UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA MATEMATIKU I
INFORMATIKU

Daniel Divjaković

OSNOVE KRIPTOLOGIJE, OTP I RSA ALGORITAM

- master rad -

Novi Sad, 2016.

Zahvaljujem se mentoru profesoru dr Petru Đapiću na uloženom trudu i vremenu za poboljšanje ovog rada. Takođe, hvala i članovima komisije dr Andreji Tepavčević i dr Branimiru Šešelji.

Sadržaj

Apstrakt

Tema ovog rada, u najširem smislu te reči jeste kriptologija, njene metode i alati i neke njene primene.

U užem smislu je postavljen akcenat na OTP algoritam kao glavnog predstavnika simetrične kriptografije te RSA algotiram kao jedan od najzastupljenijih algoritama asimetrične kriptografije.

U prvom delu će biti reči o prvim oblicima pojave steganografije, kao preteče kriptografije, zatim o razvoju kriptografije kroz istoriju, potom i o pojavi kriptoanalize. Slede neki primeri poznatih šifri kao i algoritama dešifrovanja. Potom ćemo generalno promatrati kriptologiju kao disciplinu koja se sastoji od kriptografije (metoda enkripcije) i kriptoanalize (metoda dekripcije), navešćemo osnovne podele šifri po raznim kriterijuma.

U drugom delu sledi matematički aparat - definicije i teoreme neophodne za dalji rad. Pre svega, pažnja je posvećena matematičko-teoretskom alatu koji je neophodan da bi se shvatio, a potom i dokazao mehanizam funkcionisanja RSA algoritama. Najvažnije matematičke teoreme na kojima se zasniva RSA algoritam jesu Euklidov algoritam te Ojlerova teorema. Nakon toga sledi kriptografski deo teorije, pojmovi kriptosistema i šifre, pojam savršene sigurnosti.

Treći deo idejno deli kriptografiju na dve osnovne celine : kriptografiju sa privatnim i kriptografiju sa javnim ključem. U prvoj polovini trećeg dela razrađen je jedan on najpoznatijih i najfundamentalnijih meotda kriptografije sa privatnim ključem - One Time Pad, te je pokazano kako ovaj metod ima savršenu sigurnost, ali su pored njegovih dobrih osobina i predsnosti, navedene i njegove glavne mane. Druga polovina trećeg dela posvećena je možda i najznačajnijem alatu moderne kriptografije, tj. RSA algoritmu. Tu je detaljno opisano kako on funkcioniše, procesi enkripcije i dekripcije, te je, uz pomoć ranije navedene matematičke osnove pokazano i da RSA algoritam ispunjava kriterijume neophodne da bi neki algoritam zapravo i bio šifra. U delu kriptografije sa javnim ključem formulisani su i objašnjeni pojmovi heš funkcije i digitalnog potpisa, koji su, uz RSA algoritam i ostale algoritme koji funkcionišu na istim principima kao i RSA, glavni derivati ove grane kriptografije.

Konačno, u poslednjem delu biće reči o kriptografskoj valuti *bitcoin* kao jednom od najkreativnijih produkata kriptografije i njenih metoda. Sa realnog aspekta biće predstavljen značaj, prednosti i mane ovog kriptografsko digitalnog izuma.

Glava 1

Prvi deo

1.1 Uvod

Kažu da, čovek koliko jezika zna toliko i vredi. Neko sa tim može da se složi ili ne, ali objašnjenje je očigledno - znajući što više jezika, a samim time i reči, sposobni smo da komuniciramo sa sve više ljudi na svetu, razmenjujemo mišljenja, a tako i proširujemo svoje iskustvo.

Zapravo, sve to zbog toga što komunikacijom dolazi do razmene verovatno najvažnije i najvrednije stvari na svetu - *informacije*.

Posmatrajući čoveka kroz istoriju, još od davnina, pojave pećinskog čoveka, došlo je do potrebe interakcije i komunikacije između članova zajednice. Interakcija, odnosno razmena informacija započinjala je najprostijim pokretima ruku, gestovima, mimikom, neartikulisanim glasovima koji nisu ličili na današnje reči modernog jezika. Pre svega čovek je, iz nekog razloga, svoj napredak oduvek zasnivao na *sukobu*: isprva to je bio lov životinja zarad prehranjivanja zajednice, potom međusobno ratovanje za resurse hrane ukoliko ne bi bilo dovoljno za sve, pa sledi čitava plejada ratova za nove teritorije, te kolonizacija nenaseljenih ali i naseljenih krajeva. Upravo tokom tih ratova došlo je do potrebe prenošenja informacija saveznicima, ali tako da protivnici ne mogu doći do tih istih informacija. Prve primere *šifrovanih informacija*, tj. *zaštićenih informacija* i vezujemo za antičko doba, Staru Grčku, Rim, Ahemenidsko carstvo (Prvo persijsko carstvo) itd. Upravo te primere smatramo i korenima kriptografije i nauke veoma joj srodne - steganografije.

Kriptografija se, u današnje vreme konstatno progresivnog razvoja informacionih tehnologija, internet bankarstva, kupovine preko interneta, glasanja preko interneta i sličnih stvari, nemerljivo mnogo koristi, a samim time i napreduje i razvija. U naprednijim delovima sveta, većina kupovina se obavlja preko interneta - tehnike, kućnih aparata, odeće, obuće, ali sve više i svakodnevnih potrepština poput hrane i pića. Kriptografija igra glavnu ulogu u tome da se *"digitalni novac"*

ne može dva puta potrošiti (*"kopirati"*,u informatičkom smislu te reči), ali i da, baš kao i u fizičkom svetu, informacija na šta je taj novac potrošen i koliko, bude dostupna samo kupcu i prodavcu, i nikome drugom. Što se tiče digitalnog novca, jedna od najaktuelnijih tema svetske ekonomije i finansija jeste i mogućnost oporezovanja zarade i trošenja tog novca, međutim taj proces nije toliko jednostavan, s obzirom da taj novac ne izrađuje (u fizičkom smislu) ni jedna država niti drži pod svojim nadzorom njegove tokove. Na ovakvoj motivaciji se zasniva i pojava prvih kriptografskih valuta. Takođe bitan primer gde je kriptografija od ključnog značaja jesu elektronski izbori - Kako prebrojati glasove, i dati izlaz u smislu odgovora koji kandidat je osvojio najviše glasova, a pritome da nije dostupna informacija ko je za koga glasao. Njen zadatak je i da se pobrine da ne bude takozvanih "duplih glasova". Uz progresivni napredak kriptografije i njenih alata, razvija se i naravno disciplina srodna ali suprotnih ciljeva kriptografiji - kriptoanaliza.

Takođe, na kraju uvoda, ćemo definisati samo neke bitne pojmove koje je neophodno usvojiti da bi se neometano pratio tok daljeg rada. *Otvorenim tekstom (engl. plaintext)* nazivaćemo originalni tekst poruke koju želimo zaštititi. *Šifrat (engl. cyphertext)* biće šifrovani tekst dobijen od originalnog teksta raznim kriptografskim metodama nakon obrade. Sam proces prevođenja otvorenog teksta u šifrat definisaćemo kao *kriptovanje ili šifrovanje*, a obrnut proces, dobijanja otvorenog teksta iz šifrata kao *dekriptovanje ili dešifrovanje*. *Ključ* će podrazumevati podatke i metode neophodne da se izvrši proces kriptovanja i dekriptovanja.

1.2 Motivi iz istorije - od steganografije preko kriptografije sve do kriptoanalize

Kao što smo već napomenuli u uvodu *informacija* je toliko bitna da se potreba za njom i razmenom iste javila davno u ljudskoj istoriji. Naravno, kao i dosta drugih stvari, prve pojave "prikrivanja informacija" javile su se zbog potreba veštine koja je stara gotovo koliko i sam čovek - *borbe*, odnosno *ratovanja*.

Koreni kriptografije potiču pre više od 4000 godina. Dan kada je nepoznati autor urezao niz hijeroglifa na kamene ploče, niz koji opisuje život njegovog gospodara, smatra se danom rođenja kriptografije. Desilo se to u drevnom Egiptu, u gradu *Menet Khufu*, na obodima Nila. To i nije bila kripotgrafija u pravom smislu te reči, već prosto neki vid preteče iste, jer je svaki hijeroglif za sebe imao značenje, uglavnom neke konkretne radnje.

Međutim, neki od prvih zabeleženih primera tajnovitog razmenjivanja informacija pojavljuju se u serijalu knjiga *Herodotusa (Herodot)* pod imenom *Histories* koji datira od V veka pre nove ere.

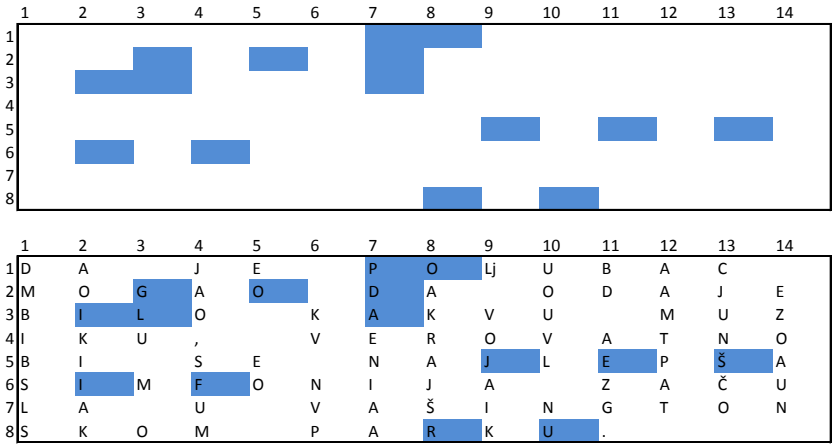
Naime, u VII Herodotovoj knjizi, prva zanimljiva anegdota govori nam o čuvenim *Spartancima* (u knjizi ih je Herodot nazivao *Lacedemoniancima*) i kralju *Kserksu I od Persije*. U svom velikom pohodu na Evropu, skupivši veliku armiju nameravajući da pokori prvo Grčku, a zatim da zađe i dalje u Evropu, Kserksove namere prozreo je *Demaratos*, bivši kralj Sparte, koji se nakon proterivanja iz Sparte pridružio Kserksu, njegovoj velikoj imepriji i vojsci Persije. Ipak, Demaratos je poželeo da javi Sparti da bude spremna, a kako je bilo teško to učiniti bez Kserksovog znanja, dosetio se kako moze informisati Spartance a da Kserks to ne sazna. Naime, uzeo je drvenu ploču sa koje je skinuo površinski sloj te na donjem sloju kore ispisao željenu poruku. Zatim je, ponovo, naneo površinski sa nekom vrstom voska, te tako zamaskiranu drvenu ploču poslao za Spartu. Kada je ploča stigla za Spartu, oni nisu mogli da shvate šta ona predstavlja, sve dok se *Gorga*, ćerka *Cleomenesa* i žena od kralja *Leonide*, nije dosetila da skinu površinski sloj drveta tj. voska na ploči i tako saznaju šta je Demaratos hteo da ih obavesti. Zahvaljujući tome Sprata, kasnije zajedno sa Grčkom, se i odbranila, a time je odbranila i čitavu Evropu od velikog imperatora Kserksa I od Persije.

Dalje, u V knjizi Herodotovoj, pominje se primer gde je *Histiaios*, koji je živeo u V veku pre nove ere, sa namerom da obaveseti *Aristagorasa* da je vreme da dignu pobunu, obrijao glavu svome najvernijem robu, te ispisao niz simbola na njegovu glavu, a potom, sačekavši da robu izraste kosa, poslao ga Aristagorasu. Iako su putevi bili dobro čuvani od strane vojske , ipak niko od čuvara putem gde je rob prolazio nije prozreo da je on ispod kose, bukvalno nosio tetovaže koje su predstavljale bitnu informaciju. Tako je rob stigao do Aristagorasa i uputio ga da mu obrije glavu, i tako je Aristagoras saznao Histiaiosove namere - da je vreme da dignu ustanak.

Navedena su dakle dva poznata antička primera, gde su pošaljioci uspeli u svojoj nameri, da bez znanja protivinika obaveste svoje saveznike o namerama ili planu. Međutim, naravno, istorija pamti i ne tako uspešne pokušaje. Naime, *Mary*

Stuart, kraljica Škotske, bila je zarobljena čitavih 18 godina, počev od 1568, od strane Engleske kraljice *Elizabete*. 1586, kada je konačno oslobođena, Meri je sa zaverenicima organizovala atentat na Elizabetu. To su radili tako što su koristili skrivene i šifrirane poruke. Međutim, metode koje su koristili Meri i zaverenici očigledno nisu bile dovoljno dobre, jer sve je to kraljica Elizabeta uspela da otkrije i iskoristi kao dokaz umešanosti skotske kraljice u zaveru i nameru atentata te donese smrtnu presudu za Meri.

Ove navedene anegdote su predstavljale prve primere **steganografije**. Steganografija predstavlja veštinu skrivanja poruka i slanja istih na najrazličitije načine. U novijoj istoriji brojni su primeri upotrebe stenografskih metoda. *Mikrotačka* (korišćena od strane Nemaca za vreme Drugog Svetskog Rata) predstavlja izum nacista, koji su čitave stranice podataka i slika smanjivali i do 200 puta, u tačku čiji je prečnik bio manji od 1 mm, i onda bi je utapali u okolinu nekog potpuno nebitnog pisma ili slike. Još neke od interesantnijih metoda bili su čuveno nevidljivo mastilo, i Kardano rešetka - struktura koja, kada bismo je spustili na neki tekst, izdvojila bi nam slova koja daju pravi, prikriveni smisao poruke.



Slika 1.1: Primer skrivenog teksta izolovanog iz proizvoljnog teksta kardano rešetkom.

Što se tiče kriptografije, smatra se da je prvu njenu upotrebu u svrhu komunikacije predstavljao tzv. spartanski *Skytale*. To je bio običan štap određene debljine, na koji bi si namotala traka papirusa, a potom se uzdužno po dužini štapa pisala poruka. Kada bi se traka papirusa razmotala sa štapa, slova u tom poretku ne bi imala nikakav smisao sve dok se ponovo papirus ne namota na štap iste debljine.

Međutim, prvi zabeleženi primer šifrovane poruke potiče iz doba *Julija Cezara*. To je zabeležio rimski istoričar *Suetonius* u svom delu *On the Life of the Ceasars*. Po tim zapisima, Cezar je koristio metod šifrovanja koji se zasnivao na zameni slova

sa slovom koje je za tri mesta udesno udaljeno u abecedi. U nastavku rada data je tabela u kojoj je prikazano koje slovo se menja kojim slovom pri procesu enkripcije (malim slovima su napisana slova koja se šifruju, a velikim kojim ih šifrujemo).

otv. tekst	a	b	c	č	ć	d	dž	đ	e	f	g	h	i	j	k
šifrat	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M

otv. tekst	l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž
šifrat	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C

Tabela 1.1: Tabela sa šablonom zamene slova srpske abecede u Cezarovoj šifri

Na primer, ukoliko bismo Cezarovom šifrom hteli da šifrujemo poruku :

soko zove orla (otvoreni tekst);

nakon procesa (s se menja sa U, o sa S, itd.) dobijamo :

USMS BSAH STNČ (šifrat).

Dakle, ovakav sistem se zove Cezarova šifra. Međutim, takva šifra sama po sebi jeste zapravo specijalni slučaj, odnosno podskup skupa šifara koje nazivamo *supstitucione šifre*. One podrazumevaju generalno zamenu slova bilo kojim drugim slovom (u slučaju Cezarove šifre to je slovom udaljenim za tri mesta u abecedi).

Posmatrajmo sada pomenute supstitucione šifre sa matematičkog aspekta.

Praktično je moguće definisati bijekciju između alfabeta koji šifrujemo (u našem slučaju srpska abeceda) i skupa ostataka pri deljenju sa 30. Konkretno, bijekciju formiramo tako što svakom slovu dodelimo njegovo mesto u alfabetu (počev od 0). To je predstavljeno u sledećoj tabeli za srpsku abecedu:

a $\leftrightarrow$ 0	dž $\leftrightarrow$ 6	i $\leftrightarrow$ 12	n $\leftrightarrow$ 18	š $\leftrightarrow$ 24
b $\leftrightarrow$ 1	đ $\leftrightarrow$ 7	j $\leftrightarrow$ 13	nj $\leftrightarrow$ 19	t $\leftrightarrow$ 25
c $\leftrightarrow$ 2	e $\leftrightarrow$ 8	k $\leftrightarrow$ 14	o $\leftrightarrow$ 20	u $\leftrightarrow$ 26
č $\leftrightarrow$ 3	f $\leftrightarrow$ 9	l $\leftrightarrow$ 15	p $\leftrightarrow$ 21	v $\leftrightarrow$ 27
ć $\leftrightarrow$ 4	g $\leftrightarrow$ 10	lj $\leftrightarrow$ 16	r $\leftrightarrow$ 22	z $\leftrightarrow$ 28
d $\leftrightarrow$ 5	h $\leftrightarrow$ 11	m $\leftrightarrow$ 17	s $\leftrightarrow$ 23	ž $\leftrightarrow$ 29

Tabela 1.2: Numerički ekvivalenti za slova srpske abecede

Ova tabela dakle, reprezentuje vizuelni prikaz bijektivne funkcije gde su članovi domena slova alfabeta a kodomena njihovi numerički ekvivalenti. U supsitucionim

šiframa *ključ* nam predstavlja celi broj n koji dodajemo na numerički ekvivalent za svako slovo alfabeta i onda opet na tako dobijen celi broj vraćamo odgovoarajuće slovo alfabeta. Taj proces se naziva *pomeranje za n pozicija.* Za $n = 0$ imamo šifrat koji je ustvari jednak otvorenom tekstu, a to u suštini i nije šifrat.

Tako gledano, lako je zaključiti da je broj mogućih kombinacija šifrovanja na način kao što je implementirano kod Cezarove šifre (zamena slova za slovo n mesta udaljeno u abecedi) jednak upravo kardinalnosti abecede nad kojom šifrujemo, tj. u slučaju engleske abecede 26 kombinacija (zapravo 25 jer je proces zamene periodičan sa periodom od 26 pa nam je 26. kombinacija zamena slova istim slovom,što zapravo i nije šifrovanje), u srpskoj abecedi je 30 tj. 29 kombinacija, a na primer, u kineskom pismu situacija je znatno složenija, jer oni imaju preko 3500 simbola koji predstavljaju slova (u zavisnosti od dijalekta, tj. dela Kine, taj broj može biti i blizu impresivne cifre od 10000), pa je samim time i najmanje 3499 kombinacija za šifrovanje kineskog pisma.

Čini li se ta brojka od 25, 29, ili čak 3499 kombinacija dovoljna?

Nekada davno možda da, ali u današnje vreme, kada se sama kriptoanaliza, u smislu dešifrovanja, zajedno sa računarima i tehnologijom toliko razvila, *prostor ključa* (baš taj broj kombinacija šifrovanja, o njemu će kasnije biti više reči) mora biti neuporedivo veći od gore navedenih cifara. Takvom analizom dolazimo do sledeće ideje - ukoliko bismo se odrekli ključa fiksne dužine n, onda bismo mogli znatno proširiti prostor ključa tako što bismo dobili mogućnost da svakom slovu alfabeta možemo dodeliti bilo koje slovo alfabeta, a ne samo ono koje je udaljeno za fiksnu duzinu (npr. 3 kod Cezarove šifre). Konkretno, govorimo o svim permutacijama nad zadatim alfabetom, čiji je broj jednak $n!$ pri čemu je n kardinalitet zadatog alfabeta. Dakle, prostor ključa kod engleskog alfabeta iznosio bi 26! što iznosi, otprilike, broj reda veličine 10^{18}, što u prevodu znači da je šifru sa ovakvim prostorom ključa praktično nemoguće razbiti metodom pokušaja i greške (probati zameniti svako slovo za svako).

Napomenimo u ovom delu da bismo supstitucionu šifru mogli kreirati i tako što slova alfabeta menjamo prirodnim brojevima uz pomoć neke bijektivne funkcije, baš kao što nam predstavlja tabela gore. Međutim, tu nam može predstavljati problem algoritam dekripcije - naime, iako smo kriptovali uz pomoć funkcije koja je bijekcija, te je intuitivno naslutiti da bismo mogli dekriptovati uz pomoć njenoj inverznoj funkciji, pri dekripciji dolazi do izostanka pojave jednoznačnosti, što nam govori da ustvari šifra na taj način ne može biti kreirana (ukoliko ne obezbeđuje jednoznačnost dekriptovanja). Uzmimo primer iz prethodne tabele i postavimo zadatak - kako bismo dekriptovali šifrat 118? Lako zaključujemo da tu jednoznačnost dekriptovanja nije moguća, jer šifrat 118 može opisivati sledeće otvorene tekstove : bbe (ukoliko razložimo šifrat kao 1 1 8), he (11 8) ili bn(1 18). Taj problem se može prevazići na manje ili više efikasne načine: najjednostavniji bi bio taj da se u šifratu pravi razmak posle broja koji predstavlja svako slovo, ali to bi u znatnoj meri olakšalo posao kriptoanalitičarima u metodi frekvencije slova (o čemu će više reči biti kasnije u ovom radu, prim. aut.). Drugi bi bio efektivniji, a možda zapravo i ne komplikovaniji, a sastojao bi se samo u tome da svaki elemenat šifrata bude

fiksne iste dužine tj. u našem slučaju gore navedene tabele samo bismo redom a,b,c... menjali sa 00,01,02... umesto sa jednocifrenim 0,1,2... . Više o razradi takve problematike i tih problema sledi u nastavku rada (poglavlje OTP).

Sledeći primer koji je ostavio velikog traga u istoriji predstavljala je *Vigenére cipher* tj. Vižnerova šifra. Ime je dobila po poznatom francuskom kriptografu *Blaise de Vigenére* koji je živeo u 16. veku, iako mnogi tvrde da je inspiraciju za takav vid šifrovanja Vižner pronašao u radu italijanskog kriptografa Leona Baptiste Albertija u drugoj polovini 15. veka. Za razliku od Cezarove šifre, ovde ključ neće predstavljati fiksiran broj n za koliko mesta ćemo pomerati svako slovo našeg alfabeta, već ce se menjati za svako slovo otvorenog teksta. Isto slovo će moći biti zamenjeno sa n različitih slova (pri čemu nam n predstavlja kardinalnost alfabeta nad kojim radimo) i na taj način dolazimo do ogromnog broja kombinacija koji smo iznad spomenuli, te ključa koji se ne sastoji od samo jednog prirodnog broja. Da budemo potpuno precizni, ključ kod Vižnerove šifre predstavlja reč, tj. *ključna reč*, uz pomoć koje dobijamo odgovor koje slovo ćemo zameniti kojim. Naime, prvo što treba da uradimo jeste da otvoreni tekst podelimo na blokove dužine koja je jednaka dužini ključne reči i svakom bloku dodelimo ključnu reč. Dalje, kriptujemo tako što, uz pomoć bijekcije definisane ranije, predstavljene u vidu tabele na stranici iznad, slovu iz otvorenog teksta dodeljujemo odgovarajući numerički ekvivalent, potom isto to uradimo za njemu odgovarajuće slovo ključne reči. Ta dva broja potom saberemo i onda nadjemo ostatak dobijenog zbira pri deljenju sa kardinalnosti alfabeta. Ilustrujmo ovaj postupak na sledećem primeru:

Primer 1.2.1 *Kriptovati otvoreni tekst "pucaj sutra u zoru" Vižnerovom šifrom, uz pomoć ključne reči VATRA.*

Dakle, prvo ćemo otvoreni tekst podeliti na blokove dužine 5 i njima dodeliti ključnu reč na sledeći način:

p	*u*	*c*	*a*	*j*	*s*	*u*	*t*	*r*	*a*	*u*	*z*	*o*	*r*	*u*
v	*a*	*t*	*r*	*a*	*v*	*a*	*t*	*r*	*a*	*v*	*a*	*t*	*r*	*a*

dodelimo sada odgovarajuće numeričke ekvivalente ovim slovima te ih saberimo po (mod 30)*:*

	21	*26*	*2*	*0*	*13*	*24*	*26*	*25*	*22*	*0*	*26*	*28*	*20*	*22*	*26*
$+_{30}$	*27*	*0*	*25*	*22*	*0*	*27*	*0*	*25*	*22*	*0*	*27*	*0*	*25*	*22*	*0*
	18	*26*	*27*	*22*	*13*	*21*	*26*	*20*	*14*	*0*	*23*	*28*	*15*	*14*	*26*

te sada vratimo slova koja odgovaraju ovim brojevima, i dobićemo sledeći šifrat:

$$NUVRJPUOKASZLKU$$

Na analogan način bi se uradio inverzni zadatak, tj. iz šifrata NUVRJPUOKASZLKU uz pomoć ključne reči VATRA dobio originalni tekst : dodelili bismo brojeve šifratu i ključu, oduzeli bismo ih po (mod 30) *i onda dobijenim ciframa dodelili odgovarajuća slova i tako dobili originalni otvoreni tekst : PUCAJ SUTRA U ZORU.*

Tabela u nastavku predstavlja Vižnerov kvadrat tj. tablicu za srpsku abecedu. Naime, redom su ispisani svi alfabeti, tj. sve kombinacije kojima se bilo koje slovo može zameniti bilo kojim slovom srpske abecede. U zavisnosti od već pomenute ključne reči biraćemo vrstu u tabeli iz koje ćemo iščitati odgovarajuće slovo kojim menjamo ono koje želimo šifrovati. Konkretno, iz primera iznad, želimo da šifrujemo slovo P uz pomoć slova V iz ključa. Slovu V odgovara numerički ekvivalent 27 pa ćemo slovo kojim treba šifrovati slovo P potražiti baš u 27. vrsti, u preseku sa kolonom u kojoj je u prvoj vrsti slovo P. Na toj lokaciji nalazimo slovo N i njime šifrujemo slovo P, baš kao što smo i uradili u primeru navedenom na prošloj stranici.

početni alfabet	a	b	c	č	ć	d	dž	đ	e	f	g	h	i	j	k	l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž
alfabet 1	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A
alfabet 2	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B
alfabet 3	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
alfabet 4	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
alfabet 5	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć
alfabet 6	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D
alfabet 7	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž
alfabet 8	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ
alfabet 9	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E
alfabet 10	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F
alfabet 11	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G
alfabet 12	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H
alfabet 13	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I
alfabet 14	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J
alfabet 15	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K
alfabet 16	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L
alfabet 17	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj
alfabet 18	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M
alfabet 19	Nj	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N
alfabet 20	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj
alfabet 21	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O
alfabet 22	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P
alfabet 23	S	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R
alfabet 24	Š	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S
alfabet 25	T	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š
alfabet 26	U	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T
alfabet 27	V	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U
alfabet 28	Z	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V
alfabet 29	Ž	A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z

Tabela 1.3: Vigenére-ova tablica za srpsku abecedu

Podižući stepen složenosti načina šifrovanja odnosno ključa, polako dolazimo i do novije istorije. Sledeći primer zasniva se na ključu koji je zapravo tabela brojeva, odnosno *matrica*. 1929. godine *Lester Hill*, američki matematičar, patentuje prvu *poligrafsku* šifru, tj. šifru gde se ne šifruje svako slovo za sebe, već se grupe od nekoliko slova šifruju zajedno. Posmatrajmo samo koliko se povećava složenost kriptovanja ukoliko bismo posmatrali blokove od po dva slova - morali bismo napraviti ključ za alfabet od $30^2 = 900$ parova slova - možete samo da pretpostavite koliko se složenost dekripcije u tom slučaju povećava. Naime, Hil je osmislio algoritam gde su uslovi sledeći:

- neka imamo otvoreni tekst p, koji je moguće podeliti na blokove dužine m;
- ključ će biti kvadratna matrica K dimenzija $m*m$ koja mora biti *invertibilna*.

Ako označimo niz blokova sa $m_1, m_2...m_p, p \in \mathbb{N}$ tada ćemo kriptovati na sledeći način : množićemo matrično numeričke ekvivalente blokova $m_i, i \in$ *1,...,p* sa matricom K i dobijati redom odgovarajuće blokove šifrata $c_i, i \in$ *1,...,p*. Analogno bismo dobili i blokove otvorenog teksta iz blokova šifrata, samo što bismo numeričke ekvivalente blokova šifrata matrično množili sa matricom K^{-1}, inverznom matricom matrice K. Čak je i sam Hil predložio da se za ovaj postupak koriste involutivne matrice, međutim time bi se prostor ključa isuviše smanjio, te bi proces kriptovanja ali i dekriptovanja bio mnogo lakši.

Pokažimo ovaj postupak na praktičnom primeru:

Primer 1.2.2 *Šifrovati Hilovom šifrom otvoreni tekst "pucaj sutra u zoru" ključem K:*

$$K = \begin{bmatrix} 10 & 16 & 44 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix}$$

Bijektivno preslikajmo slova otvorenog teksta u brojeve i dobićemo niz : 21 26 2 0 13 23 26 25 22 0 26 28 20 22 26 . Sada ćemo podeliti numerički ekvivalent otvorenog teksta na blokove dužine jednake dimenziji kvadratne matrice, tj. na blokove dužine 3. Dobijamo sledeći niz blokova:

21 26 2
0 13 23
26 25 22
0 26 28
20 22 26

I sada redom, množimo blok po blok sa matricom ključem, i tako dobijamo šifrat. Postupak će ovako izgledati za prvi blok :

$$\begin{bmatrix} 26 & 21 & 2 \end{bmatrix} \times \begin{bmatrix} 10 & 16 & 44 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix} = \begin{bmatrix} 322 & 561 & 1682 \end{bmatrix} mod 30$$

i kada nađemo ostatak brojeva vektora rezultante pri deljenju sa 30, dobijemo vektor:

$$\begin{bmatrix} 22 & 21 & 2 \end{bmatrix}$$

što nam je, zapravo, numerički ekvivalent šifrata, i kada mu pomoću bijektivne funkcije vratimo slova dobijamo šifrat : RPC. Ponovimo analogan postupak za preostala četiri bloka i dobićemo sledeće šifrate respektivno : LjLJ OPN CAO ŠOO. Dakle, šifrujući otvoren tekst "pucaj sutra u zoru" Hilovom šifrom, uz pomoć matrice K dobijamo sledeći šifrat : RPCLjLJOPNCAOŠOO.

Takođe, još jedan od poznatih primera šiforvanja jeste *šifrovanje transpozicijom.* Zasniva se na sledećem principu : otvoreni tekst podelimo na blokove dužine jednake dužini ključa, i ispišimo te blokove u tabelu horizontalno jedan ispod drugog (ukoliko se desi da dužina otvorenog teksta nije deljiva sa dužinom ključa, dopunjavamo poslednju vrstu sa znakom X). Pri tome ključ mora biti broj koji se sastoji od ispermutovanih cifara počev od 1, pa sve do broja slova u jednom bloku otvorenog teksta . Šifrat dobijamo tako što prepišemo blokove teksta u kolonama u poretku od prve kolone u tabeli pa naviše (koji je, u opštem slučaju, različit od ključa). U nastavku navodimo primer šifrovanja transpozicijom po kolonama.

Primer 1.2.3 *Šifrovati otvoreni tekst "pucaj sutra u zoru" transpozicijom po kolonama sa ključem 4132.*

4	*1*	*3*	*2*
P	*U*	*C*	*A*
J	*S*	*U*	*T*
R	*A*	*U*	*Z*
O	*R*	*U*	*X*

Ispisujući tekst po kolonama po rastućem poretku brojeva dobijamo sledeći šifrat: USARATZXCUUUPJRO. Lako je uraditi i obratno - iz ključa i šifrata napraviti tabelu i upisati šifrat po poretku kolona iz ključa te dobiti i originalni tekst.

Sledeći primeri, možda i najpoznatiji u modernoj istoriji, jesu mašine za šifrovanje. Prva takva mašina (ukoliko je možemo uopšte i nazvati mašinom, pošto u suštini nije imala nikakav mehanički deo) jeste *Jeffersonov disk.* Izmišljen je od strane američkog predsednika Thomasa Jeffersona jos krajem 19. veka, ali možemo pretpostaviti koliko je bio ispred svog vremena, s obzirom da je od strane američke vojske korišćen od 1923. pa sve do 1942. godine pod nazivom M-94. Mehanizam nije bio složen - sastojao se iz jedne šipke na koju su bili namontirani 36 diskova. Na svaki disk ponaosob bila su ispisana u proizvoljnim redom sva slova alfabeta. Rotacijom diskova mogla se "namestiti" poruka u jednoj liniji, pri čemu je bilo koji od ostalih 25 proizvoljnih nizova slova predstavljao ključ koji bi se dostavljao primaocu poruke. Bez ključa u to vreme za kriptoanalitičare bilo je veoma teško da provere sve moguće kombinacije, čak i ukoliko poseduju džefersonov disk, jer je broj mogućih poredaka diskova iznosio 26^{26}.

Dalje, amerikanac *Edward Hugh Hebern* patentirao je uređaj pod nazivom *električna mašina za kodiranje*. To je praktično bila pisaća mašina sa dve tastature od po 26 slova, gde su parovi slova bili spojeni električnim žicama, te kada bi korisnik pritisnuo jedno slovo na prvoj tastaturi, direktno bi se na drugoj otkucao njegov ekvivalent po ključu, tj. slovo kojim se ono koje je korisnik uneo šifruje. Kasnije, mašina je unapređena tako što je u nju instalirano dodatnih 5 rotora za monoalfabetsku supstituciju, te se broj kombinacija kriptovanja povećao na 26^6. Međutim, pravo otkrovenje u tadašnjem svetu električnih uređaja za kriptovanje predstavljala je mašina pod imenom *enigma*. Reč enigma potiče iz latinskog jezika i znači *zagonetka*. Isprojektovana je od strane nacističkog inženjera Artura Šerbiusa jos početkom 20. veka. Zvanično, Šerbius je prijavio patent za mašinu za šifrovanje sa rotorima 23. februara 1918. Na početku, mehanizam *enigme* sastojao se od tastarure, ekrana za ispis šifrata, tri rotora te električne prespojne ploče, što je davalo ukupno $26^3 = 17576$ mogućih kombinacija ključa, što nije bio ni približno dovoljan prostor ključa za iole ozbiljnu upotrebu. Potom je mehanizam unapređen opcijom međusobone zamene mesta rotora (3 rotora, pa 3!=6 permutacija), zatim su dodati još 10 prespojnih kablova(čija je uloga bila da na pritisak npr. slova A, šalju signal koji nosi informaciju kao da je trebalo šifrovati slovo F), te kada se sve to ukombinuje sa početnim brojem kombinacija dobio se prostor ključa koji je sadržao ukupno 150 738 274 937 250 mogućih kombinacija. Sa tolikim prostorom ključa napad ispitivanjem svih mogućih kombinacija postao je nemoguć. Nemačka vojska, tokom II svetskog rata, komunicirala je sa svojim saveznicima porukama šifrovanim upravo ovom mašinom. Ipak, i pored složenog mehanizma, mnoge ekipe iz protivničkog tabora, tj. Antante pokušavale su da dekriptuju poruke kriptovane uz pomoć *enigme*. Dve grupe kriptoanalitičara su to i uspele. Predvodnik poljske ekipe bio je *Marijan Rejewski* , a čuveni engleski matematičar *Alan Turing* predvodio je drugu ekipu, predstavnicu Engleske. Mnogi tvrde da je rat možda i okončan pobedom Antante upravo iz razloga što su nemačke namere i poruke dekriptovane i protumačene od strane ove dve ekipe. Kriptoanalitičarske ekipe su se sastojale od uglavnom prirodnjaka, matematičara i šahista. Smatra se da je uspešno izvršen zadatak timova za dešifrovanje glavni razlog zaustavljanja nemačke invazije i imperije i ključna prekretnica u zaustavljanju Trojnog Pakta. Još jedna od poznatih naprava za šifrovanje popularna sredinom 20. veka bila je C-36, delo Šveđanina *Borisa Hagelina*, u američkoj vojsci poznatija kao M-209. Radila je na principu sličnom mehanizmu enigme.

Generalno, sa razvojem kriptografije i njenih metoda, dolazi do pojave *kriptoanalize*, čiji je glavni zadatak inverz kriptografiji : od šifrata, bez poznavanja ključa, doći do originalnog otvorenog teksta. Kako je kriptografija dobijala na značaju i kako su se kriptografskim metodama prenosile sve vrednije i važnije informacije, time je i kriptoanaliza postjala sve bitnija disciplina i sve više, pre svega matematičara i informatičara, počelo se baviti dekriptovanjem šifrata. *Napadačem* zovemo osobu koja, uz pomoć kriptoanalitičkih metoda, pokušava da neautorizovano dođe do otvorenog teksta, tj. poruke koja nije upućena njemu i da je na neki način zloupotrebi. Neki ih nazivaju i *hakerima*, a po namerama i nameni razlikujemo hakere sa *belim* i *crnim* šeširima. Hakere sa crnim šesirima nazivamo napadače

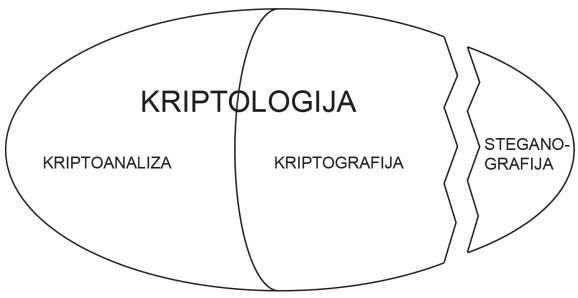
loših namera, da špijuniraju, prodaju podatke, nanesu štetu pošaljiocu ili na bilo koji drugi način zloupotrebe presretnute podatke. Hakeri sa belim šeširima su hakeri koje unajmljuju upravo institucije koje žele da pojačaju svoje kriptografske sisteme, namenski dakle unajmljuju napadače koji bi probavali da dekriptuju njihove podatke i na taj način im ukažu na slabosti implementirane u njihovom sistemu. Osnovna pretpostavka kriptoanalize je da kriptoanalitičar zna koji se kriptosistem koristi što generalo ne mora biti tačno, ali tom pretpostavkom ograničavamo sigurnost u startu. Ova pretpostavka naziva se *Kerckhoffsovo pravilo*, po *Augustu Kerckhoffsu*, poznatnom holandskom kriptologu.

1.3 Pojam kriptologije i steganografije

Kao što smo već napomenuli, **steganografija** predstavlja disciplinu koja se sastoji pre svega iz metoda skrivanja poruka. Termin *steganografija* nastao je od grčkih reči : *steganos* što znači prikriveno ili zaštićeno i *graphein* tj. pisanje. Sam termin steganografija uveo je Nemac *Johannes Trithemius* u svom najpoznatijem radu *Steganographia*, napisanom 1499. godine. Interesantno, upravo taj Johanesov rad predstavlja i prvo štampano izdanje o kriptografiji.

Steganografija, kao takva, predstavlja neki vid preteče kriptografije, međutim, ove dve naučne discipline ne nalaze se u nekoj inkluzivnoj relaciji, tj. steganografija ne predstavlja granu kriptografije, ali ipak, ove discipline imaju isti cilj, a to je da zaštite i prikriju informaciju. Razlika je u tome što se kod steganografije teži da se poruka sakrije, ili još bolje uklopi u neki sadržaj tako da se uopšte i ne posumnja da se šalje poruka, odnosno ona uopšte ne menja informaciju, nego ju "kamuflira" i samim time ne privlači pažnju na nju. Cilj kriptografije jeste da promeni informaciju (šifrira) do te mere da je ona nerazumljiva trećoj strani. Upravo u toj razlici, neki ljudi nalaze prednosti steganografije u odnosu na kriptografiju, jer šifrirana poruka će uvek privući više pažnje napadača od poruke za koju napadači i ne znaju da se šalje. Ipak, neoborivo je da je informacija najbolje zaštićena kada se ove dve dicipline kombinuju, tj. poruka se "kamuflira" da se ne može lako otkriti, a i ako se to desi, sadržaj poruke je šifrovan, tako da, sve i ako se stigne do šifrata, nije lako doći do originalnog teksta.

Kriptologija je nauka generalno o šiframa, a čine je dve funkcionalne celine: **kriptografija** (koja izučava metode kriptovanja, zaštite i čuvanja informacija te njihovog bezbednog transporta) i **kriptoanaliza** (čiji glavni zadatak je upravo suprotan kriptografiji, tj. kriptoanaliza izučava i implementira metode za "razbijanje šifri" odnosno dešifrovanje bez tajnog ključa).



Slika 1.2: Ilustracija skupovnih relacija gore navedenih disciplina.

Reč kriptografija je grčkog porekla, sastoji se od reči *kryptos* što znači skriveno ili tajna, i reči *graphein* tj. pisanje. Srž kriptografije jeste sigurna komunikacija, a ona se postiže uz pomoć četiri osnovna načela ili postulata kriptografije :

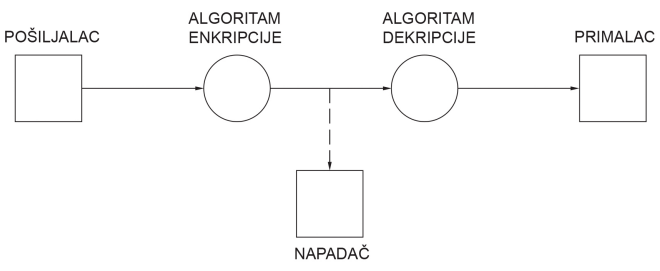
- *Poverljivost (privatnost ili tajnost)* poruke (engl. message confidentiality ili privacy) - predstavlja činjenicu da samo autorizovane osobe mogu da pristupe datoj informaciji. To se postiže na razne načine - od fizičke zaštite sadržaja sve do matematičko kriptografskih algoritama koji čine da podaci na prvi pogled izgledaju neupotrebljivo.

- *Integritet* poruke - ovo svojstvo bavi se ispitivanjem "originalnosti" poruke, u smlislu provere da li je pre prijema i dekripcije poruke došlo do neautoruizovanih promena (brisanja, izmene, umetanja teksta) na samom šifratu, a samim time i otvorenom tekstu nakon dekripcije.

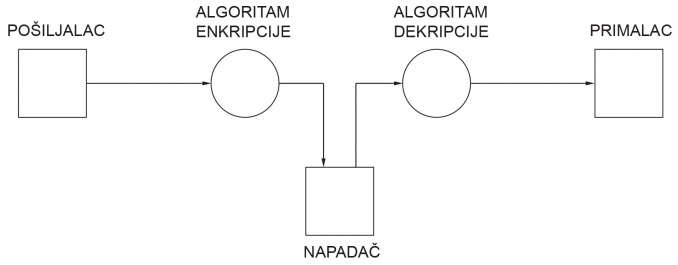
- *Autentifikacija* pošaljioca - sposobnost primaoca poruke da iz iste utvrdi identitet pošaljioca , poreklo poruke, te njen put komunikacijskim kanalom.

- *Neporicanje* pošaljioca - (engl. non-repudiation) - ovom osobinom kriptografija sprečava korisnika da "poriče" izvršavanje odnosno neizvršavanje određenih akcija u prošlosti. Za ovu i prošlu osobinu blisko je vezan pojam *digitalnog potpisa* (o kome će biti reči kasnije u radu prim. aut.) koji predstavlja neku vrstu dokaza identiteta pošaljioca i njegovih radnji pri izvesnim elektronskim akcijama.

S druge strane, kao što smo već napomenuli, **kriptoanaliza** je druga grana kriptologije koja se bavi dekripcijom šifrovanih podataka, tj. šifrata, i to bez ključa. Sama reč je nastala, naravno od grčkih reči *kryptos* što znači skriveno ili tajna, i reči *analyein* odnosno analiza ili testiranje. Bilo koji pokušaj implementiranja kriptoanalitičkih metoda na šifrat u daljem tekstu deklarisaćemo kao **napad**, a kriptoanalitičare kao **napadače**. U kriptoanalizi razlikujemo 2. vrste napada: **pasivne** (podrazumeva "samo" posmatranje i nadgledanje komunikacijskog kanala) i **aktivne** (pokušaji brisanja, izmenjivanja, te ponovnog slanja poruka). Po pravilu, pasivne napade je znatno teže identifikovati nego aktivne.



Slika 1.3: Šablon prikaza pasivnog napada.



Slika 1.4: Šablon prikaza aktivnog napada..

Razlikujemo 4 vrste aktivnih napada po onome što je napadaču poznato:

- **samo šifrat** (*engl. ciphertext-only attack*) - najteža situacija za napadača, ali najčesća u realnosti. Napadač poseduje samo presretnuti šifrat, bez ključa i otvorenog teksta. Da bi ovakav tip kriptoanalitičkog napada bio efikasan, neophodno je posedovati veliku količinu šifrata. Cilj napadača je višestruk - doći do originalnog teksta, a najčešće je potreba otkriti i ključ, ukoliko se planiraju prestretati i dekriptovati poruke poslate na isti način u budućnosti.
- **šifrat + otvoreni tekst** - ređa situacija, ali kada napadač poseduje i šifrat i deo otvorenog teksta pa iz njih pokušava da dođe do ključa kako bi dalje, uz pomoć tog ključa, mogao dešifrovati sledeće poslate šifrate.
- **odabrani šifrat** (*engl. chosen ciphertext attack*)- radi se o situaciji koja opisuje kriptoanalitički napad kod sistema sa javnim ključem. Naime, napadač je u mogućnosti da odabere deo šifrata te njemu odgovarajući otvoreni tekst. Cilj je otkriti algoritam za dešifrovanje, tj. privatni ključ.
- **odabrani otvoreni tekst** (*engl. chosen plaintext attack*)- Kriptoanalitičar bira deo otvorenog teksta, a potom dobija i njemu odgovarajući šifrat.

Od ove 4 vrste aktivnih napada prvi gore naveden (ciphertext-only attack) je najrealniji, klasičan napad koji su kriptoanalitičari sposobni da izvedu. Preostala 3 već podrazumevaju veće veštine napadača i ponekad je potrebno i više od poznavanja samo kriptoanalize da bi se došlo do podataka koji su potrebni za izvesti neki od tih vrsta napada na sistem. Ipak, ne isključujemo te opcije pod pretpostavkom da su kriptoanalitičari veoma vešti, te uzimajući u obzir da ako dođu do šifrata, mogu doći i do otvorenog teksta.

Treba napomenuti da, pored ove 4 vrste kriptoanalitičkih napada, često se u kriptoanalitičkoj literaturi može naići na još jedan pojam kada su na napadi u pitanju, a to je termin *side-channel attacks*. Pod tim terminom podrazumevamo napade koji se ne baziraju na posmatranju samih otvorenih tekstova i šifrata, već se pri takvim napadima prate neka osnovna stanje fizičkih karakteristika hardvera koji služi za primopredaju poruka (npr. računara, telefona, itd.) : vremene koje je potrebno da se pošalje poruka, količina elktrične energije koju aparat utroši prilikom obavljanja kriptografske radnje, zvuk koji aparat proizvodi prilikom rada itd. Čak postoji i kriptoanalitička disciplina koja se bavi analizom zvuka koji razni aparati proizvode prilikom enkripcije otvorenog teksta, dekripcije šifrata ili slanja šifrata, a ona se naziva *akustična kriptoanaliza* (engl. acoustic cryptoanalysis).

Postoje razne metode koje koriste kriptoanalitičari. Najjednostavnije metode kriptoanalize jesu *brute force* napadi, a najprimitivnija verzija ovih napada svodi se na mehaničko pokušavanje isprobavanja svih mogućih kombinacija za ključ (npr. ukoliko se radi o nekoj lozinki za pristup najjednostavniji brute force napad podrazumevao bi isprobavanje svih mogućih kombinacija za lozinku). Međutim, lako je zaključiti da ovakav vid napada nije preterano efikasan jer vreme koje je potrebno da on rezultuje otkrivanjem ključa direktno je proporcionalno od prostora ključa te kardinalnosti skupa alfabeta ključa. Zato se ovakav tip napada unapređivao računarskim programima koji sami generišu ključeve, te ukoliko se radi o ključu u vidu lozinke za pristup nekom profilu ili serveru, program proverava redom smislene reči iz nekog rečnika koji mu je ranije zadat (npr. kolekcije najčešće korišćenih kombinacija slova i brojeva za lozinke), i tako čini ovaj napad lakše izvodivim, tj. smanjuje vreme potrebno da se isti realizuje. Upravo zbog takvih napada pri kreiranju lozinki program nam sam ne dozvoljava da kreiramo "predvidivu" lozinku koja recimo sadrži naše ime i prezime, datum rođenja itd. Takođe, u mnogim sistemima postoji ograničenje da posle npr. 5-10 neuspešnih pokušaja logovanja (zbog pogrešne lozinke ili korisničkog imena) dolazi do blokiranja profila.

Još jedan od fundamentalnih metoda napada, možda i najpoznatiji metod kriptoanalize zasniva se na frekvenciji i analizi slova u šifratu. Naime, postoji zvanična statistika koja nam govori o frekventnosti tj. procentima pojavljivanja svakog slova abecede ponaosob u okviru nekog jezika. Tako naprimer, zvanična statistika u vidu procenata pojave slova abecede u tekstovima za engleski, nemački i srpski jezik data je u okviru sledećih tabela:

engleski jezik	
slovo	**frekvencija**
A	8.55
B	1.60
C	3.16
D	3.87
E	12.10
F	2.18
G	2.90
H	4.96
I	7.33
J	0.22
K	0.81
L	4.21
M	2.53
N	7.17
O	7.47
P	2.07
Q	0.10
R	6.33
S	6.73
T	8.94
U	2.68
V	1.06
W	1.83
X	0.19
Y	1.72
Z	0.11

nemački jezik	
slovo	**frekvencija**
A	6.34
B	2.21
C	2.71
D	4.92
E	15.99
F	1.80
G	3.02
H	4.11
I	7.60
J	0.27
K	1.50
L	3.72
M	2.75
N	9.59
O	2.75
P	1.06
Q	0.04
R	7.71
S	6.41
T	6.43
U	3.76
V	0.94
W	1.40
X	0.07
Y	0.13
Z	1.22
ä	0.54
ö	0.24
ü	0.63
ß	0.15

srpski jezik	
slovo	**frekvencija**
A	11.96
B	1.62
C	2.84
D	4.93
Dž	0.12
E	8.77
F	0.43
G	1.73
H	0.50
I	9.95
J	3.99
K	3.37
L	3.16
Lj	0.39
M	2.49
N	6.47
Nj	0.46
O	7.89
P	2.75
R	6.12
S	5.82
T	4.35
U	3.99
V	3.48
Z	2.42

Takođe, pri detaljnijoj analizi šifrata korsite se i frekvencije pojava parova slova (bigrama) te tri uzastopna slova (trigrama). U engleskom jeziku, npr. što se tiče bigrama najčešće su pojave parova TH (2.71 %) i HE (2.33 %),potom slede IN (2.03 %) i ER (1.78 %). Kada su u pitanju trigrami najfrekventnije trojke jesu THE(1.81 %), AND(0,73 %) i ING(0,72 %). Dalje, u nemačkom jeziku najčešća je pojava parova ER (3.9 %), EN (3.61 %), CH (2.36 %), DE (2.31 %), a trigrama DER (1.04 %) i EIN (0.83 %).

Što se tiče podataka, zvanična statistika za engleski i nemački jezik preuzeta je sa kriptoanalitičkog sajta [11], dok je u nedostatku takvih podataka za srpski jezik rađena samostalna analiza iz dnevne štampe. Treba napomenuti da su u tabeli za srpski jezik izostavljena slova č,ć,ž,đ,š čiji su procenti dodati respektivno slovima

c,c,z,d,s zbog jednostavnosti analize teksta. U tom smislu rezultati mogu sadržati malu devijaciju, jer je se u procentu pojave slova c,z,d,s nalaze i procenti pojave slova č,ć,ž,đ,š, međutim, devijacija bi u svakom smislu trebala biti dopustiva, jer se radi o pojavi npr. slova š od ne više od 25 puta na uzorku od preko 11000 slova, što predstavlja procenat pojave slova ne veći od 2 promila.

Što se tiče samog pojma šifre, ili drugačije, šeme enkripcije te dekripcije, postoji nekoliko podela u odnosu na način šifrovanja :

1. Podela prema alfabetu šifrata:
   - **monoalfabetne šifre** - one šifre u kojima postoji jedno i samo jedno slovo kojim se može zameniti slovo originalnog teksta. Kod njih se može uspostaviti bijekcija jer svako slovo šifrata tj. slika ima tačno jedno slovo otvorenog teksta tj. original. Primer monoalfabetne šifre jeste *Cezarova šifra.*
   - **polialfabetne šifre** - one šifre gde slovo otvorenog teksta može biti zamenjeno sa dva ili više različitih slova šifrata, u zavisnosti od nekih faktora, npr. reči koja predstavlja ključ. Takvu situaciju imamo kod *Vižnerove šifre.*
2. Podela prema ključu, tj. alogoritmima šifrovanja i dešifrovanja :
   - **simetrične šifre** - kod simetričnih šifri iz funkcije enkripcije moguće je odrediti funkciju dekripcije. U nekim situacijama one su čak i jednake. Takav slučaj je kod *One Time Pad algoritma* (algoritam jednokratne beležnice), detaljnije razrađenom kasnije u radu. Ovakve šifre se još zovu i *šifre sa privatnim ključem.*
   - **asimetrične šifre** - iako su na neki način funkcija enkripcije i dekripcije povezane, nije moguće iz funkcije enkripcije direktno otkriti tj. dobiti funkciju dekripcije. Ovoj grupi pripada, između ostalih i *RSA algororitam.* Takve šifre zovemo još i *šifre sa javnim ključem.*
   - **hibridne šifre** - šifre se zasnivaju na sistem koji koristi i simetrični i asimetrični ključ, tj. njihovu kombinaciju.
3. Podela prema tipu operacija pri šifrovanju :
   - **supstitucione šifre** - šifre kod kojih se kriptovanje zasniva na zameni slova nekim drugi slovom, te se može desiti da se slova koja postoje u otvorenom tekstu ne pojavljuju uopšte u šifratu i obratno;
   - **transpozicione šifre** - šifre kod kojih se kriptovanje zasniva na permutacijama slova iz originalnog teksta. Šifrat zapravo predstavlja samo permutaciju slova koja se pojavljuju u originalnom tekstu, te je frekvencija slova u šifratu i otvorenom tekstu potpuno ista, samo je reč o drugom redosledu.
   - **hibridne šifre** - i po ovom kriterijumu, baš kao i po prošlo navedenom, hibridnom šifrom nazivamo šifru koja kombinuje suspstitucioni i traspozicioni metod.

4. Podela prema načinu na koji se obrađuje otvoreni tekst :

   - **blokovne šifre** - delimo otvoreni tekst na blokove koje potom obrađujemo svaki zasebno.
   - **protočne šifre** - otvoreni tekst posmatramo kao neprekidni niz znakova te kriptujemo svaki za sebe, tj. "protočno" kriptujemo. Primeri ovakvi šifri su *stream cipher* ili *keystream*.

5. Podela prema kriptoanalitičkoj analizi šifri :

   - **kompromitovani algoritmi** - algoritmi koji su detaljno izanalizrani od strane napadača, te su mehanizmi za dekripciju poznati. Većina postojećih algoritama spada u ovu kategoriju.
   - **nekompromitovani algoritmi** - algoritmi koji su analizirani, ali napadači još uvek nisu uspeli da generišu sigurno pravilo za dekripciju. U takve, još uvek nerešive algoritme, spadaju simetrični algoritam AES, te asimetrični algoritam RSA.
   - **neanalizirani algoritmi** - ukoliko uopšte ovo možemo nazvati kategorijom, jer vrlo je mali vremenski interval koji prođe a da algoritam nije napadnut od strane kriptoanalitičara. Ovde dakle spadaju svi novi algoritmi dok još ne budu napadnuti od strane kriptoanalitičara. Kada se to desi, algoritam se momentalno prebacuje u jednu od dve gore navedene kategorije.

Glava 2

Drugi deo

2.1 Matematička osnova

Definicija 2.1.1 *(***Deljivost***)*
Za date brojeve $n, m \in \mathbb{Z} \setminus \{0\}$ kažemo da n deli m, odnosno da je m deljivo sa n ukoliko postoji ceo broj b takav da važi $m = b * n$. To označavamo sa $n \mid m$. Ako n ne deli m, onda pišemo $n \nmid m$. Ako $n \mid m$ onda još kažemo da je n delilac od m, odnosno da je m sadržalac od n.

Definicija 2.1.2 *Broj $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ je* **prost** *(engl. prime) broj ukoliko je deljiv samo sa ± 1 i $\pm n$, tj.*

$$\nexists m \in \mathbb{Z} \setminus \{\pm 1, \pm n\} : m \mid n$$

Broj koji nije prost nazivamo **složen** *(engl. composite).*

Definicija 2.1.3 *Za date $n, m \in \mathbb{Z}$ zajednički delilac je prirodan broj d takav da važi $d \mid n$ i $d \mid m$. Ako je barem jedan od brojeva n i m različit od nule, onda postoji samo konačno mnogo zajedničkih delilaca brojeva n i m. Najveći među njima zove se* **najveći zajednički delilac** *brojeva n i m i označava se sa NZD(n,m) (engl. GCD(n,m) (greatest common divisor)).*

Definicija 2.1.4 *Celi brojevi n i m su* **uzajamno (relativno) prosti** *(engl. relatively prime) ukoliko je $NZD(n, m) = 1$.*

Teorema 2.1.1 (Teorema o deljenju sa ostatkom) *Za proizvoljan prirodan broj b i celi broj a postoje jedinstveni celi brojevi q i r takvi da je:*

$$a = q \cdot b + r, \qquad 0 \leq r < b.$$

Broj q se zove količnik, a r se zove ostatak pri deljenju a sa b.

Dokaz. Dokaz ćemo razložiti na 3 slučaja. Neka je:

- $a = 0$ - najjednostavniji slučaj, tada su $r = q = 0$, tj. $a = b \cdot 0 + 0$;
- $a > 0$ - postojanje bar jednog para brojeva r i q pokazaćemo indukcijom po a.
  - Baza indukcije. Dokažimo postojanje brojeva r i q za $a = 1$. Ovaj slučaj takođe razdvajamo na 2 slučaja u zavisnosti od broja b:
    - $b = 1$ tada su r=0 i q=1, jer važi $1 = 1 \cdot 1 + 0$
    - $b > 1$ tada su, suprotno prethodnom primeru, r=1 i q=0, važi $1 = b \cdot 0 + 1, b \in \mathbb{N}$
  - Indukcijska hipoteza. Pretpostavimo da tvrđenje važi za $a = q \cdot b + r$, tj. da postoje takvi r i q.
  - Indukcijski korak.
    Treba pokazati da tvrđenje važi za $a + 1$, tj. da postoje q_1 i r_1 takvi da je $a + 1 = q_1 \cdot b + r_1, 0 \leq r_1 < b$. Jednostavno, ukoliko je $r + 1 < b$ traženi brojevi q_1 i r_1 će biti $q_1 = q, r_1 = r + 1$, a ukoliko je $r + 1 = b$ onda će biti $q_1 = q + 1, r_1 = 0$.
  - $a < 0$ u ovom slučaju je $-a > 0$. Analogno delu za slučaj $a > 0$ iznad, u ovom slučaju za -a i b postoje brojevi q_1 i r_1, takvi da je $-a = b \cdot q_1 + r_1$ i $0 \leq r_1 < b$. Za $r_1 = 0$ tvrđenje važi jer $a = b \cdot (-q_1) + 0$, a u slučaju kada je $r_1 > 0$ tada je $a = b(-q_1 - 1) + b - r_1$ pri čemu važi $0 < b - r_1 < b$. U ovom slučaju, dakle, odgovarajući brojevi su $-q_1 - 1$ i $b - r_1$.

Dokažimo sada još jedinstvenost ovih brojeva metodom kontradikcije, tj. pretpostavimo da postoje dva para brojeva za koje važi:

$$a = b \cdot q_1 + r_1, \quad 0 \leq r_1 < b$$

i

$$a = b \cdot q_2 + r_2, \quad 0 \leq r_2 < b$$

Ako je $r_1 \neq r_2$, razlikujemo dva slučaja:

- $r_1 < r_2$, onda je $0 < r_2 - r_1 = b(q_2 - q_1)$ i $0 < r_2 - r_1 < b$. Odatle sledi da je $q_2 - q_1 > 0$, a kako radimo u $\mathbb{Z}$ onda je $q_2 - q_1 \geq 1$. Ali iz toga sledi da je $r_2 - r_1 \geq b$ što je u kontradikciji sa ranije pokazanim $r_2 - r_1 < b$.
- $r_1 > r_2$, analogno prethodnom slučaju, onda $0 < r_1 - r_2 = b(q_1 - q_2)$ i $0 < r_1 - r_2 < b$, pa imamo $q_2 - q_1 \geq 1$, ali onda $r_1 - r_2 \geq b$, što ne može jer je $r_1 - r_2 < b$.

Dakle, mora da bude $r_1 = r_2$, a kako je to slučaj onda iz $(q_2 - q_1) \cdot b = r_2 - r_1$ sledi i da je $q_2 = q_1$ čime je i dokazana jedinstvenost brojeva r i q iz teoreme. Raščlanjivanjem na slučajeve i pronalaženjem konkretnih rešenja za svaki slučaj ponaosob je ovaj dokaz završen. ∎

Teorema 2.1.2 *Neka su a,b,q i r celi brojevi takvi da je $b > 0, 0 \leq r < b, a = b \cdot q + r$. Tada je NZD(a,b)=NZD(b,r).*

Dokaz. Označimo, za potrebe ovog dokaza, sa $\mathbb{A}$ skup svih zajedničkih delitelja a i b, a sa $\mathbb{B}$ skup svih zajedničkih delitelja b i r. Neka je d proizvoljan zajednički delilac brojeva a i b. Tada iz jednakosti $a = b \cdot q + r$ sledi da d deli i r tj. da je zajednički delilac brojeva b i r. Time je pokazano da, ako je d zajednički delilac a i b, onda je on i zajednički delilac b i r. U skupovnom smislu to znači da je skup $\mathbb{A}$ *podskup* skupa $\mathbb{B}$. Slično, ako je d zajednički delilac b i r, iz iste jednakosti sledi da je on i zajednički delilac a i b, stoga je i skup $\mathbb{B}$ podskup skupa $\mathbb{A}$. Samim time, pokazano je da su $\mathbb{A}$ i $\mathbb{B}$ jednaki skupovi. Zato su jednaki i njihovi najveći elementi, tj. NZD(a,b)=NZD(b,r). ∎

Lema 2.1.3 *Ako je $a = bq$ i $b \geq 0$, onda je NZD(a,b)=b.*

Dokaz. $b|a$ jer $a = bq$, a očigledno je da je b najveći mogući delilac samog sebe. Iz toga sledi da je NZD(a,b)=b. ∎

Sledeća teorema, tj. Euklidov algoritam za nalaženje najvećeg zajedničkog delioca dva prirodna broja je najstariji algoritam koji je i danas u upotrebi. On se zasniva na prethodno navedenim teoremama i lemi.

Teorema 2.1.4 *(***Euklidov algoritam***) Neka su $a, b > 0$ prirodni brojevi. Pretpostavimo da je uzastopnom primenom teoreme o deljenju sa ostatkom dobijen niz jednakosti*

$$\begin{aligned} a &= b \cdot q_1 + r_1, & 0 \leq r_1 < b \\ b &= r_1 \cdot q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 \cdot q_3 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots \\ r_{j-2} &= r_{j-1} \cdot q_j + r_j, & 0 \leq r_j < r_{j-1} \\ r_{j-1} &= r_j \cdot q_{j+1} \end{aligned}$$

tada je NZD(a,b) jednak r_j, tj. poslednjem ostatku različitom od nule.

Dokaz. Pre svega, prokomentarišimo zašto je ovakav niz jednakosti dobijen primenom Teoreme o deljenju sa ostatkom konačan, tj. zašto se u Euklidovom algoritmu može formulisati ovakav konačan niz jednačina. Naime, niz ostataka $r_i, i = \{1, ..., j\}, j \in \mathbb{N}$ jeste konačan jer je strogo opadajući niz prirodnih brojeva te ograničen odozdo nulom (ne može biti negativan broj). Zato je svaki par prirodnih brojeva a i b moguće predstaviti jednačinama iznad u konačno mnogo koraka.

Na osnovu Teoreme 2.1.2 za niz jednakosti navedenih u Euklidovom algoritmu važi sledeće :

$$NZD(a,b) = NZD(b,r_1) = ... = NZD(r_{j-2}, r_{j-1}) = NZD(r_{j-1}, r_j)$$

Pošto $r_j | r_{j-1}$ iz Leme 2.1.3 dobijamo i $NZD(a,b) = r_j$, što je i trebalo pokazati. ∎

Definicija 2.1.5 *Neka je dat prirodni broj $m > 1$. Dva broja $a, b \in \mathbb{Z}$ su* **kongruentna po modulu** *m ako daju isti ostatak pri deljenju sa m. Pišemo*

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

Pojam *kongruencije* uveo je nemački mamtematičar Karl Fridrih Gaus.

Svi celi brojevi koji su kongruentni sa brojem m po datom modulu formiraju jednu klasu brojeva. Po modulu m, imamo m klasa brojeva za $k \in \mathbb{N}$:

- oblika $m \cdot k$, tj. brojevi koji su kongruentni sa 0 po modulu m (deljivi su sa m);
- oblika $m \cdot k + 1$, tj. brojevi koji su kongruentni sa 1 po modulu m (ostatak pri deljenju brojem m im je 1);
- oblika $m \cdot k + 2$, tj. brojevi koji su kongruentni sa 2 po modulu m;
- .
- .
- .
- oblika $m \cdot k + m - 2$, tj. brojevi koji su kongruentni sa m-2 po modulu m;
- oblika $m \cdot k + m - 1$, tj. brojevi koji su kongruentni m-1 po modulu m;

Lako se primećuje da su, ovakvim formiranjem klasa svi celi brojevi podeljeni u m *disjunktnih podskupova* skupa celih brojeva $\mathbb{Z}$, a brojevi 0,1,2,...,m-1 su reprezenti odgovarajuće klase brojeva u kojoj se nalaze. Skup svih tih reprezenata nazivamo **potpunim sistemom ostataka**. U principu, on predstavlja skup svih mogućih ostataka pri deljenju sa brojem m. Moguće je odabrati potpun sistem ostataka pri deljenju sa m tako što se uzmu svi uzastopni brojevi od 0 do m-1, uključujući i m-1. Ovaj skup se još naziva i *sistem najmanjih nenegativnih ostataka.*

Slično, možemo formirati u skupu $\mathbb{Z}$, i *sistem ostataka najmanjih po modulu* na sledeći način :

$$-\frac{m-1}{2}, ..., -1, 0, 1, ..., -\frac{m-1}{2}, m = 2k+1, k \in \mathbb{N}$$

$$-\frac{m}{2}, ..., -1, 0, 1, ..., -\frac{m}{2} - 1, m = 2k, k \in \mathbb{N}$$

Međutim, za dalje razmatranje, najbitniji od svih sistema jeste **svedeni sistem ostataka** koji se u suštini dobija tako što iz potpunog sistema ostataka eliminišemo sve brojeve koji nisu uzajamno prosti sa m. Npr, za $m = 8$ potpuni sistem ostataka bio bi $\{0, 1, 2, 3, 4, 5, 6, 7\}$, a svedeni sistem ostataka $\{1, 3, 5, 7\}$. Broj elemenata skupa svedenog sistema ostataka definiše se kao posebna funkcija u zavisnosti od m u nastavku rada.

Definicija 2.1.6 *Neka je* $n \in \mathbb{N}, n > 1$. **Ojlerova funkcija** *predstavlja ukupan broj prirodnih brojeva koji nisu veći od* n*, a koji su uzajamno prosti sa* n*, tj. broj elemenata svedenog sistema ostataka po modulu* n *i označava se sa* $\varphi(n)$.

U sledećoj tabeli date su vrednosti Ojlerove funkcije za prvih nekoliko prirodnih brojeva:

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Tabela 2.1: Tabela sa vrednostima Ojlerove funkcije za prvih 10 prirodnih brojeva

Navešćemo sada dve bitne osobine Ojlerove funkcije:

- Ukoliko je n prost broj, onda je

$$\varphi(n) = n - 1 \tag{2.1}$$

  jer ukoliko je n prost broj, ne deli ga ni jedan broj iz skupa $\{1, 2, ..., n-1\}$, a ni njihovi faktori. Stoga su sa brojem n svi elementi skupa $\{1, 2, ..., n-1\}$ uzajamno prosti, a kako je kardinalnost tog skupa n-1, lako je zaključiti da je ovaj identitet tačan.

- Neka su $n, m \in \mathbb{Z}$ uzajamno prosti. Tada je

$$\varphi(n * m) = (n-1) * (m-1) \tag{2.2}$$

  u suštini ova formula predstavlja specijalan slučaj teoreme koja govori o ojlerovoj funkciji broja koji se može predstaviti u kanonsko faktorisanom obliku, a više o tome može se naći u literaturi [6].

Lema 2.1.5 *Osobine relacije kongruencije :*

1. $a \equiv b \pmod{m}$ *ako i samo ako je* $a = b + mt$ *za neki* $t \in \mathbb{Z}$*, tj.* $m|(a-b)$.
2. *Ako je* $NZD(a, m) = 1$ *i* $ax \equiv ay \pmod{m}$*, onda je* $x \equiv y \pmod{m}$.
3. *Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$ *onda je i* $a \cdot c \equiv b \cdot d \pmod{m}$

Dokaz. Dokazujemo redom navedene osobine relacije kongruencije:

1. Ova osobina je ustvari direktna posledica definicije kongruencije jer ako $a \equiv b \pmod{m}$ tj. daju iste ostatke pri deljenju sa m onda a i b možemo zapisati kao $a = pm + n$, a $b = qm + n$, gde su $p, q \in \mathbb{Z}$. Raspišimo njihovu razlliku

$$a - b = pm + n - (qm + n) = pm + n - qm - n = m(p - q)$$

   Dakle, razliku a-b deli m, tj. $a = b + mt$.

S druge strane, ako a možemo zapisati kao $a = b + mt$ uzmimo da a u najopštijem slučaju a pri deljenju sa m daje neki ostatak $n, 0 \leq n < m$, tj. $a = pm + n$, pri čemu $p, n \in \mathbb{Z}$. Sada, da bi pokazali da $a \equiv b \pmod{m}$ treba pokazati da i b pri deljenju sa m takođe daje ostatak $n, 0 \leq n < m$, tj. $b = pm + n$, pri čemu $q, n \in \mathbb{Z}$. Izrazimo onda traženo b iz jednakosti za koju imamo da važi, tj. :

$$b = a - mt = pm + n - mt = m(p - m) + n, \quad (p - m) \in \mathbb{Z}$$

tako da i smo time pokazali da važi i $a \equiv b \pmod{m}$.

2. Ako je $ax \equiv ay \pmod{m}$, sledi da je $a(x - y) = km, k \in \mathbb{Z}$. Kako je $NZD(a, m) = 1$, sledi da onda mora $m|x - y$ tj. $x - y = km$ a po prethodnoj osobini znači da $x \equiv y \pmod{m}$.

3. Koristeći osobinu 1. iz ove leme možemo ovo zapisati i kao $a = b + mt_1$ i $c = d + mt_2$, za neke $t_1, t_2 \in \mathbb{Z}$. Množenjem ove dve jednakosti dobijamo da je $ac = bd + mt_3$, gde je $t_3 = t_1 d + t_2 b + mt_1 t_2$ i svakako je $t_3 \in \mathbb{Z}$ pa onda važi i $a \cdot c \equiv b \cdot d \pmod{m}$.

Lema 2.1.6 *Neka je $NZD(a, m) = 1$ i neka je $\{\alpha_1, \alpha_2, ..., \alpha_k\}$ proizvoljan potpun (sveden) sistem ostataka po modulu m. Tada je $\{a\alpha_1, a\alpha_2, ..., a\alpha_k\}$ isto tako potpun (sveden) sistem ostataka po modulu m.*

Dokaz. Brojeva $a\alpha_i$ ima isto koliko i brojeva α_i, $i \in \{1, ..., k\}$, pa treba pokazati da za $i \neq j$ brojevi $a\alpha_i$ i $a\alpha_j$ pripadaju različitim klasama. Koristićemo metodu kontradikcije, tj. pretpostavićemo da pripadaju istoj klasi, tj. da $a\alpha_i \equiv a\alpha_j \pmod{m}$. Kako je $NZD(a, m) = 1$, a ispunjeni su nam uslovi iz osobine 2 iz Leme 2.1.5 iz nje bismo onda imali da je $\alpha_i \equiv \alpha_j \pmod{m}$, što je nemoguće, zbog pretpostavke u ovoj teoremi. Dakle, $a\alpha_i$ i $a\alpha_j$ zaista pripadaju različitim klasama. Ako je reč o svedenom sistemu ostataka tj. ako je $NZD(\alpha_i, m) = 1, i = 1, 2, ..., k$ odatle sledi direktno da je i $(a\alpha_i, m) = 1, i = 1, 2, ..., k$, tako da i $\{a\alpha_1, a\alpha_2, ..., a\alpha_k\}$ onda predstavlja svedeni sistem ostataka po modulu m. ∎

Teorema 2.1.7 *(**Ojlerova teorema**) Ako je $NZD(a, m) = 1$ onda je*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Dokaz. Neka je $\{\alpha_1, \alpha_2, ..., \alpha_{\varphi(m)}\}$ svedeni sistem ostataka po modulu m. Onda je prema Lemi 2.1.6 i $\{a\alpha_1, a\alpha_2, ..., a\alpha_{\varphi(m)}\}$ svedeni sistem ostataka po modulu m. Zato, za svaki broj α_i postoji samo jedan broj α_j takav da važi :

$$a\alpha_j \equiv \alpha_i \pmod{m}.$$

Kako ima $\varphi(m)$ takvih brojeva ima toliko i kongruencija :

$$\alpha_1 \equiv a\alpha_1 \pmod{m}$$

$$\alpha_2 \equiv a\alpha_2 \pmod{m}$$

...

$$\alpha_{\varphi(m)} \equiv a\alpha_{\varphi(m)} \pmod{m}$$

Pomnoživši sve ove kongruencije i dobijamo sledeću kongruenciju :

$$a^{\varphi(m)}\alpha_1\alpha_2 \cdots \alpha_{\varphi m} \equiv \alpha_1\alpha_2 \cdots \alpha_{\varphi(m)} \pmod{m}$$

a kako je ispunjen uslov leme 2.1.6 da je $(\alpha_i, m) = 1, i = 1, 2, ..., \varphi(m)$ možemo izvršiti skraćivanje, pa konačno dobijamo :

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

∎

Ojlerova teorema biće jedna od ključnih stvari za pokazivanje u daljem delu rada da RSA algoritam zadovoljava definiciju šifre.

U nastavku sledi specijalan slučaj Ojlerove teoreme, kada je broj m iz Ojerove teoreme baš prost broj.

Teorema 2.1.8 ("Mala Fermaova teorema") *Ako je* $NZD(a, m) \equiv 1 \pmod{m}$ *i pri tome je m prost broj onda je*

$$a^{m-1} \equiv 1 \pmod{m}$$

Dokaz. Iz Ojlerove teoreme i ranije pokazane činjenice u jednačini 2.1 sledi ova teorema. ∎

Kao što smo već videli, Euklidovim algoritmom dolazimo do NZD od dva broja. Međutim, uz pomoć proširenog Euklidovog algoritma možemo i više od toga, predstaviti taj NZD kao linearnu kombinaciju brojeva čiji je on NZD.

Teorema 2.1.9 *(***Prošireni Euklidov algoritam***) Neka su* $a, b > 0$ *celi brojevi, a Euklidovim algoritmom dobijen je NZD(a,b)=r. Tada postoje brojevi* $x, y \in \mathbb{Z}$ *koji zadovoljavaju jednačinu:*

$$r = x \cdot a + y \cdot b$$

Dokaz. Posmatrajmo skup celih brojeva koji su oblika $xa + yb, x, y \in \mathbb{Z}$. Primetimo da u tom skupu imamo i pozitivne i negativne cele brojeve, a i nulu (možemo izabrati takvo $x, y \in \mathbb{Z}$ da je $xa + yb = 0$). Izaberimo najmanji pozitivan element iz takvog skupa (mora da postoji jer skup sadrži nulu pa i negativne brojeve). Neka je to broj $c = x'a + y'b$, za neke konkretne cele brojeve x', y'. Dokažimo sada da $c|a$. Pretpostavimo suprotno, da c ne deli a, a onda postoje celi brojevi q i r, $0 < r < c$ takvi da važi $a = cq + r$. Onda je

$$r = a - cq = a - q(x'a + y'b) = (1 - x'q)a - y'qb$$

a broj r je po definiciji pozitivan i manji od c, a i oblika xa+yb(za konkretne $x = 1 - x'q$ i $y = y'q$), što je u suprotnosti sa pretpostavkom da je c najmanji takav pozitivan broj. Iz toga sledi da ipak $c|a$. Analogno se pokazuje da i $c|b$, tj. da je c zajednički delilac brojeva a i b, a onda i $c|d$. Iz činjenica da $d|a$,$d|b$ i da je $c = x'a + y'b$ sledi da $d|c$. Time je pokazano da je zapravo $d = c$.

Napomena 2.1.1 *Kako je NZD(a,b) uglavnom manji i od a i od b, barem jedan od x ili y će najčešće biti negativan.*

Napomena 2.1.2 *Jedna od najvećih primena ovog algoritma jeste pri izračunavanju eksponenta dekripcije d kod RSA algoritma (biće detaljno obrađeno u trećem delu rada, prim. aut.). Naime, eksponent dekripcije d predstavlja modularni multiplikativni inverz eksponenta enkripcije e po određenom modulu $\varphi(n)$. Konkretno, potrebno nam je dobiti d iz sledeće kongruencije :*

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

koje dobijamo kao rešenje sledeće jednačine rešavajući je uz pomoć proširenog euklidovog algoritma:

$$e \cdot d = k \cdot \varphi(n) + 1, k \in \mathbb{Z}$$

2.2 Pojmovi, definicije i teoreme

Definicija 2.2.1 *Neka je X,p(x) sistem gde je* $X = (x_1, ..., x_n)$ *skup svih mogućih događaja sistema, a* $(p_1, ..., p_n)$ *respektivno verovatnoće da se ti događaji dogode.* **Količina sopstvene informacije** *za* $x_i \in X, i = 1, ...n, p(x) > 0$, *definiše se sa*

$$I(x_i) := -\log_2 p(x_i)$$

(kaže se i samo : **sopstvena informacija***).*

Definicija 2.2.2 Kriptosistem *(cryptosystem) je uređena trojka* $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ *gde* $\mathcal{M}, \mathcal{C}, \mathcal{K}$ *predstavljaju respektivno :*

- *skup* $\mathcal{M}$*, koji predstavlja skup svih mogućih otvorenih tekstova (plaintexts), tj. tekstova koji nose informacije koje pošaljilac zeli da dostavi primaocu. Jedan konkretan otvoreni tekst dalje u tekstu označavaćemo sa m;*
- *skup* $\mathcal{C}$*, koji predstavlja skup svih mogućih šifrata (cyphertexts), tj. otvorenih tekstova koji su šifrovani kako bi informacije bile zaštićene od napadača - jedan konkretan šifrat dalje u tekstu označavaćemo sa c;*
- *skup* $\mathcal{K}$*, koji se naziva prostor svih ključeva (key set ili key space). Jedan konkretan ključ dalje u tekstu označavaćemo sa k.*

Definicija 2.2.3 Šifra *(cipher), definisana na kriptosistemu* $(\mathcal{M}, \mathcal{C}, \mathcal{K})$*, je par algoritama* $(\mathcal{E}, \mathcal{D})$ *gde je*

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$

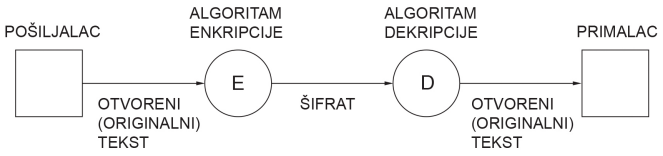
funkcija šifrovanja (kriptovanja) tj. prevođenja otvorenog teksta u šifrat, a

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

funkcija dešifrovanja (dekriptovanja) tj. prevođenja šifrata u otvoreni tekst. Za svaki par $(\mathcal{E}, \mathcal{D})$ *koji čini šifru mora da važi :*

$$\mathcal{D}\ (k, \mathcal{E}\ (k, m)) = m$$

Napomena :
$\mathcal{E}$ *je često slučajna ("randomly crypting")*
$\mathcal{D}$ *je uvek deterministički određena. (ključ i šifrat uvek u kombinaciji daju isti otvoreni tekst).*



Slika 2.1: Dijagram ilustruje šifrovanu razmenu podataka između dva entiteta.

Američki matematičar i kriptograf, koga su smatrali "ocem teorije informacija", *Klod Šenon*, 1949. godine dao je osnovnu ideju savršene sigurnosti koja je, u suštini, govorila o tome da se iz samog šifrata ne može saznati apsolutno ništa o otvorenom tekstu. Jednostavnije rečeno, kada napadač vidi šifrat, nema nikakvih informacija o otvorenom tekstu. U sledećoj formulaciji to je precizno definisano.

Definicija 2.2.4 *Šifra* $(\mathcal{E}, \mathcal{D})$ *definisana na kriptosistemu* $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ *ima* **savršenu sigurnost** *ako* $\forall m_0, m_1 \in \mathcal{M}$ *,* $\forall c \in \mathcal{C}$ *važi da*

$$P[\mathcal{E}\ (k, m_0) = c] = P[\mathcal{E}\ (k, m_1) = c]$$

gde je k *slučajna uniformna promenljiva iz* $\mathcal{K}$*.*

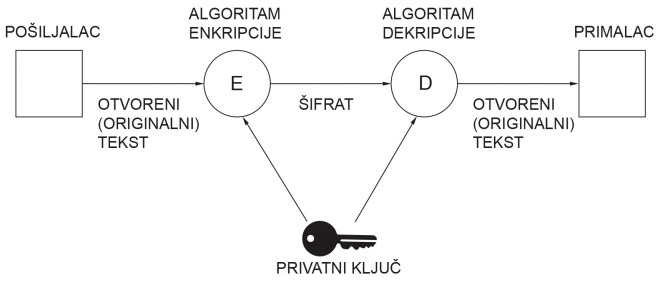
Drugim rečima rečeno, kada napadač presretne šifrat c, ne može znati koji otvoren tekst odgovara tom šifratu, jer su verovatnoće da svaki otvoreni tekstovi odgovara tom šifratu iste.

Glava 3

Treći deo

3.1 Kriptografija sa privatnim ključem

Kao što je već ranijen napomenuto kriptografija sa privatnim ključem koristi baš samo taj jedan ključ koji daje oba algoritma - i enkripcije i dekripcije. Takav simetričan proces ilustrovan je na sledećem dijagramu.



Slika 3.1: Ilustracija kriptografskog procesa sa privatnim ključem (simetričnog procesa).

U nastavku detaljnije razmatramo jedan od poznatih simteričnih kriptoloških metoda.

3.1.1 One Time Pad - OTP

One Time Pad (OTP) ili *jednokratna beležnica* predstavlja poznatu kriptografsku tehniku patentiranu od strane američkog inženjera *Žilberta Vernama* 1917. godine. Smatra se da je začetnik same ideje američki kriptolog *Frenk Miler* još 1887. godine, a priču o OTP-u je upotpunio *Joseph Mauborgne* zaključivši da,

ukoliko je ključ potpuno slučajan, kriptoanalitički napadi na ovu metodu bi bili potpuno neefikasni.

Definišimo sada jednu binarnu relaciju koja će nam biti potrebna za dalji rad i opisivanje OTP-a.

Definicija 3.1.1 *Posmatrajmo skup {0,1}. Na njemu definišemo binarnu operaciju $\oplus$ na sledeći način:*

$\oplus$	*0*	*1*
0	*0*	*1*
1	*1*	*0*

operaciju $\oplus$ nazivamo XOR (skraćeno od exclusive or), ili isključiva disjunkcija.

Značajno je zaključiti da na skupu na kom je definisana operacija $\oplus$, tj. na binarnom skupu, ona predstavlja sama sebi inverznu operaciju, tj. $\forall x \in \{0,1\}^n$ važi $x \oplus x = 0$.

U nastavku možemo i definisati sam OTP algoritam.

Definicija 3.1.2 *Neka su $M = C = K = \{0,1\}^n$, pri čemu je ključ proizvoljan niz 0. i 1. dužine n. Algoritme kriptovanja i dekriptovanja definišemo na sledeći način :*

$$\mathcal{E}\ (k,m) := k \oplus m = c$$
$$\mathcal{D}\ (k,c) := k \oplus c = m$$

Pokažimo sada da je definicija dobra, odnosno da je OTP šifra, tj. da dva gore definisana algritma daju šifrat (alogitam $\mathcal{E}$) i otvoreni tekst (alogitam $\mathcal{D}$):

$\mathcal{E}\ (k,m) = \mathcal{E}\ (k, \mathcal{D}\ (k,c)) = \mathcal{E}\ (k, k \oplus c) = k \oplus (k \oplus c) = (k \oplus k) \oplus c = 0 \oplus c = c$
$\mathcal{D}\ (k,c) = \mathcal{D}\ (k, \mathcal{E}\ (k,m)) = \mathcal{D}\ (k, k \oplus m) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$

Prednost OTP algoritma je ta što je on brz, odnosno od otvorenog teksta pomoću ključa vrlo brzo i jednostavno dobijamo šifrat, te obratno, otvoreni tekst od šifrata. Za razliku od složenijih algoritama za čiju implementaciju je uglavnom potrebna pomoć računara, OTP algoritam je moguće izvršiti samo uz pomoć papira i olovke zbog jednostavnosti operacije XOR. Iz tog razloga ovaj metod i nazivamo *jednokratnom beležnicom.* Međutim, mana mu je to što duzina ključa mora biti jednaka dužini teksta koji se šifruje pa se postavlja pitanje - kako možemo drugoj strani dostaviti ključ dužine otvorenog teksta, čak i istog alfabeta(binarnog), ukoliko nismo mogli na bezbedan način da mu pošaljemo i sam otvoreni tekst već smo ga morali kriptovati? I ukoliko taj način postoji, zašto uz pomoć njega ne bismo poslali i sam otvoreni tekst? Iz tog razloga, ovaj metod je teško upotrebljiv u praksi.

Ipak, Klod Šenon je formulisao teoremu koja se ispostavila veoma bitnom u oblasti sigurnosti kriptovanja. Ona je dobila naziv *"Bad News Lemma" ("Lema*

loših vesti"), a govorila je o tome da bi šifra imala savršenu sigurnost, dužina ključa ne sme biti imanja od dužine originalne poruke, tj. savršena sigurnost $\Longrightarrow |\mathcal{K}| \geq |\mathcal{P}|$,a ukoliko je baš $|\mathcal{K}| = |\mathcal{P}|$ tada se radi o optimalnoj savršenoj sigurnosti. Nakon takve formulacije Šenona, kako kod OTP vazi da je dužina ključa baš jednaka dužini otvorenog teksta, zaključuejmo da OTP ima (optimalnu) savršenu sigurnost. Formulišimo to kao teoremu i dokažimo je.

Teorema 3.1.1 *OTP ima savršenu sigurnost.*

Dokaz. Dakle, po definiciji savršene sigurnosti dovoljno je pokazati da $\forall m, c$ važi :

$$P[\mathcal{E}\ (k, m) = c] = const$$

Po definiciji Laplasove verovatnoće važi $\forall m, c$

$$P[\mathcal{E}\ (k, m) = c] = \frac{k_1}{k_2}$$

gde k_1 predstavlja ukupan broj svih ključeva takvih da važi $\{\ \mathrm{k} \in \mathcal{K} : \mathcal{E}\ (k, m) = c\ \}$, a $k_2 = |\mathcal{K}|$ je ukupan broj svih ključeva iz prostora ključa. Kako je $k_2 = const$, da bismo dovršili dokaz, tj. pokazali da OTP ima savršenu sigurnost, potrebno je još pokazati da je $k_1 = const$. Kod OTP-a važi da

$$\mathcal{E}\ (m, k) = c \Rightarrow k \oplus m = c/ \oplus m \Rightarrow k \oplus m \oplus m = c \oplus m \Rightarrow k = c \oplus m$$

Što znači da je ključ kod OTP-a jedinstveno određen i dobija se primenljivanjem operacije XOR na otvoreni tekst i šifrat.

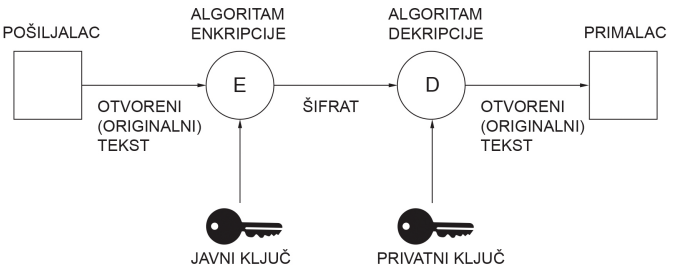
Dakle, broj ključeva za koje važi $\{\ \mathrm{k} \in \mathcal{K} : \mathcal{E}\ (k, m) = c\ \}$=1 što je svakako konstanta, a to smo i trebali pokazati. ∎ Upravo zbog ove teoreme, kao glavna prednost OTP-a, pre velike brzine kriptovanja, uzima se savršena sigurnost. Međutim, problemi koji se javljaju kod upotrebe OTP-a proističu iz fundamenta mehanizma kriptovanja koji je XOR operacija. Naime, ova tehnika kripotvanja primenljiva je samo na otvorene tekstove koji su nizovi nula i jedinica (binarni nizovi). Takođe, priroda šifrata je takva da, ukoliko bi napadač presreo dva šifrata kriptovanim istim ključem kriptografskim metodama mogao bi doći do otvorenih tekstova. Zbog toga se ovaj metod i zove jednokratna beležnica, upravo jer se ključ mora menjati pri svakom procesu kriptovanja. To zvuči prilično izvodivo, pogotovo ukoliko ovladamo algoritmom biranja slučajnog (engl. random) ključa iz prostora ključa. Ali šta sa problemom pre, tj. da li je ovaj mehanizam kriptovanja uopšte moguće primeniti na originalne tekstove koji nisu prosti nizovi nula i jedinica?

Moguće je, na taj način što ćemo te nizove koji nisu binarni pretvoriti u binarne. Naime, svako slovo alfabeta ćemo zameniti sa nizom *bitova* (bit predstavlja osnovnu jedinicu informacije u računarstvu koja predstavlja neki vid *bool* promenljive tj. promenljive koja može primati samo vrednosti 0 i 1 tj. netačno ili tačno) fiksne dužine, a često upravo sa *bajtom* (bajt predstavlja niz bitova dužine 8 - "oktet"). Bajt se standarno upotrbljava kao osnovna mera za memoriju današnjih računara i računarskih sistema, a u kriptografiji se u okviru *ASCII* (American Standard Code for Information Interchange) 8-bitne šeme standarno upotrebljava za supstituciju alfabeta pre svega američke abecede koja broji 26. slova, ali jedan bajt ima dovoljno kombinacija bitova (2^8) ne samo za tih 26 slova, već da razlikuje i mala i velika

slova, sve matematičke simbole, znake interpunkcije, čak i neke specijalne naredbe. Dakle, onda sa tako dobijenim binarnim nizom, uz odgovarajući slučajno generisan ključ izvršava se XOR operacija i tako dobija šifrat.

3.2 Kriptografija sa javnim ključem

U prethodno analiziranom OTP algortimu problematika dobijanja funkcije dekripcije kada je poznata funkcija enkripcije praktično nije niti postojala, iz razloga što je glavni binarni operator mehanizma - XOR operator $\oplus$ sam sebi i inverzni. Tako da je šifratu (koji je dobijen iz otvorenog teksta i ključa primenom operacije $\oplus$) potrebno samo operacijom $\oplus$ "dodati" ključ da bismo došli do otvorenog teksta. Iz tog razloga, OTP algoritam i ostale mehanizme kod kojih se funkcija dekripcije jednostavno dobija iz funkcije enkripcije nazivaju se simetrične metode ili metode sa privatnim ključem. Međutim, pri svakoj razmeni podataka potrebno je tajno razmeniti i ključ (najčešće jedini mogući način da se to potpuno sigurno uradi jeste lična razmena), pošto korišćenje istog više puta takođe dovodi do znatno povećane verovatnoće uspešnosti kriptoanalitičkog napada. Zbog toga danas, kada se veliki deo komunikacije obavlja preko telefona, e-maila ili interneta lako je prestresti i makar pasivno napasti ovakve poruke, ovakav način implementacije kriptografije postaje neizvodiv, te sve više dolazi do upotebe *kriptografije sa javnim ključem*, tj. **asimetrične kriptografije**. Tu je potrebno samo prvi put na siguran način razmeniti privatni ključ koji će onda imati samo lica koja primaju poruke, a javni ključ je praktično poznat i dostupan svima, pa čak i napadačima. Baš iz tog razloga u ovim situacijama nije moguće do ključa dekripcije doći samo sa znanjem i informacijama o ključu enkripcije, makar ne u praksi, tj. u razumnom (polinomnom) vremenu.



Slika 3.2: Ilustracija kriptografskog procesa sa jvanim ključem (asimetričnog procesa).

Kao interesantana simulacija takvog događaja može se razmotriti sledeća situacija: zamislite da imate standardan telefonski imenik (klasifikovan abecedno po imenima stanovnika) višemilionskog grada, te imate prvi zadatak : naći broj telefona po imenu i prezimenu čoveka. Vrlo lako za uraditi, čak i ukoliko ima više od jednog čoveka pod istim imenom, za nekoliko trenutaka izbor se svodi na nekoliko ljudi. Međutim, drugi zadatak se sastoji u tome da za dati telefonski broj trebate identifikovati kome zapravo pripada. Taj zadatak, ukoliko je u pitanju višemilionski grad, gde trebate "ručno" pretražiti milione ljudi da biste došli do vlasnika broja čini se neizvodiv, ili makar neizvodiv u razumnom vremenu.

Ovakav mehanizam asimetričnih metoda se matematički može opisati jednosmernim *one-way* funkcijama.

Definicija 3.2.1 *Funkciju $f : X \longrightarrow Y$ nazivamo* **jednosmernom funkcijom** *ako ona može biti, za proizvoljan elemenat x iz domena X, lako izračunata (u polinomnom vremenu), ali za proizvoljan elemenat $y \in f(X)$ je mnogo teže, praktično nemoguće u polinomnom vremenu, pronaći $x \in X$, takvo da važi $y = f(x)$.*

Definicija 3.2.2 *Jednosmernu funkciju $f : X \longrightarrow Y$ nazivamo* **trapdoor funkcijom** *ako, uz neku dodatnu informaciju, postaje računski izvodivo $\forall y \in f(X)$ naći elemenat iz domena $x \in X$ takav da je $f(x) = y$.*

Uz pomoć ove matematičke terminologije kratak opis mehanizma metoda sa javnim ključem bio bi sledeći : svaki korisnik javno podeli svoj ključ za kriptovanje kako bi svako ko želi mogao bezbedno komunicirati sa njim. Ključ za kriptovanje predstavlja jednu trap door funkciju, a upravo samo on poseduje dodatne informacije, pomoću kojih će samo on moći naći inverz trapdoor funkciji, tj. funkciju dekripcije, da bi dekriptovao poruke koje dobija.

U nastavku sledi analiziranje RSA algoritma, kao široko upotrebljivanog algoritma asimetrične kriptografije.

3.2.1 RSA algoritam

RSA algoritam predstavlja danas jedan od najrasprostranjenijih, a samim time i najpoznatijih metoda kriptografije sa javnim ključem. Upotrebljava se veoma široko, a samo neki od primera su : slanje šifrovanih poruka između korisnika, autentifikacija digitalnih potpisa, pristup obezbeđenim arhivama ili bazama podataka kao u sistemu sa platnim ili kreditnim karticama itd.

Kreiran je od strane 3 kriptografa 1977. godine na američkom MIT institutu (engl. *Massachusetts Institute of Technology*) : 2 amerikanca Ronalda Rivesta i Leonarda Ejdlmana i izraelca Adija Šamira, a patentiran je i zvanično zaštićen 6 godina kasnije.

Mehanizam kriptovanja RSA algoritmom. Mehanizam enkripcije i dekripcije kod RSA algortima zasniva se na modularnoj aritmetici. U nastavku je opisan taj mehanizam po koracima.

1. Prvo što nam je potrebno jesu dva velika prosta broja (svaki veličine makar 150 decimalnih cifara). Da bismo njih generisali potreban nam je *pseudo random generator* (algoritam koji nam na neki, ne potpuno proizvoljan način bira brojeve iz nekog skupa, ali na dovoljno dobar način da običan statistički test ne razlikuje taj broj odabran pseudo random generatorom od potpuno proizvoljno odabranog broja iz skupa - pseudo random generatori upotrebljavaju se zato što je u teoriji kompjuterskih nauka praktično nemoguće na potpuno proizvoljan način odabrati element iz skupa pa se zbog toga implementiraju pseudo radnom algoritmi koji su "dovoljno dobri" da zamene potpuno proizvoljno biranje-prim.aut.). Uz pomoć pseudo random generatora

odabira se proizvoljan broj n, a potom se uz pomoć kompjuterskog programa proverava da li je broj n prost. Ukoliko nije, proveravamo da li je $n+1$ prost. Ukoliko nije proveravamo da li je $n+3$ prost itd. Teorema o prostim brojevima tvrdi da je, za dovoljno veliko $n \in \mathbb{N}$, verovatnoća da je sučajno odabran broj n baš prost broj jednaka $\frac{1}{\log n}$, tako da ne bi trebalo biti previše problema oko odabira velikog prostog broja p. Na analogan način odaberimo i drugi veliki prost broj q, takav da važi $q \neq p$.

2. Pomnožimo te brojeve i dobijemo njihov proizvod $n = p \cdot q$.

3. Izračunajmo prvo *Ojlerovu funkciju* broja $n, \varphi(n)$. Odabrani p i q su prosti brojevi sami za sebe, samim time, oni su i uzajamno prosti, tj. $NZD(p,q) = 1$. Taj uslov olakšava nam izračnavanje Ojlerove funkcije n zbog osobine (2.2), te kako je $n = p * q$ onda je

$$\varphi(n) = (p-1) * (q-1)$$

4. Sada je potrebno odabrati *eksponent enkripcije e*. Broj e biramo proizvoljno iz skupa $\{1, ..., \varphi(n)-1\}$, takav da je uzajamno prost sa brojem $\varphi(n)$.

5. Zatim sledi izračunavanje *eksponenta dekripcije d*. Uz pomoć *proširenog euklidovog algoritma*, odredimo jedinstven ceo broj d iz skupa $\{1, ..., \varphi(n)\}$, takav da važi:
$$e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow e \cdot d = k \cdot \varphi(n) + 1, k \in \mathbb{Z} \tag{3.1}$$

6. Izgenerisani su svi potrebni parametri za kriptovanje RSA metodom, stoga treba slučajno generisane brojeve p i q obrisati kako kriptoanalitičari ne bi došli do informacija koje bi im u znatnoj meri povećale verovatnoću uspešnosti napada na ovaj algoritam.

Kako smo izgenerisali sve parametre iz prethodnih koraka, možemo konačno definisati i javni i privatni ključ za RSA algoritam. Uređeni par **(n,e)** parametara definisanih u koracima 2. i 4. predstavljaće **javni ključ** za našu RSA metodu i svako će moći na taj način da šifruje podatke. S druge strane, uređeni par **(n,d)** definisan u koracima 4. i 5. predstavljaće **privatni ključ** dostupan samo kreatoru brojeva sa kojima je čitav algoritam i počeo, p i q.

RSA algoritam pripada blokovnim šiframa, stoga pre postupka enkripcije uz pomoć ranije definisanog ključa, potrebno je još otvorenu poruku m podeliti na blokove m_i dužine ne veće od n. S obzirom da se otvoreni tekst, da bi se mogao kriptovati uvek prvo prevede u numerički ekvivalent (ASCII ili nekim drugim kodom), taj niz se deli na blokove tako što se nađe najveći stepen j broja 2 koji zadovoljava uslov $2^j < n$ te se potom otvoreni tekst deli u blokove dužine j. Ukoliko ukupna dužina niza (otvorenog teksta) nije deljiva sa brojem j, dopunjujemo otvoreni tekst do prvog broja $h > n$ takvog da $j \mid h$.

Nakon deljenja na blokove označimo sa m_i proizvoljan blok dužine j otvorenog teksta, i sa c_i njemu odgovarajući blok šifrata, pri čemu $i \in \{1, 2, ..., t\}$, gde t predstavlja ukupan broj blokova dužine j otvorenog teksta odnosno šifrata.

Algoritam enkripcije blokova otvorenog teksta m_i u blokove šifrata c_i je sledeći:

$$f(m_i) = c_i = m_i^e \pmod{n} \tag{3.2}$$

dok je algoritam dekripcije :

$$f^{-1}(c_i) = m_i = c_i^d \pmod{n} \tag{3.3}$$

Pokažimo sada da je, na ovaj način algoritam za šifrovanje dobro definisan, odnosno pokažimo uslov koji mora da važi po definiciji šifre $D(E(m)) = m$. Pre nego što započnemo dokaz moramo imati u vidu identitet 3.1 , te Ojlerovu teoremu, kao dve osnovne stvari koje koristimo u nizu sledećih jednakosti:

$$c^d = (m^e)^d = m^{ed} \overset{3.1}{=} m^{k\cdot\varphi(n)+1} = (m^{\varphi(n)})^k \cdot m \overset{2.1.7}{=} 1^k \cdot m = m$$

čime je pokazano da je RSA zapravo šifra.

Napomena 3.2.1 *Treba napomenuti posledicu do koje se dolazi tokom pokazivanja da je RSA šifra. Tokom niza jednakosti u jednom momentu iskorišćena je Ojlerova teorema, međutim, s obzirom da smo nju iskoristili mora biti ispoštovan uslov naveden u Ojlerovoj teoremi, koji zahteva da m (numerički ekvivalent slova kog šifrujemo) bude uzajamno prost sa brojem n (iz javnog ključa RSA algoritma), da bi dekriptovanje bilo jednoznačno i uopšte moguće. Dakle, treba izuzetno obratiti pažnju da pri deljenju poruke na blokove ne bude bloka čiji numerički ekvivalent nije uzajamno prost sa n, što, iako zvuči kao prilično neprijatno ograničenje koje bi moglo u znatnoj meri da otežа postupak enkripcije, zapravo i neće biti preveliki problem, iz prostog razloga što su jedini faktori broja n (osim 1 i njenga samog, naravno), brojevi p i q. Znači, jednostavno, onaj koji kriptuje treba se pobrinuti da numerički ekvivalenti blokova prosto ne budu jednaki prostim brojevima p i q.*

Sada sledi jedan primer komunikacije tekstom kriptovanim uz pomoć RSA algortima.

Primer 3.2.1 *Petar je preko nesigurnog komunikacijskog kanala Marka upitao koji kurs želi da pohađa. Marko je svestan da je kanal kojim komuniciraju nesiguran, a želi da njegov odgovor ostane poznat samo Petru, te će stoga upotrebiti RSA algoritam kako bi kriptovao svoj odgovor i poslao ga petru. Marko želi da Petru odgovori da će pohadjati kurs pod imenom* **kriptografija**. *Ono što je potrebno da bi Marko Petru poslao kriptovanu poruku (i obratno, ukoliko je potrebno) jesu njihovi javni ključevi, tj. uređeni parovi (n,e). Neka oni budu sledeći:*

Petrov javni ključ : K_1 = (1003,3);
Markov javni ključ : K_2 = (77,13);

Marko će prvo svakom slovu ponaosob iz reči kriptografija dodeliti numerički ekvivalent, na način koji smo definisali u tabeli 1.2 *(uz napomenu da jednocifrenim*

brojevima dodajemo 0 kao prefiks zbog jednoznačnosti dekripcije). Numerički ekvivalent reči kriptografija biće:

14 22 12 21 25 20 10 22 00 09 12 13 00

dakle, ovi blokovi od po dve cifre predstavljaju zapravo otvoreni tekst koji je potrebno kriptovati svaki za sebe. Dakle, imamo:

$$m_1 = 14, m_2 = 22, m_3 = 12, m_4 = 21, m_5 = 25, m_6 = 20, m_7 = 10$$
$$m_8 = 22, m_9 = 00, m_{10} = 09, m_{11} = 12, m_{12} = 13, m_{13} = 00$$

Koristeći algoritam kriptovanja RSA $c_i = m_i^e \pmod n$ *dobijamo sledeće šifrate:*

$$c_1 = m_1^e \pmod n = 14^3 \pmod{1003} = 738$$
$$c_2 = c_8 = m_2^e \pmod n = 22^3 \pmod{1003} = 618$$
$$c_3 = c_{11} = m_3^e \pmod n = 12^3 \pmod{1003} = 725$$
$$c_4 = m_4^e \pmod n = 21^3 \pmod{1003} = 234$$
$$c_5 = m_5^e \pmod n = 25^3 \pmod{1003} = 580$$
$$c_6 = m_6^e \pmod n = 20^3 \pmod{1003} = 979$$
$$c_7 = m_7^e \pmod n = 10^3 \pmod{1003} = 1000$$
$$c_9 = c_{13} = m_9^e \pmod n = 00^3 \pmod{1003} = 0$$
$$c_{10} = m_{10}^e \pmod n = 09^3 \pmod{1003} = 729$$
$$c_{12} = m_{12}^e \pmod n = 13^3 \pmod{1003} = 191$$

(u daljem tekstu izostavljaćemo šifrate c_8, c_{11}, c_{13} *jer su potpuno identični šifratima* c_2, c_3, c_9 *respektivno.)*

Dakle, Marko šalje Petru poruku šifrovanu Petrovim javnim ključem (1003,3) u vidu sledećeg šifrata:

738 618 725 234 580 973 1000 618 0 729 725 191 0

Sada, Petar dobija poruku (niz brojeva podeljenih u blokove) i treba je dekriptuje, tj. taj niz brojeva da prevede u smislena slova. On to može samo uz pomoć svoj privatnog ključa. Naime, samo Petar je znao činioce broja koji čini njegov javni

ključ (1003,3), tj. samo je on znao faktorizaciju broja 1003 koji je dobijen kao proizvod prostih brojeva 17 i 59. Tako je izračunao $\varphi(n) = (p-1) * (q-1)$*, tj.*

$$\varphi(1003) = 16 * 58 = 928$$

Stoga, Petar je dobio svoj privatni ključ rešavajući sledeću kongruenciju: $e \cdot d \equiv 1 \pmod{\varphi(n)}$*, tj.*

$$3 \cdot d \equiv 1 \pmod{928}$$

odnosno sledeću jednačinu uz pomoć proširenog euklidovog algoritma:

$$3 \cdot d = 928 \cdot t + 1, \quad t \in \mathbb{Z}$$

Potom, Petar je dobio eksponent dekripcije d=619, i na taj način formirao privatni ključ (619,3) koji samo on poseduje. Upravo uz pomoć tog privatnog ključa on će dekriptovati tekst koji mu je poslao Marko. Algoritam dekripcije kod RSA je sledeći : $m_i = c_i^d \pmod{n}$*. Odmah se može uočiti da bi na ovaj način proces dekripcije bio složen iz prostog razloga jer postoji potreba za stepenovanje velikog broja velikim brojem, npr.* 738^{619}*, što je poprilično teško izvodiv posao, čak i za računare današnje generacije. Zbog toga ćemo se poslužiti algoritmom koji je opisan u nastavku.*

Eksponent dekripcije, u našem slučaju broj 619 ispišimo u bazi sa osnovom 2:

$$619 = (1001101011)_2 = 512 + 64 + 32 + 8 + 2 + 1$$

iz razloga da bismo lakše razložili (veliki) eksponent šifrata. Dakle:

$$c_i^{619} = c_i^{512} * c_i^{64} * c_i^{32} * c_i^{8} * c_i^{2} * c_i^{1}$$

i te stepene možemo izračunati na sledeći način :

k	$c_1^k \pmod{1003}$	$c_2^k \pmod{1003}$	$c_3^k \pmod{1003}$	$c_4^k \pmod{1003}$
$2^0 = 1$	$\boxed{738}$	$\boxed{618}$	$\boxed{725}$	$\boxed{234}$
$2^1 = 2$	$738^2 \equiv \boxed{15}$	$618^2 \equiv \boxed{784}$	$725^2 \equiv \boxed{53}$	$234^2 \equiv \boxed{594}$
$2^2 = 4$	$15^2 \equiv 225$	$784^2 \equiv 820$	$53^2 \equiv 803$	$594^2 \equiv 783$
$2^3 = 8$	$225^2 \equiv \boxed{475}$	$820^2 \equiv \boxed{390}$	$803^2 \equiv \boxed{883}$	$783^2 \equiv \boxed{256}$
$2^4 = 16$	$475^2 \equiv 953$	$390^2 \equiv 647$	$883^2 \equiv 358$	$256^2 \equiv 341$
$2^5 = 32$	$953^2 \equiv \boxed{494}$	$647^2 \equiv \boxed{358}$	$358^2 \equiv \boxed{783}$	$341^2 \equiv \boxed{936}$
$2^6 = 64$	$494^2 \equiv \boxed{307}$	$358^2 \equiv \boxed{783}$	$783^2 \equiv \boxed{256}$	$936^2 \equiv \boxed{477}$
$2^7 = 128$	$307^2 \equiv 970$	$783^2 \equiv 256$	$256^2 \equiv 341$	$477^2 \equiv 851$
$2^8 = 256$	$970^2 \equiv 86$	$256^2 \equiv 341$	$341^2 \equiv 936$	$851^2 \equiv 35$
$2^9 = 512$	$86^2 \equiv \boxed{375}$	$341^2 \equiv \boxed{936}$	$936^2 \equiv \boxed{477}$	$35^2 \equiv \boxed{222}$

k	$c_5^k \pmod{1003}$	$c_6^k \pmod{1003}$	$c_7^k \pmod{1003}$	$c_9^k \pmod{1003}$
$2^0 = 1$	$\boxed{580}$	$\boxed{979}$	$\boxed{1000}$	$\boxed{0}$
$2^1 = 2$	$580^2 \equiv \boxed{395}$	$979^2 \equiv \boxed{576}$	$1000^2 \equiv \boxed{9}$	$0^2 \equiv \boxed{0}$
$2^2 = 4$	$395^2 \equiv 560$	$576^2 \equiv 786$	$9^2 \equiv 81$	$0^2 \equiv 0$
$2^3 = 8$	$560^2 \equiv \boxed{664}$	$786^2 \equiv \boxed{951}$	$81^2 \equiv \boxed{543}$	$0^2 \equiv \boxed{0}$
$2^4 = 16$	$664^2 \equiv 579$	$951^2 \equiv 698$	$543^2 \equiv 970$	$0^2 \equiv 0$
$2^5 = 32$	$579^2 \equiv \boxed{239}$	$698^2 \equiv \boxed{749}$	$970^2 \equiv \boxed{86}$	$0^2 \equiv \boxed{0}$
$2^6 = 64$	$239^2 \equiv \boxed{953}$	$749^2 \equiv \boxed{324}$	$86^2 \equiv \boxed{375}$	$0^2 \equiv \boxed{0}$
$2^7 = 128$	$953^2 \equiv 494$	$324^2 \equiv 664$	$375^2 \equiv 205$	$0^2 \equiv 0$
$2^8 = 256$	$494^2 \equiv 307$	$664^2 \equiv 579$	$205^2 \equiv 902$	$0^2 \equiv 0$
$2^9 = 512$	$307^2 \equiv \boxed{970}$	$579^2 \equiv \boxed{239}$	$902^2 \equiv \boxed{171}$	$0^2 \equiv \boxed{0}$

k	$c_{10}^k \pmod{1003}$	$c_{12}^k \pmod{1003}$
$2^0 = 1$	$\boxed{729}$	$\boxed{191}$
$2^1 = 2$	$729^2 \equiv \boxed{854}$	$191^2 \equiv \boxed{373}$
$2^2 = 4$	$854^2 \equiv 135$	$373^2 \equiv 715$
$2^3 = 8$	$135^2 \equiv \boxed{171}$	$715^2 \equiv \boxed{698}$
$2^4 = 16$	$171^2 \equiv 154$	$698^2 \equiv 749$
$2^5 = 32$	$154^2 \equiv \boxed{647}$	$749^2 \equiv \boxed{324}$
$2^6 = 64$	$647^2 \equiv \boxed{358}$	$324^2 \equiv \boxed{664}$
$2^7 = 128$	$358^2 \equiv 783$	$664^2 \equiv 579$
$2^8 = 256$	$783^2 \equiv 256$	$579^2 \equiv 239$
$2^9 = 512$	$256^2 \equiv \boxed{341}$	$239^2 \equiv \boxed{953}$

Izdvojićemo šifrat c_{10} iz poslednje tabele, odnosno izračunaćemo ostatak pri deljenju 738^{619} sa 1003:

$$738^{619} = 738^{512} \cdot 738^{64} \cdot 738^{32} \cdot 738^{8} \cdot 738^{2} \cdot 738^{1} \equiv$$

$$375 \cdot 307 \cdot 494 \cdot 475 \cdot 15 \cdot 738 \equiv 14 \pmod{1003} = m_1$$

na analogan način dobićemo i ostale blokove otvorenog teksta :

$$618^{619} = 936 \cdot 783 \cdot 358 \cdot 390 \cdot 784 \cdot 618 \equiv 22 \pmod{1003} = m_2 = m_8$$

$$725^{619} = 477 \cdot 256 \cdot 783 \cdot 883 \cdot 53 \cdot 725 \equiv 12 \pmod{1003} = m_3 = m_{11}$$

$$234^{619} = 222 \cdot 477 \cdot 936 \cdot 256 \cdot 594 \cdot 234 \equiv 21 \pmod{1003} = m_4$$

$$580^{619} = 970 \cdot 953 \cdot 239 \cdot 664 \cdot 395 \cdot 580 \equiv 25 \pmod{1003} = m_5$$

$$979^{619} = 239 \cdot 324 \cdot 749 \cdot 951 \cdot 576 \cdot 979 \equiv 20 \pmod{1003} = m_6$$

$$1000^{619} = 171 \cdot 375 \cdot 86 \cdot 543 \cdot 9 \cdot 1000 \equiv 10 \pmod{1003} = m_7$$

$$0^{619} \equiv 0 \pmod{1003} = m_9 = m_{13}$$

$$729^{619} = 341 \cdot 358 \cdot 647 \cdot 171 \cdot 854 \cdot 729 \equiv 9 \pmod{1003} = m_{10}$$

$$191^{619} = 953 \cdot 664 \cdot 324 \cdot 698 \cdot 373 \cdot 191 \equiv 13 \pmod{1003} = m_{12}$$

Petar je na taj način, iz Markovog šifrata, dobio sledeći niz dvocifrenih brojeva :

14 22 12 21 25 20 10 22 00 09 12 13 00

Petru ostaje još samo da, uz pomoć tabele 1.2 dvocifrenim brojevima dodeli odgovarajuća slova i time pročita Petrovu tajnu poruku : **kriptografija**.

Napomena 3.2.2 *Treba napomenuti da smo u primeru iznad radili sa malim prostim brojevima u slučaju Petrovog ključa,* $p = 17, q = 59$*, te njihovim proizvodom* $n = 1003$ *iz razloga praktičnosti i ilustrovanja funkcionisanja RSA algoritma. U praksi se RSA algoritam nikada ne kombinuje sa tako malim brojevima. Praksa su brojevi sa neuporedivo više cifara(od 2., odnosno 4.), upravo zato što se sigurnost RSA algoritma zasniva na faktorizaciji velikih brojeva, za šta još uvek ne postoji efikasan algoritam. U gore navedenom primeru relativno lako i brzo sa upotrebom računara i odgovarajućih programa faktorisao bi se broj* $1003(= 17 \cdot 59)$*, ali kao što je već rečeno, nije naveden primer velike sigurnosti već jednostavnosti zbog ilustracije mehanizma.*

Standardan šablon RSA algoritma sastojao bi se, recimo, od dva 60-ocifrena prosta broja p i q. Faktorizacija proizvoda takva dva broja, uz čak najnaprednije algoritme te najbrže računare, zahtevala bi sigurno nekoliko meseci, ako ne i nekoliko godina. Neretko brojevi p i q, kod sigurnijih RSA algoritama, dostižu i 100, te preko 100 cifara. Tada je, praktično, faktorizacija n nemoguća.

1977. godine, kada su patentirali RSA algoritam, njegovi tvorci Rivest, Šamir i Adelman, sa MIT-a, zadali su zadatak za koji su mislili da će biti potrebno milijarde godina pre nego što ga neko reši. U suštini, njihov zadatak zasnivao se na faktorizaciji sledećeg broja :

$n = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$

koji je zajedno sa eksponentom enkripcije e=9007 činio javni ključ. Ponudili su \$100 bilo kome ko dekriptuje njihovu poruku. Takođe, dodali su i digitalni potpis upotrebljavajući privatni ključ istog algoritma, tj. eksponent dekripcije d koji zadovoljava 3.1 :

$d = 167178611503808442460152713891683982454369010323583112178350384469290626554487922371144905095786086556624965779748400040570203 73$

Deo njihove šifre koji sadrži digitalni potpis imao je sledeću formu :

06091819200019151222051800230914190 01
51405000821140418050400041512120118 19

kada bi se dešifrovao on bi značio sledeće :

Prva osoba koja ovo reši osvaja stotinu dolara

što je zapravo značilo da je poruka zaista došla sa MIT-a.

Mnogo pre nego što su to ljudi sa MIT-a očekivali, 17 godina kasnije, holandski matematičar Arjen K. Lenstra sa svojim timom u 8 meseci rešio je problem, metodom sita (multiple polynomial quadratic sieve). Uz svoj tim i metodu sita, Lenstra je takođe trebao stotine saradnika širom sveta te njihove računare, a čitava kooperacija odvijala se preko interneta. Rezultat dvodnevnog računanja bila su dva prosta broja, 64-cifreni i 65-cifreni p i q. Pomoću njih Lenstra je dekriptovao poruku sa MIT-a, a ona je glasila:

The magic words are squeamish ossifrage.
(Magične reči su gadljivi bradati lešinar).

Rivest, Šamir i Adleman su, nakon što je ta, sada već u kriptografiji poznata rečenica otkrivena rekli da je ona u suštini besmislena i nema neku posebnu poruku, a takva je jer su mislili da je niko (bar za njihovo vreme) neće otkriti. Što im se činilo nemogućim rešeno je za samo sedamnaest godina, a to je samo dokaz da je kriptologija još uvek eksperimentalna nauka, tj. koliko brzo i efikasno se kriptoanaliza, a samim time i kriptografija, tačnije čitava kriptologija, razvija i napreduje.

3.2.2 Heš funkcije

Kao što je već napomenuto u glavi 3.2, kriptografija je naučna disciplina takve prirode da njeni mehanizmi često zahtevaju funkcije koje za dati elemenat domena lako izračunavaju element kodomena, ali ne dozvoljavaju da se lako uradi obratno (u pomenutoj glavi primer sa telefonskim adresarom prim.aut.). Definisali smo već takve funkcije (jednosmerne tj. one-way function), a **heš funkcije**, o kojima će sada biti reči predstavljaju neki vid jednosmernih funkcija. Ne mogu biti formulisane eksplicitno kao jednosmerne funkcije, već samo kao "dobar kandidat" za jednosmerne funkcije, iz razloga što ne postoji teoretski izveden dokaz da ukoliko je funkcija heš onda sledi da je i jednosmerna. Međutim, s druge strane, nije pronađen ni konkretan kontraprimer heš funkcije koja nije jednosmerna. Zato ćemo sumirati da heš funkcije u praksi jesu jednosmerne funkcije, ali u teoriji ne moraju biti.

Heš funkcija je funkcija koja za ulaz uzima proizvoljno dugačak dokument D, i za njega kao izlaz vraća niz simbola S. Ukoliko se radi na binarnom skupu heš funkciju bismo zapisali kao H : $\{0,1\}^m \to \{0,1\}^t$, gde je m»t.

Najbitnije osobine heš funkcija su sledeće:

- izračunavanje heš funkcije od proizvoljnog dokumenta D treba biti jednostavno i brzo (u linearnom vremenu)

- inverz heš funkcije treba biti praktično nemoguće izračunati (moguće u eksponencijalnom vremenu). Precizno rečeno, za dati niz S kao rezultat heš funkcije H teško je pronaći dokument D za koji važi da je H(D)=S.
- I najmanja izmena dokumenta nad kojim se izvršava heš funkcija, pod time se podrazumeva čak i izmena samo jednog bita, daje značajno drugačiji rezultat nakon heširanja.
- Najčešće je neophodno da heš funkcija bude *collision resistant* (otporna na sudaranje), tj. da je "teško" pronaći dva različita dokumenta D_1 i D_2 takva da vrednosti njihovih odgovarajućih heš funkcija budu jednake (u teoriji moguće jer je skup domena kod heš funckija mnogo veći od skupa kodomena jer su elementi domena nizovi karaktera mnogo veće dužine nego nizovi karaktera kodomena, mada u praksi se heš funkcije mogu birati tako da je drugi original kome odgovara slika koju heš funkcija daje praktično nemoguće naći).

Razlog zašto heš funkcija mora zadovoljavati poslednje navedenu osobinu je u primeru koji sledi. Pera pronađe dve heš funkcije iste vrednosti H(D_1)=H(D_2) koje pripadaju različitim dokumentima D_1 i D_2 respektivno. Recimo da dokument D_1 sadrži naredbu da treba isplatiti 100 dinara, a dokument D_2 sarži naredbu da treba isplatiti 10 000 dinara. Pera Marku daje 100 dinara i zatim mu Marko potpiše dokument D_1. Potpisavši taj dokument, s obzirom da on ima istu heš funkciju kao i onaj sa drugom naredbom, Marko kao da je potpisao oba dokumeta. Pera zatim odlazi u banku i sa Markovim potpisom i pravda dokument D_2 sa Markovog računa mu biva isplaćeno 10 000 dinara.

U praksi, da bi se izračunala vrednost H(D) prvo što radimo jeste da delimo D u blokove D_1,D_2,...,D_k (pri čemu k predstavlja odgovarajući broj blokova, tj. na koliko delova trebamo podeliti dokument da bismo mogli na svaki deo ponaosob da primenimo heš funkciju, jer je čitav dokument uglavnom preveliki da bi mogao da se hešira jednom heš funkcijom), tako da se D može predstaviti na sledeći način :

$$D = D_1||D_2||...||D_k$$

gde || predstavlja operator *konkatenacije*, a on ne predstavlja ništa drugo do spajanje nizova u duži niz (npr. 101||001 = 101001). Ukoliko dokument D nije deljiv sa brojem blokova k dodajemo 0 koliko je potrebno u poslednji blok D_k da bi ispunili taj uslov. Takođe treba još napomenuti da se u izračunavanju heš funkcija upotrebljava *mixing algorithm* $\mathcal{M}$ koji samo niz bitova dužine n prevodi u neki drugi niz bitova dužine n. Kada je D na taj način podeljen u k blokova, prvo se računa heš funkcija inicajalnog niza bitova H_0, koja je uvek ista. Potom izračunavamo $\mathcal{M}$ (D_1) i vrednost $H_1 = H_0 \oplus \mathcal{M}$ (D_1).

Formulom $H_i = H_{i-1} \oplus \mathcal{M}$ (D_i) izračunavanje ponavljamo k puta da bismo dobili i ostale vrednosti heš funkcija : $H_2, H_3, ...$ konačno, naša prava vrednost heš funkcije H(D) zapravo je poslenja u nizu, H_k.

Najpoznatije jednosmerne heš funkcije jesu MD5 i SHA-1. MD5 je delo Ronalda Rivesta, jedna od nekoliko u seriji MD heš funkcija, i ona obrađuje ulazne podatke u blokovima od 512 bitova(64 bajta), a kao rezultat vraća heš vrednost od 128 bitova(16 bajtova). SHA-1 (*Secure Hash Algorithm 1)* kreirana je od strane Nacionalne Bezbednosne Agencije Sjedninjenih Američkih Država (*Nacional Secure*

Agency of Unated States of America) i ta heš funkcija takođe obrađuje ulazni tekst dužine 512 bitova, ali kao heš vrednost daje izlaz dužine 160 bitova(20 bajta), te je stoga sigurniji od MD5. Kasnije, sa razvojem kriptoanalize razvijali su se i novi algoritmi, tako da su sledili SHA-224, SHA-256, SHA-512 (gde drugi deo naziva predstavlja broj bitova izlaza heš funkcije).

Logično, od što više bitova se izlaz sastoji heš funkcija je sigurnija i otpornija na koliziju, međutim pri odabiru odgovarajuće dužine izlaza treba uzeti u obzir i brzinu heš funkcije, koja je obrnuto proporcionalna dužini izlaza. Bitno je ne odabrati presporu heš funkciju jer ona obrađuje dokumente velikih dužina, i od nekoliko megabajta. Dakle, potrebno je naći ravnotežu između sigurnosti i brzine algoritma.

3.2.3 Digitalni potpis

Digitalni potpis u digitalnom svetu predstavlja neku vrstu analogona potpisa "perom i mastilom" u fizičkom svetu. Digitalni potpis predstavlja "pečat", nešto svojstvenog nama koji hoćemo da obeležimo autentičnost dokumenta najčešće pravne, finansijske, vojne, sudske ili druge prirode. Naravno, iz tehničkih razloga nije dovoljno da on bude autentičan samo u fizičkom smislu, iz prostog razloga dostupnosti *"cut-copy-paste"* operacija na računarima te na taj način relativno jednostavnog falsifikovanja potpisa. Uz određene kriptografske alate, trebamo biti u mogućnosti da samo mi lično "potpišemo" ili obeležimo naš dokument ili poruku, a onaj ko je nju i primio da određenim algoritmom proveri da li su poruka i potpis potekli baš od nas.

Inspiraciju za ovakav vid zaštite možemo naći vrativši se u nekadašnja vremena, dok računari i internet još uvek nisu predstavljali glavnu platformu za interakciju između ljudi, a autentičnost potpisa je već i tada bila ugrožena mogućnosti falsifikovanja. Nešto što je tada predstavljalo napredniju vrstu potpisa, kao neki vid ekvivalenta digitalnom potpisu u kriptografiji jeste bio pečat od voska kojim su se zatvarala pisma. Za njega je bio neophodan alat u vidu kalupa kojim bi se naneseni vosak oblikovao u autentičan oblik koji je bio dokaz porekla pošiljke. Taj alat, tj. kalup neko vreme predstavljao je prednost koju bi originalni pošiljalac imao u odnosu na falsifikatore, međutim vremenom se došlo i do ideja izlivanja istog kalupa te mogućnosti falsifikovanja pečata. Tada se takav sistem smatrao prevaziđen, baš kao što u današnje vreme razvijenih tehnologija takva ideja pošiljaocu tajne poruke ne bi davala veliku prednost u diskretnoj komunikaciji.

Vratimo se sada digitalnom potpisu. Dakle, kako taj potpis ne može predstavljati neka "konstanta", bilo u smislu kaligrafskog potpisa, običnog niza slova ili nekog vida simbola ili slike, on mora biti neka funkcija. Ta funkcija zavisiće upravo od onoga čega ona i opisuje, tj. dokumenta koji potpisujemo.

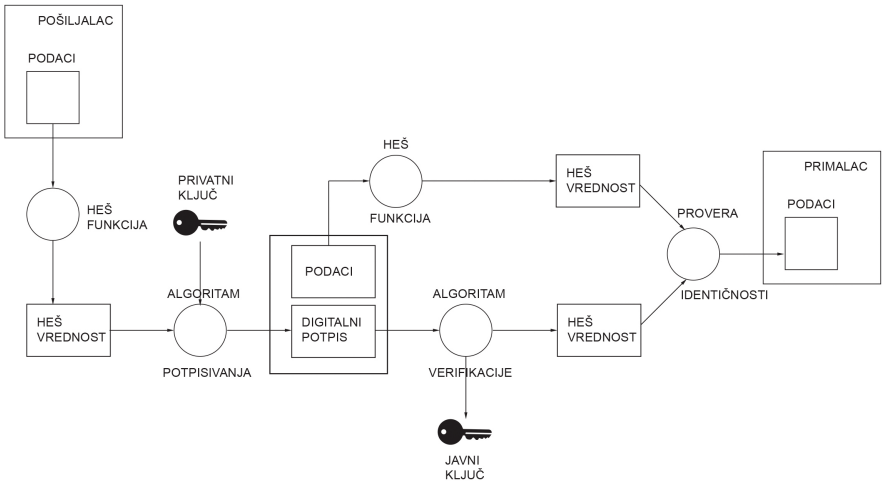
Siguran algoritam digitalnog potpisa mora da sadrži i zadovoljava uslove navedene u nastavku:

- Bilo ko može proveriti identitet pošaljioca poruke, naravno uz pomoć javnog ključa.
- Osnovno načelo asimetrične kriptografije, tj. iz javnog kljuca E napadač ne može doći do privatnog ključa K koji se koristi za potpisivanje dokumenta i

time ne može sam izmeniti sadržaj nekog dokumenta te ga potpisati u ime pravog pošaljioca.

- Iz javnog ključa E te liste dokumenata $D_1, D_2, ..., D_n$ i njihovih verzija sa digitalnim potpisom $D_1^{sign}, D_2^{sign}, ..., D_n^{sign}$ napadač ne može ni do jednog digitalnog potpisa dokumenta koji nije u listi $D_1, D_2, ..., D_n$.
- (*Uslov neporecivosti)* Pošaljilac nema mogućnost poricanja da nije poslao datu poruku, ili ograđivanja u bilo kom smislu od sadržaja te iste poruke, jer ukoliko je potpisana samo on je mogao dati sadržaj obraditi i potpisati.

Alat koji se upotrebljava da se formira digitalni potpis vrlo je sličan alatu koji služi za formiranje šifri koje koriste metode asimetrične kriptografije, tj. asimetričnih šifri. Kompletan algoritam digitalnog potpisa će se sastojati od metode algoritma za potpisivanje (*Singing algorithm)* te metode za verifikaciju digitalnog potpisa (*Verification algorithm).* Baš kao i u asimetričnoj kriptografiji pošaljioc poruke posedovaće svoj privatni ključ K koji će algoritam za potpisivanje da koristi kako bi od dokumenta koji treba biti poptisan D dao potpisani dokument D^{sign}. Primalac poruke koristiće javni ključ E u algoritmu za verifikaciju koji potpisani dokument D^{sign} uzima kao ulaz, te vraća bool vrednosti 1 (u slučaju da dati D^{sign} potiče zaista od pošaljioca koji je potpisao dokument D uz pomoć privatnog ključa K) ili 0 (u suprotnom slučaju). Šema takvog procesa data je na ilustraciji ispod.



Slika 3.3: Šema procesa implementacije digitalnog potpisa).

Čest je slučaj da dolazi i do potpisivanja heš funkcije datog dokumenta H(D), a ne samog dokumenta D, iz prostog razloga jer u mehanizmu većine algoritama za digitalni potpis postoji ograničenje da za ulaz uzimaju dužine b bita, gde je $80 \leq b \leq 100$, a kako je uglavnom dužina dokumenata znatno veća od 100 bita, takav uslov jedino mogu zadovoljavati heš funkcije takvih dokumenata.

U tekstu iznad ilustruje se simultanost ubotrebe heš funkcija, asimetrične kriptografije i digitalnog potpisa, a u nastavku naveden je primer kako uz pomoć RSA algoritma i njegovog mehanizma možemo digitalno potpisati neki dokument.

Primer 3.2.2 *Petar hoće da "potpiše" ugovor u kojem sa Markom precizira uslove oko posla i da ga pošalje Marku putem interneta. Marko mora imati dokaz da je taj ugovor "potpisao" Petar lično, da bi započeo sa ispunjavanjem navedenih tačaka u ugovoru. Nemaju mogućnost da to urade lično, tako da će digitalni potpis na ugovoru morati biti jednako validan kao i Petrov lični potpis na fizičkom papiru. Kao i u primeru ranije obrađenom za RSA algoritam Petar bira svoje višecifrene proste brojeve p=1223 i q=1987, te njihov proizvod* $N = p \cdot q = 1223 \cdot 1987 = 2430101$. *Kako zna faktore broja N Petru je lako da odredi* $\varphi(N) = (p-1)(q-1) = 2426892$, *i potom bira eksponent verifikacije v (analogan eksponentu enkripcije kod RSA algoritma), takav da zadovoljava*

$$NZD(v, \varphi(N)) = 1$$

i neka je Petar odabrao v koje zadovoljava taj uslov, $v = 948047$. *Petar šalje Marku nesigurnim komunikacijskim kanalom verifikacioni algoritam u kome su sačuvani brojevi* (N, v). *Samo Petar može da izračuna eksponent potpisivanja s koji zadovoljava sledeću kongruenciju*

$$sv \equiv 1 \pmod{\varphi(N)}$$

tj. $s \cdot 948047 = 1 \pmod{2426892}$, *a s koje to zadovljava je* $s = 1051235$. *Petar taj broj čuva samo za sebe kako bi samo on mogao potpisati dokument na taj način da Marko može izvršiti verifikaciju i uveriti se da je Petar "potpisao" dati dokument.*

Petrov dokument D koji želi da šifruje mora da zadovoljava uslov $\forall i, 1 \leq D_i < N$ *da bismo mogli primeniti RSA algoritam, i s obzirom da je numerički ekvivalent petrovog dokumenta mnogo veći od N, Petar na svoj dokument primenjuje heš funkciju H koja mu daje sledeću vrednost za njegov dokument :* $H\{D\} = 1070777$.

Petar onda uz pomoć algoritma ekvivalentnog RSA enkripciji formira svoj digitalni potpis P za heš vrednost $H\{D\}$*:*

$$P \equiv H\{D\}^s \pmod{N}$$

odnosno

$$P \equiv 1070777^{948047} \equiv 1473513 \pmod{2430101}$$

i potom šalje Marku heš funkciju $H\{D\} = 1070777$ *te njoj odgovarajući digitalni popis* $P = 1473513$. *Marko upotrebljava svoj verifikacioni algoritam da bi proverio da li je potpis P došao baš od Petra. Izračunava :*

$$P^v \equiv H\{D\} \pmod{n}$$

$$1473513^{948047} \equiv H\{D\} \pmod{2426892}$$

i tako dobija da je $H\{D\} = 1070777$ *što mu dokazuje da je digitalni potpis došao lično od Petra, a ne neke treće osobe.*

Ponekada može doći i do implementacije digitalnog potpisa bez upotrebe ova dva kriptološka alata (heš funkcija i asimetrične kriptografije) - naime, moguće je potpisivanje i uz pomoć simetričnih šifarskih sistema i arbitratora. Arbitrator predstavlja trećeg učesnika u komunikaciji između dvoje osoba, tj. učesnika koji predstavlja poverljivi entitet koji je najčešće sertifikovana ovlašćena organizacija. Broj tajnih ključeva jednak je broju učesnika u komunikaciji, a sva komunikacija odvija se preko arbitratora. Arbitrator poseduje tajne ključeve svih učesnika, oni šifruju svoje poruke te ih šalju arbitratoru koji uz pomoć njihovih tajnih ključeva proverava da li je poruka potekla baš od njih. Nakon verifikacije, šifruju dešifrovanu poruku onim ključem koji pripada učesniku mreže koji treba da primi poruku te mu je tako šifrovanu šalju, on je dekriptuje istim ključem i dobija originalnu poruku koja je potekla od pošaljioca. Dakle, u ovakvom vidu potpisivanja podrazumeva se postojanje potpuno pouzdanog učesnika bez interesa i negativnih namera, a kako je nedostatak takvih ljudi, i veliki broj upravo onih sa suprotnim namerama, jedan od glavnih razloga razvoja kriptoloških metoda, ovaj metod razmene poruka koji podrazumeva arbitratora sve je manje popularan i u upotrebi.

Glava 4

Četvrti deo

4.1 Bitcoin

Jedan od najinovativnijih patenata kriptografije jeste sve popularniji **Bitcoin**. Bitcoin predstavlja ogroman, novi i nestandardan element u finansijskoj industriji. To je nesvakodnevni fenomen čijem potencijalu se još uvek ne naziru granice.

Teoretski je osmišljen 2008. godine, a njegovim autorom se smatra osoba pod pseudonimom *Satoshi Nakamoto* čiji je stvarni identitet ostao nepoznat. U praksi, mreža Bitcoina počinje sa radom 2009. godine i od tada se razvija i stiče sve veći broj korisnika i sledbenika.

BitCoin predstavlja naprednu vrstu digitalne kripto valute, tj. digitalne valute čiji transferi su verifikovani i zaštićeni kriptografskim metodama. Za raziku od tradicionalnih *fiat* valuta (dekretnog novca), koje postoje i u fizičko-materijalnom obliku (novčanica) i u elektronskom obliku (bankovni računi), digitalne valute postoje samo u elektronskom obliku, i uopšte ne postoje kao objekti. Bitcoin je samim time atipična moneta, i ima određene kako prednosti tako i mane u odnosu na standardne fiat valute.

Definišimo još nekoliko pojmova koje ćemo koristiti u nastavku razmatranja Bitcoina, i uz to ukratko objasnimo njegovu upotrebnu svrhu i dešavanja na mreži Bitcoina (mreža na kojoj se obavljaju svi transferi Bitcoina) : *adresa* predstavlja kombinaciju brojeva i slova, odnosno niz karaktera na Bitcoin mreži na kojem je sačuvana određena količina Bitcoina. Adrese su dostupne svima, čak i podatak o količini Bitcoina na adresama, ali samo vlasnik adrese, sa privatnim ključem može joj pristupiti sa zahtevima da transferuje svoje Bitcoine sa nje na drugu adresu. *Elektronski* ili *Bitcoin novčanici* (engl. e-wallet) predstavljaju virtualne objekte koji pripadaju pojedincu, a u sebi sadrže sve adrese sa podacima o količini Bitcoina koje korisnik poseduje. Korisnik pristupa svom Bitcoin novčaniku preko ličnog privatnog ključa. *Transakcija* (transfer Bitcoina) je bilo koje premeštanje određene količine Bitcoina sa jedne adrese na drugu. *Rudar* (engl. miner) je učesnik u mreži Bitcoina čiji je zadatak da proverava i verifikuje transakcije ukoliko su validni ili da ih poništava ukoliko su plod malverzacije nekog hakera ili slično. Njegov rad

na Bitcoin mreži naziva se *rudarenje* (engl. mining). Kada odluči da ih verifikuje, rudar smešta podatke o transakciji u *blokove* - osnovne gradivne jedinice *blok lanca* (engl. block chain). Blok lanac predstavlja neku vrstu skupa istorijskih podataka svih transakcija Bitcoina koji su se desili u prošlosti i koji su verifikovani od strane rudara. Rudari za obavljenu verifikaciju dobijaju stimulans za uloženi trud u vidu Bitcoina koji se generišu za svaki kompletirani blok informacija, za svaki novi blok se generiše nagrada od 25 Bitcoina koji se ubacuju na tržiste Bitcoina i dodeljuju rudaru ili grupi rudara koji su blok isformirali te dodali u blok lanac. Treba napomenuti da je navedeni proces ubacivanja 25 Bitcoina na tržište ove valute jedini način na koji se novi Bitcoini stavljaju u promet. Algoritam saobraćaja Bitcoina osmišljen je tako da je maksimalan broj Bitcoina koji će biti u protoku ograničen na 21 milion, pri čemu je do danas (maj 2016. godine, prim. aut.) generisano oko 15 miliona. Kako sam proces rudarenja zahteva računare sa sve naprednijim komponentama u vidu grafičkih kartica, procesora, RAM memorije, posebnih kulera koji moraju da takav računar drže na odgovarajućoj temperaturi, u poslednje vreme rudarenje više praktično i nije moguće obavljati sa "običnim računarima" već sa ASIC računarima specijalizovanim za rudarenje. Naravno, cena ovakve opreme je visoka, kao i cena za potrošnju električne energije potrebne za ove procese, te je samostalno rudarenje praktično neizvodivo. Iz tih razloga rudari se zajedno udružuju u takozvane *pool*-ove gde udruženim snagama računara razrešavaju matematičke algortime potrebne da bi se transakcije verifikovale te smestile u blok, koji se potom smešta u blok lanac.

U nastavku navodimo fundamentalne razlike Bitcoina u odnosu na fiat valute.

- *decentralizovanost* - ne postoji centralna banka, institucija, država, niti generalno autoritet koji je zadužen za produkciju ove monete i vođenje monetarne politike vezane za nju. Takođe, ne postoji jedinstveni server gde se saobraća ovom monetom, već je njen tok toliko proširen da u principu i ne zavisi od bilo kog servera ponaosob. Mrežu čine svi korisnici, rudari, špekulanti na berzi Bitcoina. Jednostavno svi koji učestvuju u transakcijama Bitcoina, ali niko nema apsolutni autoritet nad njim.
- *pseudoanonimnost* - naime, pri transakcijama definitivno nismo dužni dati toliko podataka koliko bismo morali u bankama pri transferima novaca sa računa na račun. U suštini, pri otvaranju adrese nismo dužni dati bilo koji lični podatak. Međutim, nije to moguće nazvati apsolutnom anonimnosti jer pri velikom broju transfera napadači bi konstantim praćenjem saobraćaja Bitcoina i povezivanja sa adresama možda mogli doći do informacija koje nisu predviđene da im budu dostupne. Ipak, praktično neograničen broj adresa (naravno, ne neograničen i u teorijskom kontekstu) koji je dostupan svim korisnicima da otvore, raspodeljivanje ličnih Bitcoina na sve te adrese te na taj način zavaravanje tragova čini ovu anonimnost zadovoljavajućom, a u odnosu na standardni bankarski sistem u suštini i potpunom. S druge strane, mnogi kritičari Bitcoina ovu osobinu istog smatraju i za njegovu manu, jer na ovaj način ostavlja se prostor za transfer novca kako bi se isplatili neki poslovi koji nisu u skladu sa zakonom ili obavile neke protivpravne radnje (kupovina oružja, utaja poreza itd.).

- *transparentnost* - u suštini pojam koji predstavlja suprotnost anonimnosti. Ipak, blok lanac sadrži sve informacije sa tržista Bitcoina : i koliko je novca na kojoj adresi i koliko je novca prebačeno sa koje na koju adresu i kada. Te informacije su tranparantne, tj. javne i dostupne svima. Kompeltan tok i saobraćaj Bitcoina se može pratiti u svakom momentu [12].

- *nemogućnost prevare* - u smislu krivotvorenja i fasifikovanja valute, jer ista sama ni ne postoji u fizičkom smislu, a niko sem mreže ne može da generiše nove Bitcoine.

- *ireverzibilnost* - transacije su nepovratne. Kada se transakcija pošalje na obradu rudarima i kada je oni verifikuju i smeste u blok, više ne može da se poništi, a s obzirom da ne postoji centralni autoritet nikome se ne može priložiti žalba, čak ni u slučaju mehaničke greške pri transakciji. U slučaju pomenute mehaničke greške pri unosu lokacije gde se šalju Bitcoini ova osobina predstavlja manu. Međutim, u svakom drugom slučaju, tipa pokušaju malverzacije da se nakon dobijene robe ili usluge pokuša obustaviti dogovoreni transfer Bitcoina na neku adresu, ireverzibilnost predstavlja prednost te garanciju pružaocu usluge ili robe da će se započet transfer u svakom slučaju uspešno završiti.

- *brzina* - transakcije Bitcoina sa adrese na adresu zahtevaju znatno manje vremena nego prebacivanja novca sa računa na račun u bankama, pogotovo ako računi nisu u istoj banci, državi ili još gore, kontinentu. Sistem Bitcoina se razvija i povećava broj korisnika istog, sve je više transakcija, pa biva potrebno više vremena za pojedine transakcije, ali i broj rudara koji rade na transferima raste, tako da se brzina ovih procesa i dalje smatra prednosti ovog sistema.

- *jednostavnost i besplatnost* - za razliku od prilično komplikovanog otvaranja računa u banci, koji zahteva uglavnom dosta vremena te značajnu količinu ličnih i privatnih podataka, otvaranje adrese i e-walleta je krajnje jednostavno, bez ostavljanja podataka i provizija. Taj proces je potpuno besplatan, kao što je bio zamišljen i proces transakcije, međutim u današnje vreme, transakcija Bitcoina u svakom momentu je sve više, pa se obično rudarima daje neki vid stimulansa (u principu na dobrovoljnoj bazi) u vidu Bitcoina, tačnije delova Bitcoina (1 Bitcoin = 100 000 000 Satoshis, gde je Satoshi najmanji definisani deo Bitcoina, koji je dobio ime po pseudonimu kreatora tj. tvorca Bitcoina Satoshi Nakamotu) da bi stavili prioritet na određeni transfer i završili ga brže. Transakcija se obavlja između dva korisnika, bez posrednika, jedino je rudar taj koji se stara o tome da je proces transakcije legalan.

- *neregulisanost* - ovo predstavlja za pojedinca prednost, a za države manu. Naime, nigde na svetu Bitcoin nije zvanično platno sredstvo, pa njegov saobraćaj nije zakonom regulisan nigde, samim time ni oporezovan. U principu to je i nemoguće uraditi, upravo zbog prirode i porekla Bitcoina, pa mnogi smatraju da je samo pitanje vremena kada će, i ko, prvi zabraniti protok i

saobraćanje Bitcoina. Sluti se da će prve po tom pitanju reagvati SAD, kao trenutno i najveće tržište Bitcoinima, mada je drugo pitanje koliko je to i moguće uraditi, s obzirom da se saobraćanje ove valute dešava isključivo na internetu, za kojeg je takođe bilo sličnih najava oko zabrana.

- *nestabilnost* - upravo prvonavedena decentralizovanost uzrokuje nemogućnost kontrole fluktacije vrednosti Bitcoina na tržištu. Zbog velike popularnosti fluktacije su velike. Kada se tek pojavio vredeo je oko 10 dolara, maksimalna vrednost koju je Bitcoin dostigao u prošlosti, krajem 2013. godine, kada je interesovanje za njega bilo najveće iznosila je oko 1000 dolara, dok je trenutna vrednost (maj 2016. godine, prim. aut.) oko 450 dolara. Ovo bi se u suštini moglo smatrati manom, osim za preofesionalne spekulante koji bi preciznim i tačnim predviđanjem toka ove valute, ukoliko je to uopšte moguće, mogli zaraditi na fluktaciji vrednosti tako što bi kupovali Bitcoine kada im je vrednost manja a prodavali iste kada im vrednost poraste.

Zbog svih ovih osobina namena Bitcoina je višestruka :

- **slanje novca** - prvenstvena svrha Bitcoina, ideja da se unapred određena suma Bitcoina sa jednog kraja na drugi kraj planete može poslati za samo nekoliko momenata. Sa razvićem Bitcoin mreže dolazi do modifikacije ove opcije, danas se lako za fiat novac kupuje određena suma Bitcoina, ona momentalno šalje na drugu adresu, te se ponovo za tu količinu Bitcoina kupuje bilo koja druga fiat valuta bilo gde na svetu.

- **kupovina** - sa razvojem Bitcoina sve je više proizvođača, trgovina, prodavaca i generalno kompanija kojima je moguće izvršiti plaćanje ovom valutom.

- **ulaganje** - u mrežu Bitcoina je moguće ulagati kao i u sve druge valute, deonice, akcije ili bilo koji drugi finansijski derivat. Prosto se uloži određena suma novca, kupe Bitcoini u toj vrednosti i čuvaju dok se ne postigne određeni cilj. Izvodivo, ali samo onima koji su dobro potkovani znanjem i tokovima ove kriptovalute, s obzirom na nestabilnost Bitcoina kao valute.

- **spekulacija** - još rizičniji oblik ulaganja koji za cilj ima da se za kratko vreme samom kupoprodajom valute dođe do velikih profita. Uzimajući u obzir nestabilnost valute samo čudo, neka insajderska informacija (ukoliko to uopšte i postoji u mreži Bitcoina), ili pak puka slučajnost i sreća može učiniti spekulaciju efikasnom.

Da li je Bitcoin roba ili novac? Mišljenja su podeljena, ali većina ekonomista i finansijera, smatra da je i roba i novac, prosto jer ima osobine i namene oboje. Novac je jer sluzi kao sredstvo placanja, a robom se smatra jer se za njega mogu dobiti određene protivrednosti u vidu dobara ili čak novca. Bitcoin moze čak biti i kupljen uz pomoć pravog, fiat novca.

Veliku ulogu u skladištenju Bitcoina i elektronskih novčanika odigrava kriptografija sa javnim ključem, a takođe i digitalni potpis i heš funkcije. Tehnički, u elektronskim novčanicima ne čuvamo zaista Bitcoine, već samo lokacije gde se

oni nalaze (adrese). Javnim ključem zaštićene su lokacije na kojima su skladišteni Bitcoini i ti podaci su dostupni svima, a privatnim ključem kriptovan je pristup svakoj adresi ponaosob, stoga raspolagati sredstvima sa tih adresa može samo onaj ko ima privatni ključ.

Bitcoin predstavlja najvredniju, a samim time i najvažniju valutu na listi digitalnih kriptovaluta, a samo još neke od poznatijih su Litecoin, Ethereum, Dogecoin i Peercoin.

Zaključak

Kriptografija se sastoji od alata, metoda i algoritama koji su nastali u prošlosti, neophodni su za sadašnjost, a bez njih se budućnost ne može ni zamisliti.

Na žalost svih kriptografa, a na sreću kriptoanalitičara, istinita je sledeća izjava: *"Apsolutna sigurnost ne postoji"*. Zvuči malo apsurdno, s obzirom da je u radu definisan pojam savršene sigurnosti. Međutim, moramo uzeti u obzir koliko je moderna digitalna kriptografija nauka u razvoju, te upravo iz tih razloga njeni teoretski temelji nisu toliko čvrsto i koncizno postavljeni, kao recimo kod matematike. Zbog toga se često dešava da je već apostrofirana i dokazana teorija u kriptografiji u nekom vidu kontradikcije sa novokreiranim metodama. To nam govori pre svega o *relativnosti pojma sigurnosti* u kriptologiji uopšte, te nam ukazuje kako ništa ne treba prihvatati "zdravo za gotovo", jer je ovo još uvek mlada nauka.

Koliko god kriptografski metod bio napredan i koliko god mi mislili da je siguran, čim se upotrebi u komercijalne svrhe, neko počinje da implementira razne algoritme kako bi razbio šifrat i došao do otvorenog teksta. Sistem koji danas deluje potpuno bezbedno, sutra možda to neće biti, što nam pokazuje i primer koji je u ovom radu naveden u okviru poglavlja RSA algoritma.

Sa razvojem kriptografije i njenih metoda, paralelno dolazi do razvoja i kriptoanalize te metoda za dekriptovanje. Česta je situacija da najbolje kriptoanalitičare angažuju, uz mnogo veće nadoknade, u kriptografiji, jer koliko god neko želeo da dospe do određenih podataka i informacija, još više se velike i tajne korporacije trude da te svoje podatke zaštite i učine nedostupnima protivnicima, konkurentima, a nekada čak i partnerima kojima nisu baš spremni izneti tačne i istinite činjenice.

Mnogo je još prostora i perspektive za napredak kriptologije. Najlepše je to što razvoj kriptografije za sobom posledično uzrokuje i razvoj kriptoanalize i obratno. Sve to neodoljivo podseća na univerzum koji se nalazi u ravnoteži i ima svoj balans. Kriptografija i kriptoanaliza su suprotstavljeni, kao jing i jang, jedno drugom rivali, a opet, jedno ne bi imalo smisao svog postojanja da nema drugog.

O autoru

Daniel Divjaković rođen je u Osijeku, 8. Aprila 1990. godine. Osnovnu školu *"Ivo Lola Ribar"* završio je u Somboru, gde potom i upisuje Srednju Medicinsku Školu *"Dr Ružica Rip"*, smer farmaceutski tehničar. 2009. godine završava srednju školu i upisuje *Prirodno-Matematički Fakultet* u Novom Sadu, smer Primenjena Matematika, modul Tehno-matematika. Osnovne bachelor studije završava 2013. godine kada i upisuje master studije istog smera.

Hobiji su mu muzika, sport i video igrice. Poseduje znanje engleskog i nemačkog jezika.

Literatura

[1] Baldoni M.W., Ciliberto C., Piacentini Cattaneo G.M. *Elementary number theory, cruptography and codes,* Springer (2009), 332-416.

[2] Barski Conrad , Wilmer Chris *Bitcoin for the befuddled,* No Starch Press, Inc. (2015).

[3] Hoffstein Jeffrey, Pipher Jill, Silverman H. Joseph *An introduction to mathematical cryptography,* Springer (2008).

[4] Kahn David *The codebreakers - the story of secret writing,* The New American Library, Inc. (1973).

[5] Menezes Alfred J. , Van Oorschot Paul C., Vanstone Scot A. *Handbook of applied cryptography,* CRC Press, (1996).

[6] Mićić Vladimir, Kadelburg Zoran, Dukić Dušan *Uvod u teoriju brojeva,* Društvo matematičara Srbije (2004).

[7] Sarad A.V, Huettenhain Jesko *RSA encryption algorithm in a nut shell* .

[8] Šešelja Branimir , Tepavčević Andreja *Algebra 1,* Prirodno-Matematički Fakultet, Institut za matematiku u Novom Sadu.

[9] Van Houtven Laurens *Crypto 101,* (2013-2014).

[10] https://www.coursera.org/learn/crypto/

[11] http://practicalcryptography.com/cryptanalysis/

[12] http://blockchain.info

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR

Identifikacioni broj:
IBR

Tip dokumentacije: Monografska dokumentacija
TD

Tip zapisa: Tekstualni štampani materijal
TZ

Vrsta rada: Master rad
VR

Autor: Daniel Divjaković
AU

Mentor: dr Petar Đapić
MN

Naslov rada: Osnove kriptologije, OTP i RSA algoritam
NR

Jezik publikacije: srpski (latinica)
JP

Jezik izvoda: srpski/engleski
JI

Zemlja publikovanja: Republika Srbija
ZP

Uže geografsko područje: Vojvodina
UGP

Godina: 2016.
GO

Izdavač: Autorski reprint
IZ

Mesto i adresa: Univerzitet u Novom Sadu, Prirodno-matematički fakultet, Trg Dositeja Obradovića 4
MA

Fizički opis rada: 4/64/12/6/8/0/0
(broj poglavlja/strana/lit citata/tabela/slika/grafika/priloga)
FO

Naučna oblast: Matematika
NO

Naučna disciplina: Kriptologija
ND

Predmetna odrednica/Ključne reči: kriptologija, kriptografija, kriptoanaliza, otvoreni tekst, šifra, šifrat, pošiljalac, primalac, napadač, simetrična kriptografija, OTP algoritam, asimetrična kriptografija, RSA algoritam, heš funkcija, digitalni potpis, Bitcoin.
PO

UDK:

Čuva se: u biblioteci Departmana za matematiku i informatiku, Novi Sad
ČU

Važna napomena:
VN

Izvod: U najširem smislu, ovaj rad bavi se kriptologijom, nekim od njenih metoda i alata i njenim primenama.
U užem smislu, akcenat je postavljen na razmataranje simetrične kriptografije (OTP algoritam) i asimetrične kriptografije (RSA algoritam), heš funkcija i digitalnog potpisa, Bitcoina kao i njihovih primena.
IZ

Datum prihvatanja teme od strane NN Veća: 17.05.2016.
DP

Datum odbrane:
DO

Članovi komisije:

Predsednik: dr Branimir Šešelja, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Mentor: dr Petar Đapić, docent, Prirodno-matematički fakultet, Univerzitet u Novom Sadu.

Član: dr Andreja Tepavčević, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

DO

UNIVERSITY OF NOVI SAD
FACULTY OF NATURAL SCIENCES AND MATHEMATICS
KEY WORDS DOCUMENTATION

Accession number:
ANO

Identification number:
INO

Document type: Monographic type
DT

Type of record: Text printed material
TR

Contents code: Master thesis
CC

Author: Daniel Divjaković
AU

Mentor: Petar Đapić, Ph.D.
MN

Title: Fundamentals of cryptology, OTP and RSA algorithm
TI

Language of text: Serbian(Latin)
LT

Language of abstract: Serbian/English
LA

Country of publication: Republic of Serbia
CP

Locality of publication: Vojvodina
LP

Publication year: 2016.
PY

Publisher: Author's reprint
PU

Publ.place: University of Novi Sad, Faculty of Science, Trg Dositeja Obradovića 4
PP

Physical description: 4/64/12/6/8/0/0
(chapters/pages/literature/tables/pictures/graphs/additional lists)
PD

Scientific field: Mathematics
SF

Scientific discipline: Cryptology
SD

Subject / Key words: cryptology, cryptography, cryptoanalysis, plaintext, cipher, ciphertext, sender, reciver, attacker, simetric cryptographym, OTP algorithm, asimetric cryptography, RSA algorithm, hash function, digital signature, Bitcoin.
SKW

UC:

Holding data: The Library of the Department of Mathematics and Informatics, Novi Sad
HD

Note:
N

Abstract: In overall sense, this thesis works on cryptology, some of its methods and worktools and its applications.
In particular sense, an accent is put on considering simetric cryptography (OTP algorithm) and asimetric cryptography (RSA algorithm), hash functions and digital signature, Bitcoin and theirs applications.
AB

Accepted by Scientific Board on: 17.05.2016.
ASB

Defended:
DE

Thesis defend board:

President: Branimir Šešelja, Full Professor, Faculty of Science, University of Novi Sad

Mentor: Dr Petar Đapić, Assistant Professor, Faculty of Science, University of Novi Sad

Member: Dr Andreja Tepavčević, Full Professor, Faculty of Science, University of Novi Sad

DB