ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.3 (2020) 37–53

Osnove kriptografije

Josipa Barić, Ivana Grgić, Iva Jurić

Sažetak

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. U klasičnu kriptografiju ubrajamo šifre poput Cezarove i Vigenèreove koje predstavljaju način šifriranja podataka korištenjem tajnog privatnog ključa poznatog samo krajnjim osobama u komunikaciji. Do drastične promjene u kriptografiji dolazi 1976. godine kada se pojavljuju prvi sustavi s javnim ključem pomoću kojih se poruka može sigurno prenijeti bez posrednika u komunikaciji. RSA i Rabinov kriptosustav predstavljaju prve takve sustave zasnovane na problemu faktorizacije. Kriptosustavi s javim ključem imaju primjenu u različitim poljima digitalnog života. U ovom radu ćemo objasniti osnovna načela kriptografije i njene matematičke zakonitosti, te potkrijepiti to raznim primjerima i zanimljivostima.

Ključni pojmovi: kriptosustav, ključ, šifrat, otvoreni tekst, RSA

1 Klasična kriptografija–osnovni pojmovi

Riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao tajnopis.

Kriptografija je znanstvena disciplina koja se bavi problemom prijenosa informacije putem nesigurnog komunikacijskog kanala između pošiljatelja i primatelja. Moderna kriptografija počiva na disciplinama kao što su matematika, računarstvo, elektrotehnika, komunikacijske tehnologije i fizika. Primjene kriptografije uključuju internetsku trgovinu, sustav platnih kartica zasnovanih na čipovima, digitalne valute, računarske

lozinke i vojne komunikacije.

Zadatak je jednostavan: zaštititi informaciju od tzv. „treće osobe". Originalna poruka mora biti poznata samo pošiljatelju i primatelju.

Poruka koju pošiljatelj želi poslati u kriptografiji se naziva *otvoreni tekst*. Kako bi zaštitio sadržaj poruke, pošiljatelj će preoblikovati otvoreni tekst pomoću već dogovorenog *ključa*. Taj postupak naziva se *šifriranje*, a rezultira *šifriranom porukom*, odnosno *šifratom* ili *kriptogramom*. Šifrat se zatim šalje primatelju. Protivnik pokušava presresti poruku i različitim metodama otkriti njeno značenje. Za razliku od protivnika, primatelj zna ključ po kojem je poruka šifrirana pa može dešifrirati šifrat i na taj način doći do originalne poruke, odnosno otvorenog teksta. Poželjno je da ključ bude što složeniji i samim time šifrat što sigurniji.

Za razliku od dešifriranja, *kriptoanaliza* ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. *Kriptologija* je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.

Sve navedeno čini sustav koji funkcionira po strogo određenim pravilima definiranima kriptografskim algoritmom, odnosno šifrom. *Šifra* ili *kriptografski algoritam* je matematička funkcija koja se koristi za šifriranje i dešifriranje (obično su to dvije funkcije od kojih jedna služi za šifriranje, a druga za dešifriranje). Te funkcije preslikavaju elemente otvorenog teksta u elemente šifrata i obratno.

Nakon što smo upoznali osnovne pojmove definirat ćemo pojam *kriptosustava*.

Definicija 1. *Kriptosustav je uređena petorka* $(\alpha, \sigma, \kappa, \varepsilon, \phi)$ *za koju vrijedi:*

a) α *je konačan skup svih mogućih osnovnih elementa otvorenog teksta,*

b) σ *je konačan skup svih mogućih osnovnih elemenata šifrata,*

c) κ *je prostor ključeva, tj. konačan skup svih mogućih ključeva,*

d) za svaki $K \in \kappa$ *postoji funkcija šifriranja* $e_K \in \varepsilon$ *i odgovarajuća funkcija dešifriranja* $d_K \in \phi$. *Pritom su* $e_K : \alpha \to \sigma$ *i* $d_K : \sigma \to \alpha$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$, *za svaki otvoreni tekst* $x \in \alpha$.

Kriptosustave obično klasificiramo s obzirom na sljedeća tri kriterija:

Tip operacija koje se koriste pri šifriranju

Tako razlikujemo *supstitucijske* šifre u kojima se svaki element

otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje s nekim drugim elementom, te *transpozicijske* šifre u kojima se elementi otvorenog teksta permutiraju (premještaju). Npr. ako riječ TAJNA šifriramo u XIWOI, načinili smo supstituciju, a ako je šifriramo u JANAT, načinili smo transpoziciju. Postoje također i kriptosustavi koji kombiniraju ove dvije metode.

Način na koji se obrađuje otvoreni tekst

Ovdje razlikujemo *blokovne* šifre, kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ K, te *protočne* šifre (engl. stream cipher) kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom niz ključeva (engl. keystream) koji se paralelno generira.

Tajnost i javnost ključeva

Ovdje je osnovna podjela na *simetrične* kriptosustave tj. kriptosustave s tajnim ključem i *asimetrične* kriptosustave tj. kriptosustave s javnim ključem. Kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno. Ustvari, najčešće su ovi ključevi identični. Sigurnost ovih kriptosustava leži u tajnosti ključa. Kod kriptosustava s javnim ključem ili asimetričnih kriptosustava, ključ za dešifriranje se ne može (barem ne u nekom razumnom vremenu) izračunati iz ključa za šifriranje. Ovdje je ključ za šifriranje javni ključ. Naime, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku.

2 Kriptosustavi s tajnim ključem (simetrični kriptosustavi)

U nastavku ćemo opisati neke primjere kriptosustava s tajnim ključem.

2.1 Cezarova šifra

O tome iz kojeg vremena datira pojava kriptografije govori nam i činjenica da je supstitucijsku šifru koristio rimski vojskovođa Gaj Julije Cezar. Radi se o tzv. pomaknutoj šifri koja radi po principu da se svako slovo abecede zamijeni slovom koje je za tri mjesta ispred tog slova u abecedi. Cezarovu šifru možemo jednostavno opisati sljedećom tablicom.

Na primjer, riječ *GLAD* bit će supstituirana riječju *JODG*.

otvoreni tekst	A	B	C	D	E	F	G	H	I	J	K	L	M	...
šifrat	D	E	F	G	H	I	J	K	L	M	N	O	P	...

Da bismo Cezarovu šifru precizno definirali u smislu Definicije 1, uvest ćemo prirodnu korespodenciju između slova alfabeta (A – Z) i cijelih brojeva (0 – 25).

Skup $\{0, 1, 2, \ldots, 25\}$ označavat ćemo s $\mathbb{Z}_{26}$ i predstavljat će nam skup ostataka pri dijeljenju s brojem 26. Pretpostavit ćemo da su na njemu definirane operacije zbrajanja, oduzimanja i množenja na način da računamo kao u skupu cijelih brojeva, ali tako da rezultat (ukoliko nije iz skupa $\{0, 1, 2, \ldots, 25\}$) na kraju zamijenimo njegovim ostatkom pri dijeljenju s 26 što nazivamo računom *po modulu* 26. Koristit ćemo oznake: $(a+b) \bmod 26$ ili $a +_{26} b$ za zbrajanje po modulu 26, te analogne oznake za oduzimanje i množenje.

Npr. $(10 + 20) \bmod 26 = 30 - 26 = 4$, $(10 - 20) \bmod 26 = -10 + 26 = 16$. Skup $\mathbb{Z}_{26}$, uz operacije zbrajanja i množenja po modulu 26, zadovoljava aksiome matematičke strukture koja se naziva *prsten*. To znači da su operacije zbrajanja i množenja zatvorene (rezultat je ponovo iz skupa $\mathbb{Z}_{26}$), komutativne ($a +_{26} b = b +_{26} a$, $a \cdot_{26} b = b \cdot_{26} a$) i asocijativne ($(a +_{26} b) +_{26} c = a +_{26} (b +_{26} c)$, $(a \cdot_{26} b) \cdot_{26} c = a \cdot_{26} (b \cdot_{26} c)$) i vrijedi distributivnost množenja prema zbrajanju ($a \cdot_{26} (b +_{26} c) = a \cdot_{26} b +_{26} a \cdot_{26} c$).

U sljedećoj definiciji definiramo funkcije šifriranja i dešifriranja za Cezarovu metodu.

Definicija 2. *Neka je* $\alpha = \sigma = \kappa = \mathbb{Z}_{26}$. *Za* $0 \leqslant K \leqslant 25$ *definiramo* $e_K(x) = (x + K) \bmod 26$ *i* $d_K(y) = (y - K) \bmod 26$.

Šifra je definirana nad skupom $\mathbb{Z}_{26}$ jer promatramo skup od 26 slova abecede. K je ključ i određuje za koliko mjesta udesno ćemo pomicati slova pri šifriranju.

Primjer 3. *Želimo odrediti otvoreni tekst poruke DRERNI, šifrirane Cezarovom šifrom.*
Radi se o engleskoj abecedi što znači da ključ K može poprimiti jednu od 26 mogućih vrijednosti. Isključivo zbog tako malog broja mogućih ključeva, primjer ćemo riješiti „grubom silom" tj. povećavat ćemo vrijednost ključa sve dok ne dođemo do otvorenog teksta.

Kao što je vidljivo u gornjoj tablici, nakon određenog broja koraka dolazimo do otvorenog teksta. Ključ je $K = 4$, odnosno otvoreni tekst ZNANJE.

D	R	E	R	N	I
C	Q	D	Q	M	H
B	P	C	P	L	G
A	O	B	O	K	F
Z	N	A	N	J	E

2.2 Vigenèreova šifra

Cezarova je šifra, zbog svoje jednostavnosti, vrlo brzo odgonetnuta. Korak naprijed napravio je francuski kriptograf Blaise de Vigenère osmislivši šifru kod koje se svaki znak u tekstu može preslikati u jedno od n mogućih slova (gdje je n duljina ključa). Vigenèreova šifra je, u to vrijeme, bila toliko efikasna da su je prozvali *„le chiffre indechiffrable"* (nerazmrsiva šifra) i razbijena je tek 300 godina nakon što je prvi put korištena. Tajna je bila u tome što je umjesto jedne šifrirane abecede koristila čak njih 26. Kao pomoć pri šifriranju ovom metodom može se koristiti Vigenèreov kvadrat prikazan na Slici 1.

	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 1: Vigenèreov kvadrat

U Vigenèreovom kvadratu gornji redak predstavlja svih 26 slova engleske abecede. Ispod svakog slova nalazi se drugačije šifrirana abeceda tj. svaka je pomaknuta za jedno slovo u odnosu na prethodnu abecedu. Složenost ove šifre je u tome što osoba može, na primjer, prvo slovo šifrirati pomoću abecede 5. retka, drugo slovo pomoću abecede 12. retka, treće slovo pomoću 7. retka, itd. Kako bi osoba znala koji redak koristiti, Vigenère uvodi ključnu riječ (odnosno ključ) koja je poznata isključivo primatelju i pošiljatelju.

Definicija 4. *Neka je n fiksan prirodan broj i $\alpha = \sigma = \kappa = (\mathbb{Z}_{26})^n$. Za ključ $K = (k_1, k_2, ..., k_n)$, definiramo:*

$$e_K(x_1, x_2, \ldots, x_n) = (x_1 +_{26} k_1, x_2 +_{26} k_2, ..., x_n +_{26} k_n),$$
$$d_K(y_1, y_2, \ldots, y_n) = (y_1 -_{26} k_1, y_2 -_{26} k_2, \ldots, y_n -_{26} k_n).$$

Slova otvorenog teksta pomičemo za $k_1, k_2, \ldots$ ili k_n mjesta, u ovisnosti o tome na kojem se mjestu u otvorenom tekstu nalaze (pomak ovisi o ostatku koji dobijemo kada poziciju slova podijelimo s duljinom ključa n).

Primjer 5. *Korištenjem ključa ARISTOTEL, odrediti šifrat poruke NADAJEBUDANSAN.*
Zaključujemo da je $n = 9$, $K = (26, 17, 8, 18, 19, 14, 19, 4, 11)$. Brojčano je otvoreni tekst predstavljen s $(13, 26, 3, 26, 9, 4, 1, 20, 3, 26, 13, 18, 26, 13)$. Pošto se radi o blokovnoj šifri ključ se ponavlja sve dok se ne „pokriju" *sva slova otvorenog teksta. Zbrajamo brojčane vrijednosti ključa sa šiframa otvorenog teksta po modulu 26 i dobivamo brojčane vrijednosti šifrata kao u sljedećoj tablici.*

ključ	26	17	8	18	19	14	19	4	11	26	17	8	18	19
ot. tekst	13	26	3	26	9	4	1	20	3	26	13	18	26	13
šifrat	13	17	11	18	2	18	20	24	14	26	4	26	18	6

Numeričke vrijednosti šifrata prevodimo u slova pomoću Vigenèreovog kvadrata i dobivamo konačan rezultat: NRLSCSUYOAEASG.

Cezarova i Vigenèreova šifra su se najviše koristile u vojne i diplomatske svrhe. Razvojem računala i financijskih transakcija kriptografija postaje zanimljiva većem broju korisnika te se pojavljuje potreba uvođenja standarda u kriptografiji. Tako je 1976. godine nastao moderni simetrični blokovni kriptosustav Data Encryption Standard (DES) koji šifrira otvoreni tekst (blokove) duljine 64 bita koristeći ključ K duljine 56 bitova. Na taj način dobiva se šifrat koji ponovno ima 64 bita. Razbijanje DES-a se dogodilo 1998. godine (nedovoljna duljina ključa

za neke aplikacije), te ga zamjenjuje Advanced Encryption Standard (AES). AES je danas najpopularniji standard za simetrično kriptiranje, ima blokove veličine 128 bita te ključeve veličine 128, 192 ili 256 bita. Simetrični kriptosustavi se i danas koriste kao dio SSL i TLS protokola koji omogućuju aplikacijama sigurnu komunikaciju preko internet mreže (primjena u autentifikaciji poslužitelja, udaljenom pristupu resursima, osiguravanje poruka elektroničke pošte i sl.).

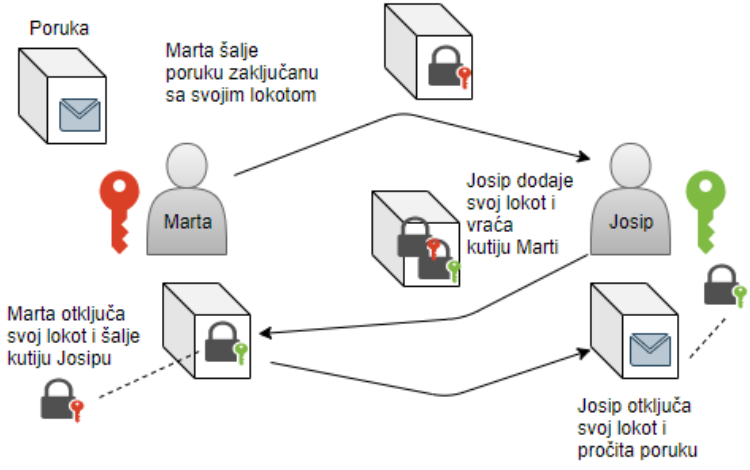
3 Kriptosustavi s javnim ključem (asimetrični kriptosustavi)

Simetrični sustavi, odnosno sustavi s tajnim ključem, uz neke svoje prednosti (velika brzina prijenosa podataka, relativno kratki ključevi) imaju i mnogo nedostataka. Održavati ključ tajnim jedna je od najvećih mana takvih sustava. Problem se povećava što je udaljenost između pošiljatelja i primatelja veća zbog nesigurnih komunikacijskih kanala kojima ključ putuje ili zbog potrebe da se osobe fizički sastanu kako bi razmijenile ključeve. Osim toga, ključevi se trebaju redovito mijenjati.

Problem sigurne distribucije ključa mučio je kriptografe kroz čitavu povijest. Do revolucije u kriptografiji dolazi razvojem kriptosustava s javnim ključem. Kriptografi Whitfield Diffie i Martin Hellman su 1976. godine predložili algoritam za razmjenu ključeva preko nesigurnog komunikacijskog kanala, čija je sigurnost bila zasnovana na teškoći nalaženja diskretnog logaritma. To u suštini nije kriptosustav, ali je predstavljao ideju za novu klasu kriptosustava kao što su asimetrični kriptosustavi ili kriptosustavi s javnim ključem. Ideja se sastojala u tome da je iz funkcije za šifriranje e_K praktično nemoguće, u nekom razumnom vremenu, izračunati funkciju za dešifriranje d_K. U tom slučaju bi funkcija za šifriranje e_K mogla biti javna.

U sljedećem jednostavnom primjeru ćemo pokazati da se poruka može sigurno prenijeti bez posrednika u komunikaciji na čemu se zasniva ideja asimetričnog kriptografskog sustava.

Primjer 6. *Marta i Josip komuniciraju putem poštara. Poštar, nažalost, čita sva njihova pisma i zbog toga odluče zaštiti svoje podatke. Marta stavi svoje pismo u željeznu kutiju i zaključa je lokotom. Jedino Marta ima ključ svog lokota. Kada kutija dođe do Josipa, Josip nema ključ lokota, ali ima svoj lokot. Josip stavlja svoj lokot na kutiju, zaključa je svojim ključem i ponovno ju šalje Marti. Marta sada otključava svoj lokot, ali na kutiji ostaje Josipov lokot te ga Marta ponovno proslijedi Josipu. Na taj način Marta i Josip prevare poštara (Slika 2).*



Slika 2: Tok komunikacije u asimetričnom sustavu

Kako bismo preciznije opisali ovakav kriptosustav potrebno je poznavati pojmove grupe, cikličke grupe i konačne grupe, stoga ćemo dati njihove definicije.

Definicija 7. *Grupa $(G, *)$ je skup G s binarnom operacijom $*$, koja zadovoljava sljedeće aksiome:*

- ***zatvorenost**: za sve a, b iz G, rezultat $a * b$ je također u G,*
- ***asocijativnost**: za sve a, b, c iz G, vrijedi $(a * b) * c = a * (b * c)$,*
- ***neutralni element**: postoji element e iz G, takav da za svaki a iz G, vrijedi $e * a = a * e = a$ i nazivamo ga neutralni element,*
- ***inverz**: za svaki a iz G, postoji element b iz G, takav da je $a * b = b * a = e$, gdje je e neutralni element.*

Grupa $(G, *)$ je Abelova grupa (prema norveškom matematičaru Nielsu Abelu) ako je operacija $*$ komutativna, odnosno, za svaki a, b iz G vrijedi $a * b = b * a$.

Za grupu G kažemo da je *ciklička* grupa ako se njeni elementi mogu generirati uzastopnom primjenom operacije koja definira grupu, primijenjene na samo jedan element te grupe. Taj element naziva se *generator* grupe.

Na primjer, ciklička grupa koja se često koristi je multiplikativna grupa $\mathbb{Z}_p^*$ svih ne-nula ostataka modulo p, gdje je p dovoljno velik prost broj. Generator grupe $\mathbb{Z}_p^*$ naziva se *primitivni korijen modulo p*. Broj $g \in \{1, 2, \ldots, p-1\}$ je primitivni korijen modulo p ako je g^{p-1} najmanja potencija broja g koja daje ostatak 1 pri dijeljenju s p. Najmanji cijeli broj x za kojeg vrijedi $a \cdot x \equiv 1 (\bmod p)$ naziva se *multiplikativni inverz* od a modulo p.

Definicija 8. *Neka je $(G, *)$ grupa i H podskup skupa G. Kažemo da je H podgrupa od G i pišemo $H \leq G$ ako je $(H, *)$ također grupa.*

Neka je G konačna Abelova grupa. Kako bi bila prikladna za primjenu u kriptografiji javnog ključa, grupa bi trebala imati svojstvo da su operacije množenja i potenciranja u njoj jednostavne, dok bi logaritmiranje, kao inverzna operacija operacije potenciranja, bilo vrlo teško.

U sljedećoj definiciji opisujemo problem diskretnog logaritma.

Definicija 9. *Neka je $(G, *)$ konačna grupa (tj. ima konačno mnogo elemenata) i $g, h \in G$. Neka je g^x oznaka za $g * g * \ldots * g$ (x puta) i $H = \{g^i : i \geq 0\}$ podgrupa od G generirana elementom g. Najmanji nenegativni cijeli broj x, takav da je $h = g^x$, naziva se diskretni logaritam i označava s $log_g h$.*

S $|G|$ ćemo označiti broj elemenata konačne grupe G tj. red grupe G.

U konačnoj multiplikativnoj grupi G reda $|G| = n$, za svaki b iz G i svaki x iz $\mathbb{Z}$ lako je izračunati b^x, dok je nasuprot tome, za zadano a iz G teško pronaći broj x iz $\mathbb{Z}$, kojim treba potencirati b da bi dobili a, tj. riješiti problem diskretnog logaritma (DLP).

Pogledajmo u sljedećem primjeru jednu jednostavnu ilustraciju primjene tzv. Diffie-Hellmanovog protokola za razmjenu tajnog ključa.

Primjer 10. *Marta i Josip se dogovore o jednom tajnom, slučajnom, elementu grupe G kojeg će kasnije koristiti kao ključ za šifriranje u nekom kriptosustavu. Jedina informacija kojom raspolažu je grupa G i njezin generator g.*

Do tajnog ključa Marta i Josip mogu doći ovako:

Marta odabere slučajan prirodan broj $a \in \{1, 2, \ldots, |G|-1\}$ pa pošalje Josipu element g^a. Josip odabere slučajan prirodan broj $b \in \{1, 2, \ldots, |G|-1\}$, te pošalje Marti element g^b. Marta izračuna $(g^b)^a = g^{ab}$. Josip izračuna $(g^a)^b = g^{ab}$. Sada je njihov tajni ključ $K = g^{ab}$.

U sljedećem primjeru pokazat ćemo još jednu razmjenu ključeva upotrebom protokola Diffie-Hellmana. Zbog jednostavnosti, u primjeru ćemo koristiti male vrijednosti brojeva p i g. U praksi ti brojevi moraju iznositi minimalno 1024 okteta kako bi se što više otežalo otkrivanje ključa od strane treće osobe.

Primjer 11. *Neka se Marta i Josip dogovore javno oko brojeva* $p = 18$ *i* $g = 7$.

- *Marta odabire svoj privatni broj, recimo da je to* $a = 2$ *i Josipu šalje broj* $X = 7^a \bmod 18 = 7^2 \bmod 18 = 13$.
- *Josip odabire svoj privatni broj* $b = 4$ *i Marti šalje broj* $Y = 7^b \bmod 18 = 7^4 \bmod 18 = 7$.
- *Nakon toga Marta i Josip mogu izračunati zajednički ključ:*
  $K_{Marta} = Y^a \bmod p = 7^2 \bmod 18 = 13$,
  $K_{Josip} = X^b \bmod p = 13^4 \bmod 18 = 13$.

Ovim postupkom Marta i Josip došli su do zajedničkog ključa $K = 13$, *poznatog samo njima.*

Protivnik koji prisluškuje razgovor Marte i Josipa, sazna brojeve p *i* g, *te vrijednosti* g^a *i* g^b. *Cilj mu je izračunati* g^{ab}, *tj. riješiti tzv. Diffie–Hellmanov problem (DHP). Ukoliko je on u mogućnosti riješiti problem diskretnog logaritma (DLP), pa iz* g^a *i* g *izračunati* a, *onda mu je lako, pomoću* a *i* g^b, *izračunati* g^{ab}. *Očito je, ako se riješi DLP da se onda zna riješiti DHP, ali otvoreno je pitanje povlači li rješavanje DHP-a i rješavanje DLP-a.*

3.1 RSA kriptosustav

Kako bi kriptosustavi postali sigurniji uvode se složeniji matematički problemi koje će otežati „razbijanje" ključa. Jedan takav problem je faktorizacija velikih prirodnih brojeva. Usprkos brojnim algoritmima, do danas je nemoguće u razumnom vremenu rastaviti na faktore dobro odabran broj s više od 250 znamenaka. Na teškoći faktorizacije zasniva se danas najpoznatiji kriptosustav na svijetu—RSA. Osmislili su ga 1977. godine Ronald Rivest, Adi Shamir i Leonard Adleman po kojima je i dobio ime. Sve do danas se koristi pri internet kupovini i internet bankarstvu. Da bismo definirali RSA algoritam najprije ćemo definirati pojam Eulerove funkcije koja predstavlja jednu od najvažnijih funkcija u teoriji brojeva.

Definicija 12. *Funkcija* $\varphi\colon \mathbb{N} \to \mathbb{N}$, *koja prirodnom broju* n *pridružuje broj prirodnih brojeva koji su strogo manji od* n *i relativno prosti s* n, *zove se Eulerova funkcija. Definiramo* $\varphi(1) = 1$.

Primjer 13. *Vrijedi:* $\varphi(20) = 8$ *jer su brojevi* $1, 3, 7, 9, 11, 13, 17, 19$ *manji od* 20 *i relativno prosti s* 20.

Ako je n prost broj onda je $\varphi(n) = n - 1$. Ako n ima rastav na faktore oblika $n = pq$, te su p i q relativno prosti brojevi, onda vrijedi

$$\varphi(n) = \varphi(p) \cdot \varphi(q).$$

Jedan od osnovnih rezultata vezanih za Eulerovu funkciju navodimo u sljedećem teoremu.

Teorem 14 (Eulerov teorem)**.** *Ako su a i n relativno prosti prirodni brojevi onda je*

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

Sada možemo definirati funkcije šifriranja i dešifriranja za RSA algoritam.

Definicija 15. *Neka je $n = p \cdot q$, gdje su p i q prosti brojevi. Neka je $\alpha = \sigma = \mathbb{Z}_n$, te $\kappa = \{(n, p, q, d, e) : n = pq,\ de \equiv 1 \pmod{\varphi(n)}\}$. Za $K = (n, p, q, d, e) \in \kappa$ definiramo funkciju šifriranja $e_K(x) = x^e \bmod n$ i funkciju dešifriranja $d_K(y) = y^d \bmod n$, pri čemu su $x, y \in \mathbb{Z}_n$. Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne.*

U nastavku teksta koristit ćemo oznaku $\mathrm{Nzm}(a, b)$ za najveću zajedničku mjeru (djelitelj) brojeva a i b.

Uvjerimo se da su funkcije e_K i d_K, iz prethodne definicije, jedna drugoj inverzne.

Primjenom Eulerovog teorema, za relativno proste brojeve x i n, dobivamo

$$d_K(e_K(x)) \equiv x^{de} \pmod{n}.$$

Iz $de \equiv 1 \pmod{\varphi(n)}$ slijedi da postoji prirodan broj k takav da je $de = k\varphi(n) + 1$.

Ako je $\mathrm{Nzm}(x, n) = 1$ slijedi

$$x^{de} = x^{k\varphi(n)+1} = (x^{\varphi(n)})^k \cdot x \equiv x \pmod{n}.$$

Ako je $\mathrm{Nzm}(n, x) = n$ onda je

$$x^{de} \equiv 0 \equiv x \pmod{n}.$$

Ako je $Nzm(n, x) = p$, onda je

$$x^{de} \equiv 0 \equiv x \pmod{p}$$

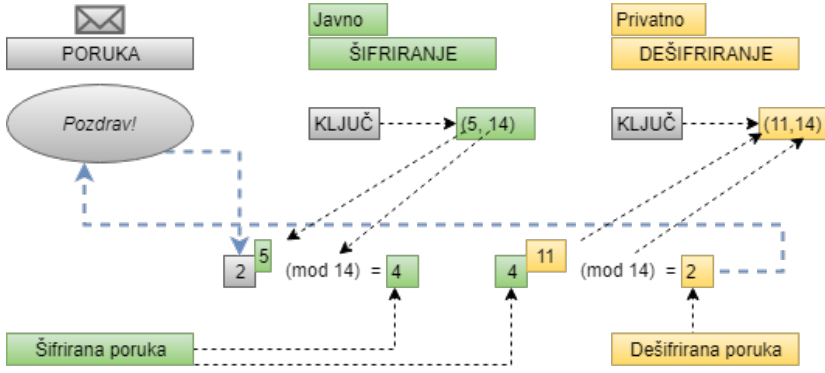
i

$$x^{de} = (x^{q-1})^{(p-1)k} \cdot x \equiv x \pmod{q}$$

pa je $x^{de} \equiv x \pmod{n}$.

Slučaj $\mathrm{Nzm}(n, x) = q$ je analogan. Slijedi da je $x^{de} \equiv x \pmod{n}$, što znači da je

$$d_K\left(e_K(x)\right) = x.$$



Slika 3: Figurativni prikaz funkcioniranja RSA

Primjer 16. *Uzmimo da je* $p = 5$ *i* $q = 7$. *Tada je*

$$n = p \cdot q = 5 \cdot 7 = 35$$

i

$$\varphi(n) = (p-1)(q-1) = 4 \cdot 6 = 24.$$

Pošto e *mora biti relativno prost s* $\varphi(n)$ *odabrat ćemo* $e = 5$. *Imamo javni ključ* $(n, e) = (35, 5)$. *Kako vrijedi da je* $\mathrm{Nzm}(e, \varphi(n)) = 1$ *slijedi da postoje cijeli brojevi* c *i* d *takvi da je*

$$ed + c\varphi(n) = 1$$

tj.

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Dobivamo $5d \equiv 1 \pmod{24}$ *iz čega ćemo izračunati* d *primjenom Euklidovog algoritma na brojeve* $\varphi(n) = 24$ *i* $e = 5$. *Slijedi*

$$\begin{aligned} 24 &= 5 \cdot 4 + 4, \\ 5 &= 4 \cdot 1 + 1, \\ 4 &= 1 \cdot 4. \end{aligned}$$

Krenuvši od pretposljednjeg retka prema gore, redom dobivamo $1 = 5 - (4 \cdot 1) = 5 - (24 - 5 \cdot 4) \cdot 1 = 5 \cdot 5 - 24 \cdot 1$. *Vidimo da* $d = 5$ *zadovoljava uvjet de* $\equiv 1 \pmod{\varphi(n)}$. *Pretpostavimo sada da nam netko želi poslati poruku* $x = 3$. *To znači da treba izračunati* $e_K(x) = 3^5 \bmod 35$. *Vrijedi*

$$3^5 \equiv 33 \pmod{35}.$$

Dakle, šifrat je $y = e_K(x) = 33$. *Kada primimo ovaj šifrat, dešifiriramo ga pomoću tajnog ključa* $d = 5$*:*

$$x = d_K(y) = 33^5 \bmod 35 \equiv (-2)^5 \bmod 35 \equiv 3 \pmod{35}.$$

Dakle, $x = 3$.

3.2 Implementacija RSA kriptosustava

Rad RSA kriptosustava najjednostavnije se može prikazati u sljedeća četiri koraka:

1. Marta odabere tajne brojeve p i q. Brojevi p i q su prosti brojevi s velikim brojem znamenaka. Zbog veće sigurnosti brojeve biramo tako da imaju različit broj znamenaka. Generiraju se na način da se prvo odredi slučajan broj m nakon čega se traži prvi prosti broj veći ili manji od m.

2. Marta izračuna $n = p \cdot q$ i $\varphi(n) = (p-1)(q-1)$.

3. Marta odabire broj e takav da je strogo manji od $\varphi(n)$ i relativno prost sa $\varphi(n)$.

4. Potom se računa d za kojeg vrijedi da je $de \equiv 1 \pmod{\varphi(n)}$, tj. $d \equiv e^{-1} \pmod{\varphi(n)}$. Računanje se vrši pomoću Euklidovog algoritma.

3.3 Razbijanje RSA

Iz postupka implementacije RSA kriptosustava zaključujemo da tajna razbijanja sustava leži u tome da se otkrije vrijednost eksponenta d. Način da se ta vrijednost otkrije je faktorizacija $n = p \cdot q$ preko koje ćemo lako saznati $\varphi(n)$ i odrediti traženi eksponent uvrštavanjem u $de \equiv 1 \pmod{\varphi(n)}$.

Međutim faktorizaciju $n = p \cdot q$ nije uvijek moguće izračunati u nekom prihvatljivom vremenu. Množenjem p i q dobivamo broj s nekoliko stotina znamenaka. Postoje mnogi načini da faktoriziramo takav broj. Možemo prvo pokušati odrediti male faktore korištenjem: ili naivne metode u kojoj dijelimo broj n prostim brojevima manjim ili jednakim $\sqrt{n}$ (ukoliko su nam poznati) ili korištenjem Pollardovog ρ algoritma. Zatim, iskoristiti moguća svojstva faktora primjenom faktorizacije pomoću eliptičnih krivulja te, ukoliko svi raniji algoritmi podbace, primijeniti opći algoritam, npr. algoritam kvadratnog sita.

Korištenjem najmodernijih računala, ovaj proces je moguć, ali neefikasan budući da može trajati godinama. Možemo sa sigurnošću reći

da su takvi kriptosustavi sigurni od ovakvog oblika napada, no izbor parametara mora se vršiti s oprezom.

Napadač uvijek traži grešku u našim koracima. Na primjer, ako se p i q nalaze preblizu jedan drugome, faktorizacija se može lakše obaviti jer će napadač u tom slučaju tražiti brojeve koji su približno jednaki $\sqrt{n}$ i time značajno skratiti vrijeme probijanja šifre. Brojevi $p-1$ ili $q-1$ u rastavu ne bi trebali imati male proste faktore, te broj e ne smije biti manji od 65537. Također, potrebno je izbjegavati mali tajni eksponent d.

Bitno je naglasiti da i dva desetljeća nakon nastanka prvog RSA kriptosustava još nije pronađena uspješna metoda njegovog razbijanja.

RSA predstavlja jedan od najsigurnijih načina tajne komunikacije i kriptosustav bez kojeg svijet ne bi mogao komunicirati na način na koji komunicira danas.

Trenutno mu je ravnopravan ECC kriptosustav (eng. ECC—Eliptic Curve Cryptography) predstavljen 80-ih godina prošlog stoljeća kao alternativa za RSA zbog svojih prednosti kao što su kraći ključevi, brže generiranje ključeva, manja računska zahtjevnost.

Kriptosustavi zasnovani na eliptičkim krivuljama smatraju se alternativnom za RSA, ali ne i njegovom zamjenom budući da imaju neke svoje nedostatke kao što su nekompatibilnost implementacije i teškoće pri generiranju prikladnih krivulja. Vrijeme će pokazati kolika je njihova vrijednost.

3.4 Rabinov kriptosustav

Rabinov kriptosustav je asimetrični kriptosustav kod kojeg se, kao i kod RSA kriptosustava, sigurnost temelji na težini faktorizacije prirodnih brojeva.

Osmislio ga je 1979. godine Michael Rabin kao unaprijeđenu inačicu RSA kriptosustava. Kao i kod RSA, Rabinov kriptosustav također ima i javni i privatni ključ. Javni ključ se koristi da se poruka šifrira prije slanja primatelju i može biti poznat svima dok je privatni ključ dostupan samo primatelju poruke.

Šifriranje u Rabinovom kriptosustavu definiramo na sljedeći način.

Definicija 17. *Neka je $n = pq$, i neka vrijedi da su p i q prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$. Neka je $\alpha = \sigma = \mathbb{Z}_n$, te*

$$\kappa = \{(n, p, q) : n = pq\}.$$

Za $K \in \kappa$ definiramo

$$e_K(x) = x^2 \bmod n,$$
$$d_K(y) = \sqrt{y} \bmod n.$$

Vrijednost od n je javna, a vrijednosti od p i q su tajne.

U prethodnoj definiciji, $a \equiv \sqrt{b} \pmod{n}$ je ekvivalentno s $a^2 \equiv b \pmod{n}$. Možemo izostaviti $p \equiv q \equiv 3 \pmod{4}$ odnosno to mogu biti drugačiji prosti brojevi, ali ovakav uvjet čini dešifriranje jedostavnijim.

Nedostatak Rabinovog sustava je to što funkcija šifriranja nije injekcija, odnosno osoba koja prima poruku mora sama odabrati otvoreni tekst između četiri dobivena kvadratna korijena[1] što ponekad i nije jednostavno. Zbog toga se uvodi *redundancija* u otvoreni tekst koja je unaprijed dogovorena. Na primjer, često se kao redundancija uvodi ponavljanje posljednja 64 bita. Na taj način primatelj poruke na jednostavan način uočava odgovarajući kvadratni korijen.

Kako izgleda korištenje Rabinovog kriptosustava pokazat ćemo na sljedećem primjeru.

Primjer 18. *Neka je $a = 11$ poruka koju Marta želi poslati Josipu. Marta odredi da je $p = 1741$ i $q = 1231$. Tada je*

$$n = p \cdot q = 1741 \cdot 1231 = 2143171.$$

Josip odabere $p' = 1297$ i $q' = 2843$. Slijedi,

$$n' = p' \cdot q' = 1297 \cdot 2843 = 3687371.$$

Marta zatim izračuna kvadratne korijene od 11 modulo n, te dobije četiri moguća rješenja:

$$x \equiv 1066157,\ 270931,\ 1872240,\ 1077014 \pmod{2143171}.$$

Recimo da Marta odabere drugo rješenje. Po dogovoru će Marta pregrupirati 270931 tako što će ga podijeliti na $x_1 = 270270$ i $x_2 = 931931$. Sada će, na x_1 i x_2 primijeniti funkciju šifriranja $e(x) = x^2 \bmod n'$ i dobiti sljedeće vrijednosti (nazovimo ih c_1 i c_2):

$$c_1 \equiv 270270^2 \equiv 2740761 \pmod{3687371},$$

$$c_2 \equiv 931931^2 \equiv 1522389 \pmod{3687371}.$$

Dobiveni šifrat, kojeg Marta šalje Josipu, je uređeni par (2740761, 1522389).

Iz primljenog šifrata, Josip najprije računa kvadratne korijene od c_1 modulo n':

$$x \equiv 270270, 3147016, 540355, 3417101 \pmod{3687371}.$$

[1] Kažemo da je x kvadratni korijen od a modulo m ako vrijedi $x^2 \equiv a \pmod{m}$.

Zatim računa kvadratne korijene od c_2 *modulo* n'*:*

$$x \equiv 2755440, 3433771, 253600, 931931 \pmod{3687371}.$$

Pošto Josip zna na koji način je Marta pregrupirala poruku, primjećuje da, od svih dobivenih rješenja, treba izabrati brojeve 270270 *i* 931931*.*

Kada Josip pregrupira ta rješenja dobiva broj 270931*. Kako bi došao do početne Martine poruke uvrštava broj* 270931 *u jednadžbu*

$$270931^2 \equiv a \bmod 2143171$$

i dobiva

$$a = 11.$$

Osim RSA i Rabinovog kriptosustava, postoji još nekoliko kriptosustava s javnim ključem, kao što su Elgamalov kriptosustav (zasnovan na teškoći računanja diskretnog logaritma u konačnim poljima), Merkle-Hellmanov kriptosustav (problem ruksaka), McElieceov kriptosustav, već spomenuti ECC kriptosustavi (EC Elgamalov, Menezes-Vanstoneov, KMOV) te jedan od najnovijih, NTRU kriptosustav, koji svoju prednost tek treba pokazati u možda ne tako skoroj budućnosti i eri kvantnih računala.

Literatura

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

[2] B. Ibrahimpašić, E. Liđan, *Digitalni potpis*, Osječki matematički list **10** (2010), 139–148.

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

[4] D. Žubrinić, *Diskretna matematika*, Element, Zagreb, 2001.

[5] *Diffie-Hellman protokol*, `https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2009-12-284.pdf` (Datum zadnjeg pristupa: 5. 9. 2019.)

[6] *Klasična kriptografija*, `https://element.hr/artikli/file/1347` (Datum zadnjeg pristupa: 5. 9. 2019.)

[7] *Korištenje eliptičnih krivulja u kriptografiji*, `https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-169.pdf` (Datum zadnjeg pristupa: 22. 12. 2019.)

Josipa Barić
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje,
Ruđera Boškovića 32, 21 000 Split, Hrvatska
E-mail adresa: jbaric@fesb.hr

Ivana Grgić
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje,
Ruđera Boškovića 32, 21 000 Split, Hrvatska
E-mail adresa: Ivana.Grgic@fesb.hr

Iva Jurić
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje,
Ruđera Boškovića 32, 21 000 Split, Hrvatska
E-mail adresa: Iva.Juric.01@fesb.hr

Zaprimljen: 2. prosinca 2019.
Prihvaćen: 10. siječnja 2020.