Пролећни Фестивал Математике

„Математички Подијум Младих 2018“

МОЋ
КРИПТОГРАФИЈЕ

Ментор:

Радослав Божић,

проф. математике

Аутори:

Уна Лукић

Јана Шумарац

С А Д Р Ж А Ј

Страна

УВОД

Криптографија је наука коју човек користи готово од настанка првих цивилизација. Сви понекад имамо потребу за коришћењем шифри. Још као деца кроз игру смишљамо личне тајне кодове. Захваљујући развоју математике, криптографија постаје све сложенија. Кроз историју потребе човека су све сложније и веће, криптографија постаје све важнија. У томе се огледа моћ крипторафије. Колика је њена моћ била довољно говори чињеница да је постала једно од најважнијих ратних оружја.

Нисмо ни свесни колико често се сусрећемо са криптографијом. Самим тим нисмо свесни ни њене моћи. У 21. веку, у време интернета и брзог развоја технологије, наши лични подаци су угрожени. Криптографијом, тј. шифрама и кодовима штитимо своје податке. Свакодневно се срећемо са њом, а да то ни не знамо. Криптографија је данас моћнија него икада, али то не значи да је достила свој врхунац. Научници предвиђају да ће се у будућности користити још више. Потреба за њом је стална, што моћ крипторафије чини изузетно великом.

1. ШТА ЈЕ КРИПТОГРАФИЈА

Криптографија (или шифровање) као наука има за задатак да проучи и открије најразноврсније и најуспешније методе како да се информација проследи у таквом облику да је само онај коме је намењена може разумети. Сама реч потиче из грчког језика и састоји се од придева *kryptos*, што значи сакривен и глагола *grafo*, што значи писати. Криптографија, заједно са криптоанализом (грчки *kryptos+analise*, *analise* - размрсити), спада у домен криптологије (грчки *krypto+logos*, *logos* – наука, дисциплина). За разлику од дешифровања, криптоанализа се бави проучавањем поступака за читање скривених порука, без познавања кључа по којем су исписане. Све науке ове области су међусобно и неизоставно повезане, а њихов развој се упоредо одвија. Предмети изучавања криптологије су писане (криптографија), говорне (криптофонија), визуелне (слике, карте, мапе, фотографије, шеме) и друге поруке. Развојем технологије, све је даља граница између појмова и дефиниција криптографије и криптологије. Данас се за криптографију сматра проучавање криптовања и декриптовања електронских података, а криптологију везујемо за примену криптографских метода кроз математичка начела.

1.1. Како се користи криптографија

Криптографија је мултидисциплинарна наука јер уз себе веже и научнотехничке дисциплине математику, статистику, лингвистику, а у новије време све више и рачунарство. Појавом рачунара, криптографија добија нови значај и нижу се стандарди и алгоритми за шифровање, а све у циљу да се подаци заштите од „радозналих очију“, али и да се потврди идентитет пошиљаоца. Криптографија се базира на математици, па се среће у рачунарском свету много чешће него што се наизглед чини. Лозинке за приступ, банкомати, пренос електронских порука, електронски потписи, електронско банкарство - само су неки од видова употребе.

У почетку, криптографија се користила само за заштиту садржаја порука шифровањем. Начин на који се подаци шифрирају дефинише шифра, почев од најпростијих као што су транспозиција и супституција до данашњег симетричног и асиматричног шифрирања. Транспозиција представља произвољни број позиција за које ће се знак померити (Цезаров код), а супституција замену знакова. Симетричо шифровање подразумева да и пошиљалац и прималац поруке знају исту шифру којом се порука

шифрира и којом се шифрирана порука лако може и дешифровати. Управо то што се неко, ако сазна шифру, у кратком временском року може послужити свим изнетим подацима, представља главни недостатак овог система. Асиметрично шифровање, односно систем јавних кључева, је један од најсигурнијих начина шифрирања. Математички повезани јавни и тајни кључ се могу користити за шифровање или потписивање садржаја. На основу јавног кључа не може се у разумном времену генерисати тајни, приватни кључ, што је додатна предност овог начина. Данас се шифрирање интензивно развија, што је условљено процватом технологије и рачунарске ере у којој живимо. Компјутери омогућавају коришћење све компликованијих програма за шифровање и дефинисање кодова. Да бисмо могли успешно да се служимо криптографијом, неопходно је претходно упознати се са следећим појмовима и дефиницијама:

- *Отворени текст* је оригинални текст поруке. Када се он трансформише на различите начине добија се *шифровани текст,* односно *шифрат* или *криптограм*.
- Обрнута операција, када се од шифрата добије отворен текст, уз познавање система за шифрирање, назива се *дешифровање*.
- Систем шифровања који се најчешће користи назива се *алгоритам* и састоји се од скупа операција којим се врше разне трансформације оригиналног текста и кључа или кључева, који могу да буду јавни или доступни само особама у тајној коресподенцији. Основне операције алгоритма су премештање, замењивање слова и комбинација ове две операције. Многи алгоритми у криптологији, су се развили из метода које су познате цивилизације користиле још пре нове ере.

1.2. Подела криптографије

Криптографија се дели на симетричну и асиметричну. Код симетричне криптографије користи се исти кључ и за шифровање и за дешифровање. Због тога је разноврсност, а самим тим и сигурност, алгоритама овакве енкрипције велика. Битан фактор је и брзина - симетрична криптографија је веома брза. Поред свих предности које има на пољу сигурности и брзине алгоритма, постоји и један велики недостатак. Како пренети тајни кључ? Проблем је у томе, што ако се тајни кључ пресретне, порука се може прочитати. Зато се овај тип криптографије најчешће користи приликом заштите података које не делимо са другима (шифру знате само ви и њу није потребно слати другоме).

Клод Шенон је дефинисао услове савршене тајности, полазећи од следећих основних претпоставки: Тајни кључ се користи само једном и криптоаналитичар има приступ само криптограму.

За разлику од симетричне криптографије, асиметрична користи два кључа — јавни и приватни. Принцип је следећи: у исто време се праве приватни и одговарајући јавни кључ. Јавни кључ се даје особама које шаљу шифроване податке. Помоћу њега те особе шифрују поруку коју желе да пошаљу. Када прималац добије шифрат, дешифрује га помоћу свог приватног кључа. На тај начин сваки прималац има свој приватни кључ а јавни се може дати било коме, пошто се он користи само за шифровање, а не и дешифровање.

Предност овог начина шифровања је у томе што не мора да се брине о случају да неко пресретне јавни кључ, јер помоћу њега може само да шифрује податке. Такође, програми са оваквим начином шифровања имају опцију да потписују електронске документе. Појам система са јавним кључевима увели су Дифи и Хелман 1976. године. 1977. године објављен је најчувенији и најпопуларнији алгоритам за симетричну криптографију, RSA, чије име представља скраћеницу сачињену од првих слова презимена аутора Рона Ривеста, Адија Шамира и Леонарда Ејдлмана.

2. ИСТОРИЈА КРИПТОГРАФИЈЕ

Од када постоји човечанство, нарочито од појаве писма, постоји и потреба да се информације безбедно размене и проследе на жељено одредиште.

2.1. Настанак и развој криптографије

Чак и цртежи по пећинама првих људи представљају неки вид шифри. Наука „Тајног кључа“, како такође неки називају криптографију, датира још од око 1900. године п.н.е., када је у древном Египту, у граду *Menet Khufu* (на ободима Нила), један писар урезао низ хијероглифа на камене плоче. Тај низ, који описује живот његовог господара, сматра се даном рођења криптографије и то је први документовани пример њене употребе. То и није била криптографија у правом смислу те речи, већ просто неки вид претече исте, јер је сваки хијероглиф за себе имао значење, угавном неке конкретне радње. Понекад су се хијероглифи користили и по принципу ребуса, њима би се постизала доза тајновитости у духовним текстовима и тако се истицала вежност истих, као и велика моћ коју су тим текстовима приписивани. У то доба настаје и гробна криптографија. Тако, су на надгробним споменицима стајали тајанствени, необични делови натписа који би људима скретали пажњу, када би људи прочитали шта ту пише, по веровању, пренели би благослов, који се налазио на плочи, покојницима.

И у Старој Индији су користили, тада само њима знан, начин комуницирања прстима, где су чланци на прстима означавали сугласнике, а зглобови самогласнике. Да је криптографија већ у раним цивилизацијама била изузетно цењена и широко примењена наука, говори и податак да је пронађена плочица из 1500. године пре нове ере, која се користила у Месоппотамији и на којој је био исписан рецепт за гравирање клинастог писма на предметима од глине. Сваки од знакова који су се користили је имао више различитих слоговних значења.

Једна од најпознатијих и најзначајнијих за даљи развој је хебрејска трансформација, супституција слова названа *„атабаш*“. Прво слобо хебрејског алфабета би се замењивало последњим, друго претпоследњим и тако редом. Постојао је још један вид трансформације који се спомиње међу старим хебрејским текстовима кога су назвали „атабах“. По том принципу, између првих 10 слова хебрејског алфабета су биране замене, тако да збир редних бројева у отвореном тексту (оригинални текст поруке) и слова које га замењује увек износи 10. Остала слова су се трансформисала на исти начин, само је тај збир износио 28.

Још су се и Стари Грци, тачније Спартанци служили разним криптографским алатима и методама, па су тако, у 5. веку пре нове ере, осмислили направу за шифровање, звану *скитал*. То је био штап око којег би намотавали траку пергамента, па на њој писали одређену поруку. Након тога трака би се одмотала, а на њој би исписан текст могао прочитати само онај ко би имао штап једнаке дебљине, јер су на траци остајали измешани трагови. Скитал представља прву познату направу за транспозицију шифара.

Грци су такође били учени и образовани о тајности комуницирања са више система тајног писма из разних књига и уџбеника на ту тему. Један од распрострањенијих система се састојао од замене самогласника тачкама. Принцип: алфа, једна тачка; епсилон, две тачке; (...), омега 7 тачака. Грчки писац Плибије (2. век пре нове ере) објаснио је замену слова бројевима употребом табеле. Данас је тај систем познат по именом шаховска табла. Она се састојала од 5 редова и 5 колона, односно 25 поља у која су уношена слова. Изнад прве врсте и лево од прве колоне били су исписани бројеви, тако да је свако слово могло да се представи као двоцифрени број. Први број је означавао број реда, а други број колоне.

У једној књизи из Херодотовог серијала (Histories) се спомиње као анегдота један од првих примера тајновитог размењивања информација. Наиме, *Histiaeus* је свом најверснијем робу исписао низ знакова на глави и сачекао да му коса израсте. Иако су путеви били добро чувани од стране војске, нико није прозрео да је роб, који је пролазио путем, испод косе, заправо носио тетоваже које су представљале битну информацију, односно поруку. Та порука је била позив за подизање устанка. То је познати историјски пример у којем је пошаљилац успео у својој намери, да без знања противника обавести своје савезнике о намерама или плану. Али, историја памети и не тако успешне покушаје. Ова анегдота је један од првих примера стенографије. Стенографија представља вештину сакривања порука и слања истих на најразличитије начине. Поред криптографије и стенографија је била врло позната и цењена наука у Старој Грчкој.

Цезаров код у криптографији представља један од најпознатијих, најкоришћенијих и најраспрострањенијих начина шифрирања. Представља тип шифре супституције (замене), у којем се свако слово отвореног текста замењује одговарајућим словом абецеде, помакнутим за одређени број места. Пример: са помаком 5, А се замењује словом Ф, Б словом Г... Данас се такво шифровање зове Цезаров алфабет. Принцип је добио име по Јулију Цезару јер га је управо он врло често користио за комуницирање са својим генералима. Према наводима, римског писца Светонија, у делу „Дванаест

Цезара“ стоји да је такву шифру, са размаком од 3 места, Цезар користио као заштиту порука од војне важности. Цезаров код је први забележен случај коришћења ове шеме, али је познато да су сличне шифре замене и раније коришћене. Није познато колико је код био учинковит, али је био релативно поуздан с обзиром да је мало људи, у то време, знало латински или било упознато са писмом, као и због немогућности примене криптоанализе. Не постоје ни записи из тог периода о било каквој техници решавања шифара једноставне замене. Данас се та шифра, врло лако може решити, те се може наћи и у дечијим играма.

Рунско писмо се јавља у Скандинавији и англосаксонској Британији у 7, 8. и 9. веку, а састојало од 3 групе по 8 слова. Исруна, криптографски систем заснован на овом писму, састојао се од замењивања слова знаковима који су одређивали број скупине и редни број његовог места у скупини. Други систем - хахалуна се састојао у томе да су се у једној дугој црти додавале косе цртице; леве би одговарале броју групе, десне редном броју унутар групе. Трећи систем - огхам, састојао се од 5 група по 5 слова. Шифровани знаци су се састојали од водоравних дугих црта и краћих које се дижу, спуштају, секу нормално, секу косо, и тако се погађало о којој је групи реч.

У арапским изворима из 1. и 15. века помињу се различити системи шифрирања: слова се замењују другим словим, речи се пишу унатрашке, редом се замењују свака 2 слова текста, слова се замењују њиховим одговарајућим редним бројевима у арапском алфабету, свако слово се замењује именом неког човека или предмета, слова се замењују лунарним називима, именима земаља, воћа, итд. У њима се први пут наилази и на криптоанализу. Њени почеци се везују за истраживање Куран и сматра се да се користила да би се, света књига муслимана, до краја разјаснила.

Qalqashandi је аутор који је записао технику за разбијање шифри која се користи и данас. Техника се заснива на томе да се запишу сви знакови из кодираног текста и преброји колико пута се појавио сваки од тих знакова у тексту. Ако сад на те податке применимо податак колико се често које слово појављује у језику којим је писана послата порука, можемо открити који симбол кодиране поруке представља које слово абецеде језика послате поруке, а то значи и написати послату поруку. Ова техника омогућава разбијање било које шифре засноване на моноалфабетској супституцији ако постоји довољно кодираног текста. Таквом техником су се развијале статистика, лексикографија, лингвистика, фонетика, што је било потребно за настанак и развој криптоанализе.

Ово је наука која је веома интересанна за проучавање како научницима природних наука, тако и историчарима, али и етнолозима, културолозима, због свог дугог и динамичног развоја, који тече упоредо са развојем човека, напретком друштва и културе. Тако се, уз помоћ дешифрованих порука којима су се наши преци служили, може сазнати доста тога и о развоју друштва. Највећа достигнућа из ове области условљена су војним потребама, дипломатским сервисом и потребама влада. Наука се користила као средство за заштиту националних тајни, договора, односно, стратегија.

2.2. Криптографија као оружје

Криптогрфија је постала једно од најмоћнијих оружја за време највећих сукоба у свету. У Првом светском рату, најважије информације су се преносиле управо помоћу крипторафије. Врхунац њене моћи дефинитино је у Другом светском рату, пред чије избијање је конструисана енигма.

Енигма је била машина за шифровање радио-телеграфских порука. Била је једно од најмоћнијих оружја Немачке, у Другом светског рату.

Реч Енигма долази из грчког језика и значи 'загонетка'. То је електромеханичка машина. Користила је принципе спојених ротора и разводне плоче. Сврха енигме била је шифровање информација, тј. њихово приказивање на начин неразумљив неовлашћеним особама.

Енигму је конструисао Немац Артур Шербиус 1923. године. Касније је ова машина даље усавршавана и на тржишту продавана као комерцијални систем за шифровање, првенствено за цивилне намене. Избијањем Другог светског рата, Енигма је постала стандардна опрема свих војних јединица.

Својим изгледом подсећа на писаћу машину. Са предње стране има тастатуру од 26 слова изнад које се налази 26 сијалица. Свака од тих сијалица представља једно од 26 излазних слова. Састојала се од тастатуре и више ваљака. Ти ваљци су имали електричне контакте, тако да се при притиску на један тастер тастатуре активира струјно коло од тастера кроз ваљак до монитора, на коме засветли притиснуто слово. Приказана слова су формирала шифровани, односно дешифровани текст. Пошто су се при сваком притиску на тастер тастатуре ваљци даље окретали, иста слова су сваки пут другачије шифрована.

Текст се уноси преко тастатуре, а излаз се добија преко сијалица. Између тастатуре и сијалица налази се главни механизам, језгро машине. Језгро машине чине ротори. Ротори имају више функција: морају осигурати пресликавање знакова и

морају ротирати.

Рад енигме заснива се на супституцији знакова: аритметичка супституција и мапирајућа супституција. Енигма у свом раду користи оба наведена алгоритма.

3. КРИПТОГРАФИЈА ДАНАС И СУТРА

Криптографија не излази из употрбе ни данас, у 21. веку. Највише је користимо за сигурносне протоколе, како бисмо заштитили своје податке.

На пример: SSL (Secure Socket Layer), TLS (Transport Layer Security), VPN (Virtual Private Network)...

Secure Socket Layer, или скраћено SSL, је предоминантни сигурносни протокол комуникација на интернету, посебно у случају услуга веба које се односе на електронску трговину и електронско банкарство.

VPN (енгл. Virtual Private Network — Виртуелна приватна мрежа) је приватна комуникациона мрежа која се користи за комуникацију у оквиру јавне мреже. Транспорт VPN пакета података одвија се преко јавне мреже (нпр. Интернет), коришћењем стандардних комуникационих протокола. VPN омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију.

Напретком људске цивилизације, криптографија се развија све више и више, тако да се сматра да ће њена употреба у будућности постати још већа. Квантна и ДНК криптографија ће можда у некој скоријој будућности представљати основу за заштиту поверљивих докумената. Квантна криптографија настала је као последица открића у области квантног рачунарства. Она се заснива на једном од основних принципа квантне физике: Хајзенберговом принципу неодређености. Један од твораца RSA алгоритма, Леонард Ејдлман, дошао је на идеју коришћења ДНК као рачунара. Он је претпоставио да се ДНК може посматрати као рачунар огромне снаге способне за паралелно извршавање операција. Тиме се брзина извршавања експоненцијално повећава у односу на обичне рачунаре.

3.1. Примери шифри

1. Цезарова шифра - Ова шифра потиче од римског војсковође Јулија Цезара који је преко ње комуницирао са својим пријатељима. Састоји се од тога да свако слово поруке замени слово које се налази на н места у алфабету. На пример, реч ЛАВ. Коритићемо се енглеским алфабетом који има 26 слова. Слова C, Č, D, Dž, Lj, Nj, S, Ž, заменићемо словима C, C, DJ, DŽ, LJ, NJ, S, Z. Ако је, на пример, n = 5, онда шифра гласи “QFA”.

2. Савршени код - Замислимо да наставник жели сазнати просечан број сати које ученик троши на учење и писање домаћих задатака сваке недеље. Постоји оправдана

сумња да ће ученици бити искрени, уколико тај податак треба да искажу јавно. Стога наставник може применити следећу процедуру која ће сачувати право на приватност сваког ученика. Протокол започиње Адам који бира тајни цели број *n*. Нека је n = −215. Тајни број *n* Адам увећава за број сати који проводи у учењу, нпр. за 5. Тако је nA = n + 5 = −210. Затим, Адам шапне број nA следећој ученици, Бранки. Бранка на школске обвезе потроши недељно 7 сати, па је nБ = nA + 7 = −203. Број nБ Бранка дошапне Милици. Милица увећава nБ за „свој“ број 4, тј. nМ= nБ + 4 = −199. Протокол се наставља редом до посљедњег ученика којем је шапнут број nВ његовог предходника, Владе. Након увећавања броја nВ, nУ = nВ +6. Последњи ученик ту информацију прослеђује првом, Адаму. Адам од коначног збира nЗ одбија “тајни” број *n*. Да би добио просечно време учења по ученику, подели тај број са бројем ученика и долази до жељене информације.

ЛИТЕРАТУРА

1. Дивјаковић Даниел, „Основе криптологије, OTP и RSA алоритам“, Нови Сад, 2016.
2. Весна Стевановић, „Криптологија некад и сад“, Београд
3. https://sr.wikipedia.org/sr-el/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%98%D0%B0

ПОДАЦИ О АУТОРИМА И МЕНТОРИМА

Аутори рада:

1. Уна Лукић, Гимназија „Светозар Марковић“, Нови Сад, II-2
2. Јана Шумарац, Гимназија „Светозар Марковић“, Нови Сад, II-2

Ментор рада:

1. Радослав Божић, професор математике, Гимназија „Светозар Марковић“, Нови Сад

Место и датум:

Нови Сад, 13.04.2018