Kriptosustavi s javnim ključem

Rajković, Lora

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni prijediplomski studij Matematika

Kriptosustavi s javnim ključem

Završni rad

Mentor:

izv. prof. dr. sc. Mirela Jukić Bokun

Student:

Lora Rajković

Osijek, 2024

Sadržaj

1 Uvod

Komunikacija ima veliku ulogu u ljudskim životima, posebice ukoliko je u pitanju prijenos važnih informacija. Osnovni su čimbenici komunikacije pošiljatelj, poruka i primatelj, no ukoliko se radi o poruci velikog značaja, čimbenik postaje i protivnik koji također želi primiti tu informaciju, iako nije namijenjena njemu. Kako bi se postigla sigurnost u komunikaciji, razvila se znanost kriptologija koja se bavi metodama šifriranja i dešifriranja podataka. Dijeli se na dvije glavne grane: kriptografiju i kriptoanalizu. Kriptografija se bavi konstruiranjem kriptografskih sustava, odnosno šifriranjem i dešifriranjem, dok se kriptoanaliza bavi razbijanjem istih radi pronalaska njihovih slabosti.

Cilj je ovog rada proučiti kriptografiju javnog ključa, odnosno definirati nekoliko kriptosustava u kojima se ključ za dešifriranje ne može dobiti na temelju ključa za šifriranje. To su primjerice RSA kriptosustav, Rabinov kriptosustav i ElGamalov kriptosustav. Nadalje, na primjerima će se objasniti kako oni funkcioniraju, razmotriti njihove prednosti i nedostatke, međusobno ih usporediti te vidjeti u koje se svrhe koriste.

2 Općenito o kriptosustavima

Definicija 1 Kriptografija *(grč. kryptós - tajno, graphein - pisati) je znanstvena disciplina koja definira i analizira metode slanja poruka preko nesigurnog komunikacijskog kanala čuvajući pritom povjerljivost i integritet podataka.*

Nesiguran komunikacijski kanal podrazumijeva da je poruku moguće na neki način otkriti od strane osobe kojoj ta poruka nije namijenjena (*protivnik*). Takvi su kanali primjerice internet ili telefonska linija. Pošiljatelj i primatelj osobe su koje razmjenjuju poruke u kojima se nalazi *otvoreni tekst*, odnosno bilo kakav sadržaj poruke. Kako bi se zaštitili od protivnika, pošiljatelj preobražava otvoreni tekst koristeći parametar *ključ* koji je poznat primatelju. Sadržaj poruke više nije otvoreni tekst nego *šifrat*, a ovaj postupak naziva se *šifriranje*. Obratan postupak, dakle pretvorba šifrata natrag u otvoreni tekst, naziva se *dešifriranje*. Funkcije koje preslikavaju elemente otvorenog teksta u elemente šifrata i obratno nazivaju se *šifre*.

Prije definicije kriptosustava, potrebno je definirati sljedeće skupove:

- $\mathcal{P}$ - konačan skup svih mogućih elemenata otvorenog teksta
- $\mathcal{C}$ - konačan skup svih mogućih šifrata
- $\mathcal{K}$ - konačan skup svih mogućih ključeva
- $\mathcal{E}$ - skup svih funkcija šifriranja
- $\mathcal{D}$ - skup svih funkcija dešifriranja.

Definicija 2 *Kriptosustav je uređena petorka $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ takva da za svaki $K \in \mathcal{K}$ postoji $e_K \in \mathcal{E}$ i odgovarajući $d_K \in \mathcal{D}$, $e_K : \mathcal{P} \to \mathcal{C}$ i $d_K : \mathcal{C} \to \mathcal{P}$, takvi da vrijedi*

$$d_K(e_K(x)) = x, \quad \forall x \in \mathcal{P}. \tag{1}$$

U nastavku ćemo pokazati da svojstvo (1) povlači injektivnost funkcija e_K. Pretpostavimo da ne povlači, tj. da vrijedi $e_K(x_1) = e_K(x_2) = y$. To znači da se za dva različita otvorena teksta x_1 i x_2 dobije isti šifrat y, odnosno nije moguće definirati $d_K(y)$ jer bi ta funkcija trebala poprimiti dvije vrijednosti za isti y, što je nemoguće. Dakle, e_K su injektivne funkcije.

Nužan dio šifriranja i dešifriranja je poznavanje ključa. Dakle, pošiljatelju je potreban ključ kako bi šifrirao otvoreni tekst, a primatelju kako bi dešifrirao šifrat. Za te se dvije radnje mogu koristiti različiti tipovi ključa, što dovodi do podjele kriptografije na *simetrične kriptosustave* i *kriptosustave s javnim ključem.*

Kod simetričnih kriptosustava ključ za šifriranje i ključ za dešifriranje mogu se izračunati jedan iz drugog, štoviše uglavnom su jednaki pa možemo reći da postoji samo jedan ključ. Dakle, kako bi poruka zaista ostala skrivena, taj ključ moraju poznavati pošiljatelj i primatelj i samo oni, što bi značilo da im je potreban neki siguran komunikacijski kanal preko kojeg će razmijeniti ključ. Razumno je pitati se zašto onda ne koriste taj sigurni komunikacijski kanal za svaku razmjenu informacija jer u tom slučaju ne bi morali šifrirati poruke. Također, ako šifriraju podatke i tako razmjenjuju više poruka, potrebno je često mijenjati ključ kako protivnik ne bi primijetio uzorak i otkrio ključ. Drugim riječima, za sigurnost simetričnih kriptosustava neophodno je da ključ ostane u tajnosti.

Ideja kriptosustava s javnim ključem leži u samom nazivu, tj. rješavanje problema tajnosti ključa čineći ga javnim. Da bi to bilo moguće, ključ za šifriranje mora se razlikovati od ključa za dešifriranje jer svatko ima pristup prvom. Ne samo da se ti ključevi razlikuju, već je nemoguće u razumnom vremenu izračunati ključ za dešifriranje iz ključa za šifriranje. Unatoč tome, u stvarnom svijetu kriptografija javnog ključa ne predstavlja zamjenu za klasične, tj. simetrične kriptosustave. U praksi su algoritmi kriptosustava s javnim ključem puno sporiji od simetričnih algoritama pa se koriste za šifriranje ključeva, a ne poruka.

3 Kriptosustavi s javnim ključem

Rečeno je kako je smisao kriptosustava s javnim ključem imati funkciju e_K iz koje nije moguće doći do d_K. Funkcija e_K u tom je slučaju javna, ali zbog očuvanja sigurnosti to ne može bili bilo kakva funkcija, već *osobna jednosmjerna funkcija* (eng. trap-door one-way function).

Definicija 3 *Za funkciju f kažemo da je* jednosmjerna *ukoliko postoji njezin inverz f^{-1}, ali ga je vrlo teško izračunati. Ako postoji dodatni podatak pomoću kojeg se inverz lagano izračuna, onda se takva funkcija f naziva* osobna jednosmjerna funkcija.

Definicija 4 Kriptosustav s javnim ključem *čine familije $\{e_K\}$ i $\{d_K\}$ funkcija za šifriranje i dešifriranje sa svojstvima:*

1. *za svaki K je d_K inverz od e_K*
2. *za svaki K je e_K javan, ali je d_K poznat samo osobi K*
3. *za svaki K je e_K osobna jednosmjerna funkcija.*

Ovdje se funkcija e_K naziva *javni ključ*, a funkcija dešifriranja d_K *tajni ključ*.

Kriptosustav s javnim ključem može se shvatiti kao brava sa šifrom, pri čemu bi kombinacija brojeva koja otključava bravu bila osobna jednosmjerna funkcija. Tehnički je moguće otključati bravu bez poznavanja kombinacije metodom pokušaja, no taj bi proces trajao predugo čak i za iskusnog bravara. Uz poznavanje kombinacije otključavanje je vrlo jednostavno.

3.1 Povijest

Whitfield Diffie i Martin Hellman kriptografi su koji su 1976. godine objavili revolucionaran rad "Novi smjerovi u kriptografiji" (eng. "New directions in cryptography") u kojemu su iskazali probleme tadašnje suvremene kriptografije te predložili rješenja nekih od tih problema. Godine 2015. osvojili su

Turingovu nagradu za navedeni rad jer se pokazao izuzetno primjenjiv, čak su postavili temelj za većinu današnjih sigurnosnih protokola na internetu. Ukazali su na razvoj tehnologije, odnosno da se počinju razvijati brzi i jeftini načini telekomunikacije, ali i njihovi problemi, primjerice osiguravanje poruka od prisluškivanja ili upitna vjerodostojnost poruka. Tadašnje rješavanje sigurnosnih problema znatno je zaostajalo za drugim područjima komunikacijske tehnologije. Dotadašnja kriptografija (simetrična) nije bila kompetentna riješti novonastale probleme, stoga su Diffie i Hellman ponudili rješenje - kriptografiju javnog ključa. Ta je inovacija minimizirala potrebu za sigurnim komunikacijskim kanalima za razmjenu ključeva te dala ekvivalent pisanog potpisa kao rješenje problema autentičnosti.

Diffie i Hellman primijetili su kako im u stvaranju kriptosustava s javnim ključem, odnosno osobnih jednosmjernih funkcija, može pomoći činjenica da je u nekim grupama logaritmiranje puno zahtjevnije od potenciranja. Iz te ideje proizašli su *kriptosustavi zasnovani na problemu diskretnog logaritma*, a jedan od njih je upravo Diffie-Hellmanov protokol za razmjenu ključeva. Postoji još neriješenih matematičkih problema koji su primjenjivi pri kreaciji takvih funkcija, primjerice *problem faktorizacije* velikih prirodnih brojeva. U nastavku ćemo reći nešto više o ovim pristupima.

4 Problem faktorizacije

Za upoznavanje problema faktorizacije potrebno je poznavati pojmove prost broj, složen broj i faktorizacija na proste faktore. Naime, svaki prirodan broj veći od jedan ima (do na poredak) jedinstvenu faktorizaciju na proste faktore, ali do nje nije uvijek jednostavno doći. Prosti brojevi imaju trivijalnu faktorizaciju na proste faktore pa je za problem faktorizacije potreban neki veliki složeni prirodni broj. Dakle, nužno je najprije provjeriti je li broj prost ili nije.

Provjera prostosti prirodnog broja n provodi se pomoću testova prostosti, primjerice Fermatov test, Miller-Rabinov test i sl. Ako n ne prođe neki od testova prostosti, onda je sigurno složen, a ako je složen, onda postoji njegova netrivijalna faktorizacija na proste faktore. Postoje razne metode faktorizacije, primjerice Pollardova ρ metoda, faktorizacija pomoću eliptičnih krivulja, metoda verižnih razlomaka itd., no za odabrane prirodne brojeve s više od 250 znamenki čak ni te metode ne mogu doći do faktorizacije. To se naziva problem faktorizacije velikog prirodnog broja te je upravo na tom problemu temeljena jedna od vrsta kriptosustava javnog ključa. Primjeri takvih kriptosustava su RSA kriptosustav i Rabinov kriptosustav, detaljnije objašnjeni u poglavljima 4.1 i 4.2.

4.1 RSA kriptosustav

Najpoznatiji kriptosustav s javnim ključem dobio je ime po svojim tvorcima, Ronaldu Rivestu, Adi Shamiru i Leonardu Adlemanu koji su ga predstavili 1977. godine. RSA kriptosustav jedan je od najranijih kriptosustava s javnim ključem, a i danas ima široke primjene. Zasnovan je na ranije spomenutom problemu faktorizacije, a parametri su mu n kao produkt dva velika prosta broja p i q te e i d čija je svrha šifriranje i dešifriranje.

Definicija 5 *Neka je $n = pq$, gdje su p i q različiti prosti brojevi. Neka je nadalje $\mathcal{C} = \mathcal{P} = \{0, 1, 2, \ldots, n-1\} = \mathbb{Z}_n$ te*

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq,\ de \equiv 1 \,(\mathrm{mod}\ \varphi(n))\}.$$

Za $K \in \mathcal{K}$ definirani su

$$e_K(x) = x^e \bmod n, \qquad d_K(y) = y^d \bmod n, \quad x, y \in \mathbb{Z}_n.$$

Vrijednosti n i e su javne, dok su p, q i d tajne.

Funkcije šifriranja i dešifriranja e_K i d_K moraju zadovoljavati svojtvo $d_K(e_K(x)) = x$. Da bi se dokazalo da ovdje zaista zadovoljavaju, potreban je Eulerov teorem, ali i Eulerova funkcija φ iz Definicije 5, stoga u nastavku dajemo definiciju i osnovna svojstva Eulerove funkcije koja će nam biti potrebna.

Definicija 6 *Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ koja prirodnom broju n pridružuje broj prirodnih brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n naziva se* Eulerova funkcija.

Teorem 1 ([5]) *Eulerova funkcija je multiplikativna.*

U definiciji RSA kriptosustava je $n = pq$ pa je vrijednost Eulerove funkcije za takav n dana s

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

Teorem 2 (Eulerov teorem, [5]) *Neka je $x \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ako su x i n relativno prosti, tj. ako je $(x, n) = 1$, tada je* $x^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\ n)$.

U nastavku je dokaz da zaista vrijedi $d_K(e_K(x)) = x$.
Iz Definicije 5 slijedi

$$d_K(e_K(x)) \equiv d_K(x^e) \,(\mathrm{mod}\ n) \equiv x^{de} \,(\mathrm{mod}\ n).$$

Znamo,

$$de \equiv 1 \pmod{\varphi(n)}$$

pa tada postoji prirodan broj m takav da je $de = m\varphi(n) + 1$, tj.

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

Postoje četiri moguća slučaja:

1° Za $(x, n) = 1$ po Eulerovom teoremu je $x^{\varphi(n)} \equiv 1 \pmod{n}$ pa slijedi

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

2° Za $(x, n) = p$ vrijedi:
kako je $n = pq$, p i q različiti prosti brojevi, tada je $(x, q) = 1$ pa prema Eulerovom teoremu slijedi

$$x^{\varphi(q)} = x^{q-1} \equiv 1 \,(\mathrm{mod}\ q),$$

iz čega nadalje slijedi

$$x^{de} = (x^{\varphi(q)\,\varphi(p)})^m \cdot x = (x^{\varphi(q)})^{\varphi(p)\cdot m} \cdot x \equiv x \,(\mathrm{mod}\ q)$$

pa zbog $(x, n) = p$ slijedi i

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

a znamo da je $n = pq$ te da su p i q relativno prosti pa onda vrijedi i

$$x^{de} \equiv x \,(\mathrm{mod}\ n).$$

3° Za $(x, n) = q$ analogno se dobije $x^{de} \equiv x \,(\mathrm{mod}\ n)$.

4° Za $(x, n) = n$ vrijedi da $n \mid x$, stoga je

$$x^{de} \equiv 0 \equiv x \,(\mathrm{mod}\ n).$$

Time smo dokazali tvrdnju.
Generiranje javnog i tajnog ključa u RSA kriptosustavu sastoji se od nekoliko koraka. Najprije se izaberu dva velika različita prosta broja p i q, a zatim se pomoću njih izračuna n. Kad je poznat n, onda se može izračunati i $\varphi(n)$. Nakon toga odabire se broj e koji je ujedno manji od $\varphi(n)$ i relativno je prost s njim. Tada su poznate sve potrebne informacije za računanje tajnog eksponenta d pomoću proširenog Euklidovog algoritma. Na kraju se dobije javni ključ (n, e) i tajni ključ (p, q, d). Najefektnije je ovaj postupak demonstrirati primjerom.

Primjer 1 *Generiranje javnog i tajnog ključa u RSA kriptosustavu.*

Rješenje: Prvo treba izabrati dva prosta broja p i q. U praksi se oni biraju pomoću generatora slučajnih brojeva i najčešće sadrže preko 100 znamenki, no ovdje su radi jednostavnosti izabrani manji brojevi.
Neka je $p = 17$ i $q = 23$. Tada je $n = pq = 391$. Vrijednost $\varphi(n)$ tada iznosi

$$\varphi(391) = \varphi(17)\,\varphi(23) = (17-1)\,(23-1) = 16 \cdot 22 = 352.$$

Sljedeći je korak odabir broja e za koji vrijedi $(e, \varphi(n)) = 1$ i $e < \varphi(n)$. Kako je $\varphi(391) = 352 = 2^5 \cdot 11$, znači da broj e ne smije biti djeljiv niti s jednim od brojeva 2 i 11. Neka je

$$e = 3 \cdot 5 \cdot 19 = 285.$$

Vrijedi $(e, \varphi(n)) = (285, 352) = 1$. Još treba odrediti tajni eksponent d. Mora vrijediti $ed \equiv 1 \pmod{\varphi(n)}$, stoga postoji neki prirodan broj m takav da je

$$ed = m \cdot \varphi(n) + 1 \quad \Rightarrow \quad ed + \varphi(n) \cdot (-m) = 1$$

te se dobije jednadžba koja uvijek ima rješenje jer je $(e, \varphi(n)) = 1$.
Uvrštavanjem poznatih vrijednosti dobije se jednadžba

$$285d + 352 \cdot (-m) = 1.$$

Ako je (x, y) rješenje jednadžbe $285x + 352y = 1$, onda je $d \equiv x \pmod{\varphi(n)}$. Rješenja te jednadžbe dobiju se korištenjem sljedećih rekurzija [7]:

$$\begin{aligned} x_{-1} &= 1, & x_0 &= 0, & x_i &= x_{i-2} - q_i x_{i-1}, \\ y_{-1} &= 0, & y_0 &= 1, & y_i &= y_{i-2} - q_i y_{i-1}. \end{aligned}$$

Tada vrijedi

$$285\, x_k + 352\, y_k = (285, 352) = 1,$$

pri čemu je k indeks posljednjeg ostatka različitog od nule u Euklidovom algoritmu. Euklidovim algoritmom dobije se:

$$\begin{aligned} 285 &= 352 \cdot 0 + 285 \\ 352 &= 285 \cdot 1 + 67 \\ 285 &= 67 \cdot 4 + 17 \\ 67 &= 17 \cdot 3 + 16 \\ 17 &= 16 \cdot 1 + 1 \\ 16 &= 1 \cdot 16. \end{aligned}$$

Spomenute rekurzivne relacije daju:

i	-1	0	1	2	3	4	5
q_i			0	1	4	3	1
x_i	1	0	1	-1	5	-16	$\boxed{21}$
y_i	0	1	0	1	-4	13	$\boxed{-17}$

Dobije se x_k, odnosno $x_5 = 21$, a kako je $d \equiv 21 \pmod{352}$, to je $d = 21$. Dakle, javni ključ je $(n, e) = (391, 285)$, a tajni ključ $(p, q, d) = (17, 23, 21)$. Primjerice, sada broj $x = 15$ šifriramo na sljedeći način:

$$e_K(15) = 15^{285} \bmod 391$$

i dobivamo šifrat

$$e_K(x) = y = 342,$$

dok za dešifriranje imamo:

$$d_K(342) = 342^{21} \bmod 391,$$

odnosno

$$d_K(y) = 15.$$

$\diamondsuit$

RSA kriptosustav danas ima široke primjene na područjima online sigurnosti, npr. za digitalne certifikate i potpise, elektroničku poštu itd. Također ima veliku ulogu u osiguranju bankarskih sustava i transakcija.

4.2 Rabinov kriptosustav

Matematičar Michael O. Rabin je 1979. godine utemeljio Rabinov kriptosustav na teškoći vađenja drugog (kvadratnog) korijena modulo $n = pq$. Ranije je rečeno kako je Rabinov kriptosustav zasnovan na problemu faktorizacije, a sada da je zasnovan na *problemu računanja kvadratnih korijena modulo prirodan broj*. Obje su tvrdnje istinite jer su sljedeće tvrdnje ekvivalentne:

- poznavanje faktora od n znači da je moguće izvući kvadratne korijene modulo n
- izvaditi drugi korijen modulo n znači da je moguće faktorizirati n.

Problem računanja kvadratnog korijena u $\mathbb{Z}_n$ je sljedeći.
Neka su p i q prosti te $n = pq$. Treba naći $x \in \mathbb{Z}$ takav da je $x^2 \equiv a \pmod{n}$, gdje je $1 \leq a \leq n-1$, a kvadratni ostatak modulo n. Ako takav x postoji, naziva se kvadratni korijen iz a $(\sqrt{a})$ modulo n.

Teorem 3 (Eulerov kriterij, [5]) *Neka je p neparan prost broj i $a \in \mathbb{Z}$. Tada je*

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

Posebno, a je kvadratni ostatak modulo p ako i samo ako je

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{3}$$

Postoji algoritam za rješavanje kongruencije $x^2 \equiv a \pmod{p}$ i taj je algoritam posebice jednostavan ukoliko je $p \equiv 3 \pmod 4$ jer će tada rješenje biti $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$. Dakle, $x^2 \equiv a^{\frac{p+1}{2}} \pmod{p}$, pa prema tvrdnji (3) vrijedi $a^{\frac{p-1}{2}} \cdot a \equiv a \pmod{p}$. Iz tog se razloga u Rabinovom kriptosustavu uzimaju prosti brojevi p i q kongruentni 3 modulo 4.

Definicija 7 *Neka su p i q prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$ te $n = pq$. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ i $\mathcal{K} = \{(n, p, q)\}$. Za $K \in \mathcal{K}$ definira se*

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

Vrijednost n je javna, a p i q su tajne. Ovaj se kriptosustav naziva Rabinov kriptosustav.

U literaturi se često pri objašnjavanju kriptosustava spominju osobe *Alice* i *Bob* kao predstavnici sudionika A (pošiljatelj) i B (primatelj) u razmjeni informacija preko nekog kriptosustava. Zato će u idućem primjeru Alice šifrirati poruku u Rabinovom kriptosustavu, a Bob će tu poruku (pokušati) dešifrirati.

Primjer 2 *Alice želi Bobu poslati poruku $x = 26$ u Rabinovom kriptosustavu, pri čemu je odabrala $p = 7$ i $q = 19$. Kako će Bob to dešifrirati?*

Rješenje: Alice je šifrirala poruku formulom

$$e_K(x) = x^2 \bmod n,$$

gdje je $n = pq = 7 \cdot 19 = 133$. Dobila je šifrat

$$y = 26^2 \bmod n = 11 \bmod 133.$$

Funkcija e_K u Rabinovom kriptosustavu nije injekcija, već postoje četiri kvadratna korijena modulo n. Bob mora izračunati sva četiri, a to može postići u 5 koraka:

1. Proširenim Euklidovim algoritmom odrediti $a, b \in \mathbb{Z}$ takve da je $ap + bq = 1$.
2. Izračunati $r = y^{\frac{p+1}{4}} \bmod p$.
3. Izračunati $s = y^{\frac{q+1}{4}} \bmod q$.
4. Izračunati m_1 pomoću formule $m_1 = (aps + bqr) \bmod n$.
5. Izračunati m_2 pomoću formule $m_2 = (aps - bqr) \bmod n$.

Četiri kvadratna korijena modulo n dana su s:

$$m_1 \bmod n, \quad -m_1 \bmod n, \quad m_2 \bmod n, \quad -m_2 \bmod n.$$

Bob prvo odredi a i b iz jednadžbe $a \cdot 7 + b \cdot 19 = 1$. Analogno kao i ranije, primjenom proširenog Euklidovog algoritma dobije se $a = -8, b = 3$. Tada je:

$$\begin{aligned} r &= y^{\frac{p+1}{4}} \bmod p = 11^2 \bmod 7 = 2, \\ s &= y^{\frac{q+1}{4}} \bmod q = 11^5 \bmod 19 = 7, \\ m_1 &= (aps + bqr) \bmod n = -278 \bmod n = 121, \\ m_2 &= (aps - bqr) \bmod n = -506 \bmod n = 26. \end{aligned}$$

Sada Bob može odrediti kvadratne korijene x_1, x_2, x_3, x_4.

$$\begin{aligned} x_1 &= m_1 \bmod 133 = 121, \\ x_2 &= -m_1 \bmod 133 = 145, \\ x_3 &= m_2 \bmod 133 = 26, \\ x_1 &= -m_2 \bmod 133 = 107. \end{aligned}$$

Dakle, kandidati za poruku x su:

$$26, \quad 107, \quad 121, \quad 145.$$

$\diamondsuit$

Kako e_K u Rabinovom kriptosustavu nije injekcija, može se reći da je taj kriptosustav čak sigurniji od RSA. Također, puno je brži od većine ostalih kriptosustava s javnim ključem, no unatoč tome Rabinov kriptosustav nema toliko široku primjenu.

5 Problem diskretnog logaritma

Za definiranje problema diskretnog logaritma, važan je pojam grupe.

Definicija 8 *Uređen par $(G, *)$ je grupa ako vrijede sljedeća svojstva:*

- $*$ *je binarna operacija na* G*, tj.* $* : G \times G \to G$
- *asocijativnost:* $(\forall a, b, c \in G) \quad a * (b * c) = (a * b) * c,$
- *postojanje neutralnog elementa:* $(\exists e \in G)\,(\forall a \in G) \quad a * e = e * a = a,$
- *postojanje inverznog elementa:* $(\forall a \in G)\,(\exists a^{-1} \in G) \quad a * a^{-1} = a^{-1} * a = e.$

Ako dodatno vrijedi i komutativnost, onda je $(G, *)$ *Abelova ili komutativna grupa.*

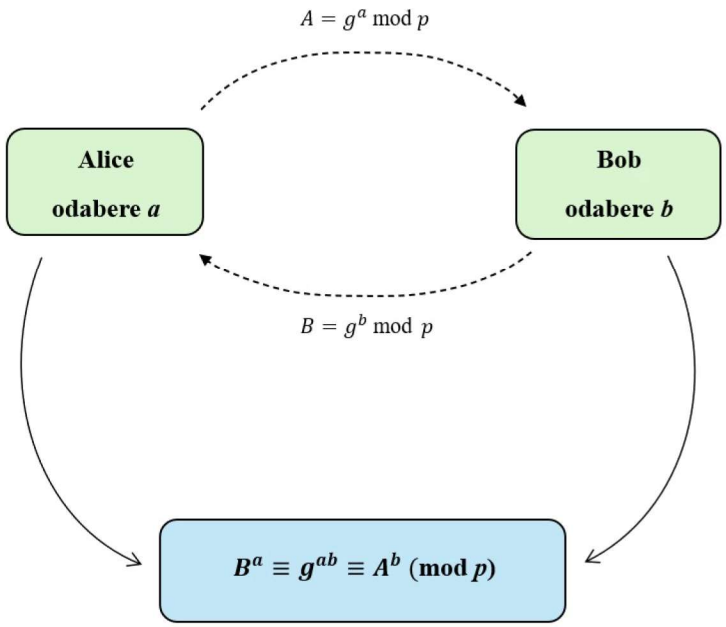
Kraća oznaka za grupu $(G, *)$ je G.
Neka je G grupa i $H \subseteq G$, $H \neq \emptyset$. Ako je H grupa s obzirom na istu operaciju kao G, onda je H podgrupa od G. Neka je G grupa i $g \in G$. Skup $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ je najmanja podgrupa od G koja sadrži g. Za $\langle g \rangle$ vrijedi da je to ciklička grupa, tj. generirana je jednim elementom. Sada su poznati svi pojmovi potrebni za definiranje problema diskretnog logaritma.

Definicija 9 *Neka je* $G = \langle g \rangle$ *konačna ciklička grupa. Za svaki* $y \in G$ *postoji točno jedan najmanji* $a \in \mathbb{N}_0$ *takav da je* $g^a = y$*. Broj* a *naziva se diskretan logaritam od* y *s bazom* g*. Računanje* $a = \log_g y$ *(uz poznate vrijednosti* g *i* y*) naziva se* problem diskretnog logaritma.

Za neke je grupe taj logaritam jednostavno izračunati, npr. za aditivnu grupu $(\mathbb{Z}_n, +_n)$, dok je recimo u multiplikativnoj grupi $(\mathbb{Z}_p^*, \cdot_p)$ računanje diskretnog logaritma vrlo teško, što je potaknulo stvaranje ElGamalova kriptosustava o kojem nešto više slijedi u potpoglavlju 5.2.

5.1 Diffie-Hellmanov problem

Diffie i Hellman primijetili su kako postoje grupe u kojima je problem diskretnog logaritma (DLP) vrlo težak pa su tu činjenicu iskoristili u svom protokolu razmjene ključeva. Bit protokola je da se dvije osobe, Alice i Bob, dogovore preko nesigurnog komunikacijskog kanala o tome što će im biti ključ za šifriranje u daljnoj komunikaciji. To rade na sljedeći način:



Slika 1: Diffie-Hellmanov protokol za razmjenu ključeva

a) Alice i Bob javno se dogovore oko cikličke grupe koju će koristiti, npr. $G = \langle g \rangle$.

b) Alice odabere neki prirodan broj $a \in \{1, 2, \ldots, |G| - 1\}$, a potom izračuna $A := g^a$. Bob odabere neki prirodan broj $b \in \{1, 2, \ldots, |G|-1\}$ te izračuna $B := g^b$ ($|G|$ je oznaka za broj elemenata od G).

c) Alice pošalje Bobu A, Bob pošalje Alice B.

d) Alice izračuna $S := B^a = (g^b)^a = g^{ab}$. Bob izračuna $S := A^b = (g^a)^b = g^{ab}$.

e) Alice i Bob mogu koristiti S kao tajni ključ za šifriranje i dešifriranje poruka.

Međutim, njihov protivnik Eva može prisluškivati njihove poruke preko nesigurnog kanala i može saznati vrijednosti G, A i B, ali da bi Eva otkrila ključ mora izračunati g^{ab}, odnosno riješiti *Diffie-Hellmanov problem* (DHP). Dakle, mora izračunati $a = \log_g A$ i $b = \log_g B$. Ako su Alice i Bob za svoju grupu G uzeli npr. multiplikativnu grupu ${\mathbb{Z}_p}^*$, ne moraju se bojati da će Eva otkriti ključ jer su za tu grupu (kao i za ostale grupe koje se koriste u kriptografiji) DHP i DLP ekvivalentni.

5.2 ElGamalov kriptosustav

Kriptosustav iz 1985. godine zasnovan na problemu diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$ je upravo ElGamalov kriptosustav.

Definicija 10 *Neka je p prost broj i $\alpha \in \mathbb{Z}_p^*$ primitivni korijen*[1] *modulo p. Neka je $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ te*

$$\mathcal{K} = \{(p, \alpha, a, \beta) \,:\, \beta = \alpha^a \ mod\ p\},$$

gdje su vrijednosti p, α, β javne, a vrijednost a tajna.
Za $K \in \mathcal{K}$ i tajni slučajni broj $h \in \{0, 1, \ldots, p-1\}$ definira se funkcija šifriranja

$$e_K(x, h) = (\alpha^h \bmod p, \quad x\beta^h \bmod p).$$

Za $y_1, y_2 \in \mathbb{Z}_p^*$ definira se funkcija dešifriranja

$$d_K(y_1, y_2) = y_2({y_1}^a)^{-1} \bmod p.$$

[1]Broj $\alpha \in \{1, 2, \ldots, p-1\}$ je *primitivni korijen modulo p* ako je α^{p-1} najmanja potencija broja α koja pri dijeljenju s p daje ostatak 1.

Općenito, sigurnost ovog kriptosustava ovisi o teškoći Diffie-Hellmanovog problema u danoj grupi te o odabiru prostog broja p. Da bi a zaista bio tajan, p mora biti dovoljno velik prost broj kako bi u $\mathbb{Z}_p^*$ DLP bio gotovo nerješiv.

Primjer 3 *Prikazati kako Alice šalje Bobu poruku $x = 6$ pomoću ElGamalova kriptosustava te kako ju Bob dešifrira.*

Rješenje: Najprije Bob odabire prost broj p i broj α kao generator grupe $\mathbb{Z}_p^*$. Npr. neka je $p = 7$. Sljedeća tablica prikazuje koji su to primitivni korijeni modulo 7, tj. generatori grupe $\mathbb{Z}_7^*$.

k	1	2	3	4	5	6
$1^k \bmod 7$	1					
$2^k \bmod 7$	2	4	1			
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1			
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1				

Očito su 3 i 5 generatori grupe $\mathbb{Z}_7^*$ pa su oni i jedine opcije za α. Bob je odlučio da je $\alpha = 5$. Odabire slučajan broj $a \in \{1, 2, 3, 4, 5, 6\}$, neka je $a = 4$ pa je tada

$$\beta = \alpha^a \bmod p = 5^4 \bmod 7 = 2.$$

Zatim šalje Alice javni ključ $(p, \alpha, \beta) = (7, 5, 2)$ kako bi ona njemu mogla poslati šifrat. Alice bira tajni eksponent $h = 8$ i računa

$$y_1 = \alpha^h \bmod p = 5^8 \bmod 7 = 4$$
$$y_2 = x\,\beta^h \bmod p = 6 \cdot 2^8 \bmod 7 = 3$$

i šalje Bobu šifrat $(y_1, y_2) = (4, 3)$. Bob računa

$$x = y_2({y_1}^a)^{-1} \bmod p = 3 \cdot (4^4)^{-1} \bmod 7.$$

Sada treba odrediti multiplikativni inverz od $4^4 \bmod 7 = 4$, tj. treba odrediti $4^{-1} \bmod 7$, a to se dobije rješavanjem linearne kongruencije $4m \equiv 1 \pmod 7$. Kako su 4 i 7 relativno prosti, Bob može jednadžbu pomnožiti s 2 i jednostavno dobiti

$$m \equiv 2 \pmod 7.$$

Dakle, $(4^4)^{-1} = 2 \bmod 7$ pa može nastaviti s dešifriranjem. Dolazi do vrijednosti x,

$$x = 3 \cdot 2 \bmod 7 = 6.$$

Na taj je način Bob preko ElGamalovog kriptosustava primio Alicinu poruku $x = 6$.

$\diamondsuit$

Literatura

[1] M. Barakat, C. Eder, T. Hanke, *An Introduction to Cryptography*, RWTH Aachen University, 2018.

[2] W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22**(6)(1976), 644–654.

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

[4] B. Ibrahimpašić, *Kriptografija kroz primjere*, Pedagoški fakultet Bihać, 2011.

[5] I. Matić, *Uvod u teoriju brojeva*, Sveučilište J. J. Strossmayera u Osijeku, Osijek, 2015.

[6] N. Smart, *Cryptography: An Introduction (3rd Edition)*, Mcgraw-Hill College, 2004.

[7] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2008.

Sažetak

Tema ovog rada je kriptografija s naglaskom na kriptosustave javnog ključa. Definirano je i oprimjereno nekoliko najvažnijih kriptosustava s javnim ključem te su za potrebe razumijevanja iskazani neki osnovni teoremi iz teorije brojeva. Objašnjen je način djelovanja pojedinog kriptosustava te su navedene njegove primjene. U primjerima je demonstriran postupak šifriranja i dešifriranja otvorenog teksta u šifrat koristeći određeni kriptosustav.

Ključne riječi

kriptosustav, ključ, osobna jednosmjerna funkcija, šifriranje, dešifriranje, faktorizacija, problem diskretnog logaritma

Public-key cryptosystems

Summary

The topic of this paper is cryptography with an emphasis on public-key cryptosystems. Several of the most important public-key cryptosystems are defined and exemplified and also, some basic theorems from number theory are presented for the purposes of understanding. The mode of operation of each cryptosystem is explained and its applications are listed. The examples demonstrate the process of encrypting and decrypting plaintext into ciphertext using a specific cryptosystem.

Keywords

cryptosystem, key, trap-door one-way function, encrypting, decrypting, factorization, discrete logarithm problem

Životopis

Rođena sam 4. listopada 2001. godine u Osijeku. Živim u Đakovu gdje sam pohađala Osnovnu školu Josipa Antuna Ćolnića. Nakon završetka osnovne škole, upisala sam Gimnaziju Antuna Gustava Matoša u Đakovu, smjer opća gimnazija. Sve razrede srednje škole završila sam s odličnim uspjehom te sam 2020. godine upisala prijediplomski studij matematike na Odjelu za matematiku, sada Fakultetu primijenjene matematike i informatike, na Sveučilištu Josipa Jurja Strossmayera u Osijeku.