Pellova jednadžba u kriptografiji javnog ključa

Atanasov, Violeta

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Violeta Atanasov

PELLOVA JEDNADŽBA U KRIPTOGRAFIJI JAVNOG KLJUČA

Diplomski rad

Voditelj rada:
doc. dr. sc. Zrinka Franušić

Zagreb, svibanj, 2015

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

Danas živimo u svijetu gdje sigurnost naših informacija i naše komunikacije nikada nije bila upitnija. Ne postoji garancija za privatnost, te broj i sofisticiranost napada raste, a uspješnost takvih napada može rezultirati ne samo velikim novčanim gubitcima, već i iznošenju u javnost važnih informacija, koje mogu narušiti ljudsku reputaciju. Zato danas, više nego ikada raste potreba za razvojem raznih tehnologija koje će zaštititi našu komunikaciju. Jedna od sastavnih disciplina koja osigurava našu komunikaciju je upravo kriptografija, koja svoje korijene vuče još iz doba Antike. Kratko rečeno, kriptografija je izučavanje i razvoj tehnika za izmjenu informacija, koje su nerazumljive svima osim onima koji žele izmijeniti željene poruke.

Komunikacija u suvremenom svijetu, odvija se pomoću kanala koji su nesigurni, kao što su mobiteli, Internet i drugi. Ako pošiljalac Alice i primalac Bob žele komunicirati koristeći nesigurni kanal, te žele osigurati da nitko drugi osim njih može pročitati njihovu poruku, koristiti će određeni kriptosustav. Uobičajeni kriptosustav možemo zamisliti kao veliku kolekciju transformacija – šifri, koje će početnu poruku prevesti u nerazumljivu šifriranu poruku, pri čemu će poruka biti razumljiva primatelju Bobu, ako zna koju je transformaciju koristila Alice. Informacija koja omogućava transformaciju koju koristi Alice zovemo ključ. Važno je istaknuti da ako neka osoba prima neku poruku i njezin kriptirani ekvivalent, ona ne bi trebala moći odredit ključ iz dan informacije. Sustav ne bi trebao biti osjetljiv na napade temeljene na snalažljivosti. Proces u kojem neka osoba pri primanju nekog šifriranog teksta određuje originalnu poruku bez prethodnog poznavanja ključa nazivamo kriptoanaliza. Kada takav proces uspije, kažemo da je sustav probijen. Kriptologija proučava kriptografiju i kriptoanalizu. Vezano za nju navedimo i slavnu izreku Edgara Allana Poe-a :

„Malo ljudi možemo uvjeriti da nije lako izmisliti metodu tajnog pisanja koja će pokvariti plan istrage. Ipak, možemo u potpunosti konstatirati da ljudska domišljatost ne može skovati šifru koju ljudska domišljatost ne može razriješiti.“

Naravno, to znači da se u danom trenutku ključ mora prenijeti od pošiljaoca do primaoca na vrlo sigurnan način. U simetričnim kriptosustavima, to se na primjer mora odviti različitim i mnogo sigurnijim komunikacijskim kanalom nego onim koji se koristi za slanje šifriranih poruka. Kako su odvojeni komunikacijski kanali skupi i nepraktični za korištenje,

jedan dio moderne kriptografije bavi se problemom sigurnog slanja ključa nesigurnim kanalom.

Tako se pojavila i metoda izbjegavanja korištenja posebnog komunikacijskog kanala koristeći kriptosustav s javnim ključem. U takvom sustavu, svaki sudionik ima dva ključa, tajni i javni. Ideja je da poznavanje javnog ključa ne otkriva nikakve podatke o tajnom ključu. Dakle, tko god želi poslati sigurnu poruku nekom od sudionika, koristi vlastiti javni ključ, lako dostupan u javnom direktoriju. Pojedinac kojemu je poruka poslana jedini zna svoj privatni ključ, te ga koristi da bi dešifrirao šifriranu poruku, što nitko drugi ne može. Prvi primjer kriptosustava s javnim ključem je poznat pod imenom RSA po imenima svojih izumitelja Rivestu, Shamiru i Adelmanu. Brzo je uslijedila i ideja digitalnog potpisa te su se verzije ova dva protokola u potpunosti prilagodila u raznim standardima i u svakodnevnoj upotrebi. Važno je naglasiti da je potrebno uložiti mnogo truda i pažnje da bi se implementirala takva tehnika šifriranja, ali ako se pravilno izvede, dana shema vrlo dobro odolijeva napadima. U ovom radu opisat ćemo kriptosustav nalik sustavu RSA koji za šifriranje koristi rješenja Pellove jednadžbe.

Ovaj rad sastoji se od tri poglavlja, od kojih su prva dva uvodnog tipa. U prvom poglavlju iznosimo neke osnovne činjenice o kriptografiji, posebice kriptografiji javnog ključa. U drugom poglavlju bavimo se Pellovom jednadžbom, $x^2 - Dy^2 = 1$, gdje je D prirodan broj koji nije potpun kvadrat. Pokazujemo da je Pellova jednadžba rješiva i opisujemo skup njenih rješenja. U trećem poglavlju opisujemo kriptosustav s javnim ključem, koji za šifriranje koristi skup rješenja Pellove jednadžbe modulo prirodan broj n, oblika $n = p \cdot q$, gdje su p i q prosti.

Poglavlje 1

Kriptografija javnog ključa

1.1 Kriptografija

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka na način da poslanu poruku ne može razumjeti nitko osim željenog primatelja. Željeli bismo omogućiti pošiljaocu i primaocu sigurnu komunikaciju koja se u današnje vrijeme odvija najčešće pomoću računalnih mreža, no i drugih komunikacijskih kanala, koji su nesigurni, te ih je lako prisluškivati i doći u posjed razno raznih podataka. Osobu koja šalje poruku se često naziva *Alice*, dok se osoba koja ju prima naziva *Bob*. Poruku koju još zovemo i *otvoreni tekst* pošiljalac Alice šalje primaocu Bobu, tako da ju transformira koristeći unaprijed dogovoreni *ključ*. Ovaj postupak transformiranja poruke nazivamo *šifriranje*, a dobivenu šifriranu poruku *šifrat*. Alice šalje šifrat preko nekog komunikacijskog kanala Bobu, koji zna ključ kojim je poruka šifrirana, te može odrediti otvoreni tekst. Postupak transformacije šifrata u otvoreni tekst nazivamo *dešifriranje*. Prilikom postupka slanja poruka, dolazi do prisluškivanja, no osoba koja prisluškuje ne može odrediti otvoreni tekst, već vidi samo šifrat. Pogledajmo formalnu definiciju kriptosustava.

Definicija 1.1.1. *Kriptosustav je uredena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1) $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta,*

2) $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata,*

3) $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva,*

4) Za svaki $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i funkcija dešifriranja* $d_K \in \mathcal{D}$*. Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$*.*

Napomena 1.1.2. *Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$. Iz njega slijedi da funkcije e_K moraju biti injekcije. Zaista, ako bi bilo*

$$e_K(x_1) = e_K(x_2) = y,$$

za dva različita otvorena teksta x_1 i x_2, onda primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2, tj. $d_K(y)$ ne bi bilo definirano. U skladu s tim imamo da ako je $\mathcal{P} = C$, onda su funkcije e_K permutacije.

Kriptosustave obično klasificiramo s obzirom na kriterije kao što su tip operacija koje se koriste pri šifriranju, gdje imamo supstitucijske te transpozicijske šifre, zatim na način na koji se obrađuje otvoreni tekst gdje razlikujemo blokovne, te protočne šifre, te kriterij tajnosti i javnosti ključeva. Zadnji kriterij dijeli kriptosustave na *simetrične* i *asimetrične*, odnosno *kriptosustave s javnim ključem*.

Kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje se može izračunati poznajući ključ za šifriranje i obratno. Štoviše, ovi su ključevi najčešće identični. Sigurnost ovih kriptosustava leži u tajnosti ključa što je i njihov veliki nedostatak, jer pošiljalac i primalac prije šifriranja moraju razmijeniti tajni ključ preko nekog sigurnog komunikacijskog kanala, te radi sigurnosti moraju često mijenjati ključeve što može biti veliki problem.

1.2 Kriptosustav s javnim ključem

Ideja javnog ključa je u tome da se konstruiraju kriptosustavi kod kojih je iz poznavanja funkcije šifriranja nemoguće, u nekom realnom vremenu izračunati funkciju dešifriranja, te je ključ za šifriranje javan. Pomoću njega, bilo tko može šifrirati poruku ali samo osoba koja ima odgovarajući ključ za dešifriranje, to jest tajni ključ, može dešifrirati tu poruku. Ključnu ulogu imaju funkcije koje zovemo *jednosmjerne funkcije*. To su funkcije za koje vrijedi da je f lako, a f^{-1} teško izračunati. Ako se f^{-1} može lako izračunati uz neki dodatni podatak (*trapdoor*- skriveni podatak), onda f nazivamo *osobna jednosmjerna funkcija*. Ideju javnog ključa prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine, kada su dali prijedlog rješenja problema razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala.

Definicija 1.2.1. *Kriptosustav s javnim ključem se sastoji od dviju familija funkcija $\{e_K\}$ i $\{d_K\}$ - za šifriranje i dešifriranje, pri čemu K prolazi skupom svih mogućih korisnika, sa svojstvima*

1. *d_K je inverz od e_K,*

2. *e_K javan, tj. javni ključ, a d_K je poznat samo osobi K, tj. tajni ključ,*

3. *e_K osobna jednosmjerna funkcija,*

Ako Alice želi Bobu poslati poruku x, tada Alice šifrira svoju poruku pomoću Bobovog javnog ključa e_B i šalje šifrat $y = e_B(x)$. Bob dešifrira šifrat koristeći svoj tajni ključ d_B, $d_B(y) = d_B(e_B(x)) = x$.

Želi li više korisnika komunicirati na ovaj način, tada svi korisnici stave svoje javne ključeve u neku javnu datoteku. Ipak, postavlja se pitanje kako Bob može biti siguran da je poruku primio od Alice, s obzirom da svatko ima pristup funkciji e_B, pa se postavlja pitanje vjerodostojnosti i autentičnosti poruke. To se može riješiti na način da Alice doda svojoj poruci slučajan broj a od recimo 10 znamenaka. Bob generira svoj slučajan 10-znamenkasti broj b, te pošalje Alice poruku $e_A(a + b)$. Alice izračuna b pomoću formule $b = d_A(e_A(a + b)) - a$, te sada ponovo pošalje svoju prvu poruku tako da joj doda b, a isto to učini i sa svakom idućom porukom koju šalje Bobu.

Kriptosustav s javnim ključem daje mogućnost digitalnog potpisa, te tada Alice ne može zanijekati da je upravo ona poslala konkretnu poruku. Pretpostavimo da je $\mathcal{P} = C$. Tada Alice može potpisati poruku x tako da Bobu pošalje šifrat $z = d_A(y) = d_A(e_B(x))$. Kad Bob primi poruku za koju pretpostavlja da mu je poslala Alice, on najprije primijeni javni ključ e_A, a potom svoj tajni ključ d_B

$$d_B(e_A(z)) = d_B(e_A(d_A(e_B(x)))) = x.$$

Sada Bob zna sigurno da je poruku poslala Alice, jer je samo on mogao upotrijebiti funkciju d_A. Da je umjesto te funkcije upotrijebljena neka treća funkcija d_C, kao rezultat ne bi dobili smislenu poruku. Ako bi Alice kasnije zanijekala da je ona poslala poruku, Bob bi to mogao dokazati iz x i z jer mora vrijediti $e_B(x) = e_A(z)$.

Glavne prednosti kriptosustava s javnim ključem u usporedbi sa simetričnima su to što nema potrebe za sigurnim komunikacijskim kanalom za razmjenu ključeva, za komunikaciju grupe od N ljudi treba $2N$ ključeva, za razliku od $N(N-1)/2$ ključeva kod simetričnog kriptosustava, te mogućnost potpisa poruke.

Dani sustav s javnim ključem ima i neke nedostatke. Algoritmi s javnim ključem puno su sporiji od modernih simetričnih algoritama. Drugi nedostatak jest da se jednostavno može odrediti otvoreni tekst ako je n mali. Ako je $y = e(x)$, gdje otvoreni tekst može poprimiti jednu od n vrijednosti, onda, budući je e javna, kriptoanalitičar treba samo šifrirati svih n mogućih otvorenih tekstova i rezultat usporediti s y.

U realnom svijetu kriptografija javnog ključa ipak ne predstavlja zamjenu za simetrične kriptosustave. Ona se ne koristi za šifriranje poruka, već za šifriranje ključeva. Naime, osobe A i B komuniciraju pomoću simetričnog kriptosustava s ključem kojeg su razmijenili pomoću kriptosustava s javnim ključem. To se zove *hibridni* kriptosustav.

1.3 Primjeri kriptosustava s javnim ključem

RSA kriptosustav

RSA kriptosustav najpoznatiji je i najšire korišteni kriptosustav s javnim ključem, a izumili su ga Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Ujedno je i i prvi kriptosustav s javnim ključem, a njegova sigurnost temelji se na teškoći faktorizacije velikih prirodnih brojeva.

Definicija 1.3.1 (RSA kriptosustav)**.** *Neka je $n = p \cdot q$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = C = \mathbf{Z}_n$, te*

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

Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo funkcije za šifriranje i dešifriranje:

$$e_K(x) = x^e \pmod{n},\ \ d_K(y) = y^d \pmod{n},$$

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

Napomena 1.3.2. *U prethodnoj definiciji $\varphi(n)$ predstavlja Eulerovu funkciju, to jest broj brojeva u nizu 1, 2, ... , n koji su relativno prosti s n. U našem konkretnom slučaju je $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.*

Sigurnost RSA leži u činjenici da je funkcija $e_K(x) = x^e \pmod{n}$ jednosmjerna. Dodatni podatak (trapdoor) koji omogućava dešifriranje je poznavanje faktorizacije $n = pq$, jer je tada lako izračunati $\varphi(n) = \varphi(pq) = (p-1)(q-1)$, te dobiti eksponent d iz $de \equiv 1 \pmod{\varphi(n)}$, pomoću Euklidovog algoritma.

Opišimo postupak kojim korisnik izabire parametre u RSA kriptosustavu:

1. Primaoc tajno odabere dva različita prosta broja p i q, od kojih svaki ima oko 100 znamenki, te obično jedan od njih ima nekoliko znamenki više od drugog. Odabir se izvrši tako da se pomoću nekog generatora slučajnih brojeva generira dovoljno velik prirodan broj m, a zatim se korištenjem nekog testa za testiranje prostosti, traži prvi prosti broj koji je veći ili jednak m. (Potrebno je $O(\log m)$ operacija.)

2. Nadalje računa $n = pq$ i $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$. (Potrebno je $O(\log^2 n)$ operacija.)

3. Na slučajan način bira broj e takav da je $e < \varphi(n)$ i $(\varphi(n), e) = 1$, te nakon toga tajno izračunava d tako da je $de \equiv 1 \pmod{\varphi(n)}$, tj. $d \equiv e^{-1} \pmod{\varphi(n)}$. To radi pomoću Euklidovog algoritma. (Potrebno je $O(\log^3 n)$ operacija.)

4. Na kraju, primaoc stavlja ključ za šifriranje (n, e) u javni direktorij.

Postupak šifriranja poruke $e_k(x)$ naziva se modularno potenciranje. Za efikasnost RSA kriptosustava je bitno da se računanje $e_K(x) = x^e \pmod{n}$ može vrlo efikasno provesti pomoću algoritma *Kvadriraj i množi*. Prvo e prikažemo u bazi 2:

$$e = e_0 + 2 \cdot e_1 + ... + 2^{s-1} \cdot e_{s-1},$$

gdje je $e_{s-1} = 1$ i $e_o, \ldots, e_{s-2} \in \{0, 1\}$. Zatim primijenimo algoritam:
$y = 1$
za $i = s - 1, \ldots, 1, 0$
$y = y^2 \pmod{n}$
ako je $e_i = 1$, onda $y = y \cdot x \pmod{n}$

Očito je ukupan broj množenja manji ili jednak $2s$. U konačnici, algoritam za RSA je polinomijalan.

Opišimo sada gornji postupak primjerom:

Primjer 1.3.3. *Radi jedostavnosti, ipak ćemo odabrati manje brojeve. Neka Bob odabere* $p = 47$ *i* $q = 59$ *i računa:*

$$n = pq = 2773$$
$$\varphi(n) = (p - 1)(q - 1) = 2668$$

Zatim odabere $e = 17$ *i pomoću proširenog Euklidovog algoritma izračuna multiplikativni inverz od e, to jest rješava kongruenciju de* $\equiv 1 \pmod{\varphi(n)}$*, te dobiva da je* $d = 157$.

Vrijednosti p, q i d su tajne, a n i e javne, te ih Bob šaje Alice ili ih stavlja u javnu datoteku.

Recimo sada, da Alice želi posati poruku DIPLOMSKI RAD. Koristeći

$$\{razmak = 00, A = 01, B = 02, ..., Y = 25, Z = 26\},$$

zapišemo poruku u obliku :

$$x = 04091612151319110900180104$$

Jer je je $x > n$*, x se grupira u blokove od po četiri znamenke, počevši sa lijeve strane. Zadnji blok, ukoliko mu nedostaje znamenki, dopuni se nulama. Sada je:*

$$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (0409, 1612, 1513, 1911, 0900, 1801, 0400).$$

Alice iz $n = 2773$ i $e = 17$ računa:

$$\begin{aligned} y_1 &= 0409^{17} \pmod{2773} = 2510 \\ y_2 &= 1612^{17} \pmod{2773} = 1908 \\ y_3 &= 1513^{17} \pmod{2773} = 1132 \\ y_4 &= 1911^{17} \pmod{2773} = 2702 \\ y_5 &= 0900^{17} \pmod{2773} = 1510 \\ y_6 &= 1801^{17} \pmod{2773} = 2003 \\ y_7 &= 0400^{17} \pmod{2773} = 17 \end{aligned}$$

Dobiveni šifrat

$$(y_1, y_2, y_3, y_4, y_5, y_6, y_7) = (2510, 1908, 1132, 2702, 1510, 2003, 0017),$$

to jest

$$y = (25101908113227021510200300 17)$$

šalje Bobu. Bob pomoću $d = 157$, koji je samo njemu poznat, računa na isti način dijeleći y na blokove,

$$x_i = y_i^{157} \pmod{2773},\ i = 1, 2, \ldots, 8,$$

te dobiva originalnu poruku DIPLOMSKI RAD.

Rabinov kriptosustav

Rabinov kriptosustav izumio je Michael Rabin, 1979. godine, te je zasnovan na teškoći nalaženja kvadratnog korijena modulo fiksni složeni broj. Pokazuje se da je ovaj problem ekvivalentan problemu faktorizacije.

Definicija 1.3.4 (Rabinov kriptosustav)**.** *Neka je $n = p \cdot q$, gdje su p i q prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$. Neka je $\mathcal{P} = \mathcal{C} = \mathbf{Z}_n$ i definiramo $\mathcal{K} = \{(n, p, q) : n = pq\}$.*

Za $K \in \mathcal{K}$ definiramo:

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

$$d_K(y) = \sqrt{y} \mod n,$$

pri čemu $x = \sqrt{y}$ predstavlja rješenje kongruencije $x^2 \equiv y \pmod n$. Vrijednost n je javna, a vrijednosti p i q su tajne.

Žele li Alice i Bob izmijeniti poruke, Alice prvo treba saznati Bobov javni ključ. Označimo taj ključ s n. Izračuna $y = x^2 \pmod n$ i šalje Alice šifrat y. Kako bi Bob rekonstruirao poruku iz šifrata, treba pronaći kvadratni korijen od x modulo n. No, postoje

točno četiri takva korijena. Zaista, rješenja kogruencije $x^2 \equiv y \pmod{p}$ gdje je $p \equiv 3 \pmod 4$ su

$$x \equiv y^{(p+1)/4} \pmod{p}.$$

Stoga rješenja kogruencije $x^2 \equiv y \pmod{n}$ zadovoljavaju sustave kongruencija

$$x \equiv y^{(p+1)/4} \pmod{p},\ x \equiv y^{(q+1)/4} \pmod{q},$$

za sve kombinacije predznaka. Jasno je da će svaki sustav dati točno jedno rješenje modulo n prema Kineskom teoremu i stoga postoje četiri moguća otvorena teksta x_1, x_2, x_3, x_4. No, kako znati koja je od dobivenih poruka ispravna. To se rješava tako što se dogovori da će poruka zapisana u binarnom zapisu sadržavati određenu pravilnost. Na primjer, posljednja četiri bita su ista.

Primjer 1.3.5. *Dvije osobe, Alice i Bob žele izmijeniti poruke, te prvo Bob odabire p i q. Neka je p=11 i q=23, te je onda n=253 javni ključ, a (11,23) tajni. Alice dobiva taj javni ključ, te šifrira svoju tajnu poruku. Neka je poruka x= 47, pa je šifrat onda jednak*

$$y = x^2 \pmod{n} = 185.$$

Alice Bobu šalje šifriranu poruku, te on mora razriješiti izraz $x^2 = 185 \pmod{253}$*, to jest*

$$x^2 = 185 \pmod{11} \quad i \quad x^2 = 185 \pmod{23}.$$

Jer je $11 \equiv 3 \pmod 4$ *i* $23 \equiv 3 \pmod 4$*, može koristiti formulu* $x \equiv y^{(p+1)/4} \pmod{p}$*, te dobiva*

$$185^{(11+1)/4} \equiv 185^3 \equiv 3 \pmod{11} \quad i \quad 185^{(23+1)/4} \equiv 185^6 \equiv 1 \pmod{23}.$$

Sada koristi Kineski teorem o ostacima da bi našao kvadratne korijene od 185 modulo $253 = 11 \cdot 23$*, rješavajući četiri sustava linearnih kongruencija*

$$x = \pm 3 (mod 11) \quad i \quad x = \pm 1 (mod 23),$$

te dobiva da je mogući otvoreni tekst $x_1 = 47, x_2 = 206, x_3 = 162, x_4 = 91$*. Zapiše li Bob ova četiri broja binarno, dobiva:* $47 = 101111$*,* $206 = 11001110$*,* $162 = 10100010$ *i* $91 = 1011011$*. Znajući da je Alice koristila dogovorenu pravilnost, te njena poruka u binarnom zapisu sadrži četiri ista bita na posljednja četiri mjesta, konačno zaključuje da je otvoreni tekst* $x = 47$*.*

Ostali kriptosustavi

Opišimo ukratko još dva kriptosustava. ElGamalov kriptosustav zasnovan je na teškoći računanja diskretnog logaritma u konačnim poljima, a izumio ga je Taher ElGamal 1985. godine. Dokazano je da je taj problem otprilike jednake težine kao problem faktorizacije velikog broja n. Navedimo i njegovu definiciju.

Definicija 1.3.6 (ElGamalov kriptosustav)**.** *Neka je p prost broj i $\alpha \in \mathbb{Z}_p*$ primitivni korijen modulo p. Neka je $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ i*

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

Vrijednosti p, α, i β su javne, a vrijednost a je tajna.
Za $K = (p, \alpha, a, \beta) \in \mathcal{K}$ i tajni slučajni broj $k \in \mathbb{Z}_p$ definiramo:

$$e_K(x, k) = (y_1, y_2),$$

gdje je $y_1 = \alpha^k \mod p$ i $y_2 = x\beta^k \mod p$.
Za $y_1, y_2 \in \mathbb{Z}p*$ definiramo

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

Napomena 1.3.7. *Primijetimo da je ovdje $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ i $\mathbb{Z}_n^* = \{0 < k < n : (k, n) = 1\}$. Također, ako je α primitivni korijen modulo p, tada je $\{\alpha^i : i = 0, 1, \ldots, p-2\} = \mathbb{Z}_p^*$.*

Merkle-Hellmanov kriptosustav temelji se na takozvanom problemu ruksaka, a izumili su ga Ralph Merkle i Martin Hellman, 1978. godine. Problem ruksaka kaže da ako imamo n predmeta s volumenima $v_1, v_2, \ldots, v_n$ koje želimo staviti u ruksak volumena V, tražiti ćemo podskup $J \subseteq \{1, 2, \ldots, n\}$ tako da je $\Sigma_j v_j = V$, gdje suma ide po svim $j \in J$. Navedimo definiciju Merkle-Hellmanovog kriptosustava.

Definicija 1.3.8 (Merkle-Hellmanov kriptosustav)**.** *Neka je $v = (v_1, v_2, \ldots, v_n)$ superrastući niz prirodnih brojeva, te neka je $p > v_1 + \cdots + v_n$ prost broj i $1 \leq a \leq p-1$. Za $1 \leq i \leq n$ definiramo $t_i = av_i \pmod{p}$ i označimo $t = (t_1, \ldots, t_n)$. Neka je $\mathcal{P} = \{0,1\}^n$, $C = \{0, 1, \ldots, n(p-1)\}$ i $\mathcal{K} = \{(v, p, a, t)\}$, gdje su v, p, a i t konstruirani na gore opisani način. Za $K = (v, p, a, t)$ definiramo:*

$$e_K(x_1, \ldots, x_n) = x_1 t_1 + x_2 t_2 + \cdots + x_n t_n.$$

Za $0 \leq y \leq n(p-1)$ definiramo $z = a^{-1} y \pmod{p}$, riješimo (superrastući) problem ruksaka za skup $\{v_1, \ldots, v_n, z\}$ i tako dobivamo $d_K(y) = (x_1, \ldots, x_n)$. Vrijednost t je javna, dok su vrijednosti p, a i v tajne.

Poglavlje 2

Pellova jednadžba

2.1 Definicija Pellove jednadžbe

U ovom poglavlju bavit ćemo se Pellovom jednadžbom, te opisati kako dolazimo do njenih rješenja. Pellova jednadžba je specijalni oblik diofantske jednadžbe drugog stupnja u dvije nepoznanice. Općenito, diofantska jednadžba je svaka polinomijalna jednadžba s cjelobrojnim koeficijentima čija rješenja tražimo u prstenu cijelih brojeva, ili iznimno u polju racionalnih. Glavno pitanje koje se uvijek postavlja jest je li dana diofantska jednadžba rješiva. Ukoliko jest, dalje se nameće pitanje ima li konačno ili beskonačno mnogo rješenja. U slučaju kada ih je beskonačno mnogo, zanima nas možemo li ih nekako okarakterizirati. Jedan od najpoznatijih primjera diofatnske jednadžbe stupnja dva je Pitagorina jednadžba

$$x^2 + y^2 = z^2. \tag{2.1}$$

Ako je $(x, y, z) \in \mathbb{Z}^3$ neko njeno rješenje, onda su to i sve trojke oblika $(\pm x, \pm y \pm z)$. Iz tog razloga jednadžbu (2.1) ima smisla rješavati samo u skupu prirodnih brojeva. Vrlo su nam dobro poznate trojke $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ koje zadovoljavaju ovu jednadžbu. Štoviše, ova jednadžba ima beskonačno mnogo rješenja. Konkretno, postoji i parametarska reprezentacija svih rješenja dana s

$$(d(n^2 - m^2), 2dmn, d(m^2 + n^2)) \tag{2.2}$$

gdje $d \in \mathbb{Z}$, $n > m > 0$, te m i n relativno prosti brojevi ($(m, n) = 1$), različite parnosti

Promotrimo sada jednadžbu

$$x^2 + ay^2 = z^2, \tag{2.3}$$

za neki cijeli broj a. Koristeći analogiju s (2.2), lako se vidi da vrijedi

$$(m^2 - an^2)^2 + a(2mn)^2 = (m^2 + an^2)^2,$$

odnosno trojke

$$(d(m^2 - an^2), 2dmn, d(m^2 + an^2)), \tag{2.4}$$

za $d, m, n \in \mathbb{Z}$ predstavljaju rješenje jednadžbe (2.3). No, pitamo se jesu li to sva rješenja od (2.3)? Za $a = 1$ je odgovor potvrdan, no za $a = -21$ imamo jednadžbu $x^2 - 21y^2 = z^2$, čije je rješenje $(5, 1, 2)$ koje nije gore navedenog oblika. To je razlog zbog kojeg jednadžbi (2.3) moramo pristupiti na drugačiji način. Bez smanjenja općenitosti pretpostavimo da je $a < 0$ i $-a$ nije potpun kvadrat, te stavimo $D = -a$. (Ako je $a > 0$, onda možemo promatrati jednadžbu $z^2 + (-a)y^2 = x^2$.)

Dakle, promotrimo jednadžbu

$$x^2 - Dy^2 = z^2. \tag{2.5}$$

Ako je $(x_0, y_0, z_0) \in \mathbb{Z}^3$ rješenje od (2.5), onda vrijedi

$$(x^2 - Dy^2)(p^2 - Dq^2) = (xp + Dyq)^2 - D(xq + yp)^2.$$

Uz uvjet da je

$$p^2 - Dy^2 = 1, \tag{2.6}$$

vrijedi da je i

$$(x_0p + Dy_0q, x_0q + y_0p, z_0),$$

rješenje jednadžbe (2.5). Uvjet (2.6) koji se pojavio prilikom generiranja novih rješenja od (2.5) i sam predstavlja jednu diofantsku jednadžbu drugog stupnja koju je potrebno izračunati.

Definicija 2.1.1. *Diofantska jednadžba dana s*

$$x^2 - Dy^2 = 1 \tag{2.7}$$

zove se ***Pellova jednadžba****.*

Jednadžba oblika

$$x^2 - dy^2 = N,$$

za $N \in \mathbb{Z} \setminus \{0\}$ *zove se* ***pellovska jednadžba****.*

Pellova jednadžba očito ima trivijalna rješenja $(\pm 1, 0)$. Postavlja se pitanje ima li i netrivijalnih rješenja. Na primjer, jednadžba $x^2 - 7y^2 = 1$, ima rješenje $(8, 3)$, stoga naše pitanje ima smisla. Nadalje, smisleno je nastaviti rješavati ovu jednadžbu samo u skupu prirodnih brojeva.

2.2 Rješenja Pellove jednadžbe

Neka je D prirodan broj koji nije potpun kvadrat. Pokazat ćemo da Pellova jednadžba (2.7) uvijek ima netrivijalno rješenje. Za to će nam biti potrebni sljedeći rezultati.

Lema 2.2.1 (Dirichletov princip - slaba forma)**.** *Neka je n prirodan broj. Ako $n+1$ raspo-redimo u n kutija, onda barem jedna kutija sadrži dva predmeta.*

Lema 2.2.2. *Neka je s prirodan broj. Postoje cijeli brojevi t i u takvi da vrijedi*

$$|t - u\sqrt{D}| < \frac{1}{s} \leq \frac{1}{|u|}.$$

Dokaz. Neka je u cijeli broj takav da je

$$0 \leq u \leq s,$$

te t najmanji cijeli broj koji je veći ili jednak od $u\sqrt{D}$, to jest $t = \lceil u\sqrt{D} \rceil$. Tada vrijedi

$$0 < t - u\sqrt{D} < 1.$$

Ako podijelimo interval $\langle 0, 1\rangle$ na s ekvidistantnih intervala (duljine $\frac{1}{s}$), prema Dirichletovom principu (Lema 2.2.1) slijedi da se barem dva para (t_1, u_1) , (t_2, u_2) od njih $s+1$ nalazi u istom intervalu. Preciznije, postoje $u_1 \neq u_2$, $0 \leq u_1 \leq s$, $i = 1, 2$ i $t_1, t_2 \in \mathbb{Z}$ takvi da je

$$|t_1 - u_1\sqrt{D} - (t_2 - u_2\sqrt{D})| < \frac{1}{s},$$

to jest

$$|t_1 - t_2 - (u_1 - u_2)\sqrt{D}| < \frac{1}{s}.$$

Kako je $|u_1 - u_2| \leq s$, vrijedi

$$|t_1 - t_2 - (u_1 - u_2)\sqrt{D}| < \frac{1}{s} \leq \frac{1}{|u_1 - u_2|}.$$

□

Korolar 2.2.3. *Postoji beskonačno mnogo parova cijelih brojeva (t, u) takvih da vrijedi:*

$$|t - u\sqrt{D}| < \frac{1}{|u|}.$$

Dokaz. Neka je S skup svih parova cijelih brojeva koji zadovoljavaju $|t - u\sqrt{D}| \leq \frac{1}{|u|}$. Pretpostavimo da je S konačan skup. Tada postoji minimum skupa $\left\{t - u\sqrt{D} : (t,u) \in S\right\}$. Nadalje, neka je $M \in \mathbb{N}$ takav da je

$$\frac{1}{M} < \min\left\{|z - u\sqrt{D}| : (t,u) \in S\right\}.$$

Prema Lemi 2.2.2 postoje $t'u' \in \mathbb{Z}$ takvi da je

$$|t' - u'\sqrt{D}| < \min\left\{\frac{1}{M}, \frac{1}{|u'|}\right\}.$$

Kako je $|t' - u'\sqrt{D}| < \frac{1}{|u'|}$, slijedi da je $(t', u') \in S$.

Nadalje,

$$|t' - u'\sqrt{D}| < \frac{1}{|M|} < \min\left\{|z - u\sqrt{D}| : (t,u) \in S\right\}$$

je očita kontradikcija. Dakle, S je beskonačan.

□

U daljnjem označavamo $S = \left\{(t,u) \in \mathbb{Z}^2 : |t - u\sqrt{D}| < \frac{1}{|u|}\right\}$.

Teorem 2.2.4. *Pellova jednadžba uvijek ima barem jedno netrivijalno rješenje.*

Dokaz. Neka je $(t,u) \in S$. Tada je

$$|t + u\sqrt{D}| \leq |t - u\sqrt{D}| + |2u\sqrt{D}| < \frac{1}{|u|} + 2|u|\sqrt{D}.$$

Slijedi

$$|t^2 - Du^2| = |t - Du||t + u\sqrt{D}| < \frac{1}{|u|}\left(\frac{1}{|u|} + 2|u|\sqrt{D}\right) = \frac{1}{u^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D}.$$

Dakle, za sve $(t,u) \in S$ vrijedi $|t^2 - Du^2| < 1 + 2\sqrt{D}$.

Jer je $1 + 2\sqrt{D}$ fiksan, po Dirichletovom principu slijedi da postoji beskonačno mnogo parova $(t,u) \in S$ takvih da vrijedi

$$t^2 - Du^2 = k,$$

za neki fiksni $k \in \mathbb{Z}$ za koji vrijedi $|k| < 1 + 2\sqrt{D}$.

Također, mora postojati beskonačno mnogo takvih parova, za koje su obje vrijednosti t i u kongruentne modulo k. Neka su (t_1, u_1) i (t_2, u_2) takva dva para gdje je $t_1 \neq \pm t_2$ i $u_1 \neq \pm u_2$. Iz jednandžbe (2.4) vidimo da vrijedi :

$$(t_1t_2 - Du_1u_2)^2 - D(t_1u_2 - t_2u_1)^2 = k^2.$$

Sada je $t_1u_2 - t_2u_1 \equiv 0 \pmod{k}$, pa je stoga $t_1t_2 - Du_1u_2 \equiv 0 \pmod{k}$, te vrijedi

$$\left(\frac{t_1t_2 - Du_1u_2}{k}\right)^2 - D\left(\frac{t_1u_2 - t_2u_1}{k}\right)^2 = 1.$$

Jer je $(t_1t_2 - Du_1u_2)/k, (t_1u_2 - t_2u_1)/k \in \mathbb{Z}$ imamo netrivijalno rješenje jednadžbe (2.7), pod uvjetom da je $t_1u_2 - t_2u_1 \neq 0$. Ipak, ako je $t_1u_2 - t_2u_1 = 0$, tada je $t_1t_2 - Du_1u_2 = \pm k$, a to se dobije jedino ako je $t_1 = \pm t_2$ i $u_1 = \pm u_2$, a takav slučaj smo isključili. □

Teorem 2.2.4. nam daje velik rezultat, no samo u teoretskom pristupu. Naime to što znamo da postoji rješenje Pellove jednadžbe nam često efektivno ne pomaže. Konkretno, ako bismo htjeli odrediti najmanje rješenje u skupu prirodnih brojeva jednadžbe

$$x^2 - 1621u^2 = 1,$$

gadno bismo se namučili, jer ono ima točno sedamdeset i šest znamenki. Stoga je očito da treba pronaći bolju strategiju kako odrediti (najmanje) rješenje jedandžbe (2.7).

U ovom dijelu okarakterizirat ćemo sva rješenja Pellove jednadžbe (2.7). Kao malo poopćenje, promatrat ćemo pellovsku jednadžbu

$$X^2 - DY^2 = 4\sigma, \tag{2.8}$$

za $\sigma \in \{-1, 1\}$. Pogledajmo u kakvoj su vezi rješenja jednadžbe (2.7) i (2.8). Očito je prema Teoremu 2.2.4. da za $\sigma = 1$, (2.8) ima netrivijalno rješenje. Zaista, ako je $x^2 - Dy^2 = 1$, onda je $X = 2x, Y = 2y$ rješenje od (2.8). Nadalje ako je $D \equiv 0 \pmod{4}$, onda za $x^2 - \frac{D}{4}y^2 = 1$, rješenja su $X = 2x$ i $Y = y$. Dakle, jednadžba (2.8) ima netrivijalno cjelobrojno rješenje (X, Y, σ).

Teorem 2.2.5. *Neka su (x_1, y_1, σ_1) i (x_2, y_2, σ_2) rješenja jednadžbe (2.8), takva da vrijedi $x_1 \neq \eta x_2$ i $y_1 \neq -\eta y_2$, za $\eta \in \{-1, 1\}$. Nadalje, neka su*

$$x_3 = \frac{x_1x_2 + Dy_1y_2}{2}, \quad y_3 = \frac{x_1y_2 + x_2y_1}{2}, \quad \sigma_3 = \sigma_1\sigma_2.$$

Tada je (x_3, y_3, σ_3) rješenje jednadžbe (2.8).

Dokaz. Pokažimo prvo da (x_3, y_3, σ_3) efektivno zadovoljava jednadžbu (2.8). Uvrstimo (x_3, y_3, σ_3) u $X^2 - DY^2 = 4\sigma$. Slijedi

$$\begin{aligned}
&\left(\frac{x_1x_2 + Dy_1y_2}{2}\right)^2 - D\left(\frac{x_1y_2 + x_2y_1}{2}\right)^2 \\
= \;& \frac{1}{4}\left(x_1^2x_2^2 + 2Dx_1x_2y_1y_2 + D^2y_1^2y_2^2\right) - \frac{1}{4}D\left(x_1^2y_2^2 + 2x_1y_2x_2y_1 + x_2^2y_1^2\right) \\
= \;& \frac{1}{4}\left(x_1^2x_2^2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - Dx_2^2y_1^2\right) \\
= \;& \frac{1}{4}\left(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2\right) = \frac{1}{4} \cdot 4\sigma_1 \cdot 4\sigma_2 = 4\sigma_3.
\end{aligned}$$

Nadalje, treba pokazati da je $x_3, y_3 \in \mathbb{Z}$, to jest

$$x_1x_2 + Dy_1y_2 \equiv 0 \pmod 2, \; x_1y_2 + x_2y_1 \equiv 0 \pmod 2.$$

Kako je

$$x_1 \equiv Dy_1 \pmod 2 \quad \text{i} \quad x_2 \equiv Dy_2 \pmod 2,$$

slijedi

$$x_1y_2 + x_2y_1 \equiv Dy_1y_2 + Dy_2y_1 = 2Dy_1y_2 \equiv 0 \pmod 2$$

i jer je umnožak dva uzastopna prirodna broja paran

$$x_1x_2 + Dy_1y_2 \equiv D^2y_1y_2 + y_1y_2 = D(D+1)y_1y_2 \equiv 0 \pmod 2.$$

Sada još treba pokazati da je $y_3 \neq 0$. Pretpostavimo da je $y_3 = 0$. Tada zbog $x_1 = \dfrac{-x_2y_1}{y_2}$ i $x_2^2 = 4\sigma_1\sigma_2$ dobivamo $x_3 = \pm 2$. Stavimo li $\eta = \dfrac{x_1}{x_2}$, tada je $\dfrac{y_1}{y_2} = -\eta$ i vidimo iz $x_3 = \pm 2$, da je $\eta(x_2^2 - Dy_2^2) = \pm 4$. Jer je $x_2^2 - Dy_2^2 = 4\sigma_2$, slijedi $|\eta| = 1$, a to je slučaj koji smo isključili. □

Napomena 2.2.6. *Ako su $x_1, x_2, x_3, y_1, y_2, y_3$ definirani kao u Teoremu 2.2.5, tada za $\lambda_1 = (x_1 + y_1\sqrt{D})/2$ i $\lambda_2 = (x_2 + y_2\sqrt{D})/2$, vrijedi*

$$\lambda_1\lambda_2 = \frac{x_3 + y_3\sqrt{D}}{2}.$$

Stoga, ako je (x_1, y_1, σ_1) neko rješenje jednadžbe (2.8), onda su trojke (x_n, y_n, σ_1^n), $\quad n \in \mathbb{N}$, gdje je

$$\frac{x_n + y_n\sqrt{D}}{2} = \lambda_1^n$$

također rješenja od (2.8).

Sva dana rješenja moraju biti različita jer kad bi vrijedilo $(x_m, y_m, \sigma_1^m) = (x_n, y_n, \sigma_1^n)$ za $n > m$, tada bi bilo $\lambda_1^n = \lambda_1^m$ i $\lambda_1^{n-m} = 1$. To znači da je $y_{n-m} = 0$, što je u kontradikciji s Teoremom 2.2.5.

Sljedeći dvije tehničke leme su nam potrebne kako bi opisali skup svih rješenja jednadžbe (2.8).

Lema 2.2.7. *Ako je (x, y, σ) rješenje jednadžbe (2.8), tada je $x + y\sqrt{D} > 2$ ako i samo ako $x > 0$ i $y > 0$.*

Dokaz. Neka su $x, y < 0$. Tada vrijedi $x + y\sqrt{D} \geq 1 + \sqrt{D} > 2$. Pretpostavimo sada $x + y\sqrt{D} < 2$. Jer je

$$(x + y\sqrt{D})(x - y\sqrt{D}) = 4\sigma,$$

slijedi

$$\frac{|x - y\sqrt{D}|}{2} = \frac{2}{x + y\sqrt{D}} < 1.$$

Dakle, $-2 < x - y\sqrt{D} < 2$. Jer je $x + y\sqrt{D} > 2$ slijedi $x, y > 0$. □

Lema 2.2.8. *Ako je* (x, y, σ) *rješenje jednadžbe (2.8), te* $x, y > 0$*, tada je* $2yD \geq 8$*. Ako je* $x > 0$ *i* $y > 1$*, tada je* $2x + 1 + (2y - 1)D > 8$.

Dokaz. Obje nejednakosti očito vrijede za $D \geq 8$. Pretpostavimo da je $D < 8$. Jer D nije kvadrat, može poprimiti samo vrijednsoti $D = 2, 3, 5, 6, 7$. Kada bi D bio jednak 2, 3, 6, 7, tada $2|x\ 2|y$, što bi značilo da je $x \geq 2, y \geq 2$ te su obje nejednakosti zadovoljene. Ako bi pak D bio jednak 5 , tada $2yD \geq 10 > 8$, i ako $x \geq 1, y > 1$, tada je $2x+1+(2y-1)D > 8$. □

Teorem 2.2.9. *Pretpostavimo da su* (x_1, y_1, σ_1) *i* (x_2, y_2, σ_2) *rješenja jednadžbe (2.8) takva da je su* $x_1, x_2, y_1, y_2 > 0$*. Imamo da je*

$$x_2 + y_2\sqrt{D} > x_1 + y_1\sqrt{D},$$

ako i samo ako $x_2 > x_1$ *i* $y_2 \geq y_1$.

Dokaz. Odmah je jasno da ako je $x_2 > x_1$ i $y_2 \geq y_1$, tada $x_2 + y_2\sqrt{D} > x_1 + y_1\sqrt{D}$. Pretpostavimo sada da je $x_2 + y_2\sqrt{D} > x_1 + y_1\sqrt{D}$. Pogledajmo sljedeća dva slučaja:

1° $x_1 - y_1\sqrt{D} > 0$

Imamo da vrijedi:

$$\frac{x_1 - y_1\sqrt{D}}{2} = \frac{2}{x_1 + y_1\sqrt{D}} > \frac{2}{x_2 - y_2\sqrt{D}} = \frac{|x_2 - y_2\sqrt{D}|}{2}.$$

Slijedi

$$\frac{y_1\sqrt{D} - x_1}{2} < \frac{x_2 - y_2\sqrt{D}}{2} < \frac{x_1 - y_1\sqrt{D}}{2}.$$

Jer je $x_2 + y_2\sqrt{D} > x_1 + y_1\sqrt{D}$, vidimo da

$$-y_2\sqrt{D} = \frac{-x_2 - y_2\sqrt{D}}{2} + \frac{x_2 - y_2\sqrt{D}}{2} < \frac{-x_1 - y_1\sqrt{D}}{2} + \frac{x_1 - y_1\sqrt{D}}{2} = -y_1\sqrt{D},$$

i $y_2 > y_1$. Jer je $y_2 \geq y_1 + 1$, imamo $Dy_2^2 > Dy_1^2 + 2Dy_1$. Slijedi da je

$$x_2^2 = Dy_2^2 + 4\sigma_2 > Dy_1^2 + 2Dy_1 + 4\sigma_2 = x_1^2 - 4\sigma_1 + 4\sigma_2 + 2Dy_1 \geq x_1^2 + 2Dy_1 - 8 \geq x_1^2$$

i $x_2 > x_1$, jer je $Dy_1 - 8 \geq 0$ prema Lemi 2.2.8.

2° $x_1 - y_1\sqrt{D} < 0$

Imamo

$$\frac{y_1\sqrt{D} - x_1}{2} = \frac{2}{x_1 + y_1\sqrt{D}} > \frac{2}{x_2 + y_2\sqrt{D}} = \frac{|x_2 - y_2\sqrt{D}|}{2},$$

što znači da

$$x_2 = \frac{x_2 - y_2\sqrt{D}}{2} + \frac{x_2 + y_2\sqrt{D}}{2} > \frac{x_1 - y_1\sqrt{D}}{2} + \frac{x_1 + y_1\sqrt{D}}{2} = x_1.$$

Ako je $y_2 < y_1$, tada $y_2 \leq y_1 - 1$, te

$$4\sigma_2 \leq (x_1 + 1)^2 - D(y_1 - 1)^2 = 4\sigma_1 + 2x_1 + 1 + (2y_1 - 1)D.$$

Jer je $y_2 > 0$, imamo $y_1 > 1$, te po Lemi 2.2.8. slijedi

$$2x_1 + 1 + (2y_1 - 1)D > 8 \geq 4\sigma_2 - 4\sigma_1 \geq 2x_1 + 1 + (2y_1 - 1)D,$$

što je kontradikcija. Dakle, $y_2 \geq y_1$.

□

Prema prethodnom teoremu postoji jedinstveno rješenje (x_1, y_1, σ_1) od (2.8) takvo da je $x_1 + y_1\sqrt{D} > 2$ najmanje moguće, to jest takozvano *fundamentalno*. Označit ćemo s

$$\epsilon = \frac{x_1 + y_1\sqrt{D}}{2}.$$

Očito je ϵ rješenje jednadžbe $x^2 - Dy^2 = \sigma_1$, no problem je u tome što nije nužno cjelobrojno.

Teorem 2.2.10. *Ako je (x', y', σ') neko rješenje jednadžbe (2.8), tada je postoji $n \in \mathbb{Z}$ takav da je*

$$\eta = \frac{x' + y'\sqrt{D}}{2} = \pm\epsilon^n.$$

Dokaz. Iz

$$\left(\frac{x' - y'\sqrt{D}}{2}\right)\left(\frac{x' + y'\sqrt{D}}{2}\right) = \sigma',$$

slijedi da je samo jedna od vrijednosti $\eta, -\eta, \eta^{-1}, -\eta^{-1}$ veća od 1. Prema Lemi 2.2.7 slijedi da ju možemo označiti s

$$\gamma = \frac{|x'| + |y'|\sqrt{D}}{2}.$$

Jer je $\gamma > 1$ i $\epsilon > 1$, postoji nenegativan broj $n \in \mathbb{Z}$ takav da vrijedi

$$\epsilon^n \leq \gamma < \epsilon^{n+1}.$$

Kada bi vrijedilo $\gamma = \epsilon^n$, bili bismo gotovi jer je $n \neq 0$ i $\eta \in \left\{\gamma, -\gamma, \gamma^{-1}, -\gamma^{-1}\right\}$. Ako je $\gamma \neq \epsilon^n$, tada je

$$1 < \gamma\epsilon^{-n} < \epsilon.$$

Jer je $\epsilon(x_1 - y_1\sqrt{D})/2 = \sigma_1$, imamo

$$\epsilon^{-n} = \sigma_1^n\left(\frac{x_1 - y_1\sqrt{D}}{2}\right)^n.$$

Jer je $(x_1, -y_1, \sigma_1)$ rješenje jednadžbe (2.8), iz Napomene 2.2.6. slijedi da je

$$\lambda = \gamma\epsilon^{-n} = \frac{x^2 + y^2\sqrt{D}}{2},$$

za neke $x_2, y_2 \in \mathbb{Z}$ takve da je $x_2 \equiv Dy_2 \pmod 2$. Također jer je $\lambda > 1$, iz Leme 2.2.8. slijedi da su $x_2, y_2 > 0$ te po Teoremu 2.2.5 imamo

$$x_2^2 - Dy_2^2 = 4\sigma'\sigma_1^n.$$

Dakle, $(x_2, y_2, \sigma'\sigma_1^n)$ je rješenje jednadžbe (2.8) i $1 < \lambda < \epsilon$. No, to je nemoguće zbog minimalnosti od ϵ. □

Definicija 2.2.11. *Najmanje rješenje* (t, u) *Pellove jednadžbe (2.7) u skupu prirodnih brojeva naziva se* ***fundamentalno rješenje****.*

Korolar 2.2.12. *Neka je* (t, u) *fundamentalno rješenje Pellove jednadžbe (2.7), te* $(T, U) \in \mathbb{N}^2$ *neko rješenje od (2.7). Tada postoji* $n \in \mathbb{N}$ *takav da je*

$$T + U\sqrt{D} = (t + u\sqrt{D})^n.$$

Dokaz. Kako su $(2t, 2u, 1)$ i $(2T, 2U, 1)$ rješenja od (2.8), iz Teorema 2.2.10 slijedi da je

$$t + u\sqrt{D} = \epsilon^k \tag{2.9}$$

te da je

$$T + U\sqrt{D} = \epsilon^m$$

za neke $k, m \in \mathbb{Z}$. Zbog toga što je (t, u) fundamentalno rješenje jednadžbe (2.7), mora vrijediti $m > k > 0$. Neka je

$$m = nk + r,$$

gdje su $n > 0$ i $0 \leq r < k$. Tada je

$$T + U\sqrt{D} = (t + u\sqrt{D})^n \epsilon^r$$

i

$$1 \leq \epsilon^r = (T + U\sqrt{D})(t - u\sqrt{D})^n.$$

Jer je $\epsilon^r = (x' + y'\sqrt{D})/2$ za neke $x', y' \in \mathbb{Z}$, iz prethodne jednadžbe vidimo da ako je $r > 0$, mora vrijediti $x' \equiv y' \equiv 0 \pmod 2$ i

$$\left(\frac{x'}{s}\right)^2 - D\left(\frac{y'}{2}\right)^2 = 1.$$

Jer je $r < k$, vrijedi $\epsilon^r < \epsilon^k = t + u\sqrt{D}$, no to je u kontradikciji s definicijom fundamentlnog rješenja. Prema tome, $r = 0$ i

$$T + U\sqrt{D} = (t + u\sqrt{D})^n.$$

□

Dakle, ukoliko možemo odrediti fundamentalno rješenje Pellove jednadžbe (2.7), onda možemo okarakterizirati sva njena rješenja. Isto vrijedi i za poopćeni oblik jednadžbe (2.8). Napomenimo još da nije uvijek moguće riješiti jednadžbu (2.8) ako unaprijed fiksiramo vrijednosti σ ili ako zahtijevamo (ne)parnost rješenja x. Na primjer, ne postoji cjelobrojno rješenje jednadžbe $X^2 - DY^2 = -4$ kada je $D \equiv -1 \pmod 4$. Također, ne postoji cjelobrojno rješenje jednadžbe $X^2 - DY^2 = 4$ za $X \equiv Y \equiv 1 \pmod 2$ i $D = 11$. Znači jednadžba (2.8) je uvijek rješiva samo ukoliko nismo apriori fiksirali vrijednost parametra σ i parnost rješenja.

Veza između $\epsilon = \dfrac{x_1 + y_1\sqrt{D}}{2}$ gdje je $x_1 + y_1\sqrt{D}$ fundamentalno rješenje od (2.8) i fundamentalnog rješenja $u + \sqrt{D} = \epsilon^k$ Pellove jednadžbe (2.7) dana je sljedećom tablicom:

$x_1 \pmod 2$	$y_1 \pmod 2$	σ_1	k
0	0	1	1
0	1	1	2
0	0,1	-1	2
1	0,1	1	3
1	0,1	-1	6

Poglavlje 3

Pellova jednadžba u kriptosustavu

3.1 Preliminarna opažanja

U ovom dijelu opisat ćemo algoritam kriptosustav s javnim ključemo koji korisiti rješenja Pellove jednadžbe. Osmislio ga je H. C. Williams i objavio 1984. godine. Ovaj kriptosustav također spada u one koji se zasnivaju na teškoći faktorizacije dovoljno velikog prirodnog broja $n = pq$, gdje su p, q prosti. Prije nego što ga izložimo, trebat će nam neka svojstva skupa rješenja Pellove jednadžbe (modulo n). Stoga će nam koristiti rezultati koje smo dobili u prethodnom poglavlju. Ako su $t, u \in \mathbb{Z}$ takvi da je $t^2 - Du^2 = 1$, tada i za nizove (T_n) i (U_n) dane s

$$T_n + \sqrt{D}U_n = (t + \sqrt{D}u)^n, \ n \in \mathbb{N}$$

vrijedi da je $T_n^2 - DU_n^2 = 1$.

Izvedimo neke korisne rekurzivne formule za nizove (T_n) i (U_n). Za $i, j \geq 0$ vrijedi

$$\begin{aligned} T_{i+j} + \sqrt{D}U_{i+j} &= (t + u\sqrt{D})^{i+j} \\ &= (t + u\sqrt{D})^i (t + u\sqrt{D})^j \\ &= (T_i + \sqrt{D}U_i)(T_j + \sqrt{D}U_j) \\ &= T_iT_j + U_iU_jD + \sqrt{D}(U_iT_j + T_iU_j), \end{aligned}$$

pa je

$$T_{i+j} = T_iT_j + DU_iU_j, \quad U_{i+j} = T_iU_j + T_jU_i \tag{3.1}$$

i

$$T_{i+j} = 2T_iT_j - T_{j-i}, \quad U_{i+j} = 2T_iU_j - U_{j-i}. \tag{3.2}$$

Stoga, ako je $i = j$, dobivamo

$$T_{2i} = T_i^2 + DU_i^2 = 2T_i^2 - 1,$$
$$U_{2i} = 2T_iU_i.$$

Iz početnih uvjeta

$$T_0 = 1,\ T_1 = t$$
$$U_0 = 0,\ U_1 = u$$

te iz formule (3.1) i (3.2) vidimo da se T_i može prikazati kao polinom u $\mathbb{Z}$, kojeg ćemo označavati $T_i(t)$. Zaista kako je

$$T_{j+1} = 2T_1T_j - T_{j-1},$$

za j =2,3,4,... dobivamo redom

$$T_2 = 2T_1T_1 - T_0 = 2tt - 1 = 2t^2 - 1$$
$$T_3 = 2T_1T_2 - T_1 = 2t(2t^2 - 1) - t = 4t^3 - 3t$$
$$T_4 = 2T_1T_3 - T_2 = 2t(4t^3 - 3t) - 2t^2 + 1 = 8t^4 - 8t^2 + 1$$
$$T_5 = 2T_1T4 - T_3 = 2t(8t^4 - 8t^2 + 1) - 4t^3 - 3t = 16t^5 - 20t^3 + 5t$$
$$\vdots$$

Također, zaključujemo da iz

$$(t + \sqrt{D}U)^{ij} = (T_j + \sqrt{D}U_j)^i$$

slijedi

$$T_{ij}(t) = T_i(T_j(t)). \tag{3.3}$$

Sada želimo pokazati kako efikasno izračunati $T_k(t) \pmod n$, za neke vrijednosti $k, n \in \mathbb{N}$. Prisjetimo se prvo algoritma *Kvadriraj i množi*, koji efikasno računa $e_K(x) = x^e \mod n$. Pretpostavimo da e ima sljedeći prikaz u bazi 2:

$$e = e_0 + 2e_1 + ... + 2^{s-1}e_{s-1}.$$

Algoritam računa:
$y = 1$
za $i = s - 1, ..., 1, 0$
$y = y^2 \pmod n$
ako je $e_i = 1$, onda $y = y \cdot x \pmod n$

Zapišimo sada k u binarnom zapisu:

$$k = 2^l b_0 + 2^{l-1} b_1 + ... + 2b_{l-1} + b_l,$$

odnosno

$$k = b_l + 2(b_{l-1} + 2(b_{l-2} + ... + 2(b_1 + 2b_0))),$$

gdje je $b_0 = 1$, $b_1, \ldots, b_l \in \{0, 1\}$ i $l = \lfloor log_2 k \rfloor$. Stavimo da je $P_1 \equiv (T_2, T_1) \pmod{n}$. Ovdje koristimo notaciju $(A_1, B_1) = (A_2, B_2) \pmod{n}$ da bismo označili $A_1 \equiv A_2 \pmod{n}$ i $B_1 \equiv B_2 \pmod{n}$.

Promotrimo što se događa po koracima:
Za $j = 0$, vrijedi $k_0 = b_0 = 1$,te je $(T_2, T_1) = (T_{k'+1}, T_{k'})$.
Za $j = 1$, $k = b_1 + 2b_0$ pri čemu stavimo da je $b_0 = k'$.

Znamenka $b_1 \in \{0, 1\}$, pa pogledajmo dva slučaja:

- Za $b_1 = 0 \Rightarrow k = 2k'$, te je $(T_{k+1}, T_k) = (T_{2k'+1}, T_{2k'})$
  Imamo stoga da je $(T_3, T_2) \equiv (2T_1T_2 - T_1, T_2) \pmod{n}$

- Za $b_1 = 1 \Rightarrow k = 2k' + 1$, te je $(T_{k+1}, T_k) = (T_{2k'+2}, T_{2k'+1})$
  Imamo da je $(T_4, T_3) \equiv (2T_2^2 - 1, 2T_1T_2 - T_1) \pmod{n}$

  $\vdots$

U koraku $j - 1$ dobivamo stoga da je $P_{j-1} \equiv (T_{k'+1}, T_{k'}) \pmod{n}$
U koraku j imamo da je $k = b_j + 2k'$.

- Za $b_j = 0 \Rightarrow k = 2k'$, te je

$$\begin{aligned}(T_{k+1}, T_k) &= (T_{2k'+1}, T_{2k'}) \\ &\equiv (2T_{k'}T_{k'+1} - T_1, 2T_{k'}^2 - 1) \pmod{n}\end{aligned}$$

- Za $b_j = 1 \Rightarrow k = 2k' + 1$, te je

$$\begin{aligned}(T_{k+1}, T_k) &= (T_{2k'+2}, T_{2k'+1}) \\ &\equiv (2T_{k'+1}^2 - 1, 2T_{k'}T_{k'+1} - T_1) \pmod{n}\end{aligned}$$

Iz toga slijedi da je

$$P_j \equiv (T_{2k'+b_j+1}, T_{2k'+b_j}) \pmod{n},$$

te je konačno

$$P_l \equiv (T_{k+1}, T_k).$$

Dakle, pokazali smo kako u l koraka vrlo efikasno računamo $(T_{k+1}, T_k) \pmod{n}$.

Prije nego što nastavimo, prisjetimo se nekih rezultata iz Teorije brojeva koji će nam biti potrebni. Navedene rezultate koristiti ćemo kao činjenice, te ih nećemo dokazivati.

Definicija 3.1.1. *Neka je* $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je* a ***kvadratni ostatak modulo*** m.

Teorem 3.1.2 (Eulerov teorem)**.** *Ako je* $(a, m) = 1$, *onda je* $a^{\varphi}(m) \equiv 1 \pmod{m}$.

Teorem 3.1.3. *Neka je* p *neparan prost broj. Reducirani sustav ostataka modulo* p *sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$*kvadratnih neostataka.*

Definicija 3.1.4. *Neka je* p *neparan prost broj i* $a \in \mathbb{Z}$. ***Legendreov simbol*** $\left(\frac{a}{p}\right)$ *je jednak* 1 *ako je* a *kvadratni ostatak modulo* p, -1 *ako je* a *kvadratni neostatak modulo* p, *a* 0 *ako* $p|a$.

Teorem 3.1.5 (Eulerov kriterij)**.**

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

Definicija 3.1.6. *Neka je* Q *neparan prirodan broj, te neka je* $Q = q_1 \dots q_s$, *gdje su* q_i *neparni prosti brojevi, ne nužno različiti. Tada se* ***Jacobijev simbol*** $\left(\frac{a}{Q}\right)$ *definira s*

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje su $\left(\frac{a}{q_j}\right)$ *Legendreovi simboli.*

Neka su sada p i q dva različita neparna prosta broja broja i stavimo da je $\eta_p \equiv p \pmod 4$ i $\eta_q \equiv q \pmod 4$, pri čemu su $\eta_p, \eta_q \in \{1, -1\}$.

Neka je $D > 0$ cijeli broj koji nije kvadrat, te vrijedi

$$\left(\frac{D}{p}\right) = -\eta_p \quad \text{i} \quad \left(\frac{D}{q}\right) = -\eta_q.$$

Iz Teorema 3.1.2 vidimo da postoji

$$\frac{p-1}{2} \quad \text{vrijednosti} \quad D \pmod{p}, \quad \text{koje zadovoljavaju} \quad \left(\frac{D}{p}\right) = -\eta_p$$

i

$$\frac{q-1}{2} \quad \text{vrijednosti} \quad D \pmod{q}, \quad \text{koje zadovoljavaju} \quad \left(\frac{D}{q}\right) = -\eta_q.$$

Neka je $a \in \{1, \ldots, p-1\}$ takav da je

$$\left(\frac{a}{p}\right) = -\eta_p,$$

te $b \in \{1, \ldots, q-1\}$ takav da je

$$\left(\frac{b}{q}\right) = -\eta_q.$$

Sustav kongruencija

$$D \equiv a \pmod{p}, \quad D \equiv b \pmod{q}$$

takav da je

$$\left(\frac{a}{p}\right) = 1, \quad \left(\frac{b}{q}\right) = -1.$$

ima jedinstveno rješenje $D = D_0 \pmod{n}$, gdje je $n = pq$, prema Kineskom teoremu. Dakle, $\left(\frac{D_0}{p}\right) = -\eta_p$ i $\left(\frac{D_0}{q}\right) = -\eta_q$. Konačno, takvih brojeva $D \pmod{n}$ možemo izabrati na točno

$$\frac{(p-1)}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}$$

načina, jer smo a, odnosno b birali na $\frac{p-1}{2}$, odnosno $\frac{q-1}{2}$ načina.

Nadalje, uočimo još da je m neparan i da vrijedi $(D, n) = 1$. S ovim smo opravdali pretpostavke sljedećeg teorema kojeg ćemo koristiti za konstrukciju našeg kriptosustava.

Teorem 3.1.7. *Neka su p i q različiti prosti neparni brojevi, te neka je $-\eta_p \equiv p \pmod{4}$ i $-\eta_q \equiv q \pmod{4}$. Ako je D prirodan broj koji nije potpun kvadrat za koji vrijedi da je*

$$\left(\frac{D}{p}\right) = -\eta_p \quad i \quad \left(\frac{D}{q}\right) = -\eta_q,$$

tada je

$$\alpha^{2k} \equiv \pm\alpha \pmod{m},$$

za

$$m = \frac{(p-\eta_p)(q-\eta_q)}{4} \quad , \quad \alpha = \frac{a + b\sqrt{D}}{a - b\sqrt{D}},$$

gdje su $a, b \in \mathbb{Z}$, takvi da je $\left(\frac{N(a+b\sqrt{D})}{n}\right) = 1$, te $k \equiv \frac{m+1}{2} \pmod{m}$.

Dokaz. Stavimo da je

$$\lambda = \frac{\gamma}{\overline{\gamma}},$$

za $\gamma = a + b\sqrt{D}$ i $\overline{\gamma} = a - b\sqrt{D}$. Pokažimo da je

$$\gamma^p \equiv \begin{cases} \gamma \pmod{p} & ,\eta_p = 1 \\ \overline{\gamma} \pmod{p} & ,\eta_p = -1, \end{cases}.$$

Prema Binomnom teoremu vrijedi

$$\gamma^p = a^p + \binom{p}{1}a^{p-1}b\sqrt{D} + \binom{p}{2}a^{p-2}(b\sqrt{D})^2 + ... + \binom{p-1}{p}a(b\sqrt{D})^{p-1} + (b\sqrt{D})^p$$

i

$$p \quad | \quad \left(\binom{p}{1}a^{p-1}b\sqrt{D} + \binom{p}{2}a^{p-2}(b\sqrt{D})^2 + ... + \binom{p-1}{p}a(b\sqrt{D})^{p-1} + (b\sqrt{D})^p\right),$$

pa je

$$\gamma^p \equiv a^p + b^p(\sqrt{D})^p \equiv a + bD^{\xi}\sqrt{D} \pmod{p},$$

jer je $a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$ prema Malom Fermatovom teoremu i $p = 2\xi + 1$.

Ako je $\left(\frac{D}{p}\right) = 1$, onda postoji $z \in \mathbb{Z}$, takav da je $D \equiv z^2 \pmod{p}$. Odavde je $D^{\xi} \equiv z^{2\xi} = z^{p-1} \pmod{p}$. Prema Eulerovom teoremu je $z^{p-1} \equiv 1 \pmod{p}$, jer $(z, p) = 1$. Stoga je $D^{\xi} \equiv 1 \pmod{p}$.

Ako je $\left(\frac{D}{p}\right) = -1$, onda se slično pokaže da je $D^{\xi} \equiv -1 \pmod{p}$.

Dalje je

$\eta_p = 1$, $\gamma^{p-\eta_p} = \gamma^{p-1} \equiv 1 \pmod{p}$

$\eta_p = -1$, $\gamma^{p-\eta_p} = \gamma^{p+1} \equiv \overline{\gamma} \cdot \gamma = N(\gamma) \pmod{p}$.

Kraće, pišemo

$$\gamma^{p-\eta_p} \equiv N^{\frac{1-\eta_p}{2}} \pmod{p}, \tag{3.4}$$

gdje je $N = N(\gamma) = a^2 + Db^2$.

Kako je

$$N\alpha = \gamma\overline{\gamma} \cdot \frac{\gamma}{\overline{\gamma}} = \gamma^2,$$

slijedi

$$\gamma^{p-\eta_p} = (\gamma^2)^{\frac{p-\eta_p}{2}} = (N\alpha)^{\frac{p-\eta_p}{2}} = N^{\frac{p-\eta_p}{2}} \cdot \alpha^{\frac{p-\eta_p}{2}}.$$

Zbog (3.4) je

$$N^{\frac{1-\eta_p}{2}} \equiv N^{\frac{p-\eta_p}{2}} \cdot \alpha^{\frac{p-\eta_p}{2}} \pmod{p}.$$

Množenjem prethodne relacije s $N^{\frac{p+\eta_p-2}{2}}$ dobivamo

$$N^{\frac{p-1}{2}} \equiv N^{p-1} \cdot \alpha^{\frac{p-\eta_p}{2}} \pmod{p},$$

Dakle,

$$\alpha^{\frac{p-\eta_p}{2}} \equiv N^{\frac{p-1}{2}} \equiv \left(\frac{N}{p}\right) \pmod{p},$$

prema Eulerovom kriteriju.

Na isti način se dobije

$$\alpha^{\frac{q-\eta_q}{2}} \equiv N^{\frac{q-1}{2}} \equiv \left(\frac{N}{q}\right) \pmod{q}.$$

Kako je $m = \frac{p-\eta_p}{2} \cdot \frac{q-\eta_q}{2}$, slijedi

$$\alpha^m = \frac{N}{p} \pmod{p} \quad , \quad \alpha^m = \frac{N}{q} \pmod{q}.$$

Nadalje, iz pretpostavke da je $\left(\frac{N}{n}\right) = \left(\frac{N}{pq}\right) = 1$, slijedi

$$\left(\frac{N}{p}\right)\left(\frac{N}{q}\right) = 1,$$

odnosno

$$\alpha^m = 1 \pmod{n} \quad \text{ili} \quad \alpha^m = -1 \pmod{n}.$$

Budući da je $2k = m + 1 + 2tm$, slijedi

$$\alpha^{2k} = \alpha^m \cdot \alpha \cdot (\alpha^m)^{2t} \equiv \pm\alpha \pmod{n}.$$

□

3.2 Konstrukcija kriptosustava

Postavke

Alice prvo odabire dva različita prosta broja p i q. Stavlja $n = pq$ i

$$\eta_p \equiv -p \pmod{4}, \ \eta_q \equiv -q \pmod{4},$$

te bira $0 < D < n$ koji nije potpun kvadrat takav da je

$$\left(\frac{D}{p}\right) = \eta_p, \ \left(\frac{D}{q}\right) = \eta_q.$$

i vrijednost $S \in \mathbb{Z}$ takvu da je Jacobijev simobol

$$\left(\frac{S^2 - D}{n}\right) = -1.$$

Nadalje, izabire vrijednost e, takvu da vrijedi $(e, m) = 1$, te konstruira svoj **javni ključ**

$$K = \{n, e, S, D\}.$$

Zatim, rješava jednadžbu

$$de \equiv (m + 1)/2 \pmod{m},$$

pri čemu je

$$m = \frac{(p - \eta_p)(q - \eta_q)}{4},$$

iz koje dobiva d - njezin **tajni ključ**. Jer su S i D obično mali, Alice-in javni ključ neće biti mnogo veći nego karakteristični javni ključ sustava RSA.

Za prostor otvorenog teksta i prostor šifrata uzimamo

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^* = \{0 < a < n \,:\, (a, n) = 1\}.$$

Napomenimo da će oznaka $c \equiv \dfrac{a}{b} \pmod{n}$ značiti da je $c \equiv ab^{-1} \pmod{n}$, gdje je b^{-1} multiplikativni inverz u grupi $\mathbb{Z}_n^*$, za $b \in \mathbb{Z}_n^*$.

Šifriranje

Neka je $0 < M < n$ poruka koju Bob želi izmijeniti s Alice. On računa

$$j_1 = \left(\frac{M^2 - D}{n}\right).$$

Jer su šanse da $j_1 = 0$ vrlo male, možemo pretpostaviti da je $|j_1| = 1$. (U biti ovo možemo izbjeći ako pretpostavimo da je $M \in \mathbb{Z}_n^*$.)

Ako je $j_1 = 1$ definira se

$$t \equiv (M^2 + D)(M^2 - D)^{-1} \pmod{n},$$

$$u \equiv 2M(M^2 - D)^{-1} \pmod{n}.$$

Uočimo da je

$$t + u\sqrt{D} \equiv \frac{M^2 + D + 2M\sqrt{D}}{M^2 - D} = \frac{M + \sqrt{D}}{M - \sqrt{D}} \pmod{n}.$$

Ako je $j_1 = -1$ stavlja se

$$t \equiv ((M^2 + D)(S^2 + D) + 4DMS)((M^2 - D)(S^2 - D))^{-1} \pmod{n},$$

$$u \equiv (2S(M^2 + D) + 2M(S^2 + D))((M^2 - D)(S^2 - D))^{-1} \pmod{n}.$$

Uočimo da je

$$t + u\sqrt{D} \cdot \frac{S - \sqrt{D}}{S + \sqrt{D}} \equiv \frac{M + \sqrt{D}}{M - \sqrt{D}} \pmod{n}.$$

Nadalje izabire $j_2 \equiv t \pmod 2$, gdje je $j_2 \in \{0, 1\}$. Za izračunate vrijednosti t i u mora vrijediti

$$t^2 - Du^2 \equiv 1 \pmod{n}.$$

Zaista,

$$t^2 - Du^2 = (t + u\sqrt{D})(t - u\sqrt{D}) \equiv \frac{M + \sqrt{D}}{M - \sqrt{D}} \cdot \frac{M - \sqrt{D}}{M + \sqrt{D}} = 1 \pmod{n}.$$

Nadalje, da bi izgradili sustav sličan RSA sustavu u kojem vrijedi $(M, n) = 1$, pretpostavit ćemo da je $(u, n) = 1$. Za danu vrijednost $T_1 = t$, Bob računa $(T_{e+1}, T_e) \pmod n$ varijantom algoritma Kvadriraj i množi, kojeg smo opisali u prethodnom dijelu.

Iz $T_1 = t$ i $U_1 = u$ i koristeći formulu (3.1) vidimo da vrijedi

$$DU_l = T_{e+1} - tT_e$$

Iz Teorema 3.1.7 slijedi

$$T_{2ed} \equiv \sigma t \pmod{n},$$

$$U_{2ed} \equiv \sigma u \pmod{n},$$

gdje je $\sigma \in \{-1, 1\}$.

Također, ako p ili q dijeli U_eT_e, tada $p|U_{2e}$ pa zato i $p|U_{2ed}$ a to bi značilo da $p|u$ što je nemoguće. Dakle, $(n, U_eT_e) = 1$. Tada, zato jer je $(n, uDU_e) = 1$, Bob može konačno izračunati šifrat

$$E \equiv DuT_e(T_{e+1} - tT_e)^{-1} \pmod{n},$$

gdje je $0 < E < n$. Bob sada Alice šalje

$$E(M) = \{E, j_1, j_2\}.$$

Dešifriranje

Alice najprije računa T_{2e} i $U_{2e} \pmod n$ koristeći:

$$T_{2e} \equiv T_e^2 + DU_e^2 \equiv \frac{T_e^2 + DU_e^2}{T_e^2 - DU_e^2} \equiv (E^2 + D)(E^2 - D)^{-1} \pmod n$$

i

$$U_{2e} \equiv \frac{2T_e U_l}{T_e^2 - DU_e^2} \equiv (2E)(E^2 - D)^{-1} \pmod n.$$

Nadalje računa

$$T_d(T_{2e}) \equiv T_{2de}(t) \pmod n$$

i

$$T_{d+1}(T_{2e}) \equiv T_{2de+2e}(t) \pmod n,$$

koristeći varijantu algoritma Kvadriraj i množi, pri čemu je početna vrijednost jednaka $T_1 = T_{2e}$.

Iz formule (3.1) slijedi da je

$$DU_{2e}U_{2ed} = T_{2ed+2e} - T_{2e}T_{2ed},$$

te iz toga Alice može izračunati

$$T_{2de} \pmod n \quad \text{i} \quad DU_{2e}U_{2ed} \pmod n.$$

Jer je po Teoremu 3.1.7

$$T_{2de} \equiv \sigma t \pmod n$$

i Alice zna da je

$$j_2 \equiv t \pmod 2,$$

slijedi da ona može odrediti σ, pa prema tome može odrediti $t \pmod n$. Razmotrimo sve slučajeve:

Ako $j_2 = 0$ i $T_{2de} \equiv 0 \pmod 2$, onda $t = T_{2de}$ i $\sigma = 1$.
Ako $j_2 = 0$ i $T_{2de} \equiv 1 \pmod 2$, onda $t = -T_{2de}$ i $\sigma = -1$.
Ako $j_2 = 1$ i $T_{2de} \equiv 0 \pmod 2$, onda $t = -T_{2de}$ i $\sigma = -1$.
Ako $j_2 = 1$ i $T_{2de} \equiv 1 \pmod 2$, onda $t = T_{2de}$ i $\sigma = 1$.

Jer je $u \equiv \sigma U_{2ed} \equiv \sigma(T_{2ed+2e} - T_{2e}T_{2ed})/(DU_{2e}) \pmod n$, također može odrediti u.

Alice sada ima $\alpha \equiv t + u\sqrt{D} \pmod n$. Stavimo da je

$$\alpha' = \begin{cases} \alpha & , \quad j_1 = 1 \\ \alpha\frac{(S - \sqrt{D})}{S + \sqrt{D}} & , \quad j_1 = -1 \end{cases}$$

Sada imamo

$$\alpha' \equiv \frac{M + \sqrt{D}}{M - \sqrt{D}} \pmod{n}$$

i Alice dobiva otvoreni tekst

$$M \equiv (\alpha' + 1)\sqrt{D}/(\alpha' - 1) \pmod{n}.$$

Zaista,

$$\frac{(\alpha' + 1)\sqrt{D}}{(\alpha' - 1)} \equiv \frac{\frac{M+\sqrt{D}}{M-\sqrt{D}} + 1}{\frac{M+\sqrt{D}}{M-\sqrt{D}} - 1}\sqrt{D} = \frac{2M}{2\sqrt{D}}\sqrt{D} = M \pmod{n}.$$

3.3 Primjeri

Primjer 1

Postavke

Odaberimo prvo dva prosta broja p i q. Neka je $p = 17$ i $q = 29$, te $n = p \cdot q = 493$. Zatim, odredimo

$$\eta_p \equiv -p = -17 \equiv -1 \pmod{4},$$

i

$$\eta_q \equiv -q = -29 \equiv -1 \pmod{4}.$$

Sada nas zanima vrijednost D. Mora vrijediti da je

$$\left(\frac{D}{p}\right) = \eta_p = -1 \quad \text{i} \quad \left(\frac{D}{q}\right) = \eta_q = -1,$$

te se dobije da je jedno od mogućih izbora za $D = 143$.

Nadalje računamo vrijednost S tako da vrijedi $\left(\frac{S^2-D}{n}\right) = -1$, te se dobije da je jedno od mogućih izbora za $S = 30$.

Za m vrijedi da mora biti neparan, te se dobije da je

$$m = \frac{(p - \eta_p)(q - \eta_q)}{4} = \frac{(17 + 1)(29 + 1)}{4} = 135.$$

Odredimo sada vrijednost e takvu da vrijedi $(e, m) = 1$. Jer je $135 = 3 \cdot 3 \cdot 3 \cdot 5$, možemo staviti $e = 7$.

Izračunajmo sada još i d. Iz

$$de \equiv \frac{(m + 1)}{2} \pmod{m},$$

računamo

$$d \equiv \frac{(m+1)}{2} \cdot e^{\varphi(m)-1} \pmod{m},$$

pa je $d = 29$. Sada imamo javni ključ

$$K = \{n, e, S, D\} = \{493, 7, 30, 143\},$$

te tajni ključ $d = 29$.

Napomenimo da smo u ovom i sljedećem primjeru multiplikativni inverz nekog elementa b računali kao $b^{-1} \equiv b^{\varphi(m)-1} \pmod{m}$ prema Eulerovom teoremu. U praksi se ta vrijednost računa koristeći prošireni Euklidov algoritam.

Šifriranje

Uzmimo sada da je poruka koju želimo šifrirati $M = 257$. Dobije se da je

$$j_1 = \left(\frac{M^2 - D}{n}\right) = \left(\frac{257^2 - 143}{493}\right) = 1.$$

Jer je $j_1 = 1$, računamo t i u po formulama

$$t \equiv (M^2 + D)(M^2 - D)^{-1} \pmod{n},$$

$$u \equiv 2M(M^2 - D)^{-1} \pmod{n},$$

te se dobije da je $t = 410$ i $u = 180$. Nadalje, dobivamo da je

$$j_2 = t \pmod 2 = 410 \pmod 2 = 0.$$

Kako je $e = 7$, odredimo sada vrijednosti T_7 i T_8 pomoću rekurzije

$$T_n \equiv (2 \cdot T_1 \cdot T_{n-1} - T_{n-2}) \pmod{n},$$

uz početne uvjete $T_1 = t$ i $T_2 = 2 \cdot t^2 - 1$. Dobivamo da je $T_7 = 367$ i $T_8 = 474$. Sada konačno možemo izračunati šifrat

$$E \equiv DuT_7(T_8 - tT_7)^{-1} \equiv 217 \pmod{n}.$$

Šaljemo šifrat

$$E(257) = \{217, 1, 0\}.$$

Dešifriranje

Sada želimo dešifrirati $E(M) = \{E, j_1, j_2\} = \{217, 1, 0\}$, pri čemu su nam poznate vrijednosti n, e, S, D i α. Izračunamo T_{2e} i U_{2e} modulo n koristeći

$$T_{2e} \equiv (E^2 + D)(E^2 - D)^{-1} \pmod{n}$$

i

$$U_{2e} \equiv (2E)(E^2 - D)^{-1} \pmod{n},$$

te dobivamo da je $T_{2e} \mod n = 199$ i $U_{2e} \mod n = 35$. Nadalje, računamo

$$T_{2de} \equiv T_d(T_{2e}) \equiv T_{29}(199) \pmod{n}$$

i

$$T_{2de+2e} \equiv T_{d+1}(T_{2e}) \equiv T_{30}(199) \pmod{n},$$

pomoću rekurzije

$$T_n \equiv (2 \cdot T_1 \cdot T_{n-1} - T_{n-2}) \pmod{n},$$

uz početne uvjete $T_1 = T_{2e} = 199$ i $T_2 \equiv 2T_{2e}^2 - 1 \equiv 321 \pmod{n}$, te se dobije da je $T_{2de} = 83$ i $T_{2de+2e}(T_{2e}) = 59$. Sada je

$$t \equiv \sigma T_{2de} \pmod{n},$$

gdje je $\sigma \in \{-1, 1\}$. Kako je $j_2 = 0$, te $T_{2de} \equiv 1 \pmod 2$ slijedi da je $\sigma = -1$, pa je prema tome

$$t \equiv -83 \equiv 410 \pmod{n}.$$

Iz $u \equiv \sigma U_{2ed}$, dobijemo da je $u = 180$. Sada imamo da je

$$\alpha' = \alpha \equiv 410 + 180\sqrt{D} \pmod{n}.$$

Konačno, računamo

$$M \equiv (uD(t-1) - uD(t+1)) \cdot ((t-1)^2 - u^2 D)^{\varphi(n)-1} = 257.$$

Primjer 2

Postavke

Odaberimo dva prosta broja p i q. Neka je $p = 13$ i $q = 19$, te $n = p \cdot q = 247$. Izračunamo

$$\eta_p \equiv -p = -13 \pmod 4 \equiv -1 \pmod 4,$$

i

$$\eta_q \equiv -q = -19 \equiv 1 \pmod 4.$$

Za D mora vrijediti da je

$$\left(\frac{D}{p}\right) = \eta_p = -1 \quad \text{i} \quad \left(\frac{D}{q}\right) = \eta_q = 1.$$

Broj $D = 138$ zadovoljava ove uvjete i kvadratno je slobodan. Nadalje, računamo vrijednost S tako da vrijedi $\left(\frac{S^2-D}{n}\right) = -1$, te se dobije da je jedno od mogućih izbora za $S = 18$. Treba nam i neparan broj m,

$$m = \frac{(p-\eta_p)(q-\eta_q)}{4} = \frac{(13+1)19-1)}{4} = 63.$$

Neka je $e = 5$. Očito je $(e, m) = 1$. Iz

$$de \equiv \frac{(m+1)}{2} \pmod m$$

dobivamo

$$d \equiv \frac{(m+1)}{2} \cdot e^{\varphi(m)-1} \pmod m,$$

pa je $d = 19$. Sada imamo javni ključ

$$K = \{n, e, S, D\} = \{247, 5, 18, 138\},$$

te tajni ključ $d = 19$.

Šifriranje

Uzmimo sada da je poruka koju želimo šifrirati $M = 251$. Dobije se da je

$$j_1 = \left(\frac{M^2 - D}{n}\right) = \left(\frac{257^2 - 143}{493}\right) = -1.$$

Jer je $j_1 = -1$, računamo t i u po formulama

$$t \equiv ((M^2 + D)(S^2 + D) + 4DMS)((M^2 - D)(S^2 - D))^{-1} \pmod n,$$

$$u \equiv (2S(M^2 + D) + 2M(S^2 + D))((M^2 - D)(S^2 - D))^{-1} \pmod n,$$

te se dobije da je $t = 100$ i $u = 227$. Nadalje, dobivamo $j_2 = 0$ jer $t \equiv 0 \pmod 2$.

Odredimo sada polinome T_5 i T_6 iz rekurzije

$$T_n \equiv (2 \cdot T_1 \cdot T_{n-1} - T_{n-2}) \pmod{n},$$

uz početne uvijete $T_1 = t$ i $T_2 = 2 \cdot t^2 - 1$. Dobivamo da je $T_5 = 177$ i $T_8 = 199$.

Sada možemo izračunati šifrat

$$E \equiv DuT_5(T_6 - tT_5)^{-1} \equiv 15 \pmod{n}.$$

Šaljemo šifrat

$$E(251) = \{15, -1, 0\}.$$

Dešifriranje

Sada želimo dešifrirati $E(251)$. Izračunamo T_{2e} i $U_{2e} \pmod{n}$ koristeći

$$T_{2e} \equiv (E^2 + D)(E^2 - D)^{-1} \pmod{n}$$

i

$$U_{2e} \equiv (2E)(E^2 - D)^{-1} \pmod{n},$$

te dobivamo da je $T_{2e} = 166$ i $U_{2e} = 77$. Nadalje računamo

$$T_{2de} \equiv T_d(T_{2e}) \pmod{n} = T_{19}(166) \pmod{n}$$

i

$$T_{2de+2e} \equiv T_{d+1}(T_{2e}) \pmod{n} = T_{20}(166) \pmod{n},$$

na način opisan ranije, te se dobije da je $T_{2de} = 147$ i $T_{2de+2e} = 49$.

Iz $T_{2de} \equiv \sigma t \pmod{n}$ i $j_2 = 0 \equiv t \pmod{2}$ vidimo da je $\sigma = -1$ i $t \equiv -147 \equiv 100 \pmod{n}$. Iz $u \equiv \sigma U_{2ed}$, dobivamo da je $u = 227$.

Sada imamo da je

$$\alpha \equiv 100 + 227\sqrt{D} \pmod{n}$$

i

$$\alpha' = \alpha \frac{(S - \sqrt{D})}{S + \sqrt{D}},$$

jer je $j_1 = -1$. Slijedi da je

$$\alpha' = \frac{77 + 4\sqrt{138}}{186}.$$

Nadalje, otvoreni tekst je

$$M \equiv (\alpha' + 1)\sqrt{D}/(\alpha' - 1) \pmod{n} = 251.$$

Bibliografija

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

[2] A. Dujella, *Uvod u teoriju brojeva (skripta)*, PMF-Matematički odjel Svečilišta u Zagrebu, (travanj 2015)

[3] M. J. Jacobson, Jr. , H. C. Williams, *Solving the Pell equation*, Springer, New York, 2009.

Sažetak

Želimo li u današnjem svijetu bez privatnosti osigurati sigurnu komunikaciju, koristit ćemo kriptosustave. Probijanje šifri biva sve češće i sofisticiranije, pa nam je u cilju imati što više raznolikih kriptosustava. Zbog toga se i razne grane matematike, te njihovi rezultati, primjenjuju na njihov razvoj. Kriptosustav opisan u ovom radu, prvi se puta pojavio 1984. godine. Jedna je od varijanti RSA kriptosustava, koja se temelji na Pellovoj jednadžbi $x^2 - dy^2 = 1$, sa sigurnosti zasnovanoj na teškoći problema faktorizacije.

Summary

With the lack of privacy in the world, we use cryptosystems, as we want to provide a safe communication. Code-breaking techniques are becoming more frequent and more sophisticated, so we need different cryptosystems at our disposal. Because of that, many different areas of mathematics and their results have been applied to their development. The cryptosystem described in this work first appeared in 1984. It is a variant of the RSA cryptosystem based on Pell's Equation $x^2 - dy^2 = 1$ with the security based on the factorization problem.

Životopis

Rođena sam 23. lipnja 1987. godine u Zagrebu, gdje od 1993. do 2001. godine pohađam osnovnu školu Alojzija Stepinca. Nakon toga, upisujem matematičku gimnaziju u Zagrebu, V. gimnaziju koju završavam 2005. godine. Iste godine upisujem preddiplomski studij matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu. Preddiplomski studij završavam 2012. godine, te nastavljam na smjeru Računarstvo i matematika, uz koji u sklopu osnovne škole Ivana Gundulića držim informatičke radionice za djecu.