RSA kriptosustav i neki kriptoanalitički napadi

Barać, Marko

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University of Split, Faculty of science / Sveučilište u Splitu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:166:882798

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-03**

Repository / Repozitorij:

Repository of Faculty of Science

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

MARKO BARAĆ

RSA kriptosustav i neki kriptoanalitički napadi

DIPLOMSKI RAD

Split, listopad 2020.

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

ODJEL ZA MATEMATIKU

RSA kriptosustav i neki kriptoanalitički napadi

DIPLOMSKI RAD

Student:
Marko Barać

Mentorica:
doc. dr. sc. Marija Bliznac
Trebješanin

Split, listopad 2020.

Uvod

Potreba za kriptiranjem podataka seže daleko u povijest. Ljudi su htjeli međusobno razmjenjivati poruke na način da ih mogu pročitati samo one osobe kojima su namijenjene. To je dovelo do razvoja kriptografije koja je osigurala pouzdane metode za razmjenu poruka. Većina tadašnjih potreba za kriptiranjem je bila u ratne i diplomatske svrhe.

Krajem 60. i početkom 70. godina 20. stoljeća, razvojem financijskih transakcija, dolazi do potrebe uvođenja standarda u kriptografiji. Kao standard je prihvaćen simetrični blokovni kriptosustav *DES*. Problem simetričnih kriptosustava je potreba za razmjenom tajnih ključeva za kriptiranje podataka. Kao rješenje problema razmjene ključeva su se pokazali kriptosustavi s javnim ključem, koji su za šifriranje koristili osobne jednosmjerne funkcije. Time je ključ za šifriranje poruke bio javan, a ključ za dešifriranje je morao biti tajan, a jednosmjernost funkcije je osiguravala da se iz poznatog javnog ključa ne mogu otkriti informacije o tajnom ključu.

Prvi, ujedno najpopularniji i najrasprostranjeniji kriptosustav s javnim ključem je RSA kriptosustav koji su izumili Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Njegova sigurnost je zasnovana na teškoći faktorizacije velikih prirodnih brojeva koja se koristi u dobivanju dodatnog podatka za osobne jednosmjerne funkcije, a u šifriranju i dešifriranju koristi modularno potenciranje.

Paralelno s razvojem kriptografije razvija se i kriptoanaliza, to jest znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje šifrata bez poznavanja ključa. Osnovna pretpostavka kriptoanalize je da kriptoanalitičar zna koji se kriptosustav koristi. Razlikujemo četiri osnovna nivoa kriptoanalitičkih napada: samo šifrat, poznat otvoren tekst, odabrani otvoren tekst i odabrani šifrat.

U komunikaciji preko računalnih mreža se najčešće koriste hibridni kriptosustavi. To su sustavi u kojima kriptosustave s javnim ključem koristimo da bismo razmijenili ključeve koji bi se dalje koristili u kriptosustavima s tajnim ključem (simetrični kriptosustavi). Kriptosustave s javnim ključem koristimo samo za razmjenu ključeva jer su dosta sporiji za šifriranje i dešifriranje veće količine podataka.

U prvom poglavlju rada uvest ćemo osnovne definicije o kriptosustavima, kriptosustavima s javnim ključem, te samom RSA kriptosustavu, te ćemo prikazati jednu od primjena RSA kriptosustava u SSL protokolu. U drugom poglavlju ćemo se detaljnije posvetiti samoj kriptoanalizi. Prikazat ćemo neke od ranih napada kao što su korištenje istog modula, Hastadov napad prijenosom i kružni napad. Zatim ćemo obraditi neke od napada s malim javnim eksponentom e: uobičajni dio poruke, povezane poruke, nasumično popunjavanje i izvlačenje informacija. Na kraju rada imamo napade koji se baziraju na malom tajnom eksponentu d. Tu ćemo detaljnije pojasniti Wienerov napad i poboljšani Wienerov napad.

Sadržaj

Uvod **iii**

Sadržaj **v**

1 RSA Kriptosustav **1**

1.1 Kriptosustavi 1

1.2 Kriptosustavi s javnim ključem 4

1.3 RSA kriptosustav 9

1.4 SSL protokol 14

1.4.1 Protokol za rukovanje 16

2 Kriptoanaliza RSA kriptosustava **18**

2.1 Pomoćni rezultati 18

2.2 Neki rani napadi 21

2.2.1 Korištenje istog modula 21

2.2.2 Hastadov napad prijenosom 24

2.2.3 Kružni napad 30

2.3 Mali javni eksponent e 32

2.3.1 Uobičajni dio poruke 32

2.3.2 Povezane poruke 33

2.3.3 Izvlačenje informacija 35

2.4 Mali tajni eksponent d 36
2.4.1 Wienerov napad 37
2.4.2 Poboljšani Wienerov napad 43

Literatura **45**

Poglavlje 1

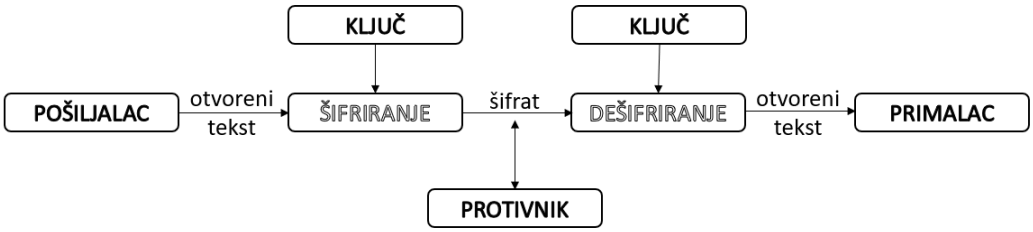
RSA Kriptosustav

U ovom poglavlju dat ćemo kratak uvod u kriptografiju i definirati RSA kriptosustav. Prvo ćemo definirati osnovne pojmove o kriptosustavu, zatim ćemo objasniti koje su značajke kriptosustava s javnim ključem i navesti neke dobre izbore parametara ovog kriptosustava. Za kraj ćemo predstaviti SSL protokol koji koristimo za kreiranje kriptirane veze između poslužitelja i korisnika, a koji u svom algoritmu može koristiti RSA kriptosustav.

1.1 Kriptosustavi

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka tako da ih može pročitati samo onaj kome je poruka namijenjena. Osnovni zadatak kriptografije je omogućiti dvjema osobama, *pošiljalac* i *primalac*, da komuniciraju preko nesigurnog komunikacijskog kanala (poštar, telefonska mreža, mobilna mreža, internet, ...) tako da treća osoba, *protivnik*, može vidjeti poruku, ali ne može razumjeti njezin sadržaj. Poruka (tekst, brojevi, ...) koju pošiljalac želi poslati primaocu zove se *otvoreni tekst*. Pošiljalac *šifrira* otvoreni tekst pomoću unaprijed dogovore-

nog *ključa*, a rezultat je poruka koju nazivamo *šifrat* ili *kriptogram*. Nakon toga šifrat se pošalje putem nekog komunikacijskog kanala. Protivnik može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Primalac koji zna ključ kojim je poruka šifrirana može *dešifrirati* šifrat i odrediti otvoreni tekst.



Slika 1.1: Shema klasične kriptografije

Kriptoanaliza ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje šifrata bez poznavanja ključa. *Kriptologija* je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.

Kriptografski algoritam ili *šifra* je matematička funkcija koja se koristi za šifriranje i dešifriranje. Funkcije za šifriranje i dešifriranje su inverzne jedna drugoj. Funkcije se biraju iz osnovne familije funkcija u ovisnosti o ključu. Skup svih mogućih ključeva nazivamo *prostor ključeva*.

Definicija 1.1 ***Kriptosustav*** *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, *za koju vrijede sljedeća svojstva:*

1. $\mathcal{P}$ *je konačan skup svih mogućih otvorenih tekstova,*

2. $\mathcal{C}$ *je konačan skup svih mogućih šifrata,*

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

4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$*, gdje su*

$$e_K : \mathcal{P} \to \mathcal{C} \ i \ d_K : \mathcal{C} \to \mathcal{P},$$

funkcije sa svojstvom

$$d_K(e_K(m)) = m, \ \forall m \in \mathcal{P}.$$

Iz svojstva $d_K(e_K(m)) = m$ slijedi da funkcije e_K moraju biti injekcije. Ako bi bilo $e_K(m_1) = e_K(m_2) = c$, za $m_1 \neq m_2$, onda primalac ne bi mogao odrediti treba li dešifrirati u m_1 ili m_2, odnosno $d_K(c)$ ne bi bio definiran. Ako je $\mathcal{P} = \mathcal{C}$ onda su funkcije e_K permutacije.

Postoji više načina podjele kriptosustava. Za ovaj rad je bitna podjela s obzirom na tajnost/javnost ključeva:

- *Kriptosustav s tajnim ključem* (*simetrični kriptosustav*)
  Ključ za dešifriranje se može dosta jednostavno dobiti poznavajući ključ za šifriranje i obratno. Najčešće su ključevi za šifriranje i dešifriranje jednaki, a iz funkcije šifriranja se lako odredi funkcija dešifriranja s danim ključem. Sigurnost ovih kriptosustava leži u tajnosti ključa.

- *Kriptosustav s javnim ključem* (*asimetrični kriptosustav*)
  Ključ za dešifriranje, to jest funkcija dešifriranja, se ne može jednostavno izračunati iz ključa za šifriranje. Ključ za šifriranje je javni ključ, te bilo tko može pomoću njega šifrirati poruku, ali samo osoba koja ima odgovarajući tajni ključ za dešifriranje može dešifrirati poruku.

Razlikujemo četiri osnovna nivoa kriptoanalitičkih napada:

1. *Samo šifrat*
   Kriptoanalitičar posjeduje samo šifrate od nekoliko poruka šifriranih

pomoću istog algoritma. Njegov zadatak je otkriti otvoreni tekst od što više poruka, ili otkriti ključ pomoću kojeg su poruke šifrirane.

2. *Poznat otvoreni tekst*

   Kriptoanalitičar posjeduje šifrat neke poruke, ali i njemu odgovarajući otvoreni tekst. Njegov zadatak je otkriti ključ i neki algoritam za dešifriranje poruka šifriranih tim ključem.

3. *Odabrani otvoreni tekst*

   Kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Ovaj napad je jači od prethodnog, ali je manje realističan.

4. *Odabrani šifrat*

   Kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može odabrati šifrat, te dobiti odgovarajući otvoreni tekst. Ovaj napad je tipičan kod kriptosustava s javnim ključem, a zadatak kriptoanalitičara je otkriti ključ za dešifriranje.

1.2 Kriptosustavi s javnim ključem

Prije definicije Diffie-Hellmanovog protokola za razmjenu ključeva, podsjetimo se pojma cikličke grupe.

Definicija 1.2 *Kažemo da je grupa G ciklička ako postoji $g \in G$ takav da je*

$$G = \{g^k \mid k \in \mathbb{Z}\}.$$

Kažemo da je element g generator grupe G.

Kod simetričnih kriptosustava za sigurnost je nužna tajnost ključa jer iz poznavanja funkcije šfiriranja e_k možemo lako odrediti funkciju dešifriranja

d_k. To znači da prije šifriranja pošiljalac i primalac moraju biti u mogućnosti na siguran način razmijeniti ključ da budu sigurni da ga imaju samo oni.

Whitfield Diffie i Martin Hellman se smatraju začetnicima *kriptografije javnog ključa*. Ponudili su jedno moguće rješenje problema razmjene ključeva zasnovano na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. Pretpostavimo da se Alice i Bob žele dogovoriti o jednom tajnom slučajnom elementu u cikličkoj grupi G, koji kasnije mogu koristiti kao tajni ključ. Jedina informacija koju imaju jest grupa G i njezin generator g. *Diffie-Hellmanov protokol* za razmjenu ključeva ima sljedeći algoritam.

1. Alice generira slučajan prirodan broj $a \in \{1, 2, \ldots, |G| - 1\}$, te pošalje Bobu element g^a.

2. Bob generira slučajan prirodan broj $b \in \{1, 2, \ldots, |G| - 1\}$, te pošalje Alice element g^b.

3. Alice izračuna $(g^b)^a = g^{ab}$.

4. Bob izračuna $(g^a)^b = g^{ab}$.

Sada je njihov tajni ključ g^{ab}.

Kriptosustavi s javnim ključem se temelje na tome da bi iz poznavanja funkcije šifriranja e_K bilo praktički nemoguće u nekom razumnom vremenu izračunati funkciju dešifriranja d_K. Tada bi funkcija šifriranja e_K mogla biti javno dostupna jer bi poruku mogao pročitati samo onaj tko poznaje funkciju dešifriranja d_K. Za ovakvu ideju kriptosustava potrebne su osobne jednosmjerne funkcije.

Definicija 1.3 *Za funkciju f kažemo da je* ***jednosmjerna funkcija*** *ako je f lako, a njezin inverz f^{-1} teško izračunati. Ako je inverz f^{-1} lako izračunati kada nam je poznat neki dodatni podatak, onda f nazivamo* ***osobna jednosmjerna funkcija****.*

Kod većine kriptosustava koji su se koristili prije sredine 20.-og stoljeća veza funkcija e_K i d_K je bila vrlo jednostavna, pa skrivanje jedne i otkrivanje druge funkcije nije imalo smisla.

Definicija 1.4 *Kriptosustav s javnim ključem se sastoji od dviju familija e_K i d_K funkcija za šifriranje i dešifriranje, gdje K ide po prostoru ključeva, sa svojstvom*

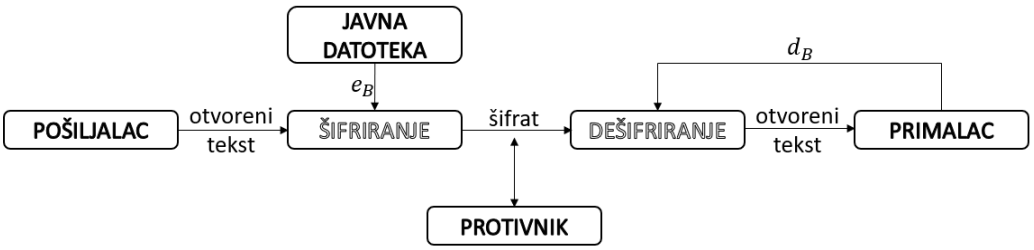
1. *Za svaki K je d_K inverz od e_K,*
2. *Za svaki K je e_K javan, ali je d_K poznat samo osobi K,*
3. *Za svaki K je e_K osobna jednosmjerna funkcija.*

Funkcija e_K se zove javni ključ, a d_K tajni ključ.

Ako Alice želi poslati poruku Bobu, onda Bob prvo pošalje svoj javni ključ e_B. Tada Alice šifrira neki otvoreni tekst m pomoću e_B i pošalje šifrat $c = e_B(m)$ Bobu. Bob dešifrira šifrat pomoću svog tajnog kjuča d_B:

$$d_B(c) = d_B(e_B(m)) = m.$$

Ukoliko više osoba želi komunicirati na ovakav način onda mogu svi svoje javne ključeve staviti u zajedničku datoteku.



Slika 1.2: Shema kriptografije javnog ključa

Postavlja se pitanje *vjerodostojnosti* poruke, to jest kako primalac Bob može biti siguran da mu poruku šalje pošaljilac Alice jer svatko ima pristup funkciji e_B. Navest ćemo jedan od načina na koji možemo riješiti taj problem:

1. Alice generira slučajan broj a, te ga šifrira pomoću javnog ključa e_B i pošalje Bobu poruku $e_B(a)$,

2. Bob dešifrira poruku sa $d_B(e_B(a)) = a$, generira svoj slučajan broj b, te pošalje Alice poruku $e_A(a + b)$,

3. Alice izračuna b pomoću formule

$$b = d_A(e_B(a + b)) - a,$$

   te sada pošalje poruku $e_B(b)$. Sada je Bob siguran da je samo Alice mogla poslati tu poruku.

Drugi problem koji rješavaju kriptosustavi s javnim ključem je nepobitnost poruke. To je riješeno na način da pošiljalac digitalno potpiše svoju poruku. Tada Alice ne može zanijekati da je upravo ona poslala poruku. Pretpostavimo da je $\mathcal{P} = \mathcal{C}$. Tada Alice može potpisati poruku m tako da Bobu pošalje šifrat

$$z = d_A(c) = d_A(e_B(m)).$$

Kada Bob primi poruku za koju pretpostavlja da je od Alice, on najprije primijeni javni ključ e_A, a potom i svoj tajni ključ d_B:

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

Sada Bob zna sigurno da je poruku poslala Alice.

Glavne prednosti kriptosustava s javnim ključem u usporedbi sa simetričnima su:

1. Nema potrebe za sigurnim komunikacijskim kanalima za razmjenu ključeva,
2. Za komunikaciju od N ljudi treba $2N$ ključeva, za razliku od $\binom{N}{2} = \frac{N(N-1)}{2}$ ključeva kod simetričnog kriptosustava,
3. Mogućnost potpisa poruke.

U realnom svijetu najčešće se koriste *hibridni kriptosustavi*. To su kriptosustavi u kojima Alice i Bob koriste simetrični kriptosustav za komunikaciju (šifriranje poruka), a kriptosustav s javnim ključem za razmjenu tajnog ključa kojeg koristimo u simetričnom kriptosustavu. Osnovni razlog nekorištenja kriptosustava s javnim ključem u cijeloj komunikaciji je razlika u brzini algoritma, sporiji su oko 1000 puta od modernih simetričnih algoritama. Drugi nedostatak kriptosustava s javnim ključem je da su slabi na napad *odabrani otvoreni tekst*. Ako je $c = e(m)$, gdje otvoreni tekst može poprimiti jednu od n vrijednosti, onda kriptoanalitičar treba samo šifritrati svaki od n mogućih otvorenih tekstova i rezultat usporediti s c.

Osnovni problemi koje treba riješiti moderni kriptosustav su:

1. *Povjerljivost*

   Poruku koju Alice šalje Bobu ne može pročitati nitko drugi.

2. *Vjerodostojnost*

   Bob zna da je samo Alice mogla poslati poruku koju je upravo primio.

3. *Netaknutost*

   Bob zna da poruka koju je poslala Alice nije promijenjena prilikom slanja.

4. *Nepobitnost*

   Alice ne može kasnije zanijekati da je poslala poruku.

Drugi, treći i četvrti problemi, za koje je potrebno koristi digitalni potpis, zahtijevaju uporabu kriptosustava s javnim ključem. Za prvi problem je dovoljno koristiti kriptosustave s tajnim ključem jer ne želimo opteretiti računalne resurse sa sporijim algoritmima kriptosustava s javnim ključem.

1.3 RSA kriptosustav

Navedimo nekoliko definicija i teorema (bez dokaza) koji su nužni za definiranje RSA kriptosustava.

Pojam djeljivosti je jedan o najjednostavnijih, ali i najvažnijih pojmova u teoriji brojeva.

Definicija 1.5 *Neka su $a \neq 0$ i b cijeli brojevi. Reći ćemo da je b djeljiv s a, ili da a dijeli b, ako postoji cijeli broj x takav da je $b = ax$. Kažemo da je a djelitelj od b te da je b višekratnik od a.*

Za potrebe definiranja RSA kriptosustava navest ćemo i Teorem o dijeljenju s ostatkom te definirati pojam najvećeg zajedničkog djelitelja i relativno proste brojeve.

Teorem 1.6 (Teorem o dijeljenju s ostatkom) *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je:*

$$b = qa + r \ , \ 0 \leq r < a.$$

Definicija 1.7 *Najveći zajednički djelitelj cijelih brojeva a i b jest najveći prirodni broj m takav da je m djelitelj svakog od brojeva a i b. Taj broj označavamo s nzd(a,b).*

Definicija 1.8 *Reći ćemo da su cijeli brojevi a i b relativno prosti ako je nzd(a,b)=1.*

Definicija 1.9 *Eulerova funkcija je preslikavanje $\varphi : \mathbb{N} \to \mathbb{N}$ koje prirodnom broju n pridružuje broj relativno prostih prirodnih brojeva manjih od n.*

Lako je za vidjeti da je $\varphi(1) = 1$, $\varphi(2) = 1$ i $\varphi(3) = 2$. U sljedećim teoremima navodimo neka svojstva Eulerove funkcije koja nam pomažu pri računanju njene vrijednosti za veće brojeve.

Teorem 1.10 *Eulerova funkcija je multiplikativna funkcija. To jest vrijedi:*

1. $\varphi(1) = 1$,
2. $\varphi(pq) = \varphi(p)\varphi(q)$, *za svaka dva relativno prosta broja p i q.*

Teorem 1.11 *Neka su p i q prosti brojevi. Vrijedi:*

1. $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, *za svaki* $\alpha \geq 1$,
2. $\varphi(pq) = (p-1)(q-1)$.

Teorem 1.12 (Eulerov teorem) *Neka su a i n prirodni brojevi. Ako je nzd(a,n)=1, onda vrijedi*

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

Navedimo algoritam za efikasno određivanje najvećeg zajedničkog djelitelja.

Teorem 1.13 (Euklidov algoritam) *Neka su b i c prirodni brojevi te neka je $b > c$. Pretpostavimo da je uzastopnom primjenom Teorema 1.6 dobiven niz jednakosti*

$$b = cq_1 + r_1,\ 0 < r_1 < c,$$

$$c = r_1q_2 + r_2,\ 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{j-2} = r_{j-1}q_j + r_j,\ 0 < r_j < r_{j-1},$$

$$r_{j-1} = r_jq_{j+1}.$$

Tada je $nzd(b, c) = r_j$, odnosno najveći zajednički djelitelj je jednak posljednjem ostatku različitom od 0 u Euklidovom algoritmu. Vrijednosti od x i y u izrazu $nzd(b, c) = bx + cy$ mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije brojeva b i c. Algoritam kojim određujemo x i y nazivamo prošireni Euklidov algoritam.

Prvi, a ujedno i najpoznatiji i najrasprostranjeniji kriptosustav s javnim ključem je RSA kriptosustav iz 1997. godine, koji su izumili Ronald Rivest, Adi Shamir i Leonard Adleman.

Sigurnost RSA kriptosustava je zasnovana na teškoći faktorizacije, a u samom šifriranju i dešifriranju koristi modularno potenciranje, dok se faktorizacija koristi u dobivanju dodatnog podatka jednosmjerne funkcije ovog kriptosustava.

Definicija 1.14 *Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te*

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

Za $K \in \mathcal{K}$ i $m, c \in \mathbb{Z}_n$ definiramo

$$e_K(m) = m^e \pmod{n},$$

$$d_K(c) = c^d \pmod{n}.$$

Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne, to jest (n, e) je javni, a (p, q, d) je tajni ključ.

Kao što smo naveli u Teoremu 1.11, u našem slučaju imamo da je

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

Dokažimo da je d_K inverz od e_K koristeći Teorem 1.12 (Eulerov teorem). Imamo da je $d_K(e_K(m)) \equiv m^{de} \pmod{n}$. Iz $ed \equiv 1 \pmod{\varphi(n)}$ slijedi da postoji prirodan broj k takav da je $ed = k\varphi(n) + 1$. Pretpostavimo da je $nzd(m, n) = 1$. Sada je po Teoremu 1.12 (Eulerov teorem):

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

Ako je $nzd(n, m) = n$, onda je

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

Ako je $nzd(n, m) = p$, onda je

$$m^{de} \equiv 0 \equiv m \pmod{p}.$$

Kako je $nzd(pq, m) = p$, gdje su p i q prosti, slijedi da je $nzd(q, m) = 1$, pa je po Teoremu 1.12 (Eulerov teorem) $m^{\varphi(q)} = m^{q-1} \equiv 1 \pmod{q}$. Stoga je

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

$$m^{de} \equiv m \pmod{n}.$$

Slučaj $nzd(n, m) = q$ je potpuno analogan. Prema tome, zaista je u svakom slučaju $m^{de} \equiv m \pmod{n}$, što znači $d_K(e_K(m)) = m$.

Primjer 1.15 *Prikazat ćemo šifriranje i dešifriranje u RSA kriptosustavu na sasvim malim parametrima. Uzmimo da je* $p = 3$ *i* $q = 11$. *Tada je* $n = 33$ *i* $\varphi(n) = 20$. *Eksponent e mora biti relativno prost s 20, pa uzmimo da je* $e = 7$. *Rješavanjem linarne kongruencije* $de \equiv 1 \pmod{\varphi(n)}$ *izračunati ćemo d:*

$$7d \equiv 1 \pmod{20}$$

$$7d = 1 - 20x,$$

$$7d + 20x = 1.$$

Pomoću Euklidovog algoritma ćemo izračunati d:

$$20 - 2 \cdot 7 = 6$$

$$7 - 1 \cdot 6 = 1$$

$$7 - (20 - 2 \cdot 7) = 1$$

$$3 \cdot 7 - 20 = 1$$

Izračunali smo da je $d = 3$. *Sada je* $(n, e) = (33, 7)$ *naš javni ključ. Pretpostavimo da nam netko želi poslati poruku* $m = 17$. *To znači da treba izračunati:*

$$e_K(m) \equiv 17^7 \pmod{33},$$

$$17^7 = 17 \cdot 17^2 \cdot 17^4 \equiv 17 \cdot 25 \cdot (-2) \equiv -25 \equiv 8 \pmod{33}.$$

Šifrat je $c = e_K(m) = 8$. *Primalac dešifrira šifrat pomoću tajnog eksponenta d:*

$$m = d_K(c) \equiv 8^3 \equiv 8 \cdot 8^2 \equiv 8 \cdot (-2) \equiv 17 \pmod{33}.$$

Sigurnost RSA kriptosustava leži u pretpostavci da je funkcija

$$e_K \equiv m^e \pmod{n}$$

osobna jednosmjerna funkcija. Dodatni podatak koji omogućava dešifriranje je poznavanje faktorizacije $n = pq$. Onaj tko zna faktorizaciju broja n može izračunati $\varphi(n) = (p-1)(q-1)$, te potom dobiti tajni eksponent d rješavajući linearnu kongruenciju

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

Reći ćemo nekoliko riječi o izboru parametara u RSA kriptosustavu:

1. Tajno izaberemo dva dovoljno velika prosta broja p i q slične veličine. To radimo tako da najprije generiramo slučajan prirodan broj m tražene veličine, pa zatim pomoću nekog od testova prostosti tražimo prvi prost broj veći ili jednak m. Treba paziti da $n = pq$ bude otporan na metode faktorizacije koje su vrlo efikasne za brojeve specijalnog oblika.Tako bi brojevi $p \pm 1$ i $q \pm 1$ trebali imati barem jedan veliki prosti faktor, jer postoje efikasne metode za faktorizaciju brojeva koji imaju prosti faktor p takav da jedan od brojeva $p-1, p+1$ ima samo male proste faktore. Također p i q ne smiju biti jako blizu jedan drugom, jer ih se onda može naći koristeći činjenicu da su blizu broja $\sqrt{n}$.

2. Izračunamo $n = pq$ i $\varphi(n) = (p-1)(q-1) = n - p - q + 1$.

3. Izaberemo broj e takav da je $nzd(e, \varphi(n)) = 1$, te pomoću proširenog Euklidovog algoritma izračunamo d takav da je $ed \equiv 1 \pmod{\varphi(n)}$. Obično se uzima da je $e < \varphi(n)$.

4. Stavimo ključ za šifriranje (n, e) u javni direktorij.

1.4 SSL protokol

SSL protokol je standardizirana sigurnosna tehnologija za kreiranje kriptirane veze između poslužitelja i korisnika. Njome se osigurava zadržavanje privat-

nosti i sigurnost svih podataka koji se razmjenjuju između sudionika. Jedna od najraširenijih primjena SSL standarda jest zaštita podataka u online transakcijama.

Omogućava autentifikaciju korisnika i poslužitelja pružajući pouzdanu kriptiranu vezu. Protokol sadrži sljedeće funkcionalnosti:

1. *Autentifikaciju poslužitelja*

   Omogućuje korisniku otkrivanje/potvrdu identiteta poslužitelja. Korisnik može koristiti tehnike kriptosustava s javnim ključem kako bi provjerio valjanost certifikata poslužitelja. Važnost ovog postupka dolazi do isticanja u sustavima gdje se razmjenjuju važni podaci.

2. *Autentifikaciju korisnika*

   Omogućuje poslužitelju potvrdu korisničkog identiteta. Uporabom digitalnog potpisa pomoću kriptosustava s javnim ključem poslužitelj može provjeriti certifikat korisnika. Ovaj postupak ima veliko značenje kod slanja povjerljivih informacija korisniku.

3. *Kriptirana SSL veza*

   Zahtjeva kriptiranje svih informacija koje se razmjenjuju između korisnika i poslužitelja kako bi se osigurao visok stupanj povjerljivosti.

SSL protokol za razmjenu ključeva i autentifikaciju (digitalni potpis) koristi kriptosustave s javnim ključem, a za komunikaciju koristi simetrične kriptosustave. Po današnjem standardu, ako protokol koristi RSA kriptosutav, za n se uzima broj veličine 2048 bita, a za javni eksponent e se uzima broj $e = 1280$.

Protokol za promjenu načina šifriranja (ChangeCipherSpec) se koristi za promjenu algoritma šifriranja. Za promjenu algoritma korisnik i poslužitelj moraju dogovoriti novi način šifriranja, kao i odgovarajuće ključeve.

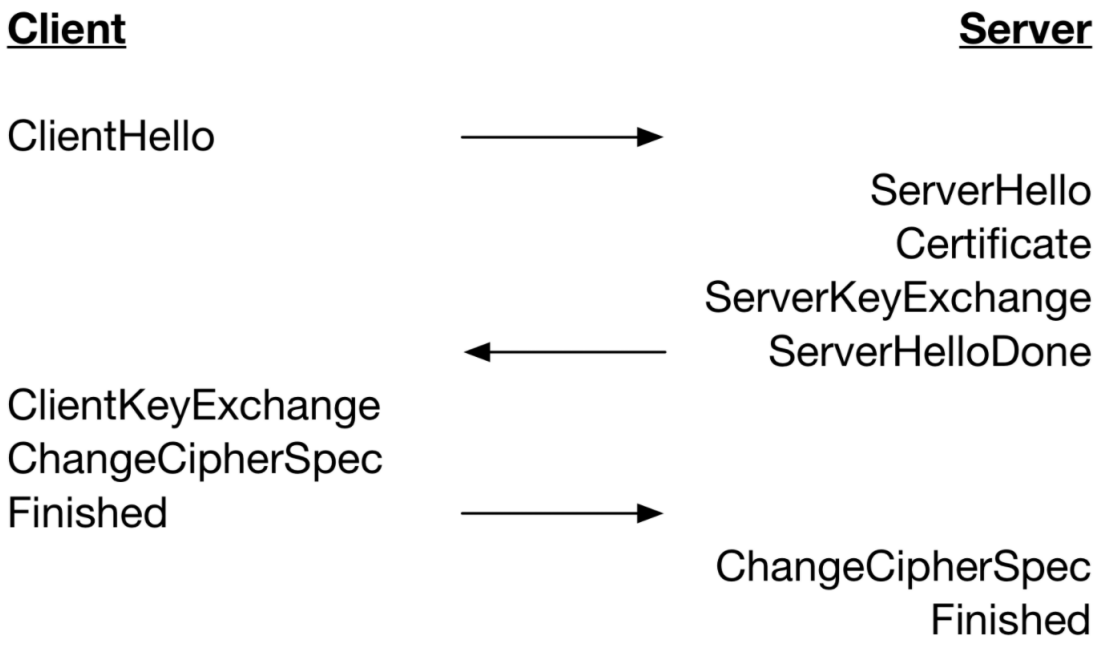
1.4.1 Protokol za rukovanje

Prilikom spajanja korisnika sa SSL poslužiteljem inicira se protokol za rukovanje. Njime se definiraju protokoli koji će biti korišteni u daljnjoj komunikaciji, određuju se kriptografski algoritmi, obavlja se autentifikacija strana, isto tako korištenjem kriptosustava s javnim ključem kreira se glavni tajni ključ iz kojeg se izvode ostali ključevi za šifriranje i autentifikaciju.

Glavni tajni ključ za svaku SSL sjednicu kreira poslužitelj koristeći pri tome inicijalni glavni ključ koji je poslao korisnik. Uz pomoć glavnog ključa generiraju se četiri ključa:

- ključ za šifriranje podataka koji se šalju od korisnika prema poslužitelju,
- ključ za šifriranje podataka koji se šalju od poslužitelja prema korisniku,
- autentifikacijski ključ za slanje podataka koji se šalju od korisnika prema poslužitelju,
- autentifikacijski ključ za slanje podataka koji se šalju od poslužitelja prema korisniku.

Protokol za rukovanje se sastoji od nekoliko koraka koje ćemo prikazati na shemi.



Slika 1.3: Shema protokola za rukovanje (handshake)

Poglavlje 2

Kriptoanaliza RSA kriptosustava

2.1 Pomoćni rezultati

Na početku ćemo navesti definicije i teoreme (bez dokaza) koje ćemo koristiti u opisima napada u ovom poglavlju.

Definicija 2.1 *Neka su f i g dvije funkcije. Kažemo da je*

$$f(n) \in O(g(n)) \iff (\exists c > 0)(\exists n_0 > 0)(\forall n \geq n_0)\ 0 \leq f(n) \leq cg(n).$$

Kažemo da će se neka funkcija f izvršiti u **polinomijalnom vremenu** ako postoji neki polinom g takav da vrijedi $f(n) \in O(g(n))$. Ako postoji eksponencijalna funkcija h takva da je $f(n) \in O(h(n))$ onda kažemo da će se f izvršiti u **eksponencijalnom vremenu**. Složenost algoritama u ovom radu nećemo dokazivati, već ćemo je samo navesti kako bismo naglasili vrijeme izvođenja pojedinog algoritma. Naime, smatrat ćemo da je algoritam polinomijalne složenosti efikasan, a za algoritam eksponencijalne složenosti

da nije efikasno izvediv u realnom vremenu za velike ulaze, u našem slučaju za velike proste brojeve p i q.

Navedimo jedan od najvažnijih teorema o rješavanju sustava linearnih kongruencija.

Teorem 2.2 (Kineski teorem o ostacima) *Neka su $m_1, m_2, \ldots, m_k$ cijeli brojevi i neka su $n_1, n_2, \ldots, n_k$ u parovima relativno prosti prirodni brojevi. Neka je*

$$n = \prod_{i=1}^{k} n_i,$$

i za svaki $i = 1, 2, \ldots, k$ definiramo c_i takav da

$$c_i \frac{n}{n_i} \equiv 1 \pmod{n_i}.$$

Tada je jedno rješenje sustava

$$x \equiv m_1 \pmod{n_1},$$

$$x \equiv m_2 \pmod{n_2},$$

$$\vdots$$

$$x \equiv m_k \pmod{n_k},$$

dano s

$$x_0 = \sum_{i=1}^{k} m_i c_i \frac{n}{n_i}.$$

Sva druga rješenje zadovoljavaju uvjet

$$x \equiv x_0 \pmod{n}.$$

Definicija 2.3 *Neka je $x \in \mathbb{R}$. Tada broj $\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}$ zovemo najveći cijeli dio od x.*

Neka je α proizvoljan realan broj. Stavimo da je $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, onda α zapišemo u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, onda α_1 zapišemo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, i stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj proces možemo nastaviti u nedogled, ukoliko nije $a_n = \alpha_n$ za neki n. Ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Tada imamo

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{+\cfrac{1}{a_n}}}}.$$

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, \ldots, a_n]$.

Pretpostavimo sada da je $a_k \neq \alpha_k$ za sve $k \leq n$ i neki prirodni broj n. Definirajmo racionalne brojeve $\frac{p_k}{q_k}$ s

$$\frac{p_k}{q_k} = [a_0, a_1, \ldots, a_k].$$

Definicija 2.4 *Ako je a_0 cijeli broj i $a_1, a_2, \ldots, a_n$ prirodni brojevi te ako je $\alpha = [a_0, a_1, \ldots, a_n]$, onda ovaj izraz zovemo razvoj broja α u konačni jednostavni verižni razlomak. Broj $\frac{p_i}{q_i}$ je i-ta konvergenta od α, a a_i je i-ti parcijalni kvocijent od α, a $r_i = [a_i, a_{i+1}, \ldots, a_n]$ je i-ti potpuni kvocijent od α.*

Ako je α iracionalan broj, onda uvodimo oznaku $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$, onda ovaj izraz zovemo razvoj od α u (beskonačni) jednostavni verižni razlomak. Broj $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent, a $\alpha_i = [a_i, a_{i+1}, \ldots]$ je i-ti potpuni kvocijent od α.

Teorem 2.5 (Legenderov Teorem) *Neka je $\alpha \in \mathbb{R}$ i $p, q \in \mathbb{Z}$ takvi da je $q \geq 1$ i*

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ neka konvergenta u razvoju broja α u verižni razlomak.

Teorem 2.6 (Worleyov teorem) *Neka je $\alpha \in \mathbb{R}$ i $c \in \mathbb{R},\ c > 0$. Ako racionalni broj $\frac{p}{q}$ zadovoljava nejednakost*

$$|\alpha - \frac{p}{q}| < \frac{c}{q^2},$$

onda je

$$\frac{p}{q} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k},$$

za neki $k \geq -1$ i nenegativne cijele brojeve r,s takve da je $rs < 2c$.

2.2 Neki rani napadi

U ovom potpoglavlju ćemo prikazati neke od ranih napada na RSA kriptosustav. Rani napadi su se bazirali na protokolarnim greškama RSA kriptosustava.

2.2.1 Korištenje istog modula

Jedna od ranih protokolarnih grešaka je šifriranje iste poruke pomoću dva različita javna ključa s istim modulom, to jest s istim ključem n. Neka su (n, e_1) i (n, e_2) dva javna ključa gdje su e_1 i e_2 relativno prosti brojevi. Tada možemo, koristeći Euklidov algoritam, lako izračunati brojeve a_1 i a_2 takve da vrijedi $a_1e_1 + a_2e_2 = 1$. Neka je m poruka koja je šifrirana s ovim dvama ključevima i kojoj odgovaraju šifrati

$$c_1 = m^{e_1} \pmod{n},$$

$$c_2 = m^{e_2} \pmod{n}.$$

Sada lako računamo

$$c_1^{a_1} c_2^{a_2} \equiv m^{a_1 e_1} m^{a_2 e_2} \equiv m^{a_1 e_1 + a_2 e_2} \equiv m \pmod{n},$$

iz čega vidimo da smo jednostavnim računom odredili poruku m.

Druga slabost kod korištenja istog modula n nastaje zbog toga što poznavajući javni ključ i njemu odgovarajući tajni ključ možemo pronaći odgovarajući tajni ključ za bilo koji drugi javni ključ s istim modulom.

Teorem 2.7 *Neka je (n, e) javni ključ s odgovarajućim tajnim eksponentom d i neka je (n, e_1) drugi javni ključ takav da je $e_1 \neq e$. Tada je tajni ključ d_1 koji odgovara ključu e_1 jednak*

$$d_1 = e_1^{-1} \pmod{\frac{ed-1}{nzd(e_1, ed-1)}}.$$

Dokaz. Ključ zadovoljava kongruenciju koju možemo zapisati i kao

$$ed \equiv 1 \pmod{\varphi(n)} \iff ed - 1 = k\varphi(n), \text{ za neki } k \in \mathbb{Z}.$$

Znamo da vrijedi $nzd(e_1, \varphi(n)) = 1$, pa vrijedi $nzd(e_1, k\varphi(n)) = k'$, za neki k' za koji vrijedi da $k'|k$. Neka je $k'' = \frac{k}{k'}$.

Imamo

$$\frac{ed-1}{nzd(e_1, ed-1)} = \frac{k\varphi(n)}{k'} = k''\varphi(n).$$

Neka je d_1 definiran kao u iskazu teorema, to jest,

$$d_1 \equiv e_1^{-1} \pmod{k''\varphi(n)}.$$

Množeći kongruenciju s e_1 lako zaključujemo

$$e_1 d_1 \equiv 1 \pmod{k''\varphi(n)},$$

$$e_1 d_1 = 1 + k_1(k''\varphi(n)),$$

$$\Longrightarrow e_1 d_1 \equiv 1 \pmod{\varphi(n)},$$

gdje je k_1 neki cijeli broj. Slijedi da je d_1 valjani tajni ključ odgovarajućem javnom ključu e_1. Svi izračuni mogu biti dovršeni u polinomijalnom vremenu u $\log(n)$. ■

Primjer 2.8 *Neka su* $(n_1, e_1) = (143, 7)$ *i* $(n_1, e_2) = (143, 17)$ *dva javna ključa, te neka su* $c_1 = 42$ *i* $c_2 = 9$ *dva šifrata istog otvorenog teksta. Izračunajmo otvoreni tekst.*

Pošto vidimo da je $nzd(7, 17) = 1$ *možemo koristiti napad korištenje istog modula. Iz jednadžbe* $a_1 e_1 + a_2 e_2 = 1$ *ćemo pomoću proširenog Euklidovog algoritma izračunati* a_1 *i* a_2

$$17 - 2 \cdot 7 = 3,$$

$$7 - 2 \cdot 3 = 1.$$

Izražavanjem svakog ostatka kao linarne kombinacije brojeva 17 *i* 7 *izračunat ćemo* a_1 *i* a_2

$$7 - 2 \cdot 3 = 1,$$

$$7 - 2(17 - 2 \cdot 7) = 1,$$

$$7 - 2 \cdot 17 + 4 \cdot 7 = 1,$$

$$-2 \cdot 17 + 5 \cdot 7 = 1.$$

Dobili smo da je $a_1 = 5$ *i* $a_2 = -2$. *Sada možemo izračunati* m

$$m \equiv c_1^{a_1} \cdot c_2^{a_2} \pmod{n},$$

$$m \equiv 42^5 \cdot 9^{-2} \pmod{143},$$

$$m \equiv 1613472 \pmod{143},$$

$$m = 3.$$

Iz ovih napada zaključujemo da bi pri implementaciji RSA kriptosustava svaki korisnik trebao imati svoj osobni javni ključ n.

2.2.2 Hastadov napad prijenosom

Navedimo bez dokaza neke rezultate Dona Coppersmitha koje ćemo koristiti u napadima.

Teorem 2.9 (Coppersmithov teorem) *Neka je $f(x) \in \mathbb{Z}[x]$ normirani polinom stupnja d te neka je n prirodan broj. Ako postoji rješenje kongruencije*

$$f(x_0) \equiv 0 \pmod{n},$$

koje zadovoljava uvjet $|x_0| \leq n^{\frac{1}{d-e}}$, tada postoji algoritam koji pronalazi x_0, a čija je složenost polinomijalna u $\ln(n)$ i $\frac{1}{e}$ (za fiksni d).

Teorem 2.10 *Neka je n cijeli broj nepoznate faktorizacije koji ima djelitelj $b \geq n^{\beta}$, za $0 < \beta < 1$, i $f(x)$ polinom stupnja k. Tada možemo pronaći sva rješenja x_0 od $f(x) \equiv 0 \pmod{b}$, koji zadovoljava uvjet $|x_0| \leq cn^{\frac{\beta^2}{k}}$ u polinomijalnom vremenu u $\log(n)$, c i broju rješenja.*

Prije definiranja napada definirat ćemo prsten $\mathbb{Z}_n[x]$ i njegova osnovna svojstva.

Definicija 2.11 *Kažemo da je grupa G Abelova ili komutativna ako vrijedi*

$$a \cdot b = b \cdot a, \ \forall a, b \in G.$$

Binarna operacija u Abelovoj grupi se označava s $+$, dok za neutralni i inverzni element uvodimo oznake 0 i $-a$.

Neka je $n \in \mathbb{N}$, definirajmo relaciju ekvivalencije na skupu $\mathbb{Z}$ s

$$x \equiv y \pmod{n} \ \text{ ako je } \ x - y = qn \ \text{ za neki } \ q \in \mathbb{Z}.$$

Neka je $\overline{x}$ klasa ekvivalencije elemenata $x \in \mathbb{Z}$, $\overline{x} = \{x + pn \mid p \in \mathbb{Z}\}$. Tada je $\overline{x} = \overline{y}$ ako i samo ako je $x - y = qn$ za neki $q \in \mathbb{Z}$. Označimo skup svih klasa ekvivalencije s

$$\mathbb{Z}_n = \{\overline{x} \mid x \in \mathbb{Z}\}.$$

Na skupu $\mathbb{Z}_n$ možemo definirati zbrajanje modulo n na prirodan način s

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Pokažimo da je ova operacija dobro definirana, odnosno da ne ovisi o predstavniku klase ekvivalencije. Ako je $\overline{x} = \overline{x}_1$ i $\overline{y} = \overline{y}_1$, onda je $x - x_1 = pn$ i $y - y_1 = qn$ za neke $p, q \in \mathbb{Z}$. U tom slučaju vrijedi

$$x + y - (x_1 + y_1) = (p + q)n,$$

što povlači $\overline{x + y} = \overline{x_1 + y_1}$. Neutralni element je klasa ekvivalencije $\overline{0}$, a inverzni element je $-\overline{x} = \overline{(-x)}$. Kako je zbrajanje komutativno zaključujemo da je $(\mathbb{Z}_n, +)$ Abelova grupa. S obzirom da je $\overline{n} = \overline{0}$, $\mathbb{Z}_n$ ima točno n elemenata

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Prsten je algebarska struktura koja se sastoji od skupa na kojem su definirane dvije binarne operacije koje nazivamo zbrajanje i množenje, i koje su povezane zakonom distributivnosti. Najjednostavniji primjer prstena je skup cijelih brojeva $\mathbb{Z}$ sa standardnim operacijama zbrajanja i množenja.

Definicija 2.12 *Prsten je neprazan skup R s dvije binarne operacije $+$ i $\cdot$ koje nazivamo zbrajanje i množenje, i koje za svaki $a, b, c \in R$ zadovoljavaju sljedeća svojstva:*

1. *$(R, +)$ je Abelova grupa,*

2. množenje je asocijativno:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

3. množenje je distributivno u odnosu na zbrajanje slijeva i zdesna:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ (a + b) \cdot c = a \cdot c + b \cdot c.$$

Definicija 2.13 *Ako je množenje u prstenu R komutativno, onda R nazivamo komutativni prsten. Kažemo da je R prsten s jedinicom ako postoji element $1 \in R$ takav da je*

$$1 \cdot a = a \cdot 1 = a, \quad \textit{za svaki } a \in R.$$

Promotrimo Abelovu grupu $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Množenje u $\mathbb{Z}_n$ definirano s

$$\overline{x} \cdot \overline{y} = \overline{xy},$$

zadovoljava aksiome prstena. $\mathbb{Z}_n$ je prsten s jedinicom $\overline{1}$ koji ima konačno mnogo elemenata.

Neka je R komutativni prsten s jedinicom. Formalna suma

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \ a_i \in R,$$

naziva se polinom u varijabli x. Ako je $a_n \neq 0$, onda a_n nazivamo vodeći koeficijent, a $a_n x^n$ vodeći član polinoma $f(x)$. Polinom $f(x) = a_0$ nazivamo konstantni polinom. Ako je $a_0 = 0$, onda $f(x) = 0$ nazivamo nul-polinom. Stupanj polinoma definiramo sa $\deg(f(x)) = n$ gdje je $a_n \neq 0$ vodeći koeficijent polinoma, dok stupanj nul-polinoma definiramo sa $\deg(0) = -\infty$.

Skup svih polinoma označavamo s $R[x]$. Zbroj polinoma

$$f(x) = \sum_{k=0}^{n} a_k x^k \ \text{ i } \ g(x) = \sum_{k=0}^{m} b_k x^k, \ n \geq m,$$

definiramo s

$$f(x) + g(x) = \sum_{k=0}^{n} (a_k + b_k)x^k,$$

gdje je $m < n$ i g je takav da je $b_{m+1} = b_{m+2} = \cdots = b_n = 0$. Umnožak polinoma je definiran s

$$\begin{aligned} f(x)g(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{m+n} \\ &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_ib_j \right) x^k \end{aligned}$$

Lako se provjeri da navedene operacije zbrajanja i množenja zadovoljavaju aksiome prstena. Stoga je $R[x]$ komutativni prsten s jedinicom. Prsten R je sadržan u $R[x]$ kao prsten konstatnih polinoma. Primjetimo da za stupanj polinoma vrijede nejednakosti

$$\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\},$$

$$\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x)).$$

Hastadov napad prijenosom je koristan u slučaju da imamo nekoliko povezanih poruka koje su šifrirane malim javnim eksponentom i različitim modulima. Razlikujemo dvije vrste napada.

1. **Isti otvoreni tekstovi**

   Istu poruku m šifriramo s nekoliko javnih ključeva (n_1, e), (n_2, e), $\ldots$, (n_i, e) s istim javnim eksponentom e i različitim modulima n_1, n_2, $\ldots$, n_i. Ako vrijedi $i \geq e$ i $m < \min\{n_1, n_2, \ldots, n_i\}$, tada se poruka može dešifrirati koristeći Kineski teorem o ostacima.

   Teorem 2.14 *Pretpostavimo da je otvoreni tekst m šifriran k puta s javnim ključevima (n_1, e), (n_2, e), $\ldots$, (n_k, e) gdje su n_1, n_2, $\ldots$, n_k u*

parovima relativno prosti brojevi i $k > e$. *Neka je*

$$n_0 = min\{n_1, n_2, \ldots, n_k\} \quad i \quad n = \prod_{i=1}^{k} n_i.$$

Ako za otvoreni tekst m *vrijedi* $m < n_0$ *tada, poznavajući* $c_i \equiv m^e \pmod{n_i}$ *i* (n_i, e), $\forall i = 1, 2, \ldots, k$, *možemo doći do otvorenog teksta u polinomijalnom vremenu u* $\log(n)$.

Dokaz. Kako su $nzd(n_i, n_j) = 1$ u parovima relativno prosti, za svaki izbor para $i, j = 1, 2, \ldots, k$ i $i \neq j$, možemo izračunati $c \equiv m^e \pmod{n}$ koristeći Kineski teorem o ostacima. Iz $m < n_0$ slijedi da je $m^e < n_1 n_2 \ldots n_k = n$ i $c = m^e$. Stoga sve što trebamo učiniti je izračunati e-ti korijen broja c u skupu cijelih brojeva da bismo odredili m. Svi izračuni mogu biti gotovi u polinomijalnom vremenu u $\log(n)$. ■

2. **Povezani otvoreni tekstovi**

Kada je više povezanih poruka šifrirano s malim javnim eksponentom i različitim modulima, tada dešifriranje možemo izvršiti koristeći Kineski teorem o ostacima i Coppersmithove rezultate. Poruke su povezane ako postoje poznati polinomi f_i takvi da je $m_i = f_i(m)$. Bez dokaza navodimo sljedeći teorem koji nam opisuje napad u tom slučaju.

Teorem 2.15 *Neka su* (n_1, e_1), (n_2, e_2), $\ldots$, (n_k, e_k) *javni ključevi gdje su* n_1, n_2, $\ldots$, n_k *u parovima relativno prosti brojevi. Neka je*

$$n_0 = min\{n_1, n_2, \ldots, n_k\}, \; n = \prod_{i=1}^{k} n_i,$$

$$f_1(x) \in \mathbb{Z}_{n_1}[x], f_2(x) \in \mathbb{Z}_{n_2}[x], \ldots, f_k(x) \in \mathbb{Z}_{n_k}[x].$$

Za otvoreni tekst $m < n_0$ *ako je* $k \geq \max_i\{e_i \deg(f_i(x))\}$ *tada za dane* $c_i = f_i(m) \pmod{n_i}$ *i* $(n_i, e_i), \forall i = 1, 2, \ldots, k$, *otvoreni tekst može biti izračunat u polinomijalnom vremenu u* $\log(n)$ *i* $\max_i\{e_i \deg(f_i(x))\}$.

Opišimo sada na primjeru Hastadov napad u slučaju istog otvorenog teksta.

Primjer 2.16 *Neka su* $(n_1, e_1) = (629, 3)$*,* $(n_2, e_2) = (2173, 3)$ *i* $(n_3, e_3) = (1159, 3)$ *javni ključevi te neka su* $c_1 = 529$*,* $c_2 = 414$ *i* $c_3 = 558$ *šifrati istog teksta* m*. Hastadovim napadom odredit ćemo otvoreni tekst* m*.*

Da bismo izračunali m *moramo riješiti sustav*

$$m^3 \equiv 529 \pmod{629},$$

$$m^3 \equiv 414 \pmod{2173},$$

$$m^3 \equiv 558 \pmod{1159},$$

koristeći kineski teorem o ostacima. Imamo

$$n = n_1 n_2 n_3,$$

$$n = 629 \cdot 2173 \cdot 1159 = 1584140903,$$

$$m_1 \equiv 2518507 y_1 \equiv 1 \pmod{629} \Longrightarrow 620 y_1 \equiv 1 \pmod{629} \Longrightarrow y_1 = 559,$$

$$m_2 \equiv 729011 y_2 \equiv 1 \pmod{2173} \Longrightarrow 1056 y_2 \equiv 1 \pmod{2173} \Longrightarrow y_2 = 1063,$$

$$m_3 \equiv 1366817 y_3 \equiv 1 \pmod{1159} \Longrightarrow 356 y_3 \equiv 1 \pmod{1159} \Longrightarrow y_3 = 433.$$

Iz ovoga dalje možemo izračunati m

$$m^3 \equiv \prod_{i=1}^{3} c_i m_i y_i \pmod{n},$$

$$m^3 \equiv 1396408796778 \pmod{1584140903},$$

$$m^3 \equiv 15625 \pmod{1584140903} \Longrightarrow m = 25.$$

2.2.3 Kružni napad

Poruku možemo dekriptirati na način da šifrat uzastopno šifriramo dok ne dobijemo opet isti šifrat. Neka je $c \equiv m^e \pmod{n}$ šifrat i (n, e) javni ključ, te neka smo nakon $l + 1$ šifriranja opet dobili isti šifrat

$$c^{e^{l+1}} \equiv c \pmod{n},$$

tada slijedi da je

$$c^{e^l} \equiv m \pmod{n}.$$

Dobili smo da je poruka otkrivena nakon l uzastopnih šifriranja. Najmanji l nazivamo **eksponent oporavka**. Postoje poruke koje imaju jako mali eksponent oporavka, na primjer trivijalna poruka $m = \pm 1$ ima eksponent oporavka $l = 1$.

Definicija 2.17 *Neka su a i b cijeli brojevi različiti od 0. Najmanji prirodan broj c za koji vrijedi da je c višekratnik brojeva a i b nazovamo najmanji zajednički višekratnik i označavamo s* $c = nzv(a, b)$.

Definirat ćemo Carmichaelovu lambda funkciju te prikazati jedno njeno svojstvo koje će nam biti od koristi u napadima.

Definicija 2.18 ***Carmichaelova lambda funkcija****,* $\lambda : \mathbb{N} \to \mathbb{N}$ *prirodnom broju n pridružuje najmanji prirodni broj* $\lambda(n)$ *takav da je*

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

za svaki prirodni broj a za koji vrijedi $nzd(a, n) = 1$*, to jest da su a i n relativno prosti.*

Za Carmichaelovu lambda funkciju vrijedi

$$\begin{aligned} &\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1), && \textit{ako je } p \textit{ neparan prost broj},\\ &\lambda(2^e) = \varphi(2^e), && \textit{ako je } e = 0, 1, 2,\\ &\lambda(2^e) = \tfrac{1}{2}\varphi(2^e), && \textit{ako je } e \geq 3, \end{aligned}$$

i konačno,

$$\lambda(n) = nzv(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_k^{e_k})), \text{ ako je } n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

gdje su $p_1, \ldots, p_k$ različiti prosti brojevi i $e_i \geq 1$ prirodni brojevi, $i = 1, 2, \ldots, k$.

Po Teoremu 1.12 znamo da je $\lambda(n) \leq \varphi(n)$ i $\lambda(n)|\varphi(n)$, a iz prethodne definicije slijedi i sljedeće svojstvo.

Propozicija 2.19 *Ako su p i q dva različita prosta cijela broja i n=pq onda vrijedi sljedeće svojstvo:*

$$\begin{aligned} \lambda(n) &= nzv(p-1, q-1) \\ &= \frac{(p-1)(q-1)}{nzd(p-1, q-1)} \\ &= \frac{\varphi(n)}{nzd(p-1, q-1)}. \end{aligned}$$

Bez dokaza navodimo teorem koji nam daje vezu eksponenta oporavka i Carmichaelove lambda funkcije.

Teorem 2.20 *Pretpostavimo da je poruka m šifrirana javnim ključem (n, e), tada eksponent oporavka dijeli $\lambda(\lambda(n))$.*

Kako bismo izbjegli napad na RSA kriptosustav trebamo paziti da je $\lambda(\lambda(n))$ velik i ima velike proste djelitelje. Potrebno je dosta vremena kako bismo pomoću cikličkog napada otkrili šifriranu poruku.

U generalizaciji cikličkog napada za šifrat c tražimo najmanji prirodni broj $k \in \mathbb{N}$ takav da je

$$nzd(c^{e^k} - c, n) > 1.$$

Ako je

$$c^{e^k} \equiv c \pmod{p} \text{ i } c^{e^k} \not\equiv c \pmod{q},$$

onda je $k = p$. Obrnuto, ako je

$$c^{e^k} \not\equiv c \pmod{p} \; i \; c^{e^k} \equiv c \pmod{q},$$

onda je $k = q$. Ovim postupkom smo pronašli jedan od prostih faktora od n. Za obranu od ovog napada trebali bi uzeti dovoljno velike slučajno odabrane proste brojeve.

Primjer 2.21 *Neka je* $(n, e) = (55, 7)$ *javni ključ i* m *neki otvoreni tekst. Ako je* $c = 51$ *šifrat, izračunajmo* m *pomoću kružnog napda.*

$$c \equiv m^7 \pmod{7},$$

$$c_1 \equiv 51^7 \pmod{55} = 6,$$

$$c_2 \equiv 6^7 \pmod{55} = 41,$$

$$c_3 \equiv 41^7 \pmod{55} = 46,$$

$$c_4 \equiv 46^7 \pmod{55} = 51 = c.$$

Slijedi da je otvoreni tekst $m = 46$.

2.3 Mali javni eksponent e

U ovom dijelu rada ćemo pokazati neke napade koji se koriste u kriptosustavima u kojima je definiran mali javni eksponent, na primjer $e = 3$.

2.3.1 Uobičajni dio poruke

Kada poznajemo dio poruke koja je šifrirana moguće je otkriti cijelu poruku uz uvjet da su javni eksponent i nepoznati dio poruke dovoljno mali. Na primjer, pretpostavimo da svakodnevno šaljemo poruku koja sadrži ključ

za taj dan, i ima oblik: *"Tajni ključ za 1. rujna 2020. je ??????"* gdje je nepoznati dio jako mali. U ovakvim slučajevima je moguće otkriti cijelu poruku, to ćemo pokazati idućim teoremom.

Teorem 2.22 *Neka je (n, e) valjani RSA javni ključ i m neka poruka. Neka je šifrat $c \equiv m^e \pmod{n}$ poznat. Ako su poznati svi osim najviše $\frac{1}{e}$ dio uzastopnih bitova otvorenog teksta, tada cijela poruka m može biti izračunata u polinomijalnom vremenu u $\log(n)$ i e.*

Dokaz. Budući da je nepoznato najviše $\frac{1}{e}$ uzastopnih bitova poruke m, m možemo zapisati kao

$$m = m_2 2^{k_2} + m_1 2^{k_1} + m_0,$$

gdje je samo m_1 nepoznat i vrijedi $|m_1| < n^{\frac{1}{e}}$. Slijedi da tražimo male nultočke od $f_n(x) \in \mathbb{Z}_n[x]$, gdje je

$$f_n(x) \equiv 2^{-k_1 e}((m_2 2^{k_2} + x 2^{k_1} + m_0)^e - c) \pmod{n},$$

jer je $f_n(m_1) = 2^{-k_1 e}(m^e - c) \equiv 0 \pmod{n}$. Kako je $|m_1| < n^{\frac{1}{e}}$ možemo koristiti Coppersmithove rezultate (Teorem 2.10) na polinom f_n, da bismo odredili m_1 u polinomijalnom vremenu u $\log(n)$ i e. Zatim ćemo lako odrediti m. ■

Da bi ovo bilo primjenjivo javni eksponent mora biti prilično mali. Ako je $e > \log_2(n)$ za napad je potrebno poznavati sve bitove otvorenog teksta. Također vrijeme izvođenja napada raste s porastom javnog eksponenta.

2.3.2 Povezane poruke

Ovaj tip napada je dokazan za $e = 3$. Bazira se na tome da napadač presretne šifriranu poruku, a pošiljatelju se predstavi kao primalac i kaže da nije primio

poruku. Sada pošiljatelj ponovno pošalje poruku malo izmijenjenu, npr. drugo vrijeme. Napadač opet presretne tu šifriranu poruku i sada ima dvije povezane šifrirane poruke. Idućim teoremom ćemo pokazati da napadač može doći do originalne poruke.

Teorem 2.23 *Neka su m_1 i m_2 dvije poruke koje zadovoljavaju $m_2 = am_1 + b$. Pretpostavimo da su obje šifrirane javnim ključem (n, e). Za dane $c_1 = m_1^3 \pmod n$, $c_2 = m_2^3 \pmod n$, a, b i javni ključ moguće je izračunati m_1, a tako i m_2, u vremenu polinomijalnom u $\log(n)$.*

Dokaz. Poznavajući c_1, c_2, a, b, e i n možemo izračunati

$$\frac{b(c_2 + 2a^3c_1 - b^3)}{a(c_2 - a^3c_1 + 2b^3)} \equiv \frac{m_1(3a^3m_1^2 + 3a^2b^2m_1 + 3ab^3)}{3a^3bm_1^2 + 3a^2b^2m_1 + 3ab^3} \equiv m_1 \pmod n.$$

Svi izračuni se vrše u polinomijalnom vremenu u $\log(n)$ ■

Primjer 2.24 *Neka je $(n, e) = (5, 5836720399)$ javni ključ. Neka su $c_1 = 2083888300$ i $c_2 = 2918851827$ dva šifrata otvorenih tekstova m_1 i m_2 koje su međusobno povezane s:*

$$m_2 = m_1 + 17.$$

Neka su

$$f_1(x) = x^5 - c_1 = x^5 - 2083888300,$$

$$f_2(x) = (x + 17)^5 - c_2,$$

$$f_2(x) = x^5 + 85x^4 + 2890x^3 + 49130x^2 + 417605x - 2917431970.$$

Izračunamo najveći zajednički djelitelj za ova dva polinoma modulo n.

$$g(x) = nzd(f_1(x), f_2(x)) = x + 5055693378 = x - m_1.$$

Izračunali smo $m = 5055693378$, sada izračunamo

$$m_2 = m_1 + 17 = 781027038.$$

Kada koristimo javni ključ $e = 3$ ne smijemo slati poruke koje su linearno povezane.

2.3.3 Izvlačenje informacija

Kada implementiramo RSA kriptosustav javni i tajni eksponent zadovoljavaju jednadžbu $ed = 1 + k\varphi(n)$ koju dobijemo iz kongruencije $ed \equiv 1 \pmod{\varphi(n)}$. Konstantu k treba čuvati u tajnosti. Uz poznavanje konstante k moguće je pronaći najvažnije bitove tajnog eksponenta.

Teorem 2.25 *Neka su (n, e) i (p, q, d) javni i tajni ključ koji zadovoljavaju jednadžbu $ed = 1 + k\varphi(n)$. Poznavanjem (n, e) i k možemo izračunati d_1 takav da je*

$$|d_1 - d| < p + q,$$

u polinomijalnom vremenu u $\log(n)$.

Dokaz. Neka je $d_1 = \lceil \frac{1}{e}(1 + kn) \rfloor$. Slijedi $d_1 = \frac{1}{e}(1 + kn) + \alpha$, za neki α takav da je $|\alpha| < 1$. Zapišimo kongruenciju $ed \equiv 1 \pmod{\varphi(n)}$ kao

$$ed = 1 + k\varphi(n) \iff ed = 1 + k(n - s),$$

gdje je $s = p + q - 1$, možemo izračunati

$$\begin{aligned} |d_1 - d| &= |\frac{1 + kn}{e} + \alpha - \frac{1 + k(n - s)}{e}| \\ &= |\frac{ks}{e} + \alpha| < s + 1 = p + q. \end{aligned}$$

■

Kada koristimo balansirane proste faktore p i q vrijedi $p + q > \frac{3}{2}n^{\frac{1}{2}}$. To znači da uz poznavanje javnog ključa i k uvijek možemo izračunati $|d_1 - d| < \frac{3}{2}n^{\frac{1}{2}}$, to jest možemo otkriti pola najvažnijih bitova tajnog eksponenta.

Teorem 2.26 *Neka je $n = pq$ za $p, q > 3$ i neka je $(n, 3)$ javni ključ. Konstanta k u jednadžbi $ed = 1 + k\varphi(n)$ mora biti $k = 2$.*

Dokaz. Iz kongruencije u definiciji ključa $ed \equiv 1 \pmod{\varphi(n)}$ imamo $ed - 1 = k\varphi(n)$. Slijedi da je $0 < k < e$. Dakle u našem slučaju je $k = 1$ ili $k = 2$. Kako je $nzd(3, p-1) = 1$, imamo da je $p - 1 \not\equiv 0 \pmod 3$. Kako je $p > 3$ imamo da je $nzd(3, p) = 1$, pa je $p - 1 \not\equiv 2 \pmod 3$. Sada imamo

$$p - 1 \equiv 1 \pmod 3,$$

$$q - 1 \equiv 1 \pmod 3,$$

slijedi

$$\varphi(n) \equiv (p-1)(q-1) \equiv 1 \pmod 3.$$

Sada ako jednadžbu $ed - 1 = k\varphi(n)$ reduciramo modulo 3 dobijemo

$$3d \equiv 1 + k\varphi(n) \pmod 3 \implies k \equiv 2 \pmod 3.$$

Kako k može biti 1 ili 2 slijedi da je $k = 2$. ■

Dakle, ako koristimo $e = 3$ uvijek će nam biti poznato pola najznačajnijih bitova tajnog eksponenta.

2.4 Mali tajni eksponent d

Sada ćemo proučiti nekoliko napada koji se baziraju na malom tajnom eksponentu d. Ovi napadi su mnogo učinkovitiji od napada s malim javnim eksponentom e iz prethodnog poglavlja. U teoremima iz ovog poglavlja smo pretpostavili da su šifriranje i dešifriranje definirani pomoću modula od $\lambda(n)$. Naime, iz Definicije 2.18 i svojstava Carmichaelove lambda funkcije, lako možemo vidjeti da je tajni i javni eksponent moguće definirati i preko $\lambda(n)$

umjesto $\varphi(n)$, što se u nekim slučajevima i radi. Također, pretpostavljamo i da su e i d manji od $\lambda(n)$.

Iz kongruencije koja vrijedi iz definicije ključa, i činjenice da $\lambda(n) \mid \varphi(n)$ imamo

$$ed = 1 + k\lambda(n),$$

a onda iz pretpostavke da su e i d manji od $\lambda(n)$ dobijemo

$$0 < k = \frac{ed-1}{\lambda(n)} < \frac{ed}{\lambda(n)} < \min\{e, d\}.$$

Iz toga slijedi posebno da je $k < d$.

2.4.1 Wienerov napad

Definicija 2.27 *Niz prirodnih brojeva $\{F_n\}_{n\in\mathbb{N}}$ definiran relacijom*

$$F_1 = 1,\ F_2 = 1,\ F_{n+2} = F_{n+1} + F_n,\ n \in \mathbb{N},$$

nazivamo niz Fibonaccijevih brojeva. Nekoliko prvih članova niza je

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

Pomoću Wienerovog napada možemo s dostupnim javnim ključem doći do faktorizacije modula koristeći informacije dobivene iz jedne od konvergenti verižnog razlomka broja $\frac{e}{n}$.

Teorem 2.28 *Za dani modul $n = pq$ i javni ključ (n, e), neka je (p, q, d) odgovarajući tajni ključ, i $k \in \mathbb{Z}$ takav da je $ed = 1 + k\lambda(n)$. Neka su $g = nzd(p-1, q-1)$, $g_0 = \frac{g}{nzd(g,k)}$ i $k_0 = \frac{k}{nzd(g,k)}$. Ako je*

$$d < \frac{pq}{2(p+q-1)g_0k_0},$$

onda se n može faktorizirati u polinomijalnom vremenu u $\log(n)$ i $\frac{g}{k}$.

Dokaz. Iz

$$\lambda(n) = nzv(p-1, q-1) = \frac{\varphi(n)}{nzd(p-1, q-1)} = \frac{n-s}{g},$$

gdje je $s = p + q - 1$. Kongruenciju u definiciji ključa možemo zapisati kao $ed = 1 + k\lambda(n)$ za koju vrijedi

$$ed = 1 + k\lambda(n) = 1 + \frac{k}{g}\varphi(n) = 1 + \frac{k_0}{g_0}(n-s),$$

gdje je $k_0 = \frac{k}{nzd(k,g)}$ i $g_0 = \frac{g}{nzd(k,g)}$.
Podijelimo obje strane jednakosti $ed = 1 + \frac{k_0}{g_0}(n-s)$ s dn. Imamo

$$\frac{e}{n} = \frac{1}{dn} + \frac{k_0}{g_0 dn}(n-s) = \frac{1}{dn} + \frac{k_0}{g_0 d} + \frac{k_0 s}{g_0 dn}.$$

Sada imamo

$$\left|\frac{e}{n} - \frac{k_0}{g_0 d}\right| = \left|\frac{1}{dn} - \frac{k_0 s}{dg_0 n}\right| < \frac{k_0 s}{dg_0 n} = \frac{1}{2(dg_0)^2}.$$

Po Legendreovom teoremu (Teorem 2.5) znamo da je $\frac{k_0}{dg_0}$ jedna od konvergenti u razvoju broja $\frac{e}{n}$ u verižni razlomak. Neka je $c_i = \frac{p_i}{q_i}$ i-ta konvergenta od $\frac{e}{n}$, tada za neki j imamo $\frac{k_0}{dg_0} = \frac{p_j}{q_j}$.
Sada imamo

$$ed = 1 + \frac{k_0}{g_0}\varphi(n) \iff \varphi(n) = e\frac{dg_0}{k_0} - \frac{g_0}{k_0} = \lfloor e\frac{q_j}{p_j}\rfloor - \lfloor\frac{g_0}{k_0}\rfloor.$$

Dakle, ako nam je poznata konvergenta c_j i vrijednost $\lfloor\frac{g_0}{k_0}\rfloor$ možemo lako izračunati $\varphi(n)$. Za pronalazak konvergente i izračun $\varphi(n)$ pratimo sljedeće korake. Počevši od $m = 0$, za svaku konvergentu računamo $\varphi_c = \lfloor\frac{e}{c_i}\rfloor + m$ te pokušavamo faktorizirati modul, to jest riješiti sustav $n = pq$ i $\varphi_c = (p-1)(q-1)$ s nepoznanicama p i q. Ako smo pronašli p i q takve da je $pq = n$, onda smo pronašli i pravu konvergentu. Ako nismo pronašli faktorizaciju, onda m povećamo za jedan i ponovimo postupak.

Ovim postupkom smo sigurni da će m u nekom trenutku biti $m = \lfloor \frac{g_0}{k_0} \rfloor$. Kako je $m < \lfloor \frac{g_0}{k_0} \rfloor$, imat ćemo najviše $\lfloor \frac{g_0}{k_0} \rfloor$ iteracija za svaku konvergentu čiji je ukupan broj polinom u $\log(n)$. ■

Najjednostavniji način za izbjegavanje ovog napada je da odaberemo e i n takve da je za njih $d > n^{\frac{1}{4}}$. Wiener je predstavio još jedno rješenje za izbjegavanje ovog napada, a to je da koristimo veći javni eksponent.

Primjer 2.29 *Neka je* $(n, e) = (2447482909, 58549809)$ *javni ključ. Računamo razvoj broja* $\frac{e}{n}$ *u verižni razlomak*

$$[0, 41, 1, 4, 23, 78, 1, 6, 81, 1, 1, 4, 3, 2],$$

zatim računamo nekoliko početnih konvergenti

$$0, \frac{1}{41}, \frac{1}{42}, \frac{5}{209}, \frac{116}{4849}, \frac{9053}{378431}, \frac{9769}{383280}, \frac{64067}{2678111}, \ldots.$$

Provjerom redom konvergenti počevši od $m = 0$ *vidimo da prve tri kovergente ne daju faktorizaciju od* n*. Za četvrtu konvergentu* $c_4 = \frac{5}{209}$ *vrijedi*

$$\varphi' = \left\lfloor \frac{e}{c_4} \right\rfloor = \left\lfloor 58549809 \left(\frac{209}{5} \right) \right\rfloor = 2447382016.$$

Rješavanjem sustava

$$\varphi' = (x - 1)(y - 1),$$

$$n = xy,$$

dobijemo proste brojeve $x = 60317$ *i* $y = 40577$*. Slijedi da je* $\varphi(n) = \varphi'$ *i time smo faktorizirali modul. Koristeći faktorizaciju možemo izračunati* $\lambda(n) = 611845504$*,* $g = 4$ *i tajni ključ* $(p, q, d) = (60317, 40577, 209)$.

Primjetimo da je uvjet iz Teorema 2.28 zadovoljen za $d = 209 < \frac{n}{2sg_0k_0} \approx 2425.82$

Sljedeći rezultat pokazuje da u slučaju izbora relativno malog tajnog eksponenta d postoji efikasan algoritam za izračun tajnog ključa.

Teorem 2.30 *Neka je $n = pq$ i $p < q < 2p$ te neka je $e < \varphi(n)$ i $d < \frac{1}{3}n^{\frac{1}{4}}$. Tada postoji polinomijalni algoritam koji iz poznavanja n i e izračunava d.*

Dokaz. Po definiciji ključa vrijedi jednakost $ed - k\varphi(n) = 1$ te dijeljenjem s $d\varphi(n)$ dobijemo:

$$|\frac{e}{\varphi(n)} - \frac{k}{d}| = \frac{1}{d\varphi(n)}. \tag{2.1}$$

Dakle, $\frac{k}{d}$ je dobra aprokskimacija broja $\frac{e}{\varphi(n)}$. Pošto ne znamo vrijednost $\varphi(n)$, aproksimirat ćemo je iz n. Iz

$$\varphi(n) = n - p - q + 1 \ \text{ i } \ p + q - 1 < 3\sqrt{n},$$

slijedi

$$|n \cdot \varphi(n)| < 3\sqrt{n}.$$

Zamijenimo li $\varphi(n)$ s n u jednakosti 2.1 imamo

$$\begin{aligned} |\frac{e}{n} - \frac{k}{d}| &= |\frac{ed - k\varphi(n) - kn + k\varphi(n)}{nd}| = |\frac{1 - k(n - \varphi(n))}{nd}| \\ &< \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}. \end{aligned}$$

Sada je $k\varphi(n) = ed - 1 < ed$, pa iz $e < \varphi(n)$ slijedi $k < d < \frac{1}{3}n^{\frac{1}{4}}$ te dobivamo

$$|\frac{e}{n} - \frac{k}{d}| \leq \frac{1}{d\sqrt[4]{n}} < \frac{1}{2d^2}. \tag{2.2}$$

Iz Legendreovog Teorema 2.5 i relacije 2.2 slijedi da je $\frac{k}{d}$ neka konvergenta razvoja u verižni razlomak od $\frac{e}{n}$. Iz rekurzije za nazivnike konvergenti $\frac{p_k}{q_k}$ verižnog razlomka slijedi da je $q_k \geq F_k$, gdje je F_k k-ti Fibonaccijev broj, što znači da nazivnici konvergenti rastu eksponencijalno. U našem slučaju ima $O(\ln(n))$ konvergenti od $\frac{e}{n}$. Jedna od njih je $\frac{k}{d}$. Dakle izračunamo sve konvergente od $\frac{e}{n}$ i testiramo koja od njih zadovoljava uvjet $(xe)^d \equiv x \pmod{n}$ za slučajno odabran broj x. To daje polinomijalni algoritam za otkrivanje tajnog eksponenta d. ■

Primjer 2.31 *Neka je* $(n, e) = (7978886869909, 3594320245477)$ *javni ključ i neka je poznato da tajni eksponent* d *zadovoljava uvjet* $d < \frac{1}{3}n^{\frac{1}{4}}$. *Da bismo primijenili Wienerov napad računamo razvoj broja* $\frac{e}{n}$ *u verižni razlomak. Dobivamo*

$$[0, 2, 4, 1, 1, 4, 1, 2, 31, 21, 1, 3, 1, 16, 3, 1, 114, 10, 1, 4, 5, 1, 2].$$

Zatim računamo pripadne konvergente

$$0, \frac{1}{2}, \frac{4}{9}, \frac{5}{11}, \frac{9}{20}, \frac{41}{91}, \frac{50}{111}, \frac{141}{313}, \frac{4421}{9814}, \ldots.$$

Provjeravamo koji od nazivnika $2, 9, 11, 20, 91, 313, \ldots$ *zadovoljava kongruenciju* $(xe)^d \equiv x \pmod{n}$ *za npr.* $x = 2$. *Tako dobivamo da je tajni eksponent* $d = 313$.

Drugom metodom provjere dobivamo najprije da je

$$(p-1)(q-1) = \frac{ed-1}{k} = 7978881112300,$$

zatim

$$\frac{p+q}{2} = \frac{n-(p-1)(q-1)+1}{2} = 2878805,$$

te

$$\frac{q-p}{2} = 555546.$$

Ovime smo ponovno provjerili da je tajni eksponent $d = 313$, *a dobili smo i faktore od* n*:*

$$p = 2878805 - 555546 = 2323259,$$
$$q = 2878805 + 555546 = 3434351.$$

U prethodnom primjeru smo vidjeli da je prava konvergenta bila upravo zadnja konvergenta koja je zadovoljavala uvjet za veličinu nazivnika. Preciznijom ocjenom za $\varphi(n)$ ne bi bilo nužno testirati sve konvergente u zadanom

rasponu. Uz razumnu pretpostavku da je $n > 10^8$, dobije se da je $\frac{k}{d}$ jedinstvena konvergenta koja zadovoljava nejednakost

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}}.$$

U jednoj od varijanti Wienerova napada na RSA tajni eksponent d je veći od $d > \sqrt[4]{n}$. Neka je $d = D\sqrt[4]{n}$. Ako D nije velik onda možemo pokušati $\frac{k}{d}$ prikazati u obliku

$$\frac{rp_{m+1} \pm sp_m}{rq_{m+1} \pm sq_m},$$

gdje su r, s nenegativni cijeli brojevi i $\frac{p_m}{q_m}$ konvergenta verižnog razlomka od $\frac{e}{n}$. Koristeći se poopćenjem Legenderova teorema, Worleyev teorem 2.6, mogu se dobiti ocjene za broj parova (r, s) koje treba ispitati u najlošijem slučaju. Te su ocjene ugrubo $O(D)^2$, dakle eksponencijalne u $\ln(D)$.

Prikazat ćemo tu varijantu Wienerova napada na sljedećem primjeru.

Primjer 2.32 *Neka je* $(n, e) = (7978886869909, 4603830998027)$ *i pretpostavimo da je* $d < 10000000$. *Razvoj u verižni razlomak broja* $\frac{e}{n}$ *je*

$$[0, 1, 1, 2, 1, 2, 1, 18, 10, 1, 3, 3, 1, 6, 57, 2, 1, 2, 14, 7, 1, 2, 1, 4, 6, 2],$$

a prvih nekoliko konvergenti je

$$0, 1, \frac{1}{2}, \frac{3}{5}, \frac{4}{7}, \frac{11}{19}, \frac{15}{26}, \frac{281}{487}, \frac{2825}{4896}, \ldots.$$

Tražimo dvije susjedne neprane konvergente između kojih se nalazi

$$\frac{e}{n} + \frac{2.122e}{n\sqrt{n}},$$

Dobivamo

$$\frac{281}{487} < \frac{e}{n} + \frac{2.122e}{n\sqrt{n}} < \frac{11}{19}.$$

Sada tajni eksponent d tražimo među brojevima nekog od oblika

$$26r + 19s,$$

$$487s - 26t,$$

$$4896r' + 487s'.$$

Primjenjujući kriterij za testiranje kandidata za razlomak $\frac{k}{d}$ *opisan u dokazu Teorema 2.30, nalazimo da je*

$$d = 5936963,$$

što dobijemo za $s = 12195$ *i* $r = 77$.

2.4.2 Poboljšani Wienerov napad

Durfee i Boneh su pronašli novi način za napad na RSA kriptosustav kada je d mali tajni eksponent. Ovaj napad je poboljšanje Wienerovog napada.

Uzmimo kongruenciju koju zadovoljava ključ s parametrima e, d i n i zapišemo je na sljedeći način

$$ed \equiv 1 \pmod{\varphi(n)} \iff ed + k(n + 1 - (p + q)) = 1.$$

Ako stavimo da je

$$s = -(p + q),\ a = n + 1,$$

i zapišemo gornju jednakost modulo e, vrijedi:

$$k(a + s) \equiv 1 \pmod{e}.$$

Također ćemo za neki α uzeti da je $e = n^{\alpha}$. Broj α većinom bude blizu 1, jer je e uobičajno približno velik kao i n. Kako se radi o napadu s malim tajnim eksponentom pretpostavit ćemo da za d vrijedi uvjet $d < n^{\delta}$ za neki δ. Pogledajmo postojeće uvjete za k i s :

- iz definicije ključa:

$$|k| < \frac{de}{\varphi(n)} \leq \frac{3de}{2n} < \frac{3}{2}e^{1+\frac{\delta-1}{\alpha}},$$

- kako je $p < 2\sqrt{n}$ i $q < 2\sqrt{n}$ imamo:

$$|s| < 3n^{\frac{1}{2}} = 3e^{\frac{1}{2\alpha}}.$$

Ako je d mali, onda očekujemo da će e biti velik, tj $e \approx \varphi(n) \approx n$. Dakle situacija je slična kao i kod Coppersmithovog rezultata, samo što se ovdje radi o polinom s dvije varijable, pa se Coppersmithov teorem (Teorem 2.9) ne može izravno primijeniti da bi se dokazala korektnost ovog napada.

Da bi se izbjegla mogućnost zadnja dva predstavljena napada, trebali bismo izbjegavati slučaj kada je $d < \sqrt{n}$, jer je poznato da su ovi napadi neprimjenivi ako je $d > \sqrt{n}$.

Literatura

[1] Dujella, Andrej; Maretić, Marcel. 2007. Kriptografija. Element. Zagreb.

[2] Dujella, Andrej. 2019. Teorija Brojeva. Školska knjiga. Zagreb.

[3] Hinek, M. Jason. Cryptanalysis of RSA and It's Variants. Taylor & Francis Group, Boca Raton.

[4] Dujella, Andrej. Uvod u teoriju brojeva (skripta). `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (pristupljeno 25. listopada 2020.).

[5] Krešić-Jurić, Saša. 2013. Algebarske strukture (skripta). `http://mapmf.pmfst.unist.hr/~skresic/Algebra/Skripta/Algebarske_strukture_v5.pdf` (pristupljeno 26. listopada 2020.).

[6] Costa Boucinha, Filipe. 2011. A Survey of Cryptanalytic Attacks on RSA. Magisarski rad. Technical University of Lisbon. Lisabon. `https://fenix.tecnico.ulisboa.pt/downloadFile/395143450047/dissertacao.pdf` (pristupljeno 25. listopada 2020.)

[7] Secure Socket Layer. CARNet. `https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2000-07-01.pdf` (pristupljeno 25. listopada 2020.)

[8] TLS protokol. CARNet. https://www.cert.hr/wp-content/uploads/2009/03/CCERT-PUBDOC-2009-03-257.pdf (pristupljeno 25. listopada 2020.)

[9] Vries, Andreas. The ray attack, an inefficient trial to break RSA cryptosystems. http://haegar.fh-swf.de/publikationen/rayAttack.pdf (pristupljeno 25. listopada 2020.)

[10] Spaić, Ines. 2017. RSA kriptosutav i njegova kriptoanaliza. Diplomski rad. Sveučilište u Osijeku, Odjel za matematiku. Osijek.

[11] Alilović, Martina. 2017. Kriptoanaliza RSA kriptosustava i njegovih inačica. Diplomski rad. Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu. Zagreb.

TEMELJNA DOKUMENTACIJSKA KARTICA

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU
ODJEL ZA MATEMATIKU

DIPLOMSKI RAD

RSA kriptosustav i neki kriptoanalitički napadi

Marko Barać

Sažetak:

Kriptosustavi s javnim ključem su važni u kriptografiji jer je ključ za šifriranje javno dostupan, to jest nema potrebe za prethodnom razmjenom tajnih ključeva. Prvi i najpopularniji kriptosustav s javnim ključem je RSA kriptosustav čija je sigurnost zasnovana na teškoći faktorizacije velikih prirodnih brojeva. U prvom dijelu rada definirani su kriptosustavi, kriptosustavi s javnim ključem, RSA kriptosustav i SSL protokol gdje smo prikazali jednu od primjena RSA kriptosustava. U drugom dijelu smo se posvetili kriptoanalizi RSA kriptosustava i navelu kako možemo izbjeći mogućnost napada. Obradili smo neke od ranih napada, napade s malim javnim eksponentom e i napade s malim tajnim eksponentom d.

Ključne riječi:

kriptoanaliza, tajni ključ, javni ključ, SSL protokol, mali javni eksponent e, mali tajni eksponent d, Wienerov napad

Podatci o radu:

44 stranice, 3 slike

Mentor(ica): *doc. dr. sc. Marija Bliznac Trebješanin*

TEMELJNA DOKUMENTACIJSKA KARTICA

Članovi povjerenstva:

prof. dr. sc. Borka Jadrijević

Dino Peran, mag. math.

Povjerenstvo za diplomski rad je prihvatilo ovaj rad *22. listopada 2020.*

TEMELJNA DOKUMENTACIJSKA KARTICA

FACULTY OF SCIENCE, UNIVERSITY OF SPLIT
DEPARTMENT OF MATHEMATICS

MASTER'S THESIS

RSA Cryptosystem and Some Cryptanalytic Attacks

Marko Barać

Abstract:

Public key cryptosystems are important in cryptography because the encryption key is publicly available, that is, there is no need for a prior exchange of secret keys. The first and most popular public key cryptosystem is the RSA cryptosystem, whose safety is based on the difficulty of factorizing large positive integers. The first chapter defines cryptosystems, public key cryptosystems, RSA cryptosystem and SSL protocol where we presented one of the uses of RSA cryptosystems. In the second chapter, we dealt with the cryptanalysis of the RSA cryptosystem. We have dealt with some early attacks, small public exponent attacks and small private exponent attacks.

Key words:

cryptanalysis, secret key, public key, SSL protocol, small public exponent e, small secret exponent d, Wiener attack

Specifications:

44 pages, 3 picture

Mentor: *Assistant professor Marija Bliznac Trebješanin*

TEMELJNA DOKUMENTACIJSKA KARTICA

Committee:

Professor Borka Jadrijević

Dino Peran, MMath

This thesis was approved by a Thesis commettee on *October 22, 2020.*