Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Dragica Nikolić

Povijest kriptografije

Završni rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Dragica Nikolić

Povijest kriptografije

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2017.

Sadržaj

Sažetak: Kriptografija je matematička disciplina koja proučava različite načine kriptiranja. Ona omogućuje komunukaciju između dviju strana tako da treća strana ne može razumjeti poruke. Treća strana može doći do poruke presretanjem, prisluškivanjem i na neke druge načine, ali ju ne može dešifrirati bez pravog ključa. Kroz povijest, od starog vijeka pa sve do danas, kriptografija je postupno napredovala i kako je vrijeme prolazilo imala je sve pouzdanije strojeve i metode kojima se mogu šifrirati poruke. Kriptografija je bila najkorisnija u ratovima, a danas ima veliku primjenu u sigurnosti raznih sustava. Na samom početku kriptiranja korišteni su ukrasni simboli, zatim kvadrati koji su sadržavali slova abecede te prvi i najjednostavniji uređaj - obični štap (skytale). Nakon toga pojavljuje se šifrarnik s kotačem, sustav s dva diska, Playfairov i drugi sustavi, dok se u 20. stoljeću razvijaju elektromehanički strojevi Enigma i Sigaba. U novije vrijeme pojavljuju se kriptografski algoritmi kao što su, primjerice, DES, AES, RSA, NTRU i ECC, a sve se više razvija i kvantna kriptografija.

Ključne riječi: kriptografija, šifra, šifriranje, dešifriranje, supstitucijske šifre, otvoreni tekst, ključ, kriptosustav

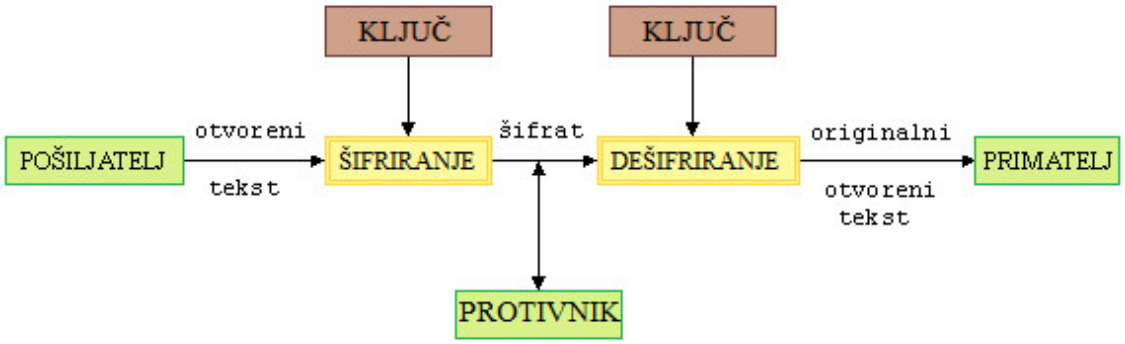
History of cryptography

Abstract: Cryptography is a mathematical discipline that studies different ways of encryption. It actually allows communication between two sides so that a third side can not understand the message. Third side can get to the message by intercepting, eavesdropping and in some other ways, but it can not be decrypted without the right key. Throughout history, from Antiquity to present day, cryptography has progressively advanced and as time went on, it had more reliable machines and methods used to encrypt certain messages. Cryptography has been most useful in wars and today has extensive application in various security systems. At the beginning of encryption were used hieroglyphics, then squares containing letters of the alphabet and the first and the most simple device - ordinary stick (skytale). After that appears a codebook with a wheel, a system with two discs, Playfair and other systems, while in the 20th century were developed electromechanical machines Enigma and Sigaba. In recent years, appears cryptographic algorithms such as, for example, DES, AES, RSA, NTRU and ECC, and has been further developed and quantum cryptography.

Key words: cryptography, cipher, encryption, decryption, substitution cipher, plaintext, key, cryptosystem

Uvod

Smatra se da je umjetnost kriptografije rođena kad i umjetnost pisanja. Kako se civilizacija razvijala ljudi su se dijelili u plemena, grupe i kraljevstva. To je dovelo do pojave ideja kao što su moć, vrhovna vlast, rat i politika. Ove ideje potiču prirodnu potrebu ljudi da tajno komuniciraju s drugima što je zauzvrat osiguralo kontinuirani razvoj kriptografije. Korijeni kriptografije potječu iz rimskih i egipatskih civilizacija. Riječ kriptografija je kombinacija dvije grčke riječi 'krypto' što znači skriveni i 'graphene' što znači pisati. Na Slici 1 možemo vidjeti proces koji se odvija između dvije strane, pošiljatelja i primatelja. Bit kriptografije je da omogućava komunikaciju između dvije osobe, tako da treća strana ne može saznati sadržaj poruke, tj. otvoreni tekst. Pošiljatelj pomoću unaprijed dogovorenog ključa šifrira otvoreni tekst, zatim se poruka šalje preko nekog komunikacijskog kanala koji nije siguran te dolazi do primatelja koji ima ključ za dešifriranje i otkrivanje originalnog otvorenog teksta. U tom procesu protivnik može čuti ili vidjeti šifrirani tekst, ali ga ne može dešifrirati ukoliko nema pravi ključ.



Slika 1: *Slanje poruke od pošiljatelja do primatelja*

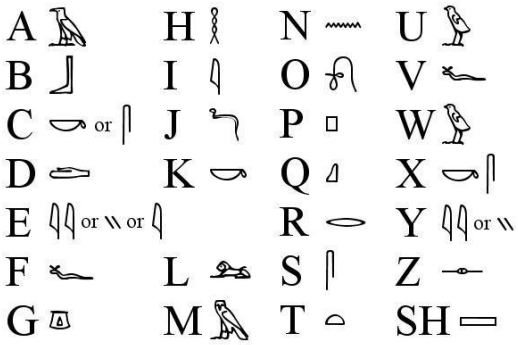
U ovom radu ćemo ukratko izložiti povijest kriprografije po razdobljima od starog vijeka pa sve do suvremenog doba. U svakom od razdoblja predstavit ćemo načine šifriranja i dešifriranja te uređaje koji su služili toj svrsi. Jonh Chadwick je rekao: *"Poriv za otkrivanje tajni duboko je utkan u ljudsku narav; čak i krajnje neradoznali um uzbuđuje misao da bi mogao doznati nešto što je drugima uskraćeno."* i to je upravo ono što je i nas zaintrigiralo kod kriptografije.

1. Stari vijek

U starom vijeku ljudi su kriptografiju smatrali mističnom znanošću. Povezivali su je s crnom magijom te mislili da se upotrebljava za komuniciranje sa zlim silama. Većina ranih kriptografa su bili znanstvenici. Ljudi su mislili da su oni sljedbenici sotone. Šifre koje su se koristile u starom vijeku su hijeroglifi, Cezarova šifra, Atbaš, Skytale, Polybiusov kvadrat i druge.

1.1. Hijeroglifi

Najstariji hijeroglifi potječu iz 3000. g. pr. Kr. Grčka riječ hieroglyphica znači "svete rezbarije" pa su kićeni simboli hijeroglifa bili idealni za zidove veličanstvenih hramova. Kroz povijest su postojali egipatski hijeroglifi i hijeroglifi starih Maya koji su se razlikovali jedni od drugih. Hijeroglifi su nađeni u području Turske, Krete, SAD-a, Kanade i Srednje Amerike, ali i u ostalim područjima. 1822. godine francuski arheolog J. F. Champollion je na temelju jednog trojezičnog natpisa uspio dešifrirati prvi niz fonetskih hijeroglifa.

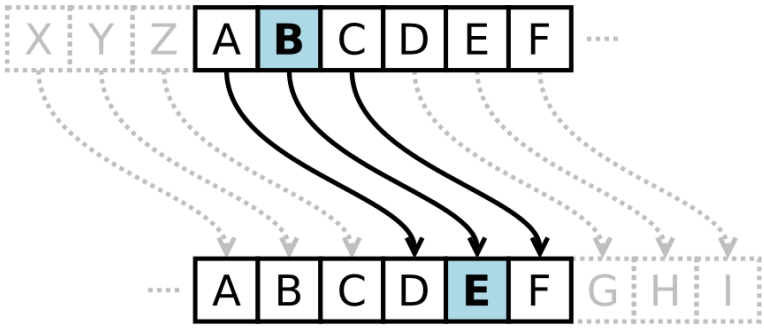


Slika 2: *Egipatski hijeroglifi*

Slika 3: *J. F. Champollion*

1.2. Cezarova šifra

Cezarova šifra je dobila ime po Juliju Cezaru, znamenitom rimskom vojskovođi, koji je koristio alfabet s lijevim pomakom od tri mjesta. To je jedan od najjednostavnijih i najrasprostranjenijih načina šifriranja u kriptografiji. Pošiljatelj i primatelj bi se unaprijed dogovorili da zamijene svako slovo otvorenog teksta odgovarajućim slovom abecede koje je pomaknuto za određeni broj mjesta. Na primjer, s pomakom 3, A se zamjenjuje slovom D, B slovom E itd., što je prikazano na Slici 4.



Slika 4: *Prikaz pomaka kod Cezarove šifre*

Julije Cezar koristio je ovu metodu za razmjenu poruka sa svojim generalima. Cezarova šifra koristi se kod složenijih načina šifriranja kao što je Vigenèreova šifra (o kojoj ćemo saznati nešto više kasnije u tekstu), a upotrebljava se i u sustavu "ROT13"(moderna kriptografija). Cezarova šifra lako se razbija i u praksi ne pruža nikakvu sigurnost u komunikaciji.

1.3. Atbaš

Atbaš je naziv za klasičnu šifru za hebrejsku abecedu i radi na principu supstitucijske šifre, tako što se prvo slovo abecede (aleph) zamijeni zadnjim slovom abecede (taw), drugo (beth) predzadnjim (shin) i tako redom. Atbaš je povezan s metodologijama židovskog misticizma kao što je Kabbalah - židovsko mistično učenje o Bogu i svijetu koje nastoji objasniti svijet na osnovi tumačenja brojčanih odnosa i tumačenja slova.

1.4. Skytale

Spartanci su 400-te god. pr. Kr. prvi upotrijebili kriptografiju u svrhu komunikacije. Koristili su štap zvan skytale, prvi kriptografski uređaj (Slika 5). Bio je to drveni štap oko kojeg se namotavala vrpca od papirusa kako bi se slale tajne poruke između grčkih ratnika. Poruka se pisala okomito te bi se nakon upisivanja poruke vrpca odmotala i na njoj bi bili izmješani znakovi. Kako bi primatelj mogao pročitati poruku morao je imati štap jednake debljine.

Slika 5: *Skytale*

1.5. Polybiusov kvadrat

Polybiusov kvadrat je kvadrat dimenzija 5×5 u koji se upisuju slova abecede (Slika 6). Redovi i stupci se označavaju brojevima od 1 do 5. Svako slovo predstavlja odgovarajući par (redak, stupac). Poruka se dešifrira tako da se svakom od parova pridruži odgovarajuće slovo abecede. Kod ovog sustava smanjen je broj simbola koji se koristi za kriptiranje.

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

Slika 6: *Polybiusov kvadrat*

Koristeći ovu šifru, riječ "kriptografija" bismo kriptirali na sljedeći način:

13 34 42 14 54 53 22 34 11 12 42 52 11.

2. Novi vijek

2.1. 16. stoljeće

U 16. stoljeću uočeno je da praksa korištenja jednog ključa za kriptiranje cijele poruke nije dobra pa se počinju koristiti šifre koje tijekom kriptiranja jednog teksta promijene nekoliko ključeva sa jasno istaknutim mjestima gdje se prethodni ključ promijenio.

2.1.1. Šifra s promjenjivim ključem

Njemački fratar Trithemius je 1518. godine napisao seriju od šest knjiga pod naslovom "Polygraphia". U petoj knjizi je razvio tablicu koju je nazvao "tabula recta", a koja je u svakom redu ponavljala abecedu tako da je abeceda u svakom sljedećem redu bila pomaknuta za jedan znak udesno. Šifriranje se vršilo tako da se prvo slovo poruke šifriralo prvim retkom tablice, drugo slovo drugim retkom itd.
Godine 1553. Giovanni Battista Belaso proširio je ovu tehniku uporabom ključne riječi koja se zapiše iznad otvorenog teksta i to tako da svako slovo ključa stoji iznad jednog slova otvorenog teksta. Ključna riječ se ponovno piše iznad svake riječi otvorenog teksta. Slovo ključne riječi koje je iznad slova otvorenog teksta određuje redak iz Trithemiusove tablice kojim ćemo šifrirati to slovo. Dakle, ako je slovo u otvorenom tekstu 'd', a iznad njega je slovo ključne riječi 'p', za šifriranje slova 'd' ćemo koristiti redak u Trithemiusovoj tablici koji počinje sa 'p'.

2.1.2. Vigenèreova šifra

Najpoznatiji kriptograf 16. stoljeća bio je Blaise de Vigenère (1523. - 1596.) koji je 1586. godine napisao "Traicte des Chiffres". U toj knjizi se nalazilo sve što se u to vrijeme znalo o kriptografiji (opisano je više polialfabetskih sustava). Vigenèreova šifra je metoda šifriranja otvorenog teksta korištenjem serije Cezarovih šifri, zasnovanih na slovima ključa. Ne služi se jednom ili dvjema šifriranim abecedama, nego poruku enkriptira pomoću njih 26. Prvi korak u šifriranju je crtanje Vigenèreova kvadrata (Slika 7). To je zapravo otvorena abeceda iza koje slijedi 26 šifriranih abeceda, pri čemu je svaka od njih pomaknuta za jedno slovo u odnosu na prethodnu.

Primjer 2.1. *Pogledajmo kako bismo šifrirali otvoreni tekst "grad na dravi" s ključnom riječi "SUNCE". Da bismo šifrirali slovo* ***g****, najprije odredimo ključno slovo iznad njega, a to je* ***S****. Ono određuje kojim ćemo se retkom u Vigenèreovom kvadratu poslužiti. Slovom* ***S*** *počinje redak 18 pa ćemo zamjensko slovo utvrditi pomoću te šifrirane abecede. Potražit ćemo sjecište stupca na čijem vrhu stoji slovo* ***g*** *i retka koji počinje sa* ***S****. Tako ćemo dobiti slovo* ***Y*** *pa ćemo njime u šifriranom tekstu zamijeniti slovo* ***g*** *u otvorenom tekstu (Slika 8). Postupak ponavljamo za svako iduće slovo naše poruke. Kada bismo odabrali dužu ključnu riječ, povećali bismo broj redaka koji sudjeluju u šifriranju i time povećali složenost šifre.*

2.2. 17. stoljeće

Francuz Antoine Rossignol (Slika 9) je 1628. godine pomogao svojoj vojsci da pobjedi Hugenote, pripadnike Protestantske reformističke crkve Francuske poznate i pod nazivom francuski kalvinisti, tako što je dešifrirao jednu poruku. Nakon toga je nastavio dešifrirati poruke za francusku vladu. Za dešifriranje poruka koristio je dvije liste: jednu u kojoj su elementi otvorenog teksta u poretku od a-z, a šifrirani elementi bez poretka, i drugu u kojoj

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Slika 7: *Vigenèreov kvadrat*

KLJUČNA RIJEČ	S	U	N	C	E	S	U	N	C	E	S
OTVORENI TEKST	g	r	a	d	n	a	d	r	a	v	i
ŠIFRIRANI TEKST	Y	L	N	F	R	S	X	E	C	Z	A

Slika 8: *Primjer šifriranja*

se vrši dešifriranje u kojoj su šifrirani elementi u poretku od a-z ili od manjih prema većim brojevima, a otvoreni tekst bez poretka. Nakon njegove smrti 1682. godine kriptografi u Francuskoj su organizirali tzv. "Mračne urede" o kojima ćemo reći nešto više u nastavku.

2.3. 18. stoljeće

"Mračni ured" je ime ureda gdje su pisma sumnjivih pošiljatelja otvarana, čitana te kopirana od strane javnih dužnosnika prije nego što stignu do primatelja. Bavili su se i dešifriranjem političkih i vojnih poruka. Dešifriranjem su se bavili pojedinci koje je to zanimalo te svećenici. Morali su to odrađivati tajno i oprezno kako se ne bi doznalo da su pisma otvarana. Bili su uobičajeni u Europi do 1700-tih. Iz 18. stoljeća imamo knjigu šifri te šifrarnik s kotačem.

2.3.1. Šifrarnik s kotačem

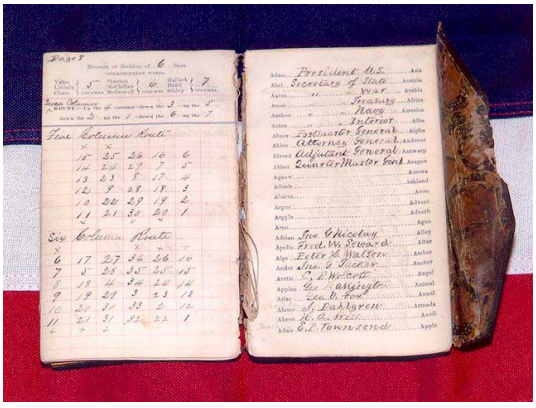
Šifrarnik s kotačem (Slika 10) izumio je Thomas Jefferson oko 1795. godine. To je sustav šifriranja pomoću niza kotača, svaki sa 26 slova abecede s nasumičnim poretkom. Svaki disk je označen jedinstvenim brojem. Rupa u središtu kotača omogućava njihovo slaganje na osovinu. Kotači se skidaju i mogu se montirati na osovinu bilo kojim redoslijedom. Redoslijed kotača je ključ za šifriranje, a pošiljatelj i primatelj moraju rasporediti kotače istim unaprijed definiranim redoslijedom. Okretanjem kotača dobila bi se poruka koju je pošiljatelj poslao primatelju.

Slika 9: *Antoine Rossignol*

Slika 10: *Šifrarnik s kotačem*

2.3.2. Knjige šifri

U knjigama šifri (Slika 11) svaka riječ otvorenog teksta zamijenila se brojem koji je označavao njezin položaj u knjizi. Na primjer, 5.2.4. značilo je 5. stranica, 2. red, 4. riječ. Pošiljatelj i primatelj morali su imati ne samo isu knjigu, nego isto izdanje te knjige.



Slika 11: *Knjiga šifri*

2.4. 19. stoljeće

Razvoj kriptografije je 1844. godine doživio drastične promjene zbog izuma telegrafa. Mnogi su se počeli interesirati za kriptografiju, ali su shvatili da tajnost algoritama koji su do

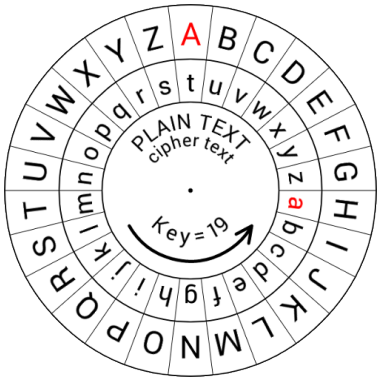
tad korišteni nije praktična zaštita sigurnosti poruke. Zapravo, shvatili su da bilo koja adekvatna kriptografska shema, uključujući šifre, treba ostati sigurna čak i ako protivnik sam u potpunosti razumije algoritam. Sigurnost ključa koji se koristio trebala je biti dovoljna za održavanje povjerljivosti. U 19. stoljeću se pojavljuju telegraf, sustav s dva diska te Playfairova šifra.

2.4.1. Telegraf

Komunikacija telegrafom nije bila sigurna pa su bile potrebne šifre za prijenos tajnih poruka. Zimmermanov telegraf služio je za tajnu komunikaciju između ministra vanjskih poslova njemačkog carstva, Arthura Zimmermana, s njemačkim ambasadorom u Meksiku, Heinrichom von Eckardtom. Telegram je sadržavao ponudu Meksiku da povrati svoj teritorij Novog Meksika, Teksasa i Arizone.

2.4.2. Sustav s dva diska

Sustav s dva diska ili Wadsworthovu šifru izumio je Decius Wadsworth, pukovnik vojske SAD-a. 1817. godine razvio je sustav šifriranja koji se temelji na šifrarniku s kotačem. Sadržavao je dva diska, jedan unutar drugog, pri čemu je vanjski disk imao 26 slova abecede i brojeve od 2 do 8, a unutarnji disk imao je samo 26 slova abecede (Slika 12). Kako bi se šifrirala poruka unutarnji disk se vrtio sve dok željeno slovo nije bilo na vrhu, s brojem okretaja potrebnim za prijenos šifriranog teksta. Wadsworth nikada nije dobio zasluge za svoj dizajn jer je Charles Wheatstone izumio gotovo identičan stroj nekoliko godina poslije te dobio sve zasluge.



Slika 12: *Sustav s dva diska*

2.4.3. Playfairov sustav

Playfairovu šifru su izumili Charles Wheatstone i Lyon Playfair 1854. godine i to je bio sustav koji je koristio parove znakova za šifriranje. Slučajan kvadrat 5 x 5 sadržavao je slova abecede, a tekst je bio podijeljen u parove. Kvadrat se konstruirao korištenjem ključne riječi.

2.4.4. Šest osnovnih zahtjeva za kriptografiju

Auguste Kerchoffs je u "La Cryptographie Millitare" ([12]) iz 1883. godine iznio šest osnovnih zahtjeva za kriptografiju:

1. Šifrani tekst treba biti neprobojan u praksi.

2. Sustav šifriranja treba biti prikladan za korisnike.
3. Ključ treba biti lako pamtljiv i promjenjiv.
4. Šifirani tekst treba biti prenosiv telegrafom.
5. Uređaj za šifriranje treba biti lako prenosiv.
6. Uređaj za šifriranje treba biti moguće relativno lako koristiti.

3. Suvremeno doba

3.1. 20. stoljeće

U prvoj polovici 20. stoljeća kriptografija se počela naglo razvijati. Napravljeni su prvi elektromehanički uređaji za šifriranje. To je omogućilo brže i lakše šifriranje poruka. Uređaji su koristili iste principe šifriranja koji su se i prije koristili. Nakon izuma prvih osobnih računala, 1970-ih godina, razvijeni su simetrični kriptografski algoritmi koji predstavljaju početak moderne kriptografije. Nedugo nakon razvoja simetričnih algoritama razvijeni su i algoritmi javnog ključa koji osim šifriranja omogućuju i digitalno potpisivanje poruka.

3.1.1. Enigma

Njemački izumitelj Arthur Scherbius i njegov bliski prijatelj Richard Ritter osnovali su 1918. godine trgovačko društvo Scherbius und Ritter, u kojemu je Scherbius bio zadužen za istraživanje i razvoj. Jedna od njegovih ideja bila je da tradicionalne kodove i šifre zamijeni enkripcijom koja bi iskoristila tehnologiju 20. stoljeća. Razvio je kriptografski stroj zvan Enigma (Slika 13). Enigma se sastojala od tipkovnice kojom se tipkao otvoreni tekst, ploče sa žaruljicama na kojoj se prikazuju rezultirajuća slova šifriranog teksta i razvodne ploče na kojoj je bilo moguće zamijeniti mjesta unutar više od šest parova slova. Oblikom je izgledala kao pisaći stroj, dimenzija $35 \times 28 \times 40$ cm i težine 12 kg. U Drugom svjetskom ratu matematičar Alan Turing sagradio je stroj kojim je otkrio najveću Enigminu slabost i onda je nemilosrdno iskoristio. Zahvaljujući upravo njemu postalo je moguće razbiti Enigmine šifre čak i u najtežim slučajevima.

Slika 13: *Enigma*

3.1.2. Sigaba

Sigaba je američki stroj za šifriranje koji radi na temelju elektromehaničkih rotora (Slika 14). Razvijen je 1937. godine od strane američke vojske i mornarice s namjerom da komunikacija između dvije strane bude apsolutno sigurna. Korišten je u Drugom svjetskom ratu i bio je toliko pouzdan da je korišten sve do pedesetih godina 20. stoljeća. Koliko je poznato, ovaj sustav nikada nije bio probijen od strane neprijatelja.

Slika 14: *Sigaba*

3.2. Moderna kriptografija

Kriptografija je danas svuda oko nas. Sigurnosni mehanizmi koji se oslanjaju na kriptografiju su sastavni dio gotovo svakog računalnog sustava. Kriptografske metode se koriste za kontrolu pristupa operacijskim sustavima te kako bi se spriječio pristup poslovnim tajnama ukoliko nam netko ukrade prijenosno računalo. Ukratko, kriptografija je prešla iz jednog oblika umjetnosti koja se bavila tajnim komunikacijama vojske u znanost koja pomaže osigurati sustave običnim ljudima. Imamo formalnu definiciju kriptosustava:

Definicija 3.1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Kriptosustave **klasificiramo** obzirom na tri kriterija:

1. **Tip operacija koje se koriste pri šifriranju**
   Ovdje imamo **supstitucijske šifre** u kojima se svaki element otvorenog teksta zamjenjuje nekim drugim elementom (npr. TAJNA - XIWOI) i **transpozicijske šifre** u kojima se elementi otvorenog teksta permutiraju (npr. TAJNA - JANAT).

2. **Način na koji se obrađuje otvoreni tekst**
   Tu imamo **blokovne šifre** kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ i **protočne šifre** kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći niz ključeva koji se paralelno generira.

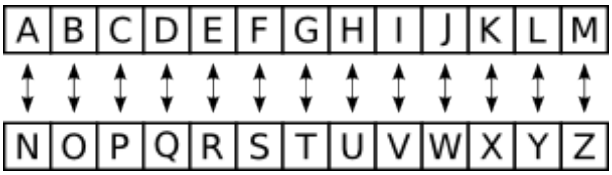
3. **Tajnost i javnost ključeva**
   Ovdje razlikujemo **simetrične kriptosustave** kod kojih se ključ za dešifriranje može

izračunati poznavajući ključ za šifriranje (ključevi su najčešće identični) i **kriptosustave s javnim ključem** kod kojih bilo tko može šifrirati poruku pomoću javnog ključa, ali ju dešifrirati može samo osoba koja ima tajni ključ.

U nastavku ćemo spomenuti samo neke od modernih kriptosustava. Više detalja o njima i o drugim poznatim kriptosustavima kao što su npr. ElGamalov, Rabinov, Merkle-Hellmanov i McElieceov može se naći u [7].

3.2.1. ROT13

ROT13 je supstitucijska šifra koja se bazira na cikličkom rotiranju slova engleske abecede za 13 mjesta u desno, tj. A se zamjenjuje slovom N, B se zamjenjuje slovom O itd, što je prikazano na Slici 15. ROT13 je zapravo poseban slučaj Cezarove šifre. Dvije primjene ROT13 daju ponovno polazni tekst i zbog toga nije pogodan za ozbiljnije šifriranje, ali koristio se od početka 1980-ih godina za prikrivanje uvredljivog sadržaja i rješenja zagonetki te za sprječavanje pristupa djece neprikladnim sadržajima.



Slika 15: *ROT13*

3.2.2. DES šifra

U modernoj kriptografiji koristi se šifriranje javnim ključem. Primjer je IBM-ova DES šifra. Ovaj algoritam je u prvotnom izdanju koristio ključ dugačak 56 bitova. Jedinstveno je definirao matematičke korake potrebne za transformaciju podataka u kriptografsku šifru te također transformaciju šifre u izvorni oblik. Danas se DES šifra zbog kratkog ključa smatra nesigurnom i više se ne koristi. Zamijenio ju je kriptosustav imena Advanced Encryption Standard [4]. AES je simetričan kriptosustav, radi sa 128-bitnim blokovima i ključevima duljine 128, 192 i 256 bitova.

3.2.3. RSA kriptosustav

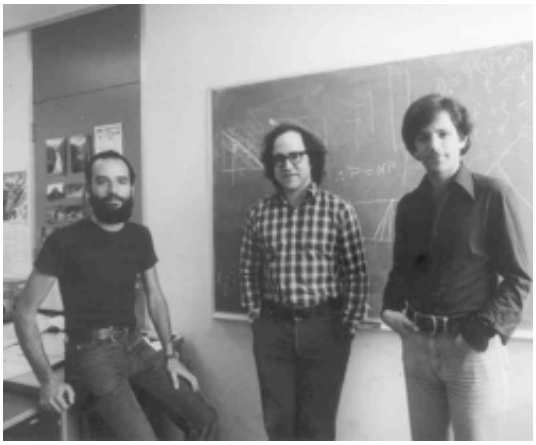
Najpopularniji i najšire korišteni kriptosustav s javnim ključem je RSA kriptosustav. Nastao je 1977. godine, a ime je dobio prema matematičarima Ronu Rivestu, Adi Shamiru i Lenu Adlemanu (Slika 16). Sigurnost RSA kriptosustava zasnovana je na teškoći faktorizacije velikih prirodnih brojeva. U nastavku ćemo detaljnije opisati ovaj kriptosustav i na primjeru pokazati njegovu primjenu.

Definicija 3.2. *Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je*

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

i neka je

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq,\ p \text{ i } q \text{ prosti}\},$$



Slika 16: *Rivest, Shamir i Aldeman*

$$de \equiv 1 \bmod \varphi(n)),$$

gdje je $\varphi(n)$ *Eulerova funkcija koja prirodnom broju* n *pridružuje broj prirodnih brojeva manjih od* n*, koji su relativno prosti s* n*. Za* $K = (n, p, q, d, e) \in \mathcal{K}$ *definiramo*

$$e_K(x) \equiv x^e \bmod n,$$

$$d_K(y) \equiv y^d \bmod n,$$

gdje su $x, y \in \mathbb{Z}_n$*.*
Vrijednosti n *i* e *su javne, a vrijednosti* p*,* q *i* d *tajne.*

RSA kriptosustav se primjenjuje na sljedeći način:

1. Odaberemo tajno dva velika različita prosta broja p i q od oko 100 znamenaka. To radimo tako da pomoću nekog generatora slučajnih brojeva generiramo prirodan broj m s traženim brojem znamenaka, a zatim korištenjem nekog testa za testiranje prostosti tražimo prvi prosti broj veći ili jednak broju m.

2. Računamo $n = pq$ i $\varphi(n) = (p-1)(q-1)$.

3. Odaberemo na slučajan način broj e takav da je $e < \varphi(n)$ i $(\varphi(n), e) = 1$. Zatim tajno računamo d tako da je $de \equiv 1 \bmod \varphi(n)$, tj. $d \equiv e^{-1} \bmod \varphi(n)$. Broj d određuje se pomoću proširenog Euklidovog algoritma koji za dane a i b računa $b^{-1} \bmod a$.

4. Stavimo ključ za šifriranje (n, e) u javni direktorij.

Primjer 3.1. *Simulirajmo kako Ana šalje poruku* GRAD NA DRAVI *Ivi i kako ju on dešifrira. Ivo bira* $p = 43$ *i* $q = 59$ *i računa*

$$\begin{aligned} n &= pq = 2537, \\ \varphi(n) &= (p-1)(q-1) = 2436. \end{aligned}$$

Zatim odabere $e = 17$ *i pomoću proširenog Euklidovog algoritma računa* d *takav da je*

$$de \equiv 1 (\bmod \varphi(n))$$

i dobiva da je $d = 1433$. *Vrijednosti* p, q, d *zadržava za sebe, a* n *i* e *šalje Ani ili ih jednostavno upisuje u javni direktorij. Ana želi poslati poruku* GRAD NA DRAVI, *čiji je numerički ekvivalent*

$$x = 07180104001401000418012209.$$

jer je razmak $= 00, A = 01, B = 02, \ldots, Y = 25, Z = 26$.
Kako je $x > n$, x *se razbija u četveroznamenkaste blokove, počevši s lijeve strane. Zadnji blok, ukoliko mu nedostaje znamenki, se dopuni nulama. Sada je*

$$\begin{aligned} x &= (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \\ &= (0718, 0104, 0014, 0100, 0418, 0122, 0900). \end{aligned}$$

Poznavajući Ivine javne $n = 2451$ *i* $e = 17$, *Ana računa*

$$\begin{aligned} y_1 &\equiv 718^{17} \bmod 2537 \equiv 2427 \\ y_2 &\equiv 104^{17} \bmod 2537 \equiv 2140 \\ y_3 &\equiv 14^{17} \bmod 2537 \equiv 2403 \\ y_4 &\equiv 100^{17} \bmod 2537 \equiv 2188 \\ y_5 &\equiv 418^{17} \bmod 2537 \equiv 744 \\ y_6 &\equiv 122^{17} \bmod 2537 \equiv 2328 \\ y_7 &\equiv 900^{17} \bmod 2537 \equiv 920. \end{aligned}$$

Dobiveni šifrat

$$\begin{aligned} y &\equiv (y_1, y_2, y_3, y_4, y_5, y_6, y_7) \\ &\equiv (2427, 2140, 2403, 2188, 0744, 2328, 0920) \\ &\equiv 24272140240321880744232800920 \end{aligned}$$

šalje Ivi. Ivo pomoću $d = 1433$, *koji je samo njemu poznat, računa, na isti način dijeleći* y *na blokove,*

$$x_i \equiv y_i^{1433} \bmod 2537, \quad i = 1, 2, \ldots, 7$$

i dobiva originalnu poruku GRAD NA DRAVI.

3.2.4. Kriptosustavi koji koriste eliptičke krivulje

Kriptografija eliptičkih krivulja (engl. **ECC** - Elliptic curve cryptography) je kriptosustav s javnim ključem koji se bazira na algebarskim strukturama nad konačnim poljima. Prednost ovog kriptosustava je što on za jednaku sigurnost kriptiranja zahtjeva manju duljinu ključa u usporedbi s drugim kriptosustavima s javnim ključem ([5]).

3.2.5. NTRU kriptosustav

Jeffrey Hoffstein, Jill Pipher i Joseph H. Silverman su 1997. predložili NTRU (Number Theory Research Unit, Number Theorists aRe Us, N-th degree truncated polynomial ring) kriptosustav. U ovom se kriptosustavu kod šifriranja koristi $R = \mathbb{Z}[X]/(X^n - 1)$. Jedna od prednosti NTRU kriptosustava je ta što se u ovom kriptosustavu šifriranje i dešifriranje obavlja brže nego u RSA kriptosustavu.

3.2.6. Kvantna računala i kriptografija

Kvantna računala su računala koja za računanje koriste kvantnomehaničke principe. Iako razvoj kvantnih računala ide dosta sporo, u današnje vrijeme vodeće korporacije ulažu sve više sredstava u njihov razvoj te se očekuje da će ona uskoro biti i realizirana na način da se iskoristi njihov potencijal. Dokazano je da bi u slučaju konstrukcije dovoljno jakih kvantnih računala npr. RSA kriptosustav i ECC bili neupotrebljivi dok se čini da bi npr. NTRU kriptosustav mogao ostati siguran. Stoga je razvoj kvantnih računala motivacija za dodatno proučavanje poznatih i uvođenje novih kriptosustava. Tako je posljednjih godina proveden značajan broj istraživanja vezanih uz tzv. kvantnu kriptografiju. Kvantna kriptografija omogućuje sigurnu razmjenu kriptografskog ključa između dvije strane. Ona koristi kvantna stanja fotona za prijenos kriptografskog ključa pomoću polariziranih fotona kako bi prikazala bitove 0 ili 1. Svaki foton, poznatiji kao Qubit, prenosi jedan dio kvantne informacije. Za primanje takvih kvantnih bitova, primatelj mora odrediti polarizaciju fotona. Foton će u tom prijenosu nepovratno mijenjati informacije šifrirane na njemu čime se detektira bilo kakvo kršenje sigurnosti. Metoda kod koje se tajni ključ dodjeljuje upotrebom kvantne kriptografije naziva se Quantum Key Distribution (QKD).

Literatura

[1] D. J. Bernstein, J. Buchmann, E. Dahmen *Post-quantum cryptography*, Springer, Berlin, 2009.

[2] F. Cohen, *A Short History of Cryptography*, 1990.
URL: `http://all.net/edu/curr/ip/Chap2-1.html`

[3] H. Čavrak, *Enigma*, Hrvatski matematički elektronski časopis, **3**(2004).
URL: `http://e.math.hr/enigma/index.html`

[4] J. Daemen, V. Rijmen *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, Berlin-Heidelberg, 2002.

[5] A. Dujella, *Eliptičke krivulje u kriptografiji*, PMF-MO, Sveučilište u Zagrebu, 2013.
URL: `https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf`

[6] A. Dujella, *Vigenèreova šifra*, Hrvatski matematički elektronski časopis, **1**(2004).
URL: `http://e.math.hr/vigenere/index.html`

[7] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[8] A. Galinović, *Povijest kriptografije*, FER, Sveučilište u Zagrebu, 2005.
URL: `http://web.zpr.fer.hr/ergonomija/2005/galinovic/index.html`

[9] A. S. Gangadeen, *History of Cryptography*
URL: `https://www.supinfo.com/articles/single/1730-history-of-cryptography-part-1#idm140445266400224`

[10] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list, **5**(2005), 101–112.

[11] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, 2007.
URL: `https://repo.zenk-security.com`

[12] A. Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, **9**(1883), 5–38, 161–191.

[13] F. S. Mammadov, *History of cryptography*
URL: `http://old.staff.neu.edu.tr/~fahri/cryptography_Chapter_1.pdf`

[14] I. Matić, *Uvod u teoriju brojeva*, Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2015.

[15] M. Murphy, *IBM thinks it's ready to turn quantum computing into an actual business*
URL: `https://qz.com/924433/ibm-thinks-its-ready-to-turn-quantum-computing-into-an-actual-business/`

[16] S. Singh, *Šifre, kratka povijest kriptografije*, Mozaik knjiga, Zagreb, 2003.

[17] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, Wiley Publishing, Indianapolis, 2008.

[18] *History of Cryptography*,Thawte Inc., 2013.
URL: `http://book.itep.ru/depository/crypto/Cryptography_history.pdf`

[19] U.S. National Security Agency, *Commercial National Security Algorithm Suite and Quantum Computing*, 2016.
URL: https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

[20] S. Wijesekera, *Quantum Cryptography for Secure Communication in IEEE 802.11 Wireless Networks*, 2011.
URL: http://www.canberra.edu.au/researchrepository/file/8d7d9273-886b-6270-1793-fd1b4d74deaf/1/full_text.pdf

[21] *Kriptografija*,
URL: https://hr.wikipedia.org/wiki/Kriptografija