Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Tea Šafar

Kriptografija javnog ključa

Diplomski rad

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Tea Šafar

Kriptografija javnog ključa

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2018.

Sadržaj

Uvod

U radu se proučavaju osnove kriptografije javnog ključa te primjeri takvih kriptosustava. U prvom poglavlju upoznajemo se s osnovnim pojmova kriptografije poput otvoreni tekst, šifrat, ključ, kriptosustav te podjelu kriptosustava i osnovne napade na njih. Sljedeće poglavlje govori o osnovnoj ideji kriptografije javnog ključa te usporedbi takvih kriptosustava s kriptosustavima s tajnim ključem poput Data Encryption Standarda (DES), Advanced Encryption Standarda (AES) i Triple DES-a. Treće poglavlje prikazuje kriptosustave zasnovane na problemu faktorizacije od kojih su obrađeni RSA i Rabinov kriptosustav. Prikazane su njihove definicije, primjeri te prednosti i mane tih kriptosustava. Kriptosustavi zasnovani na problemu diskretnog logaritma obrađeni su u četvrtom poglavlju. Unutar njega opisujemo Diffie-Hellmanov protokol za razmjenu ključeva te ElGamalov kriptosustav. U zadnjem poglavlju upoznajemo se s problemom ruksaka te sustavom zasnovanom na tom problemu, odnosno Merkle-Hellmanovim kriptosustavom.

1 Osnovni pojmovi

Kriptografija je znanstvena disciplina koja proučava poruke napisane na takav način da ih jedino onaj kojem su namijenjene može razumjeti.

Cilj kriptografije je omogućavanje komunikacije dviju osoba, koje ćemo nazivati *pošiljatelj* poruke i *primatelj* poruke, tako da neka treća osoba, koju nazivamo *protivnik*, ne može pročitati njihove poruke.

Poruka koja se šalje naziva se *otvoreni tekst*, a oblik u kojem je ta poruka zapisana i u kojem će primatelj dobiti poruku naziva se *šifrat*. Postupak kojim pošiljatelj transformira otvoreni tekst pomoću unaprijed dogovorenoga *ključa* naziva se *šifriranje*.

Pošiljatelj šalje šifrat primatelju preko komunikacijskog kanala pri čemu protivnik može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Njega može odrediti primatelj tako da pomoću ključa dešifrira šifrat.

Važno je upoznati i pojmove kriptoanalize i kriptologije. *Kriptoanaliza* ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. *Kriptologija* je grana znanosti koja obuhvaća kriptografiju i kripotanalizu.

Šifra ili *kriptografski algoritam* je matematička funkcija koja se koristi za šifriranje i dešifriranje (obično su to dvije funkcije od kojih jedna služi za šifriranje, a druga za dešifriranje). Te funkcije preslikavaju elemente otvorenog teksta u elemente šifrata i obratno. One su odabrane iz određenih familija funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključa naziva se *prostor ključeva*.

Definicija 1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *pri čemu je* $\mathcal{P}$ *konačan skup svih mogućih elemenata otvorenog teksta,* $\mathcal{C}$ *konačan skup svih mogućih elemenata šifrata,* $\mathcal{K}$ *konačan skup svih mogućih ključeva,* $\mathcal{E}$ *skup svih mogućih funkcija šifriranja,* $\mathcal{D}$ *skup svih mogućih funkcija dešifriranja. Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$*. Pritom su* $e_K \colon \mathcal{P} \to \mathcal{C}$ *i* $d_K \colon \mathcal{C} \to \mathcal{P}$ *funkcije takve da je* $d_K(e_K(x)) = x$ *za svaki* $x \in \mathcal{P}$*.*

Kriptosustavi su obično klasificirani obzirom na sljedeće kriterije:

1. obzirom na tip operacija koje se koriste pri šifriranju:

   podjela na supstitucijske šifre (svaki element otvorenog teksta zamijenjen je nekim drugim elementom), transpozicijske šifre (elementi otvorenog teksta su permutirani) i kombinacija tih dviju metoda;

2. obzirom na način na koji se obrađuje otvoreni tekst:

   podjela na blokovne šifre (obrađuje se jedan po jedan blok elemenata otvorenog teksta korištenjem istog ključa) i protočne šifre (elementi otvorenog teksta se obrađuju jedan po jedan koristeći paralelno generirani niz ključeva);

3. obzirom na tajnost ključeva:

   podjela na simetrične kriptosustave ili kriptosustave s tajnim ključem (ključ za dešifriranje može se izračunati ako je poznat ključ za šifriranje i obratno) i asimetrične kriptosustave ili kriptosustave s javnim ključem (ključ za dešifriranje se ne može izračunati u nekom razumnom vremenu ako je poznat ključ za šifriranje).

Upoznajmo se još i s napadima na kriptosustave. *Napad* na kriptosustav je svaka metoda kojom kriptoanalitičar pokušava doći do otvorenog teksta, ključa ili algoritma. Promotrimo osnovne napade:

1. napad poznatim šifratom: kriptoanalitičar posjeduje šifrat od nekoliko poruka koje su šifrirane istim algoritmom, a njegov cilj je otkriti otvoreni tekst od što više poruka ili ključ kojem su one šifrirane;

2. napad poznatim otvorenim tekstom: kriptoanalitičar posjeduje šifrat neke poruke te odgovarajući otvoreni tekst, a zadatak mu je otkriti ključ ili algoritam za dešifriranje poruka koje su šifrirane upravo tim ključem;

3. napad odabranim otvorenim tekstom: kriptoanalitičar može odabrati tekst koji će biti šifriran te dobiti njegov šifrat;

4. napad odabranim šifratom: kriptoanalitičar ima pristup alatu za dešifriranje pa može odabrati šifrat i dobiti odgovarajući otvoreni tekst.

2 Osnovno o javnom ključu

Začetnicima kriptografije javnog ključa smatraju se Whitfield Diffie i Martin Hellman koji su 1976. godine ponudili rješenje problema razmjene ključeva.

Ideja javnog ključa sastoji se u konstrukciji kriptosustava kod kojih bi u nekom razumnom vremenu bilo praktički nemoguće iz poznavanja funkcije šifriranje e_K izračunati funkciju dešifriranja d_K. U tome bi slučaju funkcija šifriranja e_K mogla biti javna.

Prije definiranja pojma kriptosustava s javnim ključem, potrebno je uvesti pojam jednosmjerne funkcije te osobne jednosmjerne funkcije.

Definicija 2. *Za funkciju f kažemo da je jednosmjerna ako je f lako, a f^{-1} teško izračunati. Ako je pritom f^{-1} lako izračunati ukoliko nam se poznat neki dodatni podatak, onda f nazivamo osobna jednosmjerna funkcija.*

Definicija 3. *Kriptosustav s javnim ključem sastoji se od familija funkcija za šifriranje $\{e_K\}$ i dešifriranje $\{d_K\}$ sa svojstvima:*

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

Tada funkciju e_K nazivamo javnim ključem, a d_K tajnim ili osobnim ključem.

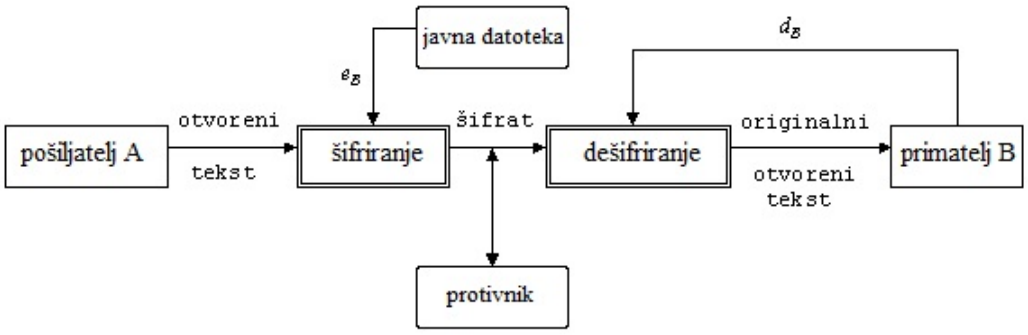
Proces slanja poruke x između pošiljatelja A i primatelja B odvija se na sljedeći način: najprije osoba B pošalje osobi A svoj javni ključ e_B pomoću kojeg osoba A šifrira svoju poruku. Potom osoba A šalje osobi B šifrat

$$y = e_B(x)$$

kojeg osoba B dešifrira koristeći svoj tajni ključ d_B te dobiva

$$d_B(y) = d_B(e_B(x)) = x.$$

Ukoliko se komunikacija odvija između više ljudi tada svi korisnici stave svoje javne ključeve u neku datoteku koja je dostupna svima. U tom slučaju osoba B ne šalje svoj javni ključ osobi A, nego osoba A pročita taj ključ iz datoteke (vidjeti Sliku 1).



Slika 1: Shema kriptografije javnog ključa

Budući da svatko može pristupiti funkciji e_B, tada se svatko može i predstaviti kao osoba A. Zato dolazi do pitanja vjerodostojnosti ili autentičnosti poruke koje se može riješiti na sljedeći način:

1. Osoba A doda svojoj poruci slučajan broj a od recimo 10 znamenaka;

2. Osoba B generira svoj slučajan 10-znamenkasti broj b i pošalje osobi A poruku $e_A(a+b)$;

3. pomoću formule
$$b = d_A(e_A(a+b)) - a$$
pošiljatelj A izračuna b i ponovno pošalje početnu poruku kojoj doda b te isto to napravi sa svakom sljedećom porukom koju će poslati primatelju B.

Često je potpis jedan od najvažnijih dijelova poruke. On primatelju govori da je poruka koju je primio doista poslana od osobe čiji se potpis nalazi na kraju poruke. Kako elektroničke poruke ne mogu biti potpisane vlastoručno, postoje kriptosustavi koji omogućuju digitalni potpis. Pretpostavimo da je $\mathcal{P} = \mathcal{C}$. U tom slučaju pošiljatelj A može potpisati svoju poruku x tako da primatelju B pošalje šifrat

$$z = d_A(y) = d_A(e_B(x)).$$

Primatelj B će najprije na tu poruku primijeniti javni ključ e_A, a zatim svoj tajni ključ d_B, odnosno

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

Pogledajmo kako to izgleda na primjeru:

Primjer 1. *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$. *Pretpostavimo da Aurora šalje Borni poruku* $x = 6$. *Neka je Aurorin javni ključ*

$$e_A(x) = (x + 4) \mod 26,$$

a tajni ključ

$$d_A(y) = (y - 4) \mod 26$$

te neka je Bornin javni ključ

$$e_B(x) = (x + 3) \mod 26$$

i tajni ključ

$$d_B(y) = (y - 3) \mod 26.$$

Aurora će najprije primijeniti Bornin javni ključ e_B *i dobiti:*

$$y = e_B(x) = (6 + 3) \mod 26 = 9.$$

Zatim će primijeniti svoj tajni ključ d_A *i poslati Borni šifrat:*

$$z = d_A(y) = (9 - 4) \mod 26 = 5.$$

Kada Borna dobije poruku $z = 5$, *najprije će primijeniti Aurorin javni ključ* e_A *i dobiti:*

$$e_A(z) = (5 + 4) \mod 26 = 9$$

te će na kraju primijeniti svoj tajni ključ d_B *i dobiti poruku*

$$d_B(e_A(z)) = (9 - 3) \mod 26 = 6.$$

Primijetimo da korištenjem bilo kojeg drugog ključa d_C ne bismo dobili isti rezultat. Stoga je na prethodno opisan način doista poruka koju je poslao pošiljatelj A upravo ona koju je primio primatelj B.

U usporedbi sa simetričnim kriptosustavima, glavne prednosti asimetričnog kriptosustava su:

1. nije potreban sigurni komunikacijski kanal za razmjenu ključeva;

2. dugovječnost: kod asimetričnih kriptosustava par ključeva može se koristiti duže vrijeme bez promjene, čak godinama, dok se kod simetričnih kriptosustava ključevi moraju mijenjati pri svakoj uporabi;

3. manji broj ključeva: za komunikaciju grupe od n ljudi potrebno je $2n$ ključeva jer su svakom od korisnika potreba samo dva ključa, javni i tajni, za komunikaciju s preostalih $n-1$ ljudi. S druge strane, kod simetričnog kriptosustava svakom od korisnika potreban je zaseban ključ za komunikaciju sa svakom od $n-1$ osoba, stoga je $\binom{n}{2} = \frac{n(n-1)}{2}$ ukupan broj potrebnih ključeva;

4. mogućnost potpisa poruke;

5. nepobitnost: pošiljatelj ne može zanijekati da je poslao poruku. Kod asimetričnih kriptosustava nepobitnost se osigura digitalnim potpisom, dok je kod simetričnih kriptosustava potrebna neka treća osoba od povjerenja.

U stvarnom životu kriptografija javnog ključa ne može zamijeniti simetrične kriptosustave jer se ona ne koristi za šifriranje poruka nego za šifriranje ključeva. Zapravo osobe A i B razmjenjuju poruke pomoću simetričnog kriptosustava koristeći ključ koji su razmijenili pomoću asimetričnog kriptosustava. To se naziva hibridni kriptosustav.

Stoga, navedimo glavne nedostatke kriptosustava s javnim ključem:

1. algoritmi s javnim ključem su znatno sporiji od modernih simetričnih algoritama (čak 1000 puta);

2. ključevi asimetričnih kriptosustava znatno su veći nego oni kod simetričnih;

3. slabi su na napad "odabrani otvoreni tekst": ako je $y = e(x)$, gdje otvoreni tekst može poprimiti jednu od n vrijednosti, tada je šifriranjem svih n mogućih otvorenih tekstova i usporedbom s y moguće otkriti x. Pritom tajni ključ d neće biti otkriven. Taj napad moguće je izvršiti jedino ako je n mali.

3 Kriptosustavi zasnovani na problemu faktorizacije

Obično se pri konstrukciji kriptosustava s javnim ključem koriste neki kompliciraniji matematički problemi kao što je problem faktorizacije velikih prirodnih brojeva.

3.1 RSA kriptosustav

Jedan od najstarijih i najpopularnijih kriptosustava s javnim ključem je upravo RSA kriptosustav. Njegovi tvorci Ronald Rivest, Adi Shamir i Leonard Adleman, po kojima je kriptosustav dobio i ime, prvi su ga puta objavili 1977. godine u časopisu "Scientific American". RSA kriptosustav se i danas koristi u bankarstvu i e-mail sigurnosti pri e-kupovini na internetu.

Rad RSA kriptosustava možemo opisati na sljedeći način: odaberemo dva prosta broja p i q te postavimo $n = pq$. Kako je poznata faktorizacija broja n, tada je lako izračunati vrijednost Eulerove funkcije φ kao

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

Zatim odaberemo cijeli broj između 1 i $\varphi(n)$ relativno prost s $\varphi(n)$ te izračunamo d tako da vrijedi

$$ed \equiv 1 \,(\mathrm{mod}\ \varphi(n)).$$

Naposljetku u javnu datoteku spremimo ključ za šifriranje (n, e).

Slijedi definicija RSA kriptosustava prema [3]:

Definicija 4. *Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Neka je $\mathcal{K} = \{(n, p, q, d, e) \colon p, q \text{ prosti}, n = pq, (e, \varphi(n)) = 1\}$. Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo funkciju šifriranja s*

$$e_K(x) = x^e \bmod n$$

te funkciju dešifriranja

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

pri čemu su $x, y \in \mathbb{Z}_n$. Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne, odnosno (n, e) je javni, a (p, q, d) je tajni ključ.

Za e se obično uzima da je $e \leq \varphi(n)$. Može se izabrati slučajno, no poželjno je odabrati što manji e kako bi se šifriranje $x^e \bmod n$ odvijalo brže. Kako broj operacija u šifriranju ovisi o veličini broja e i broju jedinica u binarnom zapisu od e, jedan od čestih odabira jest $e = 3$. No, budući da upravo odabir malog broja e narušava sigurnost kriptosustava, najbolji odabir je broj $e = 2^{16} + 1 = 65537$. Taj broj je pogodan jer je prost te dovoljno velik za izbjegavanje napada malim eksponentom. Bilo koji veći broj zahtijevao bi barem još jednu operaciju množenja ili dijeljenja, čime bi se proces računanja dodatno odužio. Možemo primijetiti da su i broj 3 kao i 65537 Fermatovi brojevi, odnosno brojevi oblika $2^{2^n} + 1$, pri čemu je n nenegativni cijeli broj. Točnije, brojevi 3,5,17,257 i 65537 su do sada poznati Fermatovi prosti brojevi, to jest brojevi oblika $2^k + 1$, za $k > 0$. Oni su također česti izbori broja e.

U sljedećem primjeru prikazat ćemo šifriranje i dešifriranje u RSA kriptosustavu pri čemu ćemo radi jednostavnosti uzeti male proste brojeve p i q.

Primjer 2. *Neka je* $p = 11$ *i* $q = 17$. *Tada je*

$$n = p \cdot q = 11 \cdot 17 = 187$$

te

$$\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160.$$

Kako znamo da e mora biti relativno prost s $\varphi(n)$, *možemo odabrati* $e = 3$. *Sada je* $(n, e) = (187, 3)$ *javni ključ. Budući da vrijedi* $(e, \varphi(n)) = 1$, *postoje cijeli brojevi* d, l *takvi da je*

$$ed + l\varphi(n) = 1,$$

odnosno

$$ed \equiv 1 \,(\text{mod } \varphi(n)).$$

Sada imamo

$$3d \equiv 1 \,(\text{mod } 160),$$

iz čega slijedi da je $d = 107$. *Uočimo kako se parametar d može odrediti iz prethodne jednadžbe direktnom primjenom Euklidova algoritma.*
Pretpostavimo sada da nam netko želi poslati poruku $x = 72$. *Tada treba izračunati* $x^e \mod n$, *tj.*

$$72^3 \bmod 187.$$

Dobivamo šifrat $y = e_K(x) = 183$. *Kada primimo ovaj šifrat, dešifriramo ga pomoću tajnog ključa d:*

$$x = d_K(y) = 183^{107} \bmod 187$$

iz čega dobivamo $x = 72$.

Pozabavimo se sada pitanjem sigurnosti RSA kriptosustava. Prema Hineku [4, str.8] sigurnost RSA kriptosustava leži u teškoći rješavanja takozvanog RSA problema. On se sastoji od određivanja poruke x ako nam je poznat javni ključ (n, e) te šifrat $y = x^e \bmod n$. Odnosno, to je problem računanja e-tog korijena modulo n, to jest određivanja inverza RSA funkcije. Problem je teško rješiv kada je otvoreni tekst $x \in \mathbb{Z}_n$ slučajno odabran te modul n dovoljno velik broj pri čemu su p i q također slučajno odabrani veliki brojevi takvi da je $n = pq$. Taj uvjet nazivamo RSA pretpostavkom koju smatramo istinitom jer nije dokazano da je neistinita otkad je RSA stvoren pa do današnjeg dana. Poželjno je da tajno izabrani parametri p i q budu veliki prosti brojevi od barem 100 znamenaka. Oni se biraju tako da se prvo generira slučajan prirodan broj m s traženim brojem znamenaka, nakon čega se traži prvi prosti broj veći ili jednak od m koristeći pritome neki test prostosti. Za $n = pq$ je važno da bude otporan na metode faktorizacije koje su uspješne kada su brojevi nekog specijalnog oblika pa bi prema tome brojevi $p \pm 1$ i $q \pm 1$ trebali imati barem jedan veliki prosti faktor. Osim toga, p i q ne smiju biti vrlo blizu jedan drugome jer ih se u tome slučaju može odrediti tako se promatraju brojevi koji su približno jednaki $\sqrt{n}$.

Druga poteškoća koja se javlja kod pitanja sigurnosti RSA kriptosustava je problem faktorizacije cijelog broja. Kada bismo uspjeli faktorizirati modul n, tada bismo mogli odrediti tajni eksponent d za svaki javni eksponent e pa bi svi šifrati šifrirani javnim ključem (n, e) mogli biti dešifrirani. Iz toga slijedi da RSA problem možemo uspješno riješiti za javni ključ (n, e) i valjani šifrat. Tada je rješavanje RSA problema jednake težine kao i rješavanje problema faktorizacije. No, ne možemo tvrditi da vrijedi i suprotno, odnosno ne možemo tvrditi da rješavanjem RSA problema možemo uspješno riješiti i problem faktorizacije.

Iako je lakše riješiti RSA problem nego problem faktorizacije cijelog broja, u praksi se pretpostavlja da su ti problemi ekvivalentni.

Osim što je potrebno izbjegavati male brojeve p i q, potrebno je i izbjegavati mali tajni eksponent d. Napad koji služi za razbijanje RSA kriptosustava u slučaju da je izabran mali tajni eksponent d zove se Wienerov napad. Nazvan je po kanadskom kriptologu Michaelu Wieneru. Sljedeći teorem govori upravo o postojanju polinomijalnog algoritma za razbijanje RSA kriptosustava u tom slučaju.

Teorem 1. *Neka je* $n = pq$ *i* $p < q < 2p$ *te neka je* $e < \varphi(n)$ *i* $d < \frac{1}{3}n^{0.25}$. *Tada*

postoji polinomijalni algoritam koji iz poznavanja n i e računa d.

Dokaz ovoga teorema nećemo prikazivati, ali ga se može pronaći u [3]. Pogledajmo kako to izgleda na primjeru:

Primjer 3. *Pretpostavimo da su zadani modul $n = 7064009$, javni eksponent $e = 5773091$ te da za tajni eksponent d vrijedi $d < \frac{1}{3}n^{0.25} < 18$. Najprije odredimo razvoj broja*

$$\frac{e}{n} = \frac{5773091}{7064000}$$

u verižni razlomak (vidjeti [3, str. 108]). Tada dobivamo:

$$[0; 1, 4, 2, 8, 2, 5, 38, 1, 1, 2, 4, 2, 3].$$

Zatim računamo pripadne konvergente (vidjeti [3, str. 109]):

$$0, 1, \frac{4}{5}, \frac{9}{11}, \frac{76}{93}, \frac{161}{197}, \frac{881}{1078}, \frac{33639}{41161}, \frac{34520}{42239}, \frac{68159}{83400}, \frac{170838}{209039}, \frac{751551}{919556}, \frac{1673860}{2048151}, \frac{5773091}{7064009}.$$

Kako je $d < 18$, provjerimo koji od nazivnika 5 i 11 zadovoljava kongruenciju $(x^e)^d \equiv x \pmod{n}$ za primjerice $x = 2$. Naposljetku dobivamo $d = 11$.

Još jedan od napada je "odabrani šifrat" koji je opasnost za sve kriptosustave s javnim ključem. Protivnik može izračunati šifrat y tako da izabere slučajan otvoreni tekst x_1 i izračuna $y_1 = yx_1^e \bmod n$ te zamoli primatelja da dešifrira y_1. Rezultat dešifriranja je xx_1 iz kojeg protivnik može izračunati traženi otvoreni tekst x. U ovom slučaju je otkriven otvoreni test, ali nisu otkriveni niti n niti tajni ključ primatelja.

Možemo zaključiti da još nije pronađena metoda koja bi razbila RSA kriptosustav pa se stoga, uz korektnu implementaciju, on može smatrati sigurnim kriptosustavom. Za opširniju analizu metoda za razbijanje RSA kriptosustava treba vidjeti [4]. Osim analiza napada poput modifikacije Wienerovog napada, takozvanog napada rešetkom te Boneh-Durfeejevog napada rešetkom, ondje se mogu vidjeti i neke varijante RSA kriptosustava: CRT-RSA koji se najviše koristi u praksi, RSA kriptosustav kod kojeg je modul n produkt od tri ili više prostih brojeva (takozvani Multi-prime RSA) te RSA kriptosustav kod kojeg $p - 1$ i $q - 1$ imaju zajedničkog velikog djelitelja (Common prime RSA).

Prednosti RSA kriptosustava su brzo šifriranje za mali e te mogućnost potpisa poruke. Opisat ćemo kako izgleda postupak potpisivanja prema [1]. Pretpostavimo

da Aurora želi poslati Borni poruku x koristeći RSA kriptosustav tako da Borna zna da je tu poruku upravo poslala Aurora. Neka Aurora koristi modul $n = pq$ te eksponente e i d, a Borna koristi $n^* = p^*q^*$ te eksponente e^* i d^*. Također, pretpostavimo da Aurora ne zna Bornin tajni ključ i obratno. Tada Aurora računa

$$e_1(x) = x^d \bmod n$$

koristeći njezin dekripcijski eksponent. Ako je $e_1(x) \geq n^*$, tada Aurora mora podijeliti $e_1(x)$ u blokove prije nego izračuna

$$e(x) = e_1(x)^{e^*} \bmod n^*$$

te pošalje Borni dobiveni šifrat. Ukoliko je $e_1(x) < n^*$ tada Aurora ne dijeli $e_1(x)$ u blokove nego samo provodi opisani postupak.

Borna će Aurorinu poruku dešifrirati tako da najprije odredi

$$e_1(x) = e(x)^{d^*} \bmod n^*.$$

Zatim koristeći Aurorin javni ključ odredi njezinu poruku tako da izračuna

$$x = e_1(x)^e \bmod n.$$

Pogledajmo kako to izgleda na primjeru:

Primjer 4. *Pretpostavimo da Aurora želi Borni poslati poruku $x = 45$ te da odabere $p = 5$ i $q = 11$. Tada je*

$$n = pq = 5 \cdot 11 = 55.$$

Ako za enkripcijski eksponent odabere $e = 3$ tada iz

$$3d \equiv 1 \,(\mathrm{mod}\ 40)$$

dobiva dekripcijski eksponent $d = 27$. Ako Borna odabere $p^* = 7$, $q^* = 17$ i $e^* = 5$, tada je

$$n^* = p^*q^* = 7 \cdot 17 = 119$$

te $d^* = 77$. Kako bi Aurora poslala poruku $x = 45$ s potpisom, najprije računa:

$$e_1(x) = 45^{27} \bmod 55 = 45.$$

Nitko drugi to ne može napraviti osim Aurore jer je njezin dekripcijski eksponent d tajan. Nakon toga, Aurora pomoću Borninog eksponenta e^* i modula $n^* = 119$ napravi šifrat

$$e(x) = 45^5 \bmod 119 = 61$$

i njega šalje Borni. Kada on primi taj šifrat, najprije odredi

$$e_1(x) = 61^{77} \bmod 119 = 45,$$

a zatim do poruke dolazi tako da izračuna

$$x = 45^3 \bmod 55 = 45.$$

3.2 Rabinov kriptosustav

Rabinov kriptosustav potječe iz 1979. godine, a ime je dobio po izraelskom informatičaru Michaelu Rabinu. Usko je povezan s problemom faktorizacije prirodnog broja, a taj problem povezan je s problemom računanja kvadratnog korijena u $\mathbb{Z}_n$. Ova činjenica pokazuje prednost Rabinovog kriptosustava pred RSA kriptosustavom.

Neka su p i q prosti brojevi te $n = pq$. Potrebno je pronaći, ukoliko postoji, $x \in \mathbb{Z}$ za kojeg vrijedi $x^2 \equiv a \pmod{n}$, pri čemu je $1 \leq a \leq n-1$. Odnosno potrebno je pronaći takav x da je a kvadratni ostatak modulo n. Postoji algoritam za rješavanje prethodno spomenute kongruencije, a on je pojednostavljen za proste brojeve p i q za koje vrijedi $p \equiv q \equiv 3 \pmod{4}$. Tada rješenje kongruencije $x^2 \equiv a \pmod{p}$ dobivamo kao $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$. Zaista, prema Eulerovom kriteriju za kvadratne ostatke (vidjeti [3, str. 190]) vrijedi

$$x^2 \equiv a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \pmod{p}.$$

Analogno dobijemo da rješenje kongruencije $x^2 \equiv a \pmod{q}$ iznosi $x \equiv \pm a^{\frac{q+1}{4}} \pmod{q}$. Tada imamo po dvije klase rješenja svake od kongruencija po modulima p i q, odnosno

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

Kombinirajući po dva rješenja iz prethodnih klasa rješenja te koristeći Kineski teorem o ostacima (vidjeti [1, str.162]) dobivamo četiri rješenja kongruencije $x^2 \equiv a$

(mod pq), odnosno $x^2 \equiv a \pmod{n}$. Stoga su kvadratni korijeni modulo n sljedeći:

$$x_{1,2} = \pm(c \cdot p \cdot a^{\frac{q+1}{4}} + d \cdot q \cdot a^{\frac{p+1}{4}}) \mod n$$

$$x_{3,4} = \pm(c \cdot p \cdot a^{\frac{q+1}{4}} - d \cdot q \cdot a^{\frac{p+1}{4}}) \mod n$$

pri čemu su c i d cijeli brojevi dobiveni primjenom Euklidova algoritma na p i q jer vrijedi $(p, q) = 1$.

Prema [1], šifriranje u Rabinovom kriptosustavu se odvija tako da otvoreni tekst x pretvorimo u šifrat e pomoću

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

gdje je $0 \leq x < n$, $0 \leq e < n$, a n je produkt dva prosta broja p i q oblika $4k + 3$ za $k \in \mathbb{Z}$. U ovom kriptosustavu je javni ključ n, a tajni ključevi su brojevi p i q. Razlog zbog kojeg n može biti javan je taj da se p i q biraju tako da budu veliki brojevi, brojevi od recimo stotinu decimala. Budući da je n umnožak ta dva velika broja, tada je njega teško faktorizirati u nekom razumnom vremenu.

Pogledajmo sada kako definiramo šifriranje u Rabinovom kriptosustavu:

Definicija 5. *Neka je $n = pq$, pri čemu su p i q prosti brojevi za koje vrijedi $p \equiv q \equiv 3 \pmod{4}$. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te $\mathcal{K} = \{(n, p, q) \colon n = pq\}$. Za $K \in \mathcal{K}$ definiramo funkciju šifriranja*

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

i funkciju dešifriranja

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

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

Primijetimo kako je postavljen uvjet da p i q moraju zadovoljavati $p \equiv q \equiv 3 \pmod{4}$. Taj uvjet nije nužan te se može izostaviti. Naime, proces je isti i ako su p i q prosti brojevi nekog drugog oblika, no najčešće se on koristi zbog jednostavnijeg i efikasnijeg procesa dešifriranja. Kanadski matematičar Hugh Williams je 1980. godine dao jednu modifikaciju Rabinova kriptosustava u kojem su brojevi p i q takvi da $p \equiv 3 \pmod{8}$ i $q \equiv 7 \pmod{8}$ (vidjeti [8]).

Pokažimo na primjeru kako funkcionira šifriranje i dešifriranje u Rabinovom sustavu.

Primjer 5. *Neka je poruka koju želimo poslati koristeći Rabinov kriptosustav riječ* KRIPTOSUSTAV.

Neka svakom slovu abecede odgovara numerički ekvivalent: A=00, B=01,..., Z=25. *Podijelimo sada našu poruku u blokove od 4 slova, odnosno*

$$\text{KRIP} \quad \text{TOSU} \quad \text{STAV}.$$

Tada blokovima odgovaraju sljedeći numerički ekvivalenti, redom:

$$10170815 \quad 19141820 \quad 18190021.$$

S obzirom na naš izbor veličine bloka i šifriranja abecede, najveći mogući numerički ekvivalent je 25252525. *Važno je odabrati broj* $n = p \cdot q$ *tako da bude veći od toga broja. Za* p *i* q *znamo da moraju biti prosti brojevi za koje vrijedi*

$$p \equiv q \equiv 3 \pmod 4.$$

Neka je $p = 5527$ *i* $q = 5591$. *Oni su naši tajni ključevi. Tada je*

$$n = p \cdot q = 5527 \cdot 5591 = 301901457$$

te je $n > 25252525$ *pa je naš izbor broja* n *valjan.*

Šifrirajmo sada prvi blok koristeći funkciju šifriranja $e_K(x) = x^2 \bmod n$*:*

$$e_K(x_1) = 10170815^2 \mod 30901457 = 7522681.$$

Dobiveni ostatak je upravo traženi šifrat. Isto ćemo napraviti za drugi i treći blok:

$$e_K(x_2) = 19141820^2 \mod 30901457 = 5359278,$$

$$e_K(x_3) = 18190021^2 \mod 30901457 = 7576253.$$

Tada je naša poruka šifrirana na sljedeći način:

$$7522681 \quad 5359278 \quad 7576253.$$

Budući da je početna poruka bila podijeljena na blokove od 4 slova te su njihovi numerički ekvivalenti bili blokovi od 8 brojeva, tada i blokovi šifrata trebaju biti iste duljine. U našem slučaju se šifrirani blokovi sastoje od 7 brojeva. Uobičajeno je u tom slučaju dodati 0 *na početak bloka kako bi se dobio blok od 8 brojeva. Tada je naš šifrat:*

$$07522681 \quad 05359278 \quad 07576253.$$

Naposljetku, pridružimo blokovima ekvivalente u obliku slova:

$$\text{HAAD} \quad \text{FJOA} \quad \text{HFKB}$$

te spojimo blokove kako bismo dobili konačnu šifriranu poruku:

$$\text{HAADFJOAHFKB}.$$

Pretpostavimo sada da nam je dan šifrat HAADFJOAHFKB*, odnosno njegov numerički ekvivalent*

$$07522681 \quad 05359278 \quad 07576253$$

te su nam poznati tajni ključevi $p = 5527$ *i* $q = 5591$*. Kako bismo dešifrirali prvi blok, riješit ćemo sljedeću kongruenciju:*

$$7522681 \equiv x^2 \pmod{30901457}.$$

Na prethodno opisani način dobiveni su sljedeći kvadratni korijeni modulo n*:*

$$x \equiv 12237913 \pmod{30901457}$$

$$x \equiv 18663544 \pmod{30901457}$$

$$x \equiv 10170815 \pmod{30901457}$$

$$x \equiv 20730642 \pmod{30901457}.$$

Jednostavnom provjerom dobivamo da je treće rješenje traženo rješenje. Odnosno, traženi blok je 10170815*. U ovom slučaju je bilo lako provjeriti točnost rješenja uzevši u obzir da su elementi abecede šifrirani brojevima od 00 do 25. Na isti način dešifriramo drugi i treći blok. Najprije iz*

$$5359278 \equiv x^2 \pmod{30901457}$$

slijede kvadratni korijeni modulo n*:*

$$x \equiv 14974462 \pmod{30901457}$$

$$x \equiv 15926995 \pmod{30901457}$$

$$x \equiv 19141820 \pmod{30901457}$$

$$x \equiv 11759637 \pmod{30901457}.$$

Dobivamo da je 19131820 *traženo rješenje drugog bloka. Te naposljetku, treći blok dešifriramo rješavanjem kongruencije*

$$7576253 \equiv x^2 \pmod{30901457}.$$

Slijedi:

$$x \equiv 19216715 \pmod{30901457}$$

$$x \equiv 18190021 \pmod{30901457}$$

$$x \equiv 25799372 \pmod{30901457}$$

$$x \equiv 11607364 \pmod{30901457}.$$

Stoga je rješenje 18190021*.*

Kako bismo odredili poruku, zapišemo blokove jednog do drugoga, podijelimo ih na blokove od dva broja te ih na kraju zamijenimo slovima. Na taj način dobivamo poruku KRIPTOSUSTAV*.*

Primijetimo kako kod ovog kriptosustava, funkcija e_K nije injekcija, što je bio uvjet kod svakog kriptosustava. Kako postoje četiri kvadratna korijena modulo n, dešifriranje nije moguće provesti na jednoznačan način, osim ako je otvoreni tekst nekakav smislen tekst ili je unaprijed zadan podatak o otvorenom tekstu. Druga slabost Rabinova kriptosustava je napad "odabrani šifrat". Pretpostavimo da protivnik uspije nagovoriti primatelja da pomoću svoga tajnog ključa dešifrira šifrat y kojeg je protivnik izabrao. Tada protivnik može pomoću algoritma faktorizacije kvadratnog korijena faktorizirati n s vjerojatnošću $\frac{1}{2}$ jer postoje četiri kvadratna korijena od a modulo n. Ukoliko protivnik uspije nagovoriti primatelja da mu dešifrira k šifrata, vjerojatnost da će protivnik nakon toga uspjeti faktorizirati n bit će $1-\frac{1}{2^k}$.

Kao i kod RSA kriptosustava, prednosti Rabinovog kriptosustava su brzo šifriranje te mogućnost potpisivanja poruke. Opišimo sada kako taj proces izgleda prema [1].

Neka Aurora želi poslati Borni poruku x tako da on zna da je poruka koju je primio upravo Aurorina. Pretpostavimo da Aurora koristi modul $n = pq$, a Borna $n^* = p^*q^*$ te da su prosti brojevi p, q, p^*, q^* oblika $4k + 3$. Također pretpostavljamo da niti Aurora zna Bornin tajni ključ niti Borna zna Aurorin tajni ključ. Ona najprije izračuna

$$e_1(x)^2 = x \bmod n.$$

Ta transformacija poruke može dovesti do četiri kvadratna korijena modulo n, ali nije bitno kojeg će Aurora odabrati jer samo ona poznaje p i q pomoću kojih rješava dani problem. Ako je $e_1(x) \geq n^*$, tada Aurora mora podijeliti $e_1(x)$ u blokove te izvršiti transformaciju

$$e(x) = e_1(x)^2 \bmod n^*.$$

Naposljetku Borni pošalje šifrat $e(x)$.
Kako bi Borna dešifrirao dobivenu poruku, najprije mora izračunati

$$e(x) = e_1(x)^2 \bmod n^*.$$

Zatim do Aurorine poruke x dolazi tako da odredi

$$x = e_1(x)^2 \bmod n.$$

Postupak potpisivanja ćemo promotriti i na sljedećem primjeru:

Primjer 6. *Neka je $x = 12$ poruka koju Aurora želi poslati Borni. Pretpostavimo da Aurora odabere $p = 2111$ i $q = 4787$. Tada je njezin $n = 10105357$. Slično napravi i Borna, odabere $p^* = 1999$ i $q^* = 5011$ pa je tada $n^* = 10016989$. Računanjem*

$$e_1(x)^2 = 12 \bmod 10105357$$

Aurora dobiva četiri rješenja:

$$e_1(x)_1 = 396738, \quad e_1(x)_2 = 8454425, \quad e_1(x)_3 = 1650932 \quad i \quad e_1(x)_4 = 9708619.$$

Pretpostavimo da Aurora odabere prvo rješenje. Budući da će pri dešifriranju Borna morati računati kvadratne korijene, važno je da zna odabrati onaj pravi. Po dogovoru će Aurora pregrupirati $e_1(x) = 396738$ na način da poruku podijeli na $x_1 = 396396$ i $x_2 = 738738$. Na te dvije poruke će tada primijeniti $e(x) = x^2 \bmod 10016989$ te tako dobiti $e(x_1) = 3299362$ i $e(x_2) = 8271924$. Tada je potpisana poruka $e(x)$ uređeni par $(3299362, 8271924)$ kojeg Aurora šalje Borni.
Kada Borna primi šifrat $e(x) = (3299362, 8271924)$, odredi

$$e_1(x)^2 = e(x) \bmod 100166989.$$

Računanjem

$$e_1(x)^2 = 3299362 \bmod 100166989$$

dobiva sljedeća rješenja:

$$e_1(x)_1 = 44572, \quad e_1(x)_2 = 396396, \quad e_1(x)_3 = 9620593 \quad i \quad e_1(x)_4 = 9972417.$$

A računanjem

$$e_1(x)^2 = 8271924 \mod 100166989$$

dobiva rješenja:

$$e_1(x)_1 = 83066, \quad e_1(x)_2 = 738738, \quad e_1(x)_3 = 9278251 \quad i \quad e_1(x)_4 = 9933923.$$

Kako Borna zna način na koji je Aurora pregrupirala poruku, prepoznaje da je traženo rješenje i u prvom i u drugom slučaju drugo rješenje. Tada Borna pregrupira ta rješenja i dolazi do $e_1(x) = 396738$*. Kako bi došao do poruke, Borna odredi*

$$x = 396738^2 \mod 10105357 = 12.$$

Važno je napomenuti da se šifriranje i dešifriranje koristi ne samo radi potvrde da je poruka zaista od pošiljatelja, nego da se osigura to da nitko osim odabranoga primatelja ne može pročitati poruku.

4 Kriptosustavi zasnovani na problemu diskretnog logaritma

Za razumijevanje ovih kriptosustava, potrebno je poznavati pojmove grupe, cikličke grupe i konačne grupe, stoga ćemo dati njihove definicije.

Definicija 6. *Neka je G neprazan skup i $*\colon G\times G \to G$ preslikavanje sa svojstvima:*

1. $(x * y) * z = x * (y * z)$, $\forall x, y, z \in G$,
2. $\exists\ e \in G\ :\ e * x = x * e = x$, $\forall x \in G$,
3. $\forall x \in G\ \exists\ x^{-1} \in G\ :\ x * x^{-1} = x^{-1} * x = e$.

Tada se $(G, *)$ zove grupa.

Ako vrijedi i $x * y = y * x \quad \forall x, y \in G$, kažemo da je $(G, *)$ komutativna ili Abelova grupa.

Za grupu G kažemo da je ciklička ako je generirana jednim elementom, a to pišemo u obliku: $\exists\ a \in G\ :\ G = \langle a \rangle$. Broj elemenata grupe G označavamo s $|G|$.

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

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

Definicija 7. *Neka je $(G, *)$ konačna grupa i $H = \{g^i\colon i \geqslant 0\}$ podgrupa grupe G generirana elementom $g \in G$ i neka je $h \in H$. Treba pronaći najmanji nenegativni cijeli broj x takav da je*

$$h = g^x = \underbrace{g * g * g \cdots * g}_{x\ puta}.$$

Takav broj x zove se diskretni logaritam i označava $\log_g h$.

Primjer 7. *Promotrimo grupu* $\mathbb{Z}_p^*$ *za* $p = 11$*, to jest* $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$*. Generator te grupe je* $g = 7$*, što možemo lako provjeriti:*

$$7^1 = 7,\ 7^2 = 5,\ 7^3 = 2,\ 7^4 = 3,\ 7^5 = 10,\ 7^6 = 4,\ 7^7 = 6,\ 7^8 = 9,\ 7^9 = 8,\ 7^{10} = 1.$$

Tada je diskretni logaritam od, primjerice, broja 3 *jednak* 4*, odnosno* $\log_7 3 = 4$*.*

4.1 Diffie-Hellmanov protokol za razmjenu ključeva

Whitfield Diffie i Martin Hellman su, koristeći činjenicu da postoje grupe u kojima je problem diskretnog logaritma težak, riješili problem razmjene ključeva. Obično se za grupu G koristi multiplikativna grupa $\mathbb{Z}_p^*$ svih ne-nul ostataka modulo p.

Pretpostavimo da se Aurora i Borna žele dogovoriti oko ključa, slučajnog elementa iz G, kojeg će koristiti za šifriranje međusobnih poruka. Aurora odabere slučajan prirodan broj između 1 i $|G| - 1$ kojeg taji te izračuna g^a kojega postavi javnim (ovdje nam $|G|$ označava broj elemenata grupe G). Borna postupi slično, odabere slučajan b iz istog skupa te objavi g^b. Tada je zajednički tajni ključ g^{ab} kojeg oboje mogu izračunati.

Diffie-Hellmanov protokol možemo zapisati na sljedeći način:

1. Pošiljatelj generira slučajan prirodan broj $a \in \{1, 2, \ldots, |G| - 1\}$ i šalje primatelju element g^a.
2. Primatelj generira slučajan prirodan broj $b \in \{1, 2, \ldots, |G| - 1\}$ te šalje pošiljatelju element g^b.
3. Pošiljatelj izračuna $(g^b)^a = g^{ab}$.
4. Primatelj izračuna $(g^a)^b = g^{ab}$.

Sada je njihov tajni ključ $K = g^{ab}$.

Pogledajmo kako taj postupak izgleda na sljedećem primjeru:

Primjer 8. *Neka se Aurora i Borna dogovaraju oko ključa te neka je* $g = 3$ *generator grupe* $G = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$*. Aurora odabere, primjerice, broj* $a = 4$*. Zatim izračuna*

$$g^a = 3^4 = 81$$

te ga pošalje Borni. On također odabere broj, primjerice $b = 6$ *te izračuna*

$$g^b = 3^6 = 729$$

kojeg pošalje Aurori. Zatim Aurora izračuna

$$(g^b)^a = 729^4 = 282429536481 = g^{ab},$$

a Borna izračuna

$$(g^a)^b = 81^6 = 282429536481 = g^{ab}.$$

Tada je njihov zajednički tajni ključ $K = g^{ab} = 282429536481$.

Razmotrimo sada što bi se dogodilo kada bi neka treća osoba, nazovimo ju Eva, prisluškivala Aurorin i Bornin razgovor. Ona bi tada znala sljedeće podatke: g, p, g^a i g^b, gdje je $p = |G|$. Kako bi dešifrirala poruku mora poznavati ključ $K = g^{ab}$. Do njega bi mogla doći tako da izračuna $(g^a)^b$ ili $(g^b)^a$, no Eva na poznaje niti vrijednost a niti vrijednost b. Kako bi Eva izračunala brojeve a ili b, morala bi riješiti kongruencije oblika

$$z \equiv g^a \pmod{p},$$

odnosno

$$z \equiv g^b \pmod{p},$$

tj. probleme diskretnog logaritma. Taj problem je težak kada je modul p velik i g generator grupe G modulo p. Upravo u tome leži tajna sigurnosti Diffie-Hellmanovog protokola za razmjenu ključeva.

4.2 ElGamalov kriptosustav

Egipatski kriptograf Taher ElGamal je 1985. godine u radu "A public key cryptosystem and a signature scheme based on discrete logarithms" objavio konstrukciju kriptosustava zasnovanog na teškoći računanja diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$. Ovaj problem je iste težine kao i problem faktorizacije složenog broja n pri čemu su p i n istog reda veličine.

Kako bismo konstruirali ElGamalov kriptosustav (vidjeti [1, str. 267] i [2, str. 172]), primatelj poruke mora odabrati veliki prosti broj p i primitivni korijen α modulo p pri čemu su oba podatka javna. Zatim tajno odabere nenegativni cijeli broj a manji od $p-1$ te izračuna

$$\beta = \alpha^a \bmod p,$$

pri čemu je β javan. Tada je a javni ključ. Pošiljatelj tada za poruku x, pri čemu je x cijeli broj takav da $0 \leq x < p$, odabere cijeli broj k za kojeg vrijedi $1 \leq k \leq p-2$.

Nakon toga izračuna

$$y_1 = \alpha^k \bmod p$$

te

$$y_2 = x \cdot \beta^k = x \cdot (\alpha^a)^k \bmod p.$$

Tada je šifrat uređeni par (y_1, y_2).

Kako bi primatelj dešifrirao poruku (y_1, y_2) koristeći tajni ključ a, mora izračunati

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

Pogledajmo sada kako je prema [3] definiran ElGamalov kriptosustav:

Definicija 8. *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 $\mathcal{K} = \{(p, \alpha, a, \beta) \colon \beta = \alpha^a \bmod p\}$. Vrijednosti p, α i β su javne, a vrijednost a je tajna. Za ključ $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, 2, \ldots, p-1\}$ definiramo funkciju šifriranja s*

$$e_K(x, k) = (\alpha^k \bmod p, x \cdot \beta^k \bmod p) = (y_1, y_2).$$

Za šifrat $(y_1, y_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ definiramo funkciju dešifriranja s

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

Pokažimo kako ElGamalov kriptosustav izgleda na sljedećem primjeru:

Primjer 9. *Neka je u ElGamalovom kriptosustavu $p = 641$, $\alpha = 3$ i $a = 19$. Tada je*

$$\beta = \alpha^a \bmod p = 3^{19} \bmod 641 = 267.$$

Dakle, ključ je

$$K = (p, \alpha, a, \beta) = (641, 3, 19, 267).$$

Pretpostavimo sada da Aurora želi Borni poslati poruku $x = 238$ te neka je njezin tajno izabrani ključ $k = 16$. Tada Aurora računa

$$y_1 = \alpha^k \bmod p = 3^{16} \bmod 641 = 366$$
$$y_2 = x \cdot \beta^k \bmod p = 238 \cdot 267^{16} \bmod 641 = 192$$

i šalje poruku $(y_1, y_2) = (366, 192)$.
Borna, nakon što primi poruku, dešifrira ju na način:

$$x = y_2 \cdot (y_1^a)^{-1} \bmod p = 192 \cdot (366^{19})^{-1} \bmod 641 = 192 \cdot 275 \bmod 641 = 238,$$

te tako dobiva originalni otvoreni tekst.

Primijetimo kako se ovdje otvoreni tekst x zapravo "zamaskira" množeći s β^k. Stoga onaj koji poznaje tajni eksponent a pomoću α^k može izračunati β^k i "ukloniti masku". Zaključujemo da bi u $\mathbb{Z}_p^*$ problem diskretnog logaritma bio praktički nerješiv ukoliko bi prost broj p bio dovoljno velik, a time bi eksponent a doista i bio tajan.

Ispitajmo i zašto broj k mora biti tajan prema [6]. Kako je šifrat $(y_1, y_2) = (\alpha^k \bmod p, x \cdot \beta^k \bmod p)$ javan, tada Eva, koja želi pročitati Aurorine i Bornine poruke, može izračunati x iz

$$x = x\alpha^{ak}(\alpha^a)^{-k}.$$

Također, k se ne smije upotrijebiti više od jednom. Pretpostavimo da Aurora koristi k za dvije različite poruke m_1 i m_2 te da Eva poznaje m_1. Tada su dva šifrata $(\alpha^k, m_1\alpha^{ak})$ i $(\alpha^k, m_2\alpha^{ak})$. Tada do poruke m_2 dolazi na sljedeći način:

$$m_2\alpha^{ak}m_1^{-1}m_1\alpha^{-ak} = m_2.$$

Pogledajmo sada kako je prema Mollinu [6] sigurnost ElGamalovog kriptosustava bazirana na problemu diskretnog logaritma. Za početak je potrebno pokazati ekvivalentnost ElGamalovog kriptosustava i Diffie-Hellmanovog protokola za razmjenu ključeva. Pretpostavimo da Eva želi odrediti poruku x iz šifrata $(\alpha^k, x\alpha^{ak})$ te da zna riješiti Diffie-Hellmanov problem. Tada može iz α^a i α^k odrediti

$$\beta = \alpha^{ak} \bmod p.$$

Stoga, može doći poruke x na sljedeći način:

$$x = \beta^{-1}x\alpha^{ak} \bmod p.$$

Odnosno, ako Eva može riješiti Diffie-Hellmanov problem, tada može "razbiti" ElGamalov kriptosustav. Ako Eva zna tako riješiti ElGamalov kriptosustav, tada može odrediti svaku poruku x ako poznaje $p, \alpha, \alpha^a, \alpha^k$ i $x\alpha^{ak}$. Ako Eva želi odrediti α^{ak} iz $p, \alpha, \alpha^a, \alpha^k$, tada računa:

$$(x\alpha^{ak})x^{-1} = \alpha^{ak} \bmod p.$$

Drugim riječima, pokazali smo kako je kriptoanaliza ElGamalova kriptosustava jednaka kripotanalizi Diffie-Hellmanova problema. Zapravo, ElGamalov kriptosustav možemo promatrati kao Diffie-Hellmanov protokol za $K = \alpha^{ak}$ koji se koristi za

šifriranje poruke x. Na osnovu pokazanog, možemo zaključiti kako je sigurnost ElGamalovog kriptosustava bazirana na problemu diskretnog logaritma.

Pomoću ElGamalovog kriptosustava možemo potpisivati poruke. Pogledajmo kako se to radi prema [6]. Pretpostavimo da Aurora šalje Borni poruku x te da je (p, α, β) javni ključ dobiven na način opisan prethodno u ovom potpoglavlju. Kako bi potpisala poruku, Aurora najprije odabere slučajan broj r takav da je $0 \leq r \leq p-2$ relativno prost s $p-1$. Nakon toga računa

$$v = \alpha^r \bmod p$$

te

$$w = (m - a \cdot v)r^{-1} \bmod p - 1.$$

Za ključ (p, α, a, β) Auora šalje Borni potpisanu poruku (v, w) zajedno s x.
Borna, koristeći Aurorin javni ključ (p, α, β), provjeri vrijedi li $v \in \mathbb{Z}^*$. Zatim računa

$$z = \beta^v v^w \bmod p$$

te

$$m = \alpha^x \bmod p.$$

Poruka je Aurorina ako je $m = z \bmod p$. U suprotnom, to znači da poruka nije od Aurore, stoga ju odbacujemo. Promotrimo potpisivanje na primjeru:

Primjer 10. *Neka su* $p = 3023$ *te* $\alpha = 5$ *te neka Aurora odabere* $a = 171$ *kao tajni ključ te izračuna*

$$\beta = \alpha^a \bmod p = 5^{171} \bmod 3023 = 1295.$$

Tada je njezin javni ključ $(p, \alpha, \beta) = (3023, 5, 1295)$. *Pretpostavimo da Aurora šalje poruku* $x = 2143$ *te da odabere* $r = 157$. *Tada odredi*

$$v = \alpha^r \bmod p = 5^{157} \bmod 3023 = 2959$$

te

$$w = (x - av)r^{-1} \bmod p - 1 = (2143 - 171 \cdot 2959)157^{-1} \bmod 3022 = 294$$

te pošalje Borni popisanu poruku $(v, w) = (2959, 294)$. *Tada Borna izračuna*

$$z = \beta^v v^w \bmod p = 1295^{2959} 2959^{294} \bmod 3023 = 2203 = 5^{2143} \bmod 3023 = \alpha^x \bmod 3023$$

te prihvati potpis kao valjan.

5 Ostali kriptosustavi s javnim ključem

Osim kriptosustava zasnovanih na problemu faktorizacije i onih zasnovanih na problemu diskretnog logaritma, postoje i drugi kriptosustavi s javnim ključem. Oni se rjeđe koriste u praksi nego prethodno nabrojani kriptosustavi. U ovom poglavlju prikazat ćemo problem ruksaka te Merkle-Hellmanov kriptosustav.

5.1 Problem ruksaka

Pretpostavimo da imamo ruksak u kojeg želimo spremiti velik broj stvari, recimo njih k, koje imaju volumen v_i, $i = 0, 1, \ldots, k-1$ pri čemu ruksak ima volumen V. Kako bismo spremili stvari moramo pronaći podskup $I \subset \{1, \ldots, k\}$ takav da

$$\sum_{i \in I} v_i = V,$$

ako takav podskup postoji.

Za definiranje tog problema, najprije ćemo definirati problem sume podskupa:

Definicija 9. *Neka su $m, n \in \mathbb{N}$ te skup $S = \{v_j : v_j \in \mathbb{N}, j = 1, 2, \ldots n\}$ koji se naziva ruksak skup. Potrebno je odrediti postoji li podskup S_0 od S takav da je suma elemenata iz S_0 jednaka m. Drugim riječima, ako je dan skup S i $m \in \mathbb{N}$, potrebno je odrediti postoji li $a_j \in \{0, 1\}$, za $j = 1, 2 \ldots, n$ takav da*

$$\sum_{j=1}^{n} a_j v_j = m.$$

Sada opći problem ruksaka možemo definirati na sljedeći način:

Definicija 10. *Neka su dani prirodni brojevi m_1, m_2 te skupovi $\{v_j : v_j \in \mathbb{N}, j = 1, 2, \ldots, n\}$ i $\{w_j : w_j \in \mathbb{N}, j = 1, 2, \ldots, n\}$. Potrebno je odrediti postoji li skup S_0 takav da*

$$\sum_{j \in S_0} v_j \leq m_1$$

i

$$\sum_{j \in S_0} w_j \geq m_2.$$

Poseban slučaj problema ruksaka je superrastući problem ruksaka. To je slučaj kada rastući niz $v_1, \ldots, v_m$ ima svojstvo da je svaki element v_i veći od sume svih prethodnih članova niza. Pogledajmo i definiciju superrastućeg niza:

Definicija 11. *Neka je* $n \in \mathbb{N}$. *Za niz* $(v_1, v_2, \ldots, v_n)$, *pri čemu je* $v_j \in \mathbb{N}$ *za* $j = 1, 2, \ldots, n$ *kažemo da je superrastući niz ako vrijedi*

$$v_i > \sum_{j=1}^{i-1} v_j,$$

za svaki $i \in \{2, 3, \ldots, n\}$.

Pogledajmo primjer superrastućeg niza:

Primjer 11. *Konačan niz* $v = (1, 2, 4, 8, 16, 32)$ *je superrastući. To lako možemo provjeriti:*

$$\begin{aligned} 2 &> 1 \\ 4 &> 1 + 2 \\ 8 &> 1 + 2 + 4 \\ 16 &> 1 + 2 + 4 + 8 \\ 32 &> 1 + 2 + 4 + 8 + 16 \end{aligned}$$

Kao što vidimo, svaki član tog niza je veći od sume svih prethodnih članova niza, stoga je dani niz superrastući. Osim toga, niz (v_n) *gdje je* $v_n = 2^{n-1}$ *je beskonačan superrastući niz.*

Za rješavanje problema ruksaka postoje razni softveri. Lako se mogu naći gotovi programi napisani u Pythonu i Javi. Primjerice u Wolfram Mathematici postoji funkcija KnapsackSolve namijenjena upravo tome. U sljedećem primjeru ćemo primijeniti tu funkciju kako bismo riješili problem.

Primjer 12. *Pretpostavimo da spremamo stvari u ruksak te neka je maksimalno opterećenje ruksaka* 9 *kilograma. Predmeti koje stavljamo u ruksak imaju* $2, 3$ *ili* 4 *kilograma. Naš cilj je spremiti što više predmeta u ruksak tako da njihova ukupna masa ne bude veća od* 9 *kilograma. Taj problem možemo riješiti tako da u programu Wolfram Mathematica upišemo* KnapsackSolve$[\{2, 3, 4\}, 9]$. *Kao rezultat dobijemo* $\{3, 1, 0\}$ *što protumačimo tako da ćemo u ruksak spremiti po tri predmeta od* 2 *kilograma i jedan predmet od* 3 *kilograma. Tada smo u ruksak spremili predmete čija je ukupna masa upravo jednaka* 9 *kilograma.*

U nastavku ćemo opisati postupak rješavanja problema sume podskupa za superrastući niz prema Mollinu [6]. Kako bismo pronašli podskup S_0 skupa $S = \{v_1, v_2, \ldots, v_n\}$ sa svojstvom da mu je suma elemenata jednaka danom $d \in \mathbb{N}$ (ako takav podskup S_0 postoji), potrebno je postaviti $x_n = 1$ ako je $v_n \leq d$ te $x_n = 0$, inače. Tada za svaki v_{n-i}, gdje je $i = 1, 2, \ldots, n$, postavimo da je $x_{n-i} = 1$ ako je

$$v_{n-i} \leq d - \sum_{j=n-i+1}^{n} b_j$$

te $x_{n-i} = 0$, inače. Tada je

$$d = \sum_{j=1}^{n} x_j v_j.$$

Kasnije ćemo na primjeru pokazati kako rješavamo superrastući problem ruksaka kod dešifriranja poruke u Merkle-Hellmanovom kriptosustavu.

5.2 Merkle-Hellmanov kriptosustav

Merkle-Hellmanov kriptosustav iz 1978. godine baziran je na problemu ruksaka. Ime je dobio po njegovim tvorcima, američkom informatičaru Ralphu Merkleu i američkom kriptologu Martinu Hellmanu. Glavna ideja ovog kriptosustava je "zamaskirati" superrastući niz tako da izgleda kao slučajan niz. Na taj način jedino primatelj može pročitati poruku rješavajući superrastući problem dok će drugi rješavati opći problem ruksaka, koji je znatno teži.

U svrhu definiranja Merkle-Hellmanovog kriptosustava, pojasnimo što znači oznaka $\{0,1\}^n$. Ona predstavlja skup svih vektora duljine n koji se sastoje jedino od nula i jedinica. Stoga, Merkle-Hellmanov kriptosustav možemo zapisati na sljedeći način:

Definicija 12. *Neka je $v = (v_1, \ldots, v_n)$ superrastući niz prirodnih brojeva, $p > v_1 + \cdots + v_n$ prost broj te $1 \leq a \leq p-1$. Za $i \in \{1, 2, \ldots, n\}$ definiramo*

$$t_i = av_i \bmod p$$

i označimo $t = (t_1, t_2, \ldots, t_n)$. Neka je $\mathcal{P} = \{0,1\}^n$, $\mathcal{C} = \{0, 1, \ldots, n(p-1)\}$ i $\mathcal{K} = \{(v, p, a, t)\}$, pri čemu su v, p, a i t konstruirani na prethodno opisani način. Za $K \in \mathcal{K}$ definiramo

$$e_K(x_1, x_2, \ldots, x_n) = x_1t_1 + x_2t_2 + \cdots + x_nt_n.$$

Za $0 \leq y \leq n(p-1)$ *definiramo*

$$z = a^{-1}y \bmod p,$$

gdje je a^{-1} *multiplikativni inverz od* a *modulo* p *te riješimo superrastući problem ruksaka za skup* $\{v_1, \ldots, v_n\}$ *te dobivamo*

$$d_K(y) = (x_1, x_2, \ldots, x_n).$$

Vrijednost t *je javna, a vrijednosti* p, a *i* v *su tajne.*

Kako bismo bolje razumjeli Merkle-Hellmanov kriptosustav, pogledat ćemo kako on izgleda na primjeru.

Primjer 13. *Neka je* $v = (1, 3, 6, 11, 23, 47)$ *superrastući niz te neka je* $p = 97$ *te* $a = 53$*. Kako superrastući niz ima 6 elemenata, tada je* $n = 6$*. Prvo je potrebno odrediti niz* $t = (t_1, t_2, \ldots, t_6)$*, gdje je* $t_i = av_i \bmod p$*. Računamo redom:*

$$\begin{aligned} t_1 &= 53 \cdot 1 \bmod 97 = 53, \\ t_2 &= 53 \cdot 3 \bmod 97 = 62, \\ t_3 &= 53 \cdot 6 \bmod 97 = 27, \\ t_4 &= 53 \cdot 11 \bmod 97 = 1, \\ t_5 &= 53 \cdot 23 \bmod 97 = 55, \\ t_6 &= 53 \cdot 47 \bmod 97 = 66. \end{aligned}$$

Tada dobivamo $t = (53, 62, 27, 1, 55, 66)$ *pa je ključ* K *jednak*

$$K = (v, p, a, t) = ((1, 3, 6, 11, 23, 47), 97, 53, (53, 62, 27, 1, 55, 66)).$$

Neka je poruka koju želimo poslati $x = 101101$*. U skladu s definicijom promotrimo ju u obliku* $x = (1, 0, 1, 1, 0, 1)$*. Šifriramo ju na sljedeći način:*

$$e_K(x) = \sum_{i=1}^{6} x_i t_i = 1 \cdot 53 + 0 \cdot 62 + 1 \cdot 27 + 1 \cdot 1 + 0 \cdot 55 + 1 \cdot 66 = 147.$$

Pretpostavimo sada da smo dobili poruku $y = 147$ *te da su nam poznati* $a = 53$ *i* $p = 97$*. Nju ćemo dešifrirati tako da najprije izračunamo:*

$$z = a^{-1}y \bmod p = 53^{-1}147 \bmod 97 = 11 \cdot 147 \mod 97 = 65.$$

Zatim odredimo poruku x tako da prvo zapišemo z kao sumu elemenata iz v, odnosno:

$$65 = 1 + 6 + 11 + 47.$$

Naposljetku, do poruke dolazimo na način da na i-to mjesto poruke stavimo znamenku 1 ukoliko je broj v_i jedan od pribrojnika sume z ili znamenku 0 u slučaju da broj v_i nije jedan od pribrojnika od z. Kako su $1, 6, 11$ i 47 brojevi koji u sumi daju broj $z = 65$ te su njihovi indeksi u skupu v redom 1,3,4 i 6, tada na prvo, treće, četvrto i šesto mjesto traženog šesteroznamenkastog broja stavljamo znamenku 1, a na ostala znamenku 0. Odnosno dobivamo da je poruka

$$x = d_K(y) = 101101.$$

Prednost ovog sustava u odnosu na ostale kriptosustave s javnim ključem je činjenica da je šifriranje njime znatno brže. No, Adi Shamir je 1982. pronašao polinomijalni algoritam za njegovo razbijanje (vidjeti [7]). Stoga se Merkle-Hellmanov kriptosustav ne može smatrati sigurnim, no ideja na kojoj je zasnovan je zanimljiva. Ona se bazira na korištenju jednostavnog specijalnog slučaja nekog teškog problema ruksaka pri čemu se taj specijalni slučaj prikrije tako da izgleda kao opći.

Literatura

[1] D. Bishop, *Introduction to cryptography with Java applets*, Jones and Bartlett Publishers, Sudbury, 2003.

[2] S. Coutinho, *The mathematics of ciphers: number theory and RSA cryptography*, A k Peters/CRC Press, Natick, 1999.

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

[4] M. Hinek, *Cryptoanalysis of RSA and its variants*, Chapman & Hall/CRC, Boca Raton, 2010.

[5] N. Kobliz, *A course in number theory and cryptography*, 2nd edition, Springer, Berlin, 1994.

[6] R. Mollin, *An introduction to cryptography*, 2nd edition, Chapman & Hall/CRC, Boca Raton, 2007.

[7] A. Shamir, *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*, Advances in cryptology: Proceedings of CRYPTO 82, (R. L. Rivest and A. T. Sherman and D. Chaum, eds.), Plenum, New York, 1982, 279–288.

[8] H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Transaction on Information Theory **26** (1980), 726–729.

Sažetak

Osnovna ideja kriptografije javnog ključa je konstruiranje kriptosustava u kojima netko tko poznaje funkciju šifriranja ne može u razumnom vremenu izračunati funkciju dešifriranja. Upravo zato funkcija šifriranja može biti javna. Za otkriće kriptografije javnog ključa zaslužni su Whitfield Diffie i Martin Hellman koji su osmislili protokol za razmjenu ključeva baziran na problemu diskretnog logaritma. Na istom problemu zasnovan je ElGamalov kriptosustav. Kriptografija javnog ključa zasniva se na općenito "težim" matematičkim zadacima pa osim problema diskretnog logaritma, konstruiranje takvih kriptosustava bazira se i na problemu faktorizacije prirodnog broja. Primjeri takvih kriptosustava su RSA i Rabinov kriptosutav. RSA je najstariji i najpopularniji kriptosustav koji se i danas koristi u bankarstvu i sigurnosti kupovine putem interneta. Rabinov kriptosustav zasnovan je problemu računanja kvadratnog korijena u $\mathbb{Z}_n$ koji je usko vezan s problemom faktorizacije. Zajednička prednost prethodno nabrojanih kriptosustava je mogućnost potpisa poruke, a mana je slabost na napad odabranim šifratom. U stvarnosti kriptografija javnog ključa ne može zamijeniti one s tajnim jer se ona koristi za šifriranje ključeva, a ne za šifriranje poruka.

Summary

The idea of a public key cryptography is construction of a cryptosystem which one who knows the enciphering function, in some reasonable time cannot find the corresponding dechipering function. Thus the enciphering key can be public. The founders of a public key cryptography, Whitfield Diffie and Martin Hellman, have found the way for key exchange which is based on discrete logarithm problem. ElGamal cryptosystem is also based on that problem. In general, public key cryptography, is based on some harder mathematical problems. Besides discrete logarithm problem, public key cryptography uses factorisation problems to construct cryptosystems like RSA and Rabin cryptosystem. The RSA cryptosystem is the oldest one and the most popular cryptosystem which is used in banking and web shoping. Rabin cryptosystem is based on the difficulty of calculating the square root in $\mathbb{Z}_n$. Common advantage of all previously mentioned cryptosystems is the digital signature, while the disadvantage is the weakness to chosen cipher attack. In reality, public key cryptography cannot replace symmetric crypography because it is used for key encryption but not for encryption of certain message.

Životopis

Rođena sam u Našicama 23. studenog 1994. godine. Osnovnu školu Ivane Brlić-Mažuranić završila sam 2009. godine u Orahovici. Iste godine upisala sam Opću gimnaziju u srednjoj školi "Stjepan Ivšić" u Orahovici. Nakon završetka srednje škole, 2013. godine, upisala sam Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku u Osijeku.