваки посебан део се зове блок (*block* - одатле и потиче назив *blockchain* односто у буквалном преводу: ланац блокова). Ови делови садрже информације о дигиталним трансакцијама које није могуће изменити и избрисати без промене свих наредних блокова (на овај начин се може пратити историја промена у блоковима). Могуће је само додати нове информације. Сваки блок садржи хеш функцију блока који је креиран пре њега, захваљујући чему можемо да одредимо редослед блокова, а потом и редослед трансакција.

Не зна се ко је тачно творац блокчејна, као ни то да ли је у питању једна особа или организација, зна се само псеудоним који је коришћен: Сатоши Накамото. Шифровање које стоји иза блокчејн технологије је претежно шифровање елиптичном кривом које се користи за прављење потписа.

Као конкретан пример узећу да је $M = 199$, који је прост број[25]и координате $(p_1, p_2) = (2, 24)$. За овако одабране бројеве видимо да је ред тачке $(p_1, p_2) = (2, 24)$ једнак 211. Сада одаберемо да нам је приватни кључ $k_1 = 151$ и онда рачунамо јавни кључ $(p_1, p_2)$ који ће одговарати приватном кључу, то се ради на следећи начин: $(r_1, r_2) = k_1 \cdot (p_1, p_2)$. Када се то уради добије се $(p_1, p_2) = (64, 80)$.

Пошто су кључеви направљени може се одабрати информација коју треба пренети, нека је то $z_1 = 104$. Сада за ову информацију треба конструисати потпис. За то пратимо следеће кораке:

1. Бирамо број $k_2$ имеђу 1 и 210 (ред тачке -1);
2. Рачунамо $(s_1, s_2) = k_2 \cdot (p_1, p_2)$, ако је $s_1 = 0$ враћамо се на претходни корак;
3. Рачунамо $s_2 = \frac{(z_1 + s_1 \cdot k_1)}{k_2} \pmod{211}$, ако је $s_2 = 0$ вратимо се на почетни корак.

Бројеви $(s_1, s_2)$ чине дигитални потпис, у овом случају тај потпис има вредност $(s_1, s_2) = (99, 52)$

Претпоставимо да смо сада ми прималац поруке и хоћемо да проверимо ко ју је послао, то радимо на следећи начин:

[24] blockchain

[25] Овај број, као и сви остали бројеви и тачке у овом примеру преузети су са странице https://mathinvestor.org/2017/08/the-mathematics-behind-blockchain/

1. Прво рачунамо $u_1 = s_2 - 1 \pmod{n}$;
2. Затим $u_3 = s_1 \cdot u_1 \pmod{n}$;
3. Па $(t_1, t_2) = u_2 \cdot (p_1, p_2) + u_3 \cdot (r_1, r_2)$;
4. И на крају треба да проверимо да ли је $t_1$ једнако $s_1$.

Када се све ово уради добија се да је $(t_1, t_2) = (99, 44)$ и пошто је $t_1 = 99 = s_1$ потпис је поврђен (очигледно, није нам битно да се $t_2$ и $s_2$ поклапају).

Иако је овај алгоритам базиран на шифровању елиптичном кривом видимо да ипак не можемо избећи конгруенције и просте бројеве што теорију бројева чини круцијалном у свим овим алгоритмима. Наравно овде су, због једноставности, узети много мањи бројеви од оних који се користе у пракси, али ипак довољни су да илуструју како се употребљава овај алгоритам.

# 6 Закључак

У овом раду бавили смо се, као што сам назив рада каже, применом теорије бројева у криптографији. На почетку рада, појмови теорија бројева и криптографија су дефинисани. Поред појма криптографија, упознали смо се и са појмовима криптологија, криптоанализа и стенографија који, мање или више, имају везе са појмом криптографија. Након тога видели смо како су се поруке шифровале кроз историју и како су неке од тих најранијих шифри користиле теорију бројева за шифровање, али и за дешифровање порука. Видели смо како су те шифре временом постајале све компликованије и како су људи, у једном моменту, кренули да производе машине у ту сврху. Прва таква машина била је Енигма. Енигму су временом наследили модерни компјутери који за модерно шифровање користе много комплексније појмове и теореме из теорије бројева. Упознали смо се са алгоритмима које они користе и корак по корак их анализирали.

За крај смо се упознали са још два занимљива појма: протоколом бацања новчића и блокчејном. С обзиром да ови протоколи гарантују интегритет информација, без њих је скоро немогуће замислити данашње време.

# 7 Биографија

Бранка Милаковић рођена је 29. децембра 1997. године у Сремској Митровици. Основну школу „Трива Витасовић - Лебарник“ завршила је у Лаћарку 2012. године као одличан ђак и са специјалном дипломом из физике. Након завршене основне школе образовање је наставила у средњој школи „Митровачка гимназија“ у Сремској Митровици уписавши општи смер. Средњу школу завршава 2016. године са специјалном дипломом из књижевности. Затим уписује студије на Природно - математичком факултету у Новом Саду на студијском програму Дипломирани професор математике. У четвртој години се пребацује на нови студијски програм, интегрисане академске студије Мастер професор математике на истом факултету. У току студирања је волонтирала у организацији Весели воз која обезбеђује припремне часове за пријемни ученицима осмог разреда и радила као замена наставника математике у основним школама и као професор математике у средњој школи коју је завршила.

# Литература


[1] Richard Crandall, Carl Pomerance, Prime Numbers, A Computational Perspective, Second Edition, Springer, USA, 2005.

[2] Igor Dolinka, Kratak uvod u analizu algoritama, Prirodno-matematički fakultet u Novom Sadu, 2008.

[3] Bernadin Ibrahimpašić, Dragana Kovačević, Diskretni logaritam, MAT-KOL (Banja Luka), ISSN 0354-6969 (p), ISSN 1986-5228 (o), Vol. XVII (2)(2011), 43-52

[4] Ana Draganović, Kriptoanaliza Vigenénerove šifre, master rad, Matematički fakultet, Univerzitet u Beogradu, 2009.

[5] Hans Riesel, Prime Numbers and Computer Methods for Factorization, Second Edition, Reprint of the 1994 Edition, Birkauser, 2012.

[6] Dawson Shores, The Evolution of Cryptography Through Number Theory, November 30, 2020.

[7] Mladen Veinović, Saša Adamović, Kriptologija i osnove za analizu i sintezu šifarskih sistema, Univerzitet Singidunum, Beograd, 2013.

[8] Damian Weber, Thomas Denny, The Solution of McCurley's Discrete Log Challenge, Annual International Cryptology Conference, 1998.

[9] https://mathworld.wolfram.com/PolynomialTime.html

[10] https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/

[11] https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

[12] https://mathinvestor.org/2017/08/the-mathematics-behind-blockchain/

УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРИРОДНО - МАТЕМАТИЧКИ ФАКУЛТЕТ
КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

**Редни број:**
**РБР**

**Идентификациони број:**
**ИБР**

**Тип документације:** Монографска документација
**ТД**

**Тип записа:** Текстуални штампани материјал
**ТЗ**

**Врста рада:** Мастер рад
**ВР**
**Аутор:** Бранка Милаковић
**АУ**

**Ментор:** др Бојан Башић
**МЕ**

**Наслов рада:** Примена теорије бројева у криптографији
**НР**

**Језик публикације:** Српски (ћирилица)
**ЈП**

**Језик извода:** с / ен
**ЈИ**

**Земља публиковања:** Република Србија
**ЗП**

**Уже географско подручје:** Војводина
**УГП**

**Година:** 2023
**ГО**

**Издавач**: Ауторски репринт
**ИЗ**

**Место и адреса:** Нови Сад, Трг Д. Обрадовића 4
**МА**

**Физички опис рада:** (6/63/13/1/7/9/0)(број поглавља/број страна/број литерарних цитата/број табела/број слика/број графика/број прилога)
**ФО**

**Научна област:** Математика
**НО**

**Научна дисциплина:** Теорија бројева
**НД**

**Кључне речи:** Теорија бројева, криптографија, криптологија, шифровање, Цезарова шифра, Виженерова шифра, Дифи–Хелман шифровање, прости бројеви, RCA шифровање, хеш функција, шифровање помоћу елиптичне криве, протокол бацања новчића, блокчејн
**ПО, УДК**

**Чува се:** У библиотеци Департмана за математику и информатику, Природно-математички факултет, Универзитет у Новом Саду
**ЧУ**

**Важна напомена:**
**ВН**

**Извод:**
**ИЗ**

У овом раду се бавимо везом између теорије бројева и криптографије, тачније анализирали смо неке криптографске алгоритме који при раду користе теорију бројева. У првој глави смо се упознали

са појмовима теорија бројева и криптографија и рекли нешто више о ове две дисциплине. У другој глави је приказан историјски развој криптографије где видимо да је теорија бројева била присутна у криптографији још од њеног настанка. Поред тога представљен је појам стеганографија. На почетку треће главе уводимо појмове са који су коришћени у раду, а затим представљамо начине шифровања који се данас користе. То су: Дифи–Хелман шифровање, RSA шифровање и шифровање елиптичном кривом. За сваки од ових начина укратко је објашњена идеја која стоји иза њих и дати су алгоритми који приказују сваки тип шифровања. Након тога, у четвртом и петом поглављу смо се укратко упознали са протоколом бацања новчића и блокчејн технологијом.

**Датум прихватања теме од стране НН већа:**
**ДП**

**Датум одбране:**
**ДО**

**Чланови комисије:**
**ЧК**

**Председник:** др Петар Ђапић, ванредни професор, Природно - математички факултет, Универзитет у Новом Саду
**Ментор:** др Бојан Башић, редовни професор, Природно - математички факултет, Универзитет у Новом Саду
**Члан:** др Владо уљаревић, доцент, Природно - математички факултет, Универзитет у Новом Саду

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCES
KEY WORDS DOCUMENTATION

**Accession number:**
**ANO**

**Identification number:**
**INO**

**Document type:** Monograph type
**DT**

**Type of record:** Printed text
**TR**

**Contents Code:** Master's thesis
**CC**

**Author:** Branka Milaković
**AU**

**Mentor:** Bojan Bašić, Ph.D.
**MN**

**Title:** Application of number theory in cryptography
**TI**

**Language of text:** Serbian (Cyrillic)
**LT**

**Language of abstract:** s / en
**LA**

**Country of publication:** Republic of Serbia
**CP**

**Locality of publication:** Vojvodina
**LP**

**Publication year:** 2023
**PY**

**Publisher:** Author's reprint
**PU**

**Publication place:** Novi Sad, Trg D. Obradovića 4
**PP**

**Physical description:** (6/63/13/1/7/9/0)(chapters/ pages/ quotations/ tables/ pictures/ graphics/ enclosures)
**PD**

**Scientific field:** Mathematics
**SF**

**Scientific discipline:** Number theory
**SD**

**Subject/Key words:** Number theory, cryptography, cryptology, caesar cipher, vigenere cipher, Diffie–Hellman key exchange, RSA algorithm, hash funcion, ECC, Elliptic-curve cryptography, An Optimally Fair Coin Toss, Coin toss, Coin-flip protocol, blockchain
**SKW**

**Holding data:** The Library of the Department of Mathematics and Informatics, Faculty of Science and Mathematics, University of Novi Sad
**HD**

**Note:**
**N**

**Abstract:**
**AB**

In this paper, we deal with the connection between number theory and cryptography, more precisely, we have analyzed some cryptographic algorithms that use number theory. In the first chapter, we were introduced

to the concepts of number theory and cryptography and we said a little more about these two disciplines. In the second chapter, the historical development of cryptography is shown, where we see that number theory has been present in cryptography since its beginning. In addition, we introduce concept of stenography. At the beginning of the third chapter, we introduce the concepts used in the paper, and then we present the encryption methods that are used today. These concepts are: Diffie–Hellman encryption, RSA encryption and elliptic curve encryption. For each of these methods, the idea behind them is briefly explained and the algorithms that demonstrate each type of encryption are given. After that, in the fourth and fifth chapter, we are briefly introduced to the coin flip protocol and blockchain technology.

**Accepted by the Scientific Board on:**
**ASB**

**Defended:**
**DE**

**Thesis defend board:**
**DB**

**President:** Petar Đapić, Ph.D, Associate professor, Faculty of Science, University of Novi Sad
**Mentor:** Bojan Bašić, Ph.D, Full professor, Faculty of Science, University of Novi Sad
**Member:** Vlado Uljarević, Ph.D, Assistant professor, Faculty of Science, University of Novi Sad