# Kvadratni ostaci i kvadratni korijeni u kriptografiji javnog ključa

**Solar, Tomislava**

**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Tomislava Solar

# KVADRATNI OSTACI I KVADRATNI KORIJENI U KRIPTOGRAFIJI JAVNOG KLJUČA

Diplomski rad

Voditelj rada:
akad. Andrej Dujella

Zagreb, studeni, 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

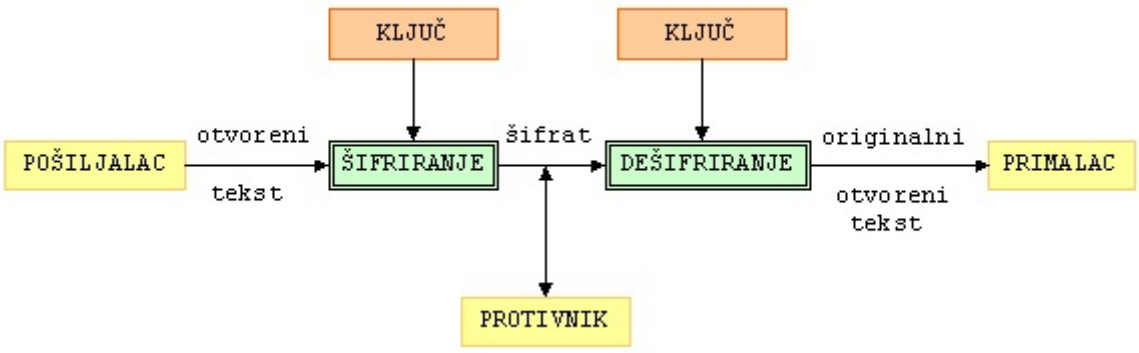
1. _____
2. _____
3. _____

# Sadržaj

# Uvod

*Kriptografija* je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Riječ kriptografija dolazi od grčkog pridjeva kriptós - ”skriven” i glagola gráfo - ”pisati” te bi se doslovno mogla prevesti kao *tajnopis*. Početci kriptografije sežu do starih Grka koji su koristili napravu za kriptiranje zvanu *skital* (radi se o drvenom štapu na kojeg se namatala vrpca te se na nju zapisivala poruka). Tijekom povijesti metode kriptiranja su znatno napredovale te ćemo u ovom radu proučiti dvije modernije metode kriptiranja.

Osnovna ideja kriptografije je da se poruka prenese s jednog mjesta na drugo, što je sigurnije moguće. Dvije osobe koje komuniciraju nazivamo *pošiljatelj* i *primatelj*. Poruka koju pošiljatelj želi poslati primatelju se naziva *otvoreni tekst*. Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ* te tako dobiva kriptiranu poruku koju šalje komunikacijskim kanalom. Primatelj zna ključ te pomoću njega može dekriptirati poruku i dobiti otvoreni tekst. Osobu koja prisluškuje komunikacijski kanal nazivamo *protivnik*. Protivnik ne zna ključ te stoga ne može dekriptirati kriptiranu poruku. Na Slici 1. je prikazana opisana situacija. Znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa naziva se *kriptoanaliza*. Kriptologija je grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.




Slika 0.1: Osnovni pojmovi

Sada navodimo formalnu definiciju kriptosustava:

**Definicija 0.0.1.** *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 elemenata otvorenog teksta.*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata kriptiranog teksta.*
3. $\mathcal{K}$ *je konačan skup svih mogućih ključeva.*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija kriptiranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija* $d_K \in \mathcal{D}$. *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 dijelimo na kriptosustave s *tajnim ključem* i kriptosustave s *javnim ključem*. Kod kriptosustava s tajnim ključem, ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno. Stoga taj ključ trebaju znati samo pošiljatelj i primatelj, a sigurnost kriptosustava ovisi o 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 odgovaraju ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku. Ideju javnog ključa prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine, kada su ponudili jedno moguće rješenje razmjene ključeva. U ovom radu ćemo upoznati dva kriptosustava s javnim ključem, Goldwasser-Micalijev kriptosustav i Rabinov kriptosustav. [1]

Rad započinje pogavljem Kvadratni ostaci u kojem ćemo promotriti kvadratne ostatke po prostom i složenom modulu, pokazati ćemo neke rezultate vezane uz kvadratne ostatke te ćemo pokazati postupak određivanja kvadratnih ostataka. Drugo poglavlje opisuje Goldwasser-Micalijev kriptosustav s javnim ključem. Najprije navodimo definiciju tog kriptosustava te opisujemo postupak kriptiranja i dekriptiranja u tom kriptosustavu. Zatim govorimo o sigurnosti Goldwasser-Micali kriptosustava. Posljednje poglavlje govori o Rabinovom kriptosustavu s javnim ključem. Najprije navodimo definiciju Rabinovog kriptosustava, zatim detaljno opisujemo postupak kriptiranja i dekriptiranja u tom kriptosustavu, pri čemu objašnjavamo i postupak računanja kvadratnih korijena po prostom i složenom modulu. Nakon toga promatramo na čemu se temelji sigurnost Rabinovog kriptosustava te ukratko radimo usporedbu s RSA kriptosustavom.

# Poglavlje 1

# Kvadratni ostaci

U ovom poglavlju ćemo promotriti kvadratne ostatke po prostom i složenom modulu te ćemo pokazati postupak određivanja kvadratnih ostataka.

Element grupe $\mathbb{G}$, $y \in \mathbb{G}$, je *kvadratni ostatak* ako postoji $x \in \mathbb{G}$ takav da je $x^2 = y$. Takav element $x$ nazivamo *kvadratni korijen* od $y$. Element koji nije kvadratni ostatak nazivamo *kvadratni neostatak*. U slučaju grupe $\mathbb{Z}_p^*$, $y \in \mathbb{Z}_p^*$ je kvadratni ostatak ako postoji $x \in \mathbb{Z}_p^*$ takav da vrijedi $x^2 \equiv y \pmod{p}$.

## 1.1 Kvadratni ostaci modulo prost broj

U narednim poglavljima s $p$ i $q$ ćemo označavati neparne proste brojeve, a s $N = pq$ umnožak dva različita neparna prosta broja.

Pogledajmo sada dokaz jedne jednostavne tvrdnje.

**Propozicija 1.1.1.** *Neka je $p > 2$ prost broj. Tada svaki kvadratni ostatak u skupu $\mathbb{Z}_p^*$ ima točno dva kvadratna korijena.*

*Dokaz.* Neka je $y \in \mathbb{Z}_p^*$ kvadratni ostatak. Prema definiciji tada znamo da postoji $x \in \mathbb{Z}_p^*$ takav da vrijedi $x^2 \equiv y \pmod{p}$. Očito vrijedi $(-x)^2 = x^2 \equiv y \pmod{p}$. Najprije ćemo pokazazati da je $-x \not\equiv x \pmod{p}$. Pretpostavimo suprotno, odnosno da je $-x \equiv x \pmod{p}$. Onda vrijedi $2x \equiv 0 \pmod{p}$, iz čega slijedi da $p \mid 2x$. Budući da je $p$ prost broj zaključujemo da ili $p \mid 2$ ili $p \mid x$. No, prva tvrdnja je nemoguća jer je $p$ prost broj strogo veći od 2. Druga tvrdnja je nemoguća zato jer je $0 < x < p$ ($x \in \mathbb{Z}_p^*$). Stoga možemo zaključiti da je $-x \not\equiv x \pmod{p}$, odnosno da $y$ ima barem dva kvadratna korijena.
Neka je sada $x' \in \mathbb{Z}_p^*$ kvadratni korijen od $y$. Tada vrijedi $x^2 \equiv y \equiv (x')^2 \pmod{p}$, odnosno $x^2 - (x')^2 \equiv 0 \pmod{p}$. Lijevu stranu jednakosti možemo rastaviti na faktore $(x-x')(x+x') \equiv 0 \pmod{p}$. Možemo zaključiti da vrijedi sljedeće: $p \mid (x - x')$ ili $p \mid (x + x')$. U prvom

slučaju vrijedi $x' \equiv x \pmod{p}$, a u drugom slučaju vrijedi $x' \equiv -x \pmod{p}$. Stoga možemo zaključiti da $y$ ima točno dva kvadratna korijena i to su $\pm x \pmod{p}$. □

Propozicija 1.1.1 nam pokazuje da za svaki prost broj $p > 2$ vrijedi da su točno pola elemenata skupa $\mathbb{Z}_p^*$ kvadratni ostaci modulo $p$. Označimo skup kvadratnih ostataka modulo $p$ s $QR_p$ te skup kvadratnih neostataka modulo $p$ s $QNR_p$. Možemo zaključiti da vrijedi:

$$| QR_p | = | QNR_p | = \frac{| \mathbb{Z}_p^* |}{2} = \frac{p-1}{2}.$$

Za $p > 2$ prost broj i $x \in \mathbb{Z}_p^*$ definiramo Legendreov simbol od $x$ modulo $p$:

$$\left(\frac{x}{p}\right) \overset{\text{def}}{=} \begin{cases} 1 & \text{, ako je } x \text{ kvadratni ostatak modulo } p \\ -1 & \text{, ako } x \text{ nije kvadratni ostatak modulo } p \end{cases}.$$

Želimo opisati kvadratne ostatke u grupi $\mathbb{Z}_p^*$ te se stoga prisjećamo da je grupa $\mathbb{Z}_p^*$ ciklička reda $p-1$. Neka je $g$ generator od $\mathbb{Z}_p^*$. Tada znamo da je

$$\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots, g^{p-2}\}.$$

Kvadriranjem svakog elementa grupe i oduzimanjem $p-1$ u eksponentu dobivamo da je skup kvadratnih ostataka u $\mathbb{Z}_p^*$:

$$QR_p = \{g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^2, \ldots, g^{p-3}\}.$$

Vidimo da se svaki kvadratni ostatak ponavlja dva puta te stoga zaključujemo da su kvadratni ostaci u $\mathbb{Z}_p^*$ oni elementi koji se mogu zapisati u obliku $g^i$ pri čemu je $i \in \{0, \ldots, p-2\}$ paran cijeli broj. Ova karakterizacija nas dovodi do sljedeće propozicije koja daje jednostavan način za određivanje je li neki element kvadratni ostatak.

**Propozicija 1.1.2.** *Neka je $p > 2$ prost broj. Tada je $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}$.*

*Dokaz.* Neka je $g$ proizvoljan generator od $\mathbb{Z}_p^*$. U prvom slučaju, neka je $x$ kvadratni ostatak modulo $p$. Ranije smo uočili da se tada $x$ može zapisati kao $x = g^i$ za neki paran cijeli broj $i$. Za $i = 2j$, za neki $j$ cijeli broj, imamo

$$x^{\frac{p-1}{2}} = (g^{2j})^{\frac{p-1}{2}} = g^{(p-1)j}$$

Korištenjem Malog Fermaovog teorema dobivamo

$$(g^{p-1})^j \equiv 1^j \equiv 1 \pmod{p}.$$

Dakle,

$$\left(\frac{x}{p}\right) = +1 \equiv x^{\frac{p-1}{2}} (\text{mod } p).$$

U drugom slučaju, neka je $x$ kvadratni neostatak modulo $p$. Tada je $x = g^i$ za neki neparan cijeli broj $i$. Vrijedi $i = 2j + 1$, za $j$ neki cijeli broj. Slijedi

$$x^{\frac{p-1}{2}} = (g^{2j+1})^{\frac{p-1}{2}} = (g^{2j})^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} \equiv 1 \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \text{ (mod } p).$$

Sada slijedi $(g^{\frac{p-1}{2}})^2 = g^{p-1} \equiv 1 \text{ (mod } p)$. Prema propoziciji 1.1.1 znamo da 1 ima dva kvadratna korijena, pa vrijedi $g^{\frac{p-1}{2}} \equiv \pm 1 \text{ (mod } p)$.
No, $g$ je generator grupe $\mathbb{Z}_p^*$ reda $p-1$ te zbog toga zaključujemo $g^{\frac{p-1}{2}} \not\equiv 1 \text{ (mod } p)$. Slijedi

$$\left(\frac{x}{p}\right) = -1 \equiv x^{\frac{p-1}{2}} (\text{mod } p).$$

□

Ova propozicija nam omogućava jednostavno određivanje je li element skupa $\mathbb{Z}_p^*$, za $p$ prost broj, kvadratni ostatak ili kvadratni neostatak.

Sada ćemo još pogledati neke jednostavne rezultate vezane uz temu.

**Propozicija 1.1.3.** *Neka je $p > 2$ prost broj i neka su $x, y \in \mathbb{Z}_p^*$. Tada je*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right)$$

*Dokaz.* Koristeći propoziciju 1.1.2 imamo,

$$\left(\frac{xy}{p}\right) \equiv (xy)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} \cdot y^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) \text{ (mod } p).$$

□

**Korolar 1.1.4.** *Neka je $p > 2$ prost broj i neka su $x, x' \in QR_p$ te $y, y' \in QNR_p$. Tada je:*

1. *$xx'$ mod $p \in QR_p$*
2. *$yy'$ mod $p \in QR_p$*
3. *$xy$ mod $p \in QNR_p$*

[2]

## 1.2 Kvadratni ostaci modulo složen broj

Sada ćemo promatrati kvadratne ostatke modulo složen broj $N$, pri čemu je $N = pq$. Najprije se moramo prisjetiti Kineskog teorema o ostacima:

**Teorem 1.2.1** (Kineski teorem o ostacima)**.** *Neka je $N = pq$, pri čemu su $p$ i $q$ relativno prosti. Tada vrijedi*

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q$$

*i*

$$\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Prema tom teoremu $y \in \mathbb{Z}_N^*$ možemo zapisati kao $y \leftrightarrow (y_p, y_q)$ pri čemu je $y_p \equiv y \pmod{p}$ i $y_q \equiv y \pmod{q}$.

**Propozicija 1.2.2.** *Neka je $N = pq$, pri čemu su $p$ i $q$ različiti prosti brojevi, i $y \in \mathbb{Z}_N^*$, gdje je $y \leftrightarrow (y_p, y_q)$. Tada vrijedi: $y$ je kvadratni ostatak modulo $N$ ako i samo ako je $y_p$ kvadratni ostatak modulo $p$ i $y_q$ kvadratni ostatak modulo $q$.*

*Dokaz.* Neka je $y$ kvadratni ostatak modulo $N$. Po definiciji, tada postoji $x \in \mathbb{Z}_N^*$ takav da je $x^2 \equiv y \pmod{N}$. Neka je $x \leftrightarrow (x_p, x_q)$. Tada je

$$(y_p, y_q) \leftrightarrow y \equiv x^2 = (x_p^2 \bmod p, x_q^2 \bmod q),$$

pri čemu je $(x_p, x_q)^2$ kvadrat elementa $(x_p, x_q)$ u grupi $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.
Sada smo pokazali da vrijedi $y_p \equiv x_p^2 \pmod{p}$ i $y_q \equiv x_q^2 \pmod{q}$, odnosno da su $y_p$ i $y_q$ kvadratni ostaci po odgovarajućim modulima.
Obrnuto, neka je $y = (y_p, y_q)$ i $y_p$, $y_q$ su kvadratni ostaci modulo $p$, odnosno $q$. Po definiciji, tada postoje $x_p \in \mathbb{Z}_p^*$ i $x_q \in \mathbb{Z}_q^*$ takvi da vrijedi $y_p \equiv x_p^2 \pmod{p}$ i $y_q \equiv x_q^2 \pmod{q}$. Neka je $x \leftrightarrow (x_p, x_q)$. Sada je

$$(x_p^2 \bmod p, x_q^2 \bmod q) = x^2 \equiv (y_p, y_q) \leftrightarrow y.$$

Možemo zaključiti da je tada $x$ kvadratni korijen od $y$ modulo $N$. □

**Primjer 1.2.3** (Kvadratni ostaci modulo 21)**.**

Kvadratne ostatke modulo složen broj određujemo koristeći propoziciju 1.2.2. Kvadratni ostaci modulo 21 su ($21 = 3 \cdot 7$):

- 1
  Najprije računamo $1 \bmod 3 = 1$ i $1 \bmod 7 = 1$ .
  Vrijedi da je 1 kvadratni ostatak modulo 3 jer je $1^2 \equiv 1 \bmod 3$ te da je 1 kvadratni ostatak modulo 7 jer je $1^2 \equiv 1 \bmod 7$.
  Dakle, prema propoziciji 1.2.2 vrijedi da je 1 kvadratni ostatak modulo 21.

- 4
  Računamo 4 mod 3 = 1 i 4 mod 7 = 4.
  Vrijedi da je 1 kvadratni ostatak modulo 3 jer je $1^2 \equiv 1 \bmod 3$ i da je 4 kvadratni ostatak modulo 7 jer je $2^2 \equiv 4 \bmod 7$.
  Dakle, prema propoziciji 1.2.2 vrijedi da je 4 kvadratni ostatak modulo 21.

- 16
  Računamo 16 mod 3 = 1 i 16 mod 7 = 2.
  Vrijedi da je 1 kvadratni ostatak modulo 3 jer je $1^2 \equiv 1 \bmod 3$ i da je 2 kvadratni ostatak modulo 7 jer je $3^2 \equiv 2 \bmod 7$.
  Dakle, prema propoziciji 1.2.2 vrijedi da je 16 kvadratni ostatak modulo 21.

Iz propozicije 1.2.2 slijedi da svaki kvadratni ostatak $y \in \mathbb{Z}_N^+$ ima točno četiri kvadratna korijena:

$$(x_p, x_q), (-x_p, x_q), (x_p, -x_q), (-x_p, -x_q).$$

pri čemu je $y \leftrightarrow (y_p, y_q)$ i $x_p$, $x_q$ su kvadratni korijeni od $y_p$ i $y_q$ modulo $p$, odnosno $q$. Kineski teorem o ostacima nam osigurava da su to četiri različita elementa skupa $\mathbb{Z}_N^*$. Označimo s $QR_N$ skup kvadratnih ostataka modulo $N$. Možemo zaključiti da je

$$\frac{|QR_N|}{|\mathbb{Z}_N^*|} = \frac{|QR_p| \cdot |QR_q|}{|\mathbb{Z}_N^*|} = \frac{\frac{p-1}{2} \cdot \frac{q-1}{2}}{(p-1)(q-1)} = \frac{1}{4}.$$

Sada možemo proširiti definiciju Legendreovog simbola za $N = pq$ umnožak različitih prostih brojeva. Taj novi simbol nazivamo Jacobijev simbol i označavamo ga s $\left(\frac{x}{N}\right)$ ili $J_N(x)$ (u daljnjem tekstu se koristi ova druga oznaka).

Za $x$ relativno prost s $N$ vrijedi:

$$J_N(x) \stackrel{\text{def}}{=} J_p(x) \cdot J_q(x) = J_p(x \bmod p) \cdot J_q(x \bmod q).$$

Neka je $J_N^{+1}$ skup svih elemenata iz $\mathbb{Z}_N^*$ za koje je Jacobijev simbol jednak 1 te neka je $J_N^{-1}$ skup svih elemenata iz $\mathbb{Z}_N^*$ za koje je Jacobijev simbol jednak -1. Prethodna propozicija nam osigurava sljedeće: ako je $x$ kvadratni ostatak moduolo $N$ tada su $x \pmod p$ i $x \pmod q$ kvadratni ostaci modulo $p$, odnosno $q$ (vrijedi $J_p(x) = J_q(x) = 1$). Stoga slijedi $J_N(x) = 1$. Dakle, ako je $x$ kvadratni ostatak modulo $N$, tada je $J_N(x) = 1$. No, $J_N(x) = 1$ se također može dogoditi u slučaju kada je $J_p(x) = J_q(x) = -1$, odnosno kada $x \bmod p$ i $x \bmod q$ nisu kvadratni ostaci modulo $p$ i $q$ (stoga $x$ nije kvadratni ostatak modulo $N$). Uvodimo sljedeću oznaku:

$$QNR_N^{+1} \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_N^* \mid x \text{ nije kvadratni ostatak modulo } N, \text{ ali } J_N(x) = 1\}.$$

Pogledajmo sada propoziciju:

**Propozicija 1.2.4.** *Neka je $N = pq$ za $p, q$ različite neparne proste brojeve. Tada vrijedi:*

1. *Točno pola elemenata skupa $\mathbb{Z}_N^*$ je sadržano u skupu $J_N^{+1}$.*
2. *$QR_N \subseteq J_N^{+1}$*
3. *Točno pola elemenata skupa $J_N^{+1}$ su elementi skupa $QR_N$ (preostali su elementi skupa $QNR_N^{+1}$).*

*Dokaz.* 1. Znamo da je $J_N(x) = 1$ ako je $J_p(x) = J_q(x) = 1$ ili $J_p(x) = J_q(x) = -1$. U poglavlju o kvadratnim ostacima modulo prost broj smo uočili da su točno pola elemenata $x \in \mathbb{Z}_p^*$ kvadratni ostaci modulo $p$ ($J_p(x) = 1$), a pola kvadratni neostaci ($J_p(x) = -1$). Analogno zaključujemo za $\mathbb{Z}_q^*$. Za skupove $J_p^{+1}$, $J_p^{-1}$, $J_q^{+1}$, i $J_q^{-1}$ vrijedi

$$\begin{aligned} |J_N^{+1}| &= |J_p^{+1} \times J_q^{+1}| + |J_p^{-1} \times J_q^{-1}| \\ &= |J_p^{+1}| \cdot |J_q^{+1}| + |J_p^{-1}| \cdot |J_q^{-1}| \\ &= \frac{(p-1)}{2}\frac{(q-1)}{2} + \frac{(p-1)}{2}\frac{(q-1)}{2} = \frac{\phi(N)}{2} \end{aligned} \tag{1.1}$$

Fukciju $\phi$ nazivamo Eulerova funkcija, a $\phi(N)$ je broj brojeva u nizu $1, 2, 3, \ldots N$ koji su relativno prosti sa $N$ (u dokazu koristimo svojstvo multiplikativnosti te funkcije).

2. Ranije smo vidjeli da za kvadratne ostatke modulo $N$ vrijedi $J_N(x) = 1$. Stoga je $QR_N \subseteq J_N^{+1}$.

3. Za $x \in QR_n$ vrijedi da je $J_p(x) = J_q(x) = 1$. Stoga znamo da je

$$|QR_N| = |J_p^{+1} \times J_q^{+1}| = \frac{(p-1)}{2}\frac{(q-1)}{2} = \frac{\phi(N)}{2} = \frac{|J_N^{+1}|}{2}.$$

U prethodnom koraku smo pokazali da je $QR_N \subseteq J_N^{+1}$, pa možemo zaključiti da su pola elemenata skupa $J_N^{+1}$ elementi skupa $QR_N$.

□

Sljedeća dva rezultata su analogoni propozicije 1.1.3 i korolara 1.1.4 iz poglavlja 1.1.

**Propozicija 1.2.5.** *Neka je $N = pq$ umnožak dvaju različitih neparnih prostih brojeva i neka su $x, y \in \mathbb{Z}_N^*$. Tada vrijedi $J_N(xy) = J_N(x) \cdot J_N(y)$.*

*Dokaz.* Prema definiciji Jacobijevog simbola i propoziciji 1.1.3 slijedi:

$$\begin{aligned} J_N(xy) &= J_p(xy) \cdot J_q(xy) \\ &= J_p(x) \cdot J_p(y) \cdot J_q(x) \cdot J_q(y) \\ &= J_p(x) \cdot J_q(x) \cdot J_p(y) \cdot J_q(y) \\ &= J_N(x) \cdot J_N(y). \end{aligned} \tag{1.2}$$

□

**Korolar 1.2.6.** *Neka je $N = pq$ umnožak dvaju različitih neparnih prostih brojeva i neka su $x, x' \in QR_N$ i $y, y' \in QNR_N^{+1}$. Tada je:*

1. *$xx' \bmod N \in QR_N$*
2. *$yy' \bmod N \in QR_N$*
3. *$xy \bmod N \in QNR_N^{+1}$.*

*Dokaz.* 1. Budući da je $x \in QR_N$ znamo da vrijedi $J_p(x) = J_q(x) = 1$. Analogno, jer je $x' \in QR_N$, znamo da vrijedi $J_p(x') = J_q(x') = 1$. Prema propoziciji 1.1.3 vrijedi

$$J_p(xx') = J_p(x) \cdot J_q(x') = 1 \text{ i } J_q(xx') = J_q(x) \cdot J_q(x') = 1$$

te slijedi $J_N(xx') = J_p(xx') \cdot J_q(xx') = 1$. Dakle, $xx' \in QR_N$.

2. Budući da je $y \in QNR_N^{+1}$ znamo da vrijedi $J_p(y) = J_q(y) = -1$. Analogno, jer je $y' \in QNR_N^{+1}$, znamo da vrijedi $J_p(y') = J_q(y') = -1$. Prema propoziciji 1.1.3 vrijedi

$$J_p(yy') = J_p(y) \cdot J_q(y') = 1 \text{ i } J_q(yy') = J_q(y) \cdot J_q(y') = 1$$

te slijedi $J_N(yy') = J_p(yy') \cdot J_q(yy') = 1$. Dakle, $yy' \in QR_N$.

3. Budući da je $x \in QR_N$ znamo da vrijedi $J_p(x) = J_q(x) = 1$. Analogno, jer je $y \in QNR_N^{+1}$, znamo da vrijedi $J_p(y) = J_q(y) = -1$. Prema Propoziciji 1.1.3. vrijedi

$$J_p(xy) = J_p(x) \cdot J_q(y) = -1 \text{ i } J_q(xy) = J_q(x) \cdot J_q(y) = -1,$$

te je $J_N(xy) = 1$. Jer je $J_p(xy) = -1$, što znači da $xy \bmod p$ nije kvadratni ostatak modulo $p$, zaključujemo da $xy$ nije kvadratni ostatak modulo $N$. Dakle, $xy \in QNR_N^{+1}$. □

Sada vidimo da za $x \in \mathbb{Z}_N^*$ možemo jednostavno odrediti je li kvadratni ostatak ukoliko znamo rastav broja $N$ na proste faktore.

Ukoliko rastav broja $N$ na proste faktore nije poznat, ne postoji algoritam polinomijalne složenosti kojim bi se moglo odrediti je li dani element kvadratni ostatak modulo $N$ ili ne. No, ipak postoji algoritam te složenosti kojim se određuje $J_N(x)$ bez poznavanja rastava broja $N$ na proste faktore.

To nas dovodi do parcijalnog testa je li $x$ kvadratni ostatak. Ako vrijedi $J_N(x) = -1$, tada sigurno znamo da $x$ nije kvadratni ostatak. Ako vrijedi $J_N(x) = 1$ , tada nam ovaj test ne govori ništa o tome i nema algoritma polinomne složenosti kojim bi odredili je li $x$ kvadratni ostatak modulo $N$. [2]

# Poglavlje 2

# Goldwasswer - Micalijev kriptosustav s javnim ključem

U ovom poglavlju ćemo opisati Goldwasser - Micalijev kriptosustav s javnim ključem koji se temelji na određivanju kvadratnih ostataka. Taj kriptosustav su razvili Shawi Goldwasser i Silvio Micali početkom osamdesetih godina prošlog stoljeća na MIT-u. Goldwasser-Miclijev kriptosustav je najpoznatiji po tome što je to prvi vjerojatnosni kriptosustav s javnim ključem koji je dokazivo siguran po standardu kriptografskih pretpostavki. No, ovaj kriptosustav nije efikasan jer kriptirani tekst može biti nekoliko stotina puta veći od otvorenog teksta.

## 2.1 Definicija Goldwasser - Micalijevog kriptosustava s javnim ključem

**Definicija 2.1.1** (Goldwsser - Micalijev kriptosustav s javnim ključem)**.** *Neka je $N = pq$ pri čemu $p$ i $q$ su različiti neparni prosti brojevi. Neka je $y \in QNR_N^{+1}$. Javni ključ je uređeni par $(N, y)$, a prosti faktori broja $N$ su tajni. Neka je $\mathcal{P} = \{0, 1\}$, $C = \mathbb{Z}_N^*$ i neka je $\mathcal{K} = \{(N, p, q, y)\}$. Za $K = (N, p, q, y)$, $m \in \mathcal{P}$, $c \in C$ i slučajno izabrani $x \in \mathbb{Z}_N^*$ definiramo*

$$e_K(m, x) = y^m x^2 \ mod \ N$$

*i*

$$d_K(c) = \begin{cases} 0 \text{ ako je } c \in QR_N \\ 1 \text{ ako je } c \in QNR_N \end{cases}$$

[3]

Sada ćemo malo detaljnije objasniti proces kriptiranja i dekriptiranja za ovaj kriptosustav. Najprije pogledajmo kako korisnik ovakvog kriptosustava odabire ključeve:

- Prvo nasumično odabire dva velika različita prosta broja $p$ i $q$.
- Zatim računa $N = pq$.
- Odabire $y \in QNR_N^{+1}$.
- Javni ključ korisnika je uređeni par $(N, y)$, a tajni ključ je par $(p, q)$.

Promotrimo sada metodu kriptiranja. Zamislimo da osoba B želi poslati poruku osobi A. Osoba B kod kriptiranja treba napraviti sljedeće:

- Dobaviti javni ključ osobe A, par $(N, y)$.
- Svoju poruku $m$ prikazati kao binarni string $m = m_1 m_2 \dots m_t$ duljine $t$.
- Za svaki bit poruke $m_i$ ($i \in \{1, \dots, \}$) nasumično odabrati $x \in \mathbb{Z}_N^*$. Ako je $m_i = 1$, tada postavi $c_i \leftarrow yx^2 \bmod N$. Inače $c_i \leftarrow x^2 \bmod N$.
- Kriptirana poruka je $c = (c_1, c_2, \dots, c_t)$.

Osoba A dekriptira poruku $c$ na sljedeći način:

- Za svaki $i \in \{1, \dots, \}$ izračuna Jacobijev simbol $e_i = J_p(c_i)$. Ako je $e_i = 1$, tada postavi $m_i \leftarrow 0$. Inače $m_i \leftarrow 1$.
- Dekriptirana poruka je $m = m_1 m_2 \dots m_t$.

Uvjerimo se da postupak dekriptiranja zaista funkcionira. Ako je $m_i = 0$, tada je $c_i = x^2 \bmod N$ kvadratni ostatak modulo N. Ako je $m_i = 1$, tada je $c_i \in QNR_N^{+1}$ jer je $y \in QNR_n^{+1}$. Primatelj poruke zna rastav broja $N$ na proste faktore i prema Propoziciji 1.2.1. može odrediti $J_p(c_i)$ te doći do originalne poruke $m_i$. [3]

**Primjer 2.1.2.** *Izaberite dva 3-znamenkasta prosta broja p, q. Pomoću Kineskog teorema o ostacima nađite $y \in QNR_N^{+1}$. Recite što je javni, a što tajni kljuc. Šifrirajte binarnu poruku 101, tako da izaberete slučajno x-eve iz $\mathbb{Z}_N^*$ (različite za svaki bit). Dešifrirajte poruku.*

Najprije odabiremo dva troznamenkasta prosta broja, neka su $p = 373$ i $q = 491$. Tada je $N = pq = 373 \cdot 491 = 183143$. Zatim pomoću Kineskog teorema o ostacima i koristeći propoziciju 1.2.2 određujemo $y \in QNR_N^{+1}$. Tražimo takav $y$ da vrijedi $J_p(y) = -1$ i $J_q(y) = -1$. Neka je $y = 8$, jer prema propoziciji 1.1.2 vrijedi $J_p(y) = \left(\frac{8}{373}\right) \equiv 8^{\frac{373-1}{2}} \pmod{373} = -1$ i $J_q(8) = \left(\frac{8}{491}\right) \equiv 8^{\frac{491-1}{2}} \pmod{491} = -1$. Javni ključ je uređeni par $(183143, 8)$, a tajni ključ je uređeni par $(373, 491)$.

Sada ćemo šifrirati poruku $m = 101$. Poruku šifriramo bit po bit. Dakle, $m_1 = 1$, $m_2 = 0$, $m_3 = 1$. Za $m_1$ najprije odabiremo $x \in \mathbb{Z}_N^*$, neka je $x = 2$. Sada računamo $c_1 = e_k(1,2) = 8 \cdot 2^2 \bmod 183143 \equiv 32 \bmod 183143 = 32$. Za $m_2$ neka je $x = 3$ i tada je $c_2 = e_k(0,3) = 3^2 \bmod 183143 \equiv 9 \bmod 183143 = 9$. Za $m_3$ neka je $x = 4$ i tada je $c_3 = e_k(1,4) = 8 \cdot 4^2 \bmod 183143 \equiv 128 \bmod 183143 = 128$. Šifrirana poruka je $c = (32, 9, 128)$.

Dešifrirajmo poruku $c = (32, 9, 128)$. Za svaki $c_i$ računamo $e_i = J_p(c_i)$. Ako je $e_i = 1$, tada je $m_i = 0$. Inače $m_i = 1$. Dakle, za $c_1 = 32$ računamo $J_p(32) = \left(\frac{32}{373}\right) \equiv 32^{\frac{373-1}{2}} \pmod{373} = -1$ te je stoga $m_1 = 1$. Analogno, za $c_2 = 9$ računamo $J_p(9) = \left(\frac{9}{373}\right) \equiv 9^{\frac{373-1}{2}} \pmod{373} = 1$, pa je $m_2 = 0$. Za $c_3 = 128$ računamo $J_p(816) = \left(\frac{128}{373}\right) \equiv 128^{\frac{373-1}{2}} \pmod{373} = -1$, pa je $m_3 = 1$. Početni otvoreni tekst je $m = 101$.

## 2.2 Sigurnost Goldwasser - Micalijevog kriptosustava s javnim ključem

Sigurnost Goldwasser - Micalijevog kriptosustava je osigurana sljedećim teoremom, koji nećemo dokazivati u ovom radu zbog kompleksnosti dokaza.

**Teorem 2.2.1.** *Ako je problem određivanja je li element kvadratni ostatak težak, tada je Goldwasser - Micalijev kriptosustav CPA-siguran.*

Sada ćemo objasniti što znači da je neki kriptosustav *CPA-siguran*. Kratica CPA dolazi od izraza *chosen - plaintext attacks*, što bi mogli prevesti kao napadi odabranim otvorenim tekstovima. Zamislimo situaciju u kojoj dvije strane komuniciraju koristeći zajednički ključ $k$. Kod CPA napada, napadač ima mogućnost kriptirati odabrani otvoreni tekst ključem $k$ i slati šifrirani tekst dvjema stranama putem kanala koji može nadzirati. Također putem tog kanala može promatrati poruke nepoznatog sadržaja koje su kriptirane istim ključem $k$. Pretpostavimo da napadač zna da je poruka $m$ jedna od dviju mogućnosti $m_0, m_1$. Kada kažemo da je kriptosustav CPA-siguran, smatramo da napadač ne može odlučiti koja od poruka je početna poruka $m$ bilo kakvim postupkom čija je vjerojatnost veća od vjerojatnosti nasumičnog pogađanja.

Sada ćemo navesti i formalnu definiciju. U formalnoj definiciji CPA napade modeliramo tako da protivniku $\mathcal{A}$ omogućimo pristup takozvanoj „crnoj kutiji "koja kriptira poruke koje odabire protivnik $\mathcal{A}$ koristeći ključ $k$, ali tako da protivnik ne zna ključ $k$. Zamislimo da protivnik $\mathcal{A}$ ima pristup šalje upit „crnoj kutiji ", svoju poruku $m$, a zauzvrat dobiva kriptirani tekst $c \leftarrow Enc_k(m)$. Protivnik $\mathcal{A}$ može proizvoljno pristupati „crnoj kutiji", koliko god puta želi.

Pogledajmo sada sljedeći eksperiment. Neka je $\Pi = (Gen, Enc, Dec)$ shema enkripcije gdje je *Gen* funkcija koja generira ključ, *Enc* funkcija koja kriptira javni tekst, a *Dec* je funkcija koja dekriptira kriptirani tekst. Neka je $\mathcal{A}$ protivnik te neka je vrijednost $n$ parametar sigurnosti.

**Eksperiment CPA neprimjetnosti** $PrivK^{cpa}_{\mathcal{A},\Pi}(n)$:

1. Ključ $k$ je generiran koristeći funkciju $Gen(1^n)$.
2. Protivniku $\mathcal{A}$ je dan ulaz $1^n$ i pristup „crnoj kutiji "te on za izlaz daje dvije poruke $m_0, m_1$ koje su jednake duljine.
3. Uniformno se odabire bit $b \in \{0, 1\}$ i zatim se računa kriptirani tekst $c \leftarrow Enc_k(m_b)$ koji se daje protivniku $\mathcal{A}$.
4. Protivnik $\mathcal{A}$ i dalje ima pristup „crnoj kutiji "te producira izlaz, bit $b'$.
5. Izlaz eksprerimenta je definiran kao 1 ako je $b = b'$, odnosno 0 inače. U prvom slučaju kažemo da je protivnik $\mathcal{A}$ uspio.

**Definicija 2.2.2.** *Shema enkripcije* $\Pi = (Gen, Enc, Dec)$ *s privatnim ključem je CPA-sigurna ako za svaki vjerojatnosni polinomijalni protivnik* $\mathcal{A}$ *postoji zanemariva funkcija negl takva da je*

$$P(PrivK^{cpa}_{\mathcal{A},\Pi}(n) = 1) \leq \frac{1}{2} + negl(n)$$

*gdje se vjerojatnost uzima nad svim slučajnim protivnicima* $\mathcal{A}$ *i nad svim slučajnostima korištenim u eksperimentu.*

[2]

# Poglavlje 3

# Rabinov kriptosustav s javnim ključem

Rabinov kriptosustav s javnim ključem se temelji na određivanju kvadratnih korijena modulo neki složen broj. Taj kriptosustav je razvio Michael O. Rabin u siječnju 1979. godine. Rabinov kriptosustav je prvi asimetrični kriptosustav u kojem je dohvaćanje otvorenog teksta pomoću kriptiranog teksta teško kao rastavljanje broja na proste faktore. U ovom poglavlju ćemo opisati taj kriptosustav, zatim promotriti algoritam za određivanje kvadratnih korijena po prostom i složenom modulu i nakon toga ćemo pogledati na čemu se temelji sigurnost ovog kriptosustava.

## 3.1 Definicija Rabinovog kriptosustava s javnim ključem

**Definicija 3.1.1** (Rabinov kriptosustav s javnim ključem)**.** *Neka je $N = pq$, pri čemu $p$ i $q$ su različiti neparni prosti brojevi i $p, q \equiv 3 \ mod \ 4$. Neka je $\mathcal{P} = C = \mathbb{Z}_N^*$ i neka je $\mathcal{K} = \{(N, p, q)\}$. Za $K = (N, p, q)$, definiramo*

$$e_K(x) = x^2 \ mod \ N$$

*i*

$$d_K(y) = \sqrt{y} \ mod \ N.$$

*Vrijednost N je javni ključ, a vrijednosti $(p, q)$ su tajni ključ.*

[4]

Dakle, proces odabira ključeva je vrlo jednostavan. Potrebno je nasumično odabrati dva velika različita prosta broja $p$ i $q$ i zatim izračunati $N = pq$.

Promotrimo sada metodu kriptiranja. Zamislimo da osoba B želi poslati poruku osobi A. Osoba B kod kriptiranja treba napraviti sljedeće:

- Dobaviti javni ključ $N$ osobe A.

- Svoju poruku prikazati kao broj $m$ iz skupa $\{1, 2, \ldots, n-1\}$.
- Izračunati $c = m^2 \bmod N$.

Nakon tih koraka, osoba B šalje kriptiranu poruku $c$ osobi A. Osoba A zatim provodi sljedeće korake kako bi odredila početnu poruku:

- Izračunati kvadratne korijene od $c$ modulo $N$, označimo ih s $m_1, m_2, m_3, m_4$.
- Odlučiti koji od tih korijena je $m$.

[3]

Kako bi bolje razumjeli postupak dekriptiranja, u ovom poglavlju ćemo promotriti algoritam za određivanje kvadratnih korijena.

## Računanje kvadratnih korijena modulo prost broj

Najprije promatramo računanje kvadratnih korijena modulo prost broj $p$. Pretpostavimo da je $p \equiv 3 \pmod 4$, jer nam se taj slučaj pojavljuje u definiciji Rabinovog kriptosustava.

Neka je $a \in \mathbb{Z}_p^*$ kvadratni ostatak. Želimo odrediti kvadratne korijene od $a$ modulo $p$. Budući da je $p \equiv 3 \pmod 4$, vrijedi $p = 4i + 3$ za neki cijeli broj $i$. Budući da je $a \in \mathbb{Z}_p^*$ kvadratni ostatak, prema Propoziciji 1.1.2. znamo da je $J_p(a) = 1 = a^{\frac{p-1}{2}}$. Množenjem obiju strana s $a$ dobivamo:

$$a = a^{\frac{p-1}{2}+1} = a^{2i+2} \equiv (a^{i+1})^2 \pmod p,$$

dakle $a^{i+1} \equiv a^{\frac{p+1}{4}} \pmod p$ je kvadratni korijen od $a$ modulo $p$. Uvjet $p \equiv 3 \pmod 4$ nam osigurava da je $\frac{p+1}{4}$ cijeli broj te je stoga $a^{\frac{p+1}{4}} \pmod p$ dobro definirano.

Dakle, za $a \in \mathbb{Z}_p^*$ i $p \equiv 3 \pmod 4$ kvadratni korijen od $a$ računamo na sljedeći način:

$$x \equiv a^{\frac{p+1}{4}} \pmod p.$$

[2]

Za slučaj kada je $p \equiv 1 \pmod 4$ također postoji algoritam za određivanje kvadratnih korijena, no nećemo ga detaljno objašnjavati jer nam nije potreban u daljnjem radu. Može se pokazati da je i taj algoritam polinomijalne složenosti.

## Računanje kvadratnih korijena modulo složen broj

Algoritam iz prethodnog potpoglavlja se lako može proširiti tako da se računaju kvadratni korijeni modulo složeni broj kojem je poznat rastav na proste faktore. Neka je $N = pq$ pri

čemu su $p$ i $q$ različiti neparni prosti brojevi. Prema Kineskom teoremu o ostacima već smo zaključili da za $a \in \mathbb{Z}_N^*$ vrijedi $a \leftrightarrow (a_p, a_q)$. Računanje kvadratnih korijena $x_p, x_q$ od $a_p, a_q$ modulo $p$, odnosno $q$, računa se kao u prethodnom potpoglavlju. Zatim koristeći Kineski teorem promijenimo prikaz, $(x_p, x_q) \leftrightarrow x$. Dakle, $x$ je kvadratni korijen od $a$ modulo $N$. [2]

Pogledajmo sada jedan primjer dekriptiranja u Rabinovom kriptosustavu.

**Primjer 3.1.2.** *U Rabinovom kriptosustavu s parametrima* $(N, p, q) = (5561, 67, 83)$*, dekriptirajte šifrat* $y = 3241$*. Poznato je da je otvoreni tekst prirodan broj* $x < N$ *kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.*

Prvo trebamo naći kvadratne korijene modulo 67 i modulo 83. Budući da vrijedi $67 \equiv 83 \equiv 3 \bmod 4$ kvadratne korijene određujemo po formuli $\pm y^{\frac{p+1}{4}} \bmod p$. Odredimo najprije kvadratne korijene modulo 67: $x_{1,2} = \pm 3241^{\frac{67+1}{4}} \bmod 67 = \pm 3241^{17} \bmod 67 = \pm 62$. Analogno određujemo kvadratne korijene modulo 83: $x_{3,4} = \pm 3241^{\frac{83+1}{4}} \bmod 67 = \pm 3241^{21} \bmod 67 = \pm 81$. Kako bi pronašli kvadratne korijene od 3241 modulo 5561 koristimo Kineski teorem o ostacima. Rješavamo četiri sustava linearnih kongruencija

$$x \equiv \pm 62 \ (\bmod 67),\ x \equiv \pm 81 \ (\bmod 83).$$

Sustav od dvije linearne kongruencije rješavamo primjenom Euklidovog algoritma:

$$\begin{aligned} 83 &= 67 \cdot 1 + 16 \\ 67 &= 16 \cdot 4 + 3 \\ 16 &= 3 \cdot 5 + 1 \\ 3 &= 1 \cdot 3 \end{aligned} \tag{3.1}$$

| $i$ | | | 1 | 2 | 3 |
|---|---|---|---|---|---|
| $q_i$ | | | 1 | 4 | 5 |
| $x_i$ | 1 | 0 | 1 | -4 | 21 |
| $y_i$ | 0 | 1 | -1 | 5 | -26 |

Sada je $u = -26$ i $v = 21$ te možemo izračunati kvadratne korijene od 3241 modulo 5561:

$$\begin{aligned} x_1 &= -26 \cdot 67 \cdot 81 + 21 \cdot 83 \cdot 62 \ (\text{mod } 5561) \\ &\equiv -141101 + 108066 \ (\text{mod } 5561) \equiv -33036 \ (\text{mod } 5561) = 330 \\ x_2 &= -26 \cdot 67 \cdot 81 + 21 \cdot 83 \cdot (-62) \ (\text{mod } 5561) \\ &\equiv -141101 - 108066 \ (\text{mod } 5561) \equiv -249160 \ (\text{mod } 5561) = 1077 \\ x_3 &= -26 \cdot 67 \cdot (-81) + 21 \cdot 83 \cdot 62 \ (\text{mod } 5561) \\ &\equiv 141101 + 108066 \ (\text{mod } 5561) \equiv 249168 \ (\text{mod } 5561) = 4484 \\ x_4 &= -26 \cdot 67 \cdot (-81) + 21 \cdot 83 \cdot (-62) \ (\text{mod } 5561) \\ &\equiv 141101 - 108066 \ (\text{mod } 5561) \equiv 33036 \ (\text{mod } 5561) = 5231 \end{aligned} \tag{3.2}$$

Kako bi odredili koji kvadratni korijen je otvoreni tekst svaki od tih brojeva trebamo prikazati u binarnom zapisu. Rješenje je onaj broj kojemu su zadnje četiri znamenke u binarnom zapisu jednake.

$$x_1 = 330 = 1\ 0100\ 1010$$

$$x_2 = 1077 = 100\ 0011\ 0101$$

$$x_3 = 4484 = 1\ 0001\ 1000\ 0100$$

$$x_4 = 5231 = 1\ 0100\ 0110\ 1111$$

Dakle, otvoreni tekst je $x_4 = 5231$.

## 3.2 Sigurnost Rabinovog kriptosustava s javnim ključem

U prethodnom poglavlju smo vidjeli da je računanje kvadratnih korijena modulo $N$ algoritam polinomijalne složenosti ako je poznat rastav broja $N$ na proste faktore. U ovom poglavlju ćemo vidjeti da je računanje kvadratnih korijena modulo složen broj $N$, za kojeg nije poznat rastav na proste faktore, jednako teško kao i određivanje prostih faktora broja $N$.

Neka je $GenModulus$ polinomijalni algoritam koji za ulaz $1^n$ daje rezultat uređenu trojku $(N, p, q)$, gdje je $N = pq$, a $p$ i $q$ su $n$-bitni prosti brojevi, skoro uvijek, tj. vjerojatnost neuspjeha je zanemariva u odnosu na $n$. Za dani algoritam $\mathcal{A}$ i parametar $n$ promotrimo sljedeći eksperiment.

**Eksperiment računanja kvadratnih korijena** $SQR_{\mathcal{A},GenModulus}(n)$:

1. Pokrenuti algoritam $GenModulus(1^n)$ kako bi dobili $N, p, q$.
2. Uniformno odabrati $y \in QR_N$.
3. Algoritam $\mathcal{A}$ za ulaz $(N, y)$ daje izlaz $x \in \mathbb{Z}_N^*$.
4. Rezultat eksperimenta je 1 akoje $x^2 \equiv y \pmod N$, odnosno 0 inače.

**Definicija 3.2.1.** *Kažemo da je računanje kvadratnih korijena teško u odnosu na GenModulus ako za svaki vjerojatnosni polinomijalni algoritam $\mathcal{A}$ postoji zanemariva funkcija negl takva da vrijedi*

$$P(SQR_{\mathbb{A},GenModulus}(n) = 1) \leq negl(n).$$

Jednostavno se pokazuje da ako je računanje kvadratnih korijena modulo složen broj $n$ teško u odnosu na $GenModulus$, tada je rastavljanje broja $N$ na proste faktore također teško u odnosu na $GenModulus$. Naime, ako bi se faktorizacija broja $n$ mogla lako odrediti,

tada bi također bilo jednostavno odrediti kvadratne korijene modulo $N$ kako je opisano u prethodnom poglavlju.

Nas zanima dokaz obrnute tvrdnje: ako je određivanje prostih faktora broja $N$ teško u odnosu na $GenModulus$, tada je problem računanja kvadratnih korijena modulo $N$ težak u odnosu na $GenModulus$. U dokazu te tvrdnje ćemo koristiti sljedeću lemu.

**Lema 3.2.2.** *Neka je $N = pq$ za $p$ i $q$ različite proste brojeve. Za brojeve $x, \hat{x}$ takve da je $x^2 \equiv y \pmod N$, ali $x \not\equiv \pm\hat{x} \pmod N$, moguće je odrediti rastav broja $N$ na proste faktore u polinomijalnom vremenu s obzirom na $||N||$ (pri čemu je $||N||$ broj bitova od $N$).*

*Dokaz.* Tvrdimo da je barem jedan od brojeva $nzd(N, x+\hat{x}), nzd(N, x-\hat{x})$ jednak jednom od prostih faktora broja $N$. Budući da je algoritam računanja najvećeg zajedničkog djelitelja polinomne složenosti, tada slijedi tvrdnja leme.

Ako je $x^2 \equiv \hat{x}^2 \pmod N$, tada je

$$0 \equiv x^2 - \hat{x}^2 \equiv (x - \hat{x}) \cdot (x + \hat{x}) \pmod N,$$

i stoga $N|(x - \hat{x})(x + \hat{x})$. Slijedi da $p|(x - \hat{x})(x + \hat{x})$, odnosno $p$ dijeli jednog od faktora. Uzmimo da $p|(x + \hat{x})$ (dokaz je sličan ukoliko uzmemo drugi slučaj). Ako bi vrijedilo da $q|(x + \hat{x})$, tada bi slijedilo da $N|(x + \hat{x})$ što je nemoguće zbog uvjeta $x \not\equiv \pm\hat{x} \pmod N$. Stoga vrijedi $q \not| (x + \hat{x})$, odnosno $nzd(N, x + \hat{x}) = p$. □

Navedimo još jednu definiciju koju ćemo koristiti u dokazu sljedećeg teorema. Promotrimo sljedeći eksperiment za dani algoritam $\mathcal{A}$ i parametar $n$.

Ekspreriment računanja prostih faktora $Factor_{\mathcal{A},GenModulus}$:

1. Pokrenuti algoritam $GenModulus(1^n)$ kako bi dobili $(N, p, q)$.
2. Algoritam $\mathcal{A}$ za zadani $N$ daje rezultat $p', q' > 1$.
3. Rezultat eksperimenta je 1 ako vrijedi $p' \cdot q' = N$, odnosno 0 inače.

**Definicija 3.2.3.** *Određivanje prostih faktora je teško u odnosu na GenModulus ako za sve vjerojatnosne polinomijalne algoritme $\mathcal{A}$ postoji zanemariva funkcija $negl$ takva da vrijedi*

$$P(Factor_{\mathcal{A},GenModulus}(n) = 1) \leq negl(n).$$

**Teorem 3.2.4.** *Ako je problem rastava broja na proste faktore težak u odnosu na GenModulus, tada je problem računanja kvadratnih korijena težak u odnosu na GenModulus.*

*Dokaz.* Neka je $\mathcal{A}$ vjerojatnosni polinomijalni algoritam koji računa kvadratne korijene. Neka je $\mathcal{A}_{fact}$ vjerojatnosni polinomijalni algoritam za računanje prostih faktora složenog broja.

Algoritam $\mathcal{A}_{fact}$: (Ulazni podatak algoritma je $N$.)

- Uniformno odabrati $x \in \mathbb{Z}_N^*$ i izračunati $y \equiv x^2 \bmod N$.
- Koristeći algoritam $\mathcal{A}(N, y)$ dobiti $\hat{x}$.
- Ako je $\hat{x}^2 \equiv y \pmod N$ i $\hat{x} \not\equiv \pm x \pmod N$ tada izračunati proste faktore od $n$ koristeći lemu 3.2.2.

Prema lemi 3.2.2 znamo da algoritam $\mathcal{A}_{fact}$ može izračunati proste faktore od $N$ onda kada je $\hat{x} \not\equiv \pm x \pmod N$ i $\hat{x}^2 \equiv y \pmod N$. Stoga je

$$P(Factor_{\mathcal{A}_{fact},GenModulus}(n) = 1) = P(\hat{x} \not\equiv \pm x \pmod N \wedge \hat{x}^2 \equiv y \pmod N)$$

$$= P(\hat{x} \not\equiv \pm x \pmod N \mid \hat{x}^2 \equiv y \pmod N) \cdot P(\hat{x}^2 \equiv y \pmod N), \quad (3.3)$$

pri čemu se gornje vjerojatnosti odnose na eksperiment $Factor_{\mathcal{A}_{fact},GenModulus}$. U tom eksperimentu modul $N$, koji je algoritmu $\mathcal{A}_{fact}$ ulazni podatak, dobiven je algoritmom $GenModulus$, a rezutat je rastav broja $N$ na faktore. Također, $y$ je uniformno odabran kvadratni ostatak modulo $N$ (jer je $x$ uniformno odabran iz skupa $\mathbb{Z}_N^*$). Sada vidimo da je rezultat algoritma $\mathcal{A}$ koji računa kvadratne korijene isti kao rezultat eksprerimenta $SQR_{\mathcal{A},GenModulus}(n)$, te vrijedi:

$$P(\hat{x}^2 \equiv y \pmod N) = P(SQR_{\mathcal{A},GenModulus}(n) = 1).$$

Uz uvjete eksperimenta $Factor$ na $y$ vidimo da vrijednost $x$ jednako vjerojatno može biti bilo koji od četiri kvadratna korijena od $y$. Budući da algoritam $\mathcal{A}$ za rezultat daje neki kvadratni korijen od $y$ možemo zaključiti da je vjerojatnost da je $\hat{x} \equiv \pm x \pmod N$ jednaka $\frac{1}{2}$ (uz naglasak da nema pretpostavki o tome kako je $\hat{x}$ distribuiran među kvadratnim korijenima od $y$). Dakle, vrijedi

$$P(\hat{x} \not\equiv \pm x \pmod N \mid \hat{x}^2 \equiv y \pmod N) = \frac{1}{2}.$$

Kombiniranjem prethodnih rezultata slijedi:

$$P(Factor_{\mathcal{A}_{fact},GenModulus}(n) = 1) = \frac{1}{2} \cdot P(SQR_{\mathcal{A},GenModulus}(n) = 1).$$

Budući da je problem rastava broja na proste faktore težak u odnosu na $GenModuls$, prema definiciji 3.2.2. postoji zanemariva funkcija $negl$ takva da vrijedi

$$P(Factor_{\mathcal{A}_{fact},GenModulus}(n) = 1) \leq negl(n),$$

iz čega slijedi $P(SQR_{\mathcal{A},GenModulus}(n) = 1) \leq 2 \cdot negl(n)$. Budući da je algoritam $\mathcal{A}$ bio proizvoljan, vrijedi tvrdnja teorema. □

Ovaj teorem nas navodi na promatranje familije jednosmjernih funkcija (Za funkciju $f$ kažemo da je jednosmjerna (one-way) ako je $f$ lako, a $f^{-1}$ teško izračunati):

- Algoritam *Gen* za ulaz $1^n$ pokreće algoritam $GenModulus(1^n)$ da bi dohvatio $(N, p, q)$ i za rezultat ima $I = N$. Domena je $D_I = \mathbb{Z}_N^*$, a slika funkcije je $R_I = QR_N$.
- Algoritam $Samp$ za ulazni podatak $N$ vraća uniformno odabrani $x \in \mathbb{Z}_N^*$.
- Algoritam $f$ za ulazne podatke $N$ i $x \in \mathbb{Z}_N^*$ vraća rezultat $x^2 \bmod N$.

Teorem 3.2.4 pokazuje da je ova familija funkcija jednosmjerna ako je rastavljanje broja na proste faktore teško u odnosu na *GenModulus*. Za $N = pq$, pri čemu su $p$ i $q$ različiti prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$ i za $D_I \subseteq \mathbb{Z}_N^*$ prethodno definirana familija jednosmjernih funkcija postaje familija jednosmjernih permutacija.

**Propozicija 3.2.5.** *Neka je $N = pq$, pri čemu su $p$ i $q$ različiti prosti brojevi takvi da je $p \equiv q \equiv 3$ (mod 4). Tada svaki kvadratni ostatak modulo $N$ ima točno jedan kvadratni korijen koji je kvadratni ostatak modulo $N$.*

*Dokaz.* Iz propozicije 1.1.2 slijedi da $-1$ nije kvadratni ostatak modulo $p$, niti modulo $q$. To slijedi zbog toga jer za $p \equiv q \equiv 3 \pmod 4$ vrijedi $p = 4i + 3$ za neki $i$, pa slijedi

$$(-1)^{\frac{p-1}{2}} = (-1)^{2i+1} \equiv -1 \bmod p$$

(jer je broj $2i + 1$ neparan). Neka je $y \leftrightarrow (y_p, y_q)$ proizvoljan kvadratni ostatak modulo $N$ s četiri kvadratna korijena

$$(x_p, x_q),\ (x_p, -x_q),\ (-x_p, x_q),\ (-x_p, -x_q).$$

Tvrdimo da je točno jedan od njih kvadratni ostatak modulo $N$. Pretpostavimo da je $J_p(x_p) = 1$ i $J_q(x_q) = -1$. Primjenom propozicije 1.1.3 slijedi da je

$$J_q(-x_q) = J_q(-1) = J_(x_q) = 1,$$

te je $(x_p, -x_q)$ kvadratni ostatak modulo $N$ (primjenom propozicije 1.2.2). Slično, $J_p(-x_p) = -1$ te niti jedan drugi kvadratni korijen od $y$ nije kvadratni ostatak modulo $N$. □

Kada malo drugačije izrazimo propoziciju 3.2.5, dobivamo da je za $N = pq$, pri čemu su $p$ i $q$ različiti prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$, funkcija $f_N : QR_N \to QR_N$, zadana pravilom pridruživanja $f_N(x) = x^2 \bmod N$, permutacija nad $QR_N$. Prilagodbom algoritma $Samp$ tako da vraća uniformno odabrani $x \in QR_N$ dobivamo familiju jednosmjernih permutacija koja se naziva Rabinova familija permutacija.

**Teorem 3.2.6.** *Neka je GenModulus algoritam koji za ulazan podatak $1^n$ daje rezultat $(N, p, q)$ pri čemu je $N = pq$ i $p$ i $q$ su različiti prosti brojevi skoro uvijek (tj. vjerojatnost neuspjeha je zanemariva) i vrijedi $p \equiv q \equiv 3$ (mod 4). Ako je rastavljanje broja na proste faktore teško u odnosu na GenModulus, tada postoji Rabinova familija permutacija.*

## Usporedba Rabinovog kriptosustava i RSA kriptosustava

RSA kriptosustav su izumili Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Navodimo definiciju tog kriptosustava:

**Definicija 3.2.7.** *Neka je $N = p \cdot q$, gdje su $p$ i $q$ prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$, te $\mathcal{K} = \{(n, p, q, d, e) \ : \ N = pq,\ p, q \text{ prosti}, de \equiv 1 \ (mod\ \phi(n))\}$. Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo*

$$e_K(x) = x^e \ mod\ N \text{ i } d_K(y) = y^d \ mod\ N,\ x, y \in \mathbb{Z}_N.$$

*Vrijednosti $N$ i $e$ su javne, a vrijednosti $p$, $q$ i $d$ su tajne.*

Kada govorimo o sigurnosti koju ovi kriptosustavi pružaju znamo da je računanje kvadratnih korijena modulo složen broj jednako teško kao određivanje prostih faktora složenog broja. Nije poznato je li sigurnost RSA kriptosustava implicirana razinom složenosti određivanja prostih faktora složenog broja. Stoga možemo reći da je Rabinova familija permutacija bazirana na slabijoj pretpostavci: teoretski je moguće da netko razvije učinkovit algoritam za rješavanje RSA problema, ali računanje kvadratnih korijena će ostati jednako teško. Također je moguće da netko razvije algoritam za rješavanje RSA problema koji će biti brži od poznatih algoritama za rastavljanje broja na proste faktore. Lema 3.2.2 nam osigurava da računanje kvadratnih korijena modulo $N$ ne može biti mnogo brže od najboljeg algoritma za rastavljanje broja $N$ na proste faktore.

Kada govorimo o učinkovitosti, ova dva kriptosustava su jako slična. Ako se kod RSA kriptosustava koristi veliki eksponent $e$, tada je računanje $e$-te potencije (kao u RSA kriptosustavu) malo sporije od kvadriranja (kao u Rabinovom kriptosustavu). S druge strane, potrebno je biti malo pažljiviji kod rada s Rabinovom familijom permutacija jer se radi samo od podskupu skupa $\mathbb{Z}_N^*$.

RSA permutacije se više koriste u praksi nego Rabinove permutacije, ali razlog tome je više povijesna slučajnost (RSA je objavljen dvije godine ranije) nego tehnička prednost.

# Bibliografija


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

[2] Katz, J., Lindell Y.: *Introduction to modern cryptography*. CRC Press, 2015.

[3] Menezes, A., van Oorschot P. Vanstone V.: *Handbook of Applied Cryptography*. CRC Press, 1996.

[4] Stinson, D. R.: *Cryptography. Theory and practice*. CRC Press, 2006.

# Sažetak

U ovom radu smo proučavali dva kriptosustava s javnim ključem, Goldwasser-Micalijev kriptosustav i Rabinov kriptosustav. Da bismo mogli nešto reći o sigurnosti tih kriptosustava, proučavali smo kvadratne ostatke po prostom i složenom modulu te određivanje kvadratnih korijena po prostom i složenom modulu.

U prvom poglavlju smo promotrili osnovne rezultate vezane u kvadratne ostatke po prostom i složenom modulu. Najprije smo dokazali tvrdnju da svaki kvadratni ostatak u skupu $\mathbb{Z}_p^*$, pri čemu je $p$ prost broj, ima točno dva kvadratna korijena. Zatim smo definirali Legendreov simbol te pokazali propoziciju koja nam je omogućila jednostavno određivanje je li element skupa $\mathbb{Z}_p^*$ kvadratni ostatak ili neostatak, pri čemu je $p$ prost broj. Zatim smo te rezultate poopćili na složeni modul koristeći Kineski teorem o ostacima, definirali smo Jacobijev simbol, te smo pokazali primjer određivanja kvadratnih ostataka po složenom modulu.

U sljedećem poglavlju smo proučavali Goldwasser-Micalijev kriptosustav s javnim ključem. Najprije smo detaljno promotrili definiciju tog kriptosustava te proces kriptiranja i dekriptiranja. Proces kriptiranja i dekriptiranja smo pokazali i na jednostavnom primjeru. Zatim smo promotrili sigurnost tog kriptosustava te smo uočili da je sigurnost tog kriptosustava osigurana činjenicom da je problem određivanja je li element kvadratni ostatak težak. Na kraju ovog poglavlja smo definirali i opisali CPA-sigurnost kriptosustava, odnosno otpornost kriptosustava na napade odabranim javnim tekstovima.

U posljednjem poglavlju smo naveli definiciju Rabinovog kriptosustava te opisali proces kriptiranja i dekriptiranja. Zatim smo pobliže proučili računanje kvadratnih korijena po prostom i složenom modulu kako bi mogli detaljnije objasniti proces dekriptiranja što smo pokazali i na primjeru. Zatim smo promatrali sigurnost Rabinovog kriptosustava te smo uz niz rezultata došli do zaključka da je sigurnost Rabinovog kriptorustava osigurana činjenicom da je problem računanja kvadratnih korijena jednako težak kao određivanje prostih faktora složenog broja. I na kraju smo ukratko usporedili Rabinov kriptosustav s RSA kriptosustavom te smo uočili da su vrlo slični, podjednako učinkoviti te da je sigurnost Rabinovog kriptosustava osigurana činjenicom da je problem računanja kvadratnih korijena jednako težak kao određivanje prostih faktora složenog broja, za razliku od RSA kriptosustava za koji ne možemo dokazati takvu implikaciju.

# Summary

In this thesis we observed two public key cryptosystems, Goldwasser-Micali and Rabin cryptosystem. In order to say something about security of those cryptosystems we studied quadratic residues modulo a prime and composite number, and computing square roots module a prime and composite number.

In first chapter we showed several results about quadratic residues modulo a prime and composite number. First we showed that every quadratic residue in $\mathbb{Z}_p^*$ has exactly two square roots. Then we defined Legendre's symbol and showed proposition that enabled simple algorithm for testing whether an element $x \in \mathbb{Z}_p^*$ is a quadratic residue. Then we expanded those results to composite module using Chinese remainder theorem, defined Jacobi symbol and showed an example of computing quadratic residues modulo a composite number.

In next chapter we defined Goldwasser-Micali public key cryptosystems. We explained encryption and decryption process and showed a simple example. Then we looked at security of this cryptosystem and noticed that it is assured by the fact that quadratic residuosity problem is hard. At the end of this chapter we described and defined CPA-security of cryptosystem.

In final chapter we studied Rabin public key cryptosystems. We defined Rabin cryptosystem and explained encryption and decryption process. Then we studied computing square roots modulo a prime and composite number. We used those results to show decryption process in more details. Then we showed that security of Rabin cryptosystem is assured by the fact that computing square roots is hard. In the end we compared Rabin and RSA cryptosystem. These cryptosystems are very similar and equally efficient. In terms of security we showed that hardness of computing square roots is equivalent to hardness of factoring, whereas hardness of solving the RSA problems not known to be implied by the hardness of factoring.

# Životopis

Rođena sam 5.11.1990. u Zagrebu. Moja obitelj je 1995. godine preselila u Suhaju, malo selo pored grada Čazme, gdje živimo i danas. Živim s majkom, ocem i dva brata. Osnovnu i srednju školu sam pohađala u Čazmi te sam opću gimnaziju završila 2009. godine. Tijekom školovanja u srednjoj školi otkrila sam svoje zanimanje za matematiku te sam nakon toga upisala Preddiplomski studij Matematika na Prirodoslovno-matematičkom fakultetu u Zagrebu koji sam završila 2014. godine i stekla zvanje sveučilišne prvostupnice matematike. Zatim sam upisala Diplomski studij Matematika i informatika; smjer: nastavnički. Tijekom diplomskog studija sam stekla znanja o edukaciji matematike i informatike u osnovnoj i srednjoj školi te sam postala jako zainteresirana za rad u školi. U listopadu 2016. godine sam započela s radom u osnovnoj školi te planiram graditi svoju karijeru u tom zanimanju.