Univerzitet u Banjoj Luci

Prirodno-matematički fakultet

Studijski program: Matematika i informatika

Smjer: Informatika

SEMINARSKI RAD

Predmet: Informacione tehnologije i društvo

Tema: RSA kriptosistem

Profesor:

vanr. prof. dr Dragan Matić

Student:

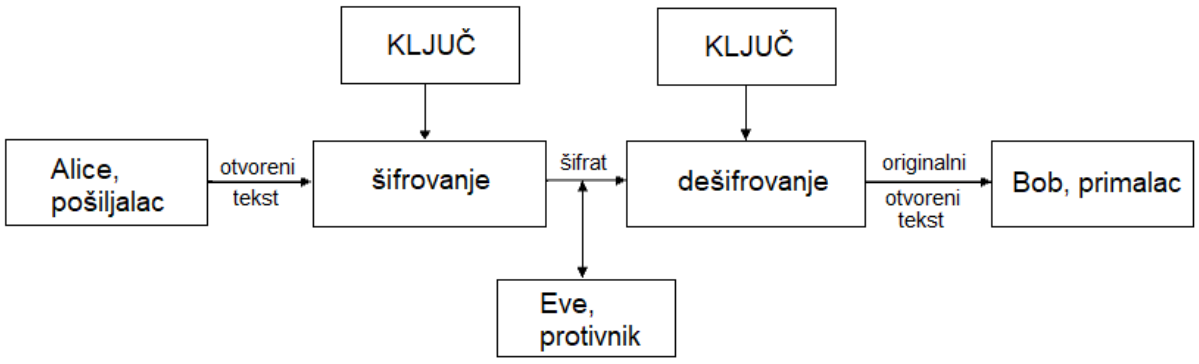
Teodora Milanović, 22/19

Sadržaj

1. Uvod

1.1 Osnovni pojmovi

Kriptografija ili **šifrovanje** je nauka koja se bavi metodima očuvanja tajnosti informacija tj. metodima koji omogućavaju slanje poruka u obliku u kojem nisu razumljive nikom osim osobi kojoj su poslane. Riječ potiče od grčkih riječi kriptós što znači "skriven" i gráfo što znači "pisati".
Kriptografske tehnike koje se koriste za očuvanje bezbjednosti su **šifra** tj. algoritam za šifrovanje i dešifrovanje, i **digitalni potpis** tj. skup podataka koji služe za identifikaciju potpisnika i potvrdu autentičnosti poruke.
Osnovni zadatak kriptografije jeste omogućavanje komunikacije preko nezaštićenog komunikacionog kanala tako da osoba kojoj poruke nisu namijenjene ne može da ih razumije. U stranoj literaturi su pošiljalac i primalac nazvani Alice i Bob, a napadač ili protivnik Eve.
Poruku koju Alice šalje Bobu i koja treba da se zaštiti zovemo **otvoreni tekst** (tekst, brojevi, numerički podaci itd.). Ključ šifrovanja i otvoreni tekst su ulazni parametri u šifarski sistem. Dužina ključa tj. broj cifara koji čine ključ zavisi od šifarskog sistema, te je jedan od parametara sigurnosti tog sistema. Alice transformiše otvoreni tekst koristeći ključ šifrovanja kako bi onemogućila Eve da ga razumije. Taj proces se naziva **šifrovanje**, a rezultat šifrovanja naziva se **šifrat**. Potom Alice šalje šifrat Bobu. Obrnut proces, **dešifrovanje**, omogućava dobijanje originalnog otvorenog teksta iz šifrata. U ovom slučaju Bob koristi ključ dešifrovanja, a argumenti funkcije za dešifrovanje su ključ i šifrat.



Slika 1.1 Kriptografija

U kriptografiji, **kriptosistem** je skup algoritama koji su potrebni za implementaciju bezbjednosnih usluga, najčešće zarad postizanja povjerljivosti. Kriptosistem se obično sastoji od tri algoritma: jednog za stvaranje ključeva, jednog za šifrovanje i jednog za dešifrovanje. Pošto se izraz šifra koristi za označavanje algoritama za šifrovanje i dešifrovanje, pojam kriptosistem se najčešće koristi kada je algoritam generisanja ključeva važan. Iz tog razloga, termin kriptosistem se obično koristi za označavanje tehnika javnih ključeva; međutim, i „šifra“ i „kriptosistem“ koriste se za simetrične tehnike.

Definicija 1.1
Matematički se kriptosistem može definisati kao uređena petorka $(\mathcal{P},C,\mathcal{K},\mathcal{E},\mathcal{D})$ za koju vrijedi:

1. $\mathcal{P}$ je prostor otvorenih tekstova tj. konačan skup svih mogućih otvorenih tekstova.
2. C je prostor šifrata tj. konačan skup svih mogućih šifrata.
3. $\mathcal{K}$ je prostor ključeva tj. konačan skup svih mogućih ključeva.
4. Za svaki ključ $k \in \mathcal{K}$ postoji algoritam šifrovanja $\mathcal{E}_k \in \mathcal{E}$ i algoritam dešifrovanja $\mathcal{D}_k \in \mathcal{D}$, gdje su $\mathcal{E}_k: \mathcal{P} \rightarrow C$ i $\mathcal{D}_k: C \rightarrow \mathcal{P}$ funkcije sa osobinom da za svaki $e \in \mathcal{K}$ postoji $d \in \mathcal{K}$ tako da $\mathcal{D}_d(\mathcal{E}_e(p)) = p$ za svaki $p \in \mathcal{P}$.

U odnosu na tajnost ključa, kriptosistemi se dijele na:

1. **Simetrične kriptosisteme** kod kojih se za šifrovanje i dešifrovanje koristi isti (simetričan) ključ, te distribucija ključeva mora da se obavlja putem zaštićenog kanala (najpouzdaniji je fizički susret). Postupak dešifrovanja poruke je inverzan postupku šifrovanja. Ključevi se moraju čuvati u tajnosti, zato se i zovu kriptosistemi s tajnim ključem.
2. **Asimetrične kriptosisteme** kod kojih se ključ za dešifrovanje ne može odrediti iz ključa za šifrovanje u nekom razumnom vremenu. U ovom slučaju je ključ za šifrovanje javni ključ koji je svima dostupan. To znači da bilo ko može šifrovati poruku pomoću njega, ali jedino osoba kojoj je poruka upućena i koja ima odgovarajući ključ za dešifrovanje (tajni ključ) može da je dešifruje. Zato se zovu kriptosistemi javnog ključa.

Za razliku od kriptografije, **kriptoanaliza** (od grčkog kryptós što znači skriveno i analýein što znači razmrsiti) je praksa razbijanja šifara. Bavi se otkrivanjem sadržaja šifrovanih informacija, bez poznavanja tajnih podataka potrebnih za dešifrovanje. To uglavnom podrazumijeva pronalaženje tajnog ključa. Različite tehnike kriptoanalize nazivaju se napadi.

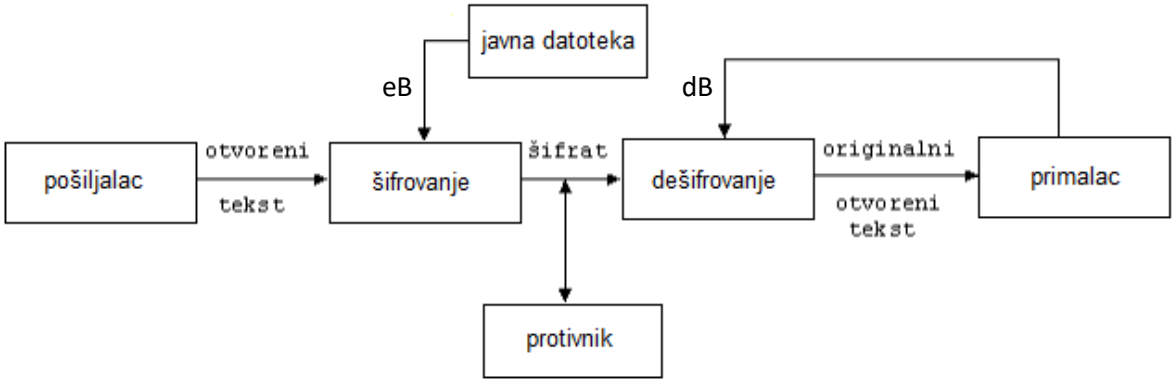
Vrste kriptoanalitičkih napada:

1. Napad poznatim šifratom: Najteža vrsta napada, jer kriptoanalitičar posjeduje samo šifrat na osnovu koga treba da otkrije otvoreni tekst ili ključ.
2. Napad poznatim otvorenim tekstom: Kriptoanalitičar posjeduje šifrat i otvoreni tekst, a treba da otkrije ključ kojim je poruka šifrovana.
3. Napad odabranim otvorenim tekstom: Kriptoanalitičar bira tekst koji će biti šifrovan, a potom dobija njegov šifrat. Ovo omogućava pronalaženje slabosti u algoritmu.
4. Napad odabranim šifratom: Kriptoanalitičar može odabrati šifrat i dobiti odgovarajući otvoreni tekst na osnovu koga treba da otkrije ključ za dešifrovanje.
5. Napad korištenjem sličnih ključeva: Ovaj napad može otkriti slabosti u postupku generisanja ključeva.

1.2 Kriptosistem javnog ključa

Glavni problem u simetričnom šifrovanju je rukovođenje tajnim šiframa, ključevima koji su korišteni za šifrovanje i dešifrovanje poruke. Zbog toga su **Whitfield Diffie** i **Martin Hellman**. 1976. godine iznijeli ideju o kriptosistemu koji je potpuno drugačijeg tipa nego simetrični kriptosistem. Nazvali su ga kriptosistem javnog ključa. Ideja se sastojala u tome da se koriste funkcije za šifrovanje iz kojih je praktički nemoguće izračunati funkciju za dešifrovanje u nekom razumnom vremenu. Za razliku od simetrične kriptografije, koriste se dva ključa, javni i privatni. Stvaranje javnog i privatnog ključa je povezano matematičkim postupkom, nakon čega se dobijeni tekst javnog ključa može podijeliti, ali se skriveni tekst može otključati samo privatnim ključem. Tajnost informacije ne bi bila ugrožena u slučaju da neko dođe do javnog ključa u procesu distribucije, jer pomoću njega se mogu samo šifrovati podaci. To je jedna od prednosti u odnosu na simetrične kriptosisteme.

Da bi se realizovali kriptosistemi sa javnim ključem potrebno je koristiti trapdoor jednosmjerne funkcije. Trapdoor jednosmjerna funkcija je funkcija koju je lako izračunati u jednom smjeru, ali je teško izračunati u suprotnom smjeru bez posebne informacije koja se naziva „trapdoor". U ovom slučaju trapdoor je tajni ključ.
Ako Alice želi poslati poruku x Bobu, potrebno je da Bob pošalje Alice svoj javni ključ e_B. Zatim Alice koristi njegov ključ da šifruje svoju poruku te mu vraća šifrat $y = e_B(x)$. Nakon toga, Bob dešifruje šifrat pomoću svog tajnog ključa d_B i dobija $d_B(y) = d_B(e_B(x)) = x$. Na taj način on sanzaje njenu originalnu poruku.
Ukoliko se komunikacija odvija izmedu više ljudi tada je potrebno da svi korisnici stave svoje javne ključeve u neku javnu datoteku. Datoteka mora biti takva da se javni ključevi ne mogu mijenjati. Ako Alice želi poslati poruku Bobu, potrebno je da iz datoteke pročita njegov javni ključ e_B uz pomoć kog će da izvrši šifrovanje. Pošto svako može pristupiti javnom ključu e_B, tada se svako može i predstaviti kao Alice. Zato dolazi do pitanja vjerodostojnosti poruke koja se može riješiti pomoću potpisa. P je potpis od Alice koji može da uključuje bilo koji lični podatak. Potrebno je da Alice dopiše $e_B d_A$ (P) u poruci koju šalje, te da izmijenjeni šifrat pošalje Bobu. Zatim, Bob dešifruje šifrat pomoću d_B i dobija tekst poruke i nejasni dio d_A (P). S obzirom da Bob zna da je tu poruku trebalo da pošalje Alice, on koristi njen javni ključ e_A kako bi dešifrovao d_A (P), te dobija P. Pošto je d_A tajni ključ, Bob zna da je Alice poslala tu poruku.



Slika 1.2 Shema kriptosistema javnog ključa

Prednosti kriptosistema sa javnim ključem (asimetrični) u odnosu na kriptosisteme sa tajnim ključem (simetrični):

- nije potreban siguran komunikacioni kanal za razmjenu ključeva i samim tim je eliminisan problem distribucije,
- povećana sigurnost jer se tajni ključ ne dijeli ni sa kim,
- kod asimetričnih kriptosistema ključevi mogu da se koriste godinama prije nego što se promjene, dok se kod simetričnih ključevi mijenjaju svaki put kad dođe do razmjene poruka,
- svakom korisniku su potrebna samo dva ključa (javni i tajni) za komunikaciju sa ostalim korisnicima, dok je kod simetričnog kriptosistema svakom potreban onoliki broj ključeva koliko ima korisnika.
- mogućnost potpisa poruke koji osigurava vjerodostojnost,
- pošiljalac ne može poreći da je poslao poruku jer postoji opcija digitalnog potpisa.

Nedostaci:

- algoritmi kriptosistema sa javnim ključem su i do 1000 puta sporiji od određenih algoritama kriptosistema sa tajnim ključem,
- potrebni su dosta duži ključevi u odnosu na simetrične (1024-2048 bita (RSA) prema 128-256 bita (AES)),
- podložan je uspješnim napadima u slučaju da je bilo koji od parametara nedovoljno veliki. Takođe, sa razvojem kvantnih računara faktorizacija ogromnih brojeva će biti izvodljiva u razumnom vremenu.
- često se koriste za razmjenu simetričnog ključa

2. RSA kriptosistem

2.1 Opis algoritma

RSA je algoritam za asimetričnu kriptografiju koji se koristi za siguran prenos podataka, ali i u sistemima elektronskog potpisa. Nastao je 1977. na MIT univerzitetu. Objavili su ga **Ronald Rivest**, **Leonard Ejdlman** i **Adi Šamir**, dok je naziv **RSA** formiran od početnih slova njihovih prezimena. Kliford Koks, britanski matematičar koji je radio za britansku obavještajnu agenciju Head Communications Headquarters (GCHQ), objavio je 1973. godine ekvivalentan sistem za asimetričnu kriptografiju, ali to je tek objavljeno 1997. godine jer je bilo državna tajna.

U RSA algoritmu ključnu ulogu vrši izbor velikih prostih brojeva (100 i više cifara) jer sigurnost RSA zavisi od složenosti faktorizacije velikih brojeva. Pretpostavlja se da je dobijanje otvorenog teksta na osnovu šifrata i javnog ključa ekvivalentno faktorizaciji proizvoda dva velika broja.

RSA kriptosistem implementira dvije važne ideje:

1. Korištenje javnih ključeva: Ono omogućava šifrovanje poruke bez potrebe za razmjenom ključeva preko zaštićenog komunikacionog kanala. Svako može da pristupi ključevima za šifrovanje jer su oni javni. Suprotno od njih, ključevi za dešifrovanje su tajni i nema potrebe za njihovom razmjenom, te samo osoba koja posjeduje odgovarajući tajni ključ može da dešifruje poruku.
2. Digitalni potpis: Omogućava rješavanje problema vjerodostojnosti i autentičnosti poruke. Pošto se prilikom potpisivanja koristi tajni ključ, ne može se izvršiti lažiranje potpisa. Samim tim, ni pošiljalac ne može poreći slanje poruke.

Ove dvije ideje su bitne za kupovinu i prodaju preko interneta, bankarstvo, elektronsku poštu, elektronsku saradnju itd.

2.2 Implementacija algoritma

RSA algoritam uključuje četiri koraka:

1. Generisanje ključeva
2. Distribucija ključeva
3. Šifrovanje poruke
4. Dešifrovanje poruke

Generisanje ključeva

1. Odaberu se ili slučajno generišu dva velika prosta broja p i q.
    - Iz sigurnosnih razloga, cijeli brojevi p i q treba da budu odabrani nasumično i treba da budu slični po veličini, ali da se razlikuju u dužini za nekoliko cifara kako bi faktorizacija bila teža. P i q se čuvaju u tajnosti.
2. Izračuna se $n = pq$.
    - n se koristi kao modul i za javne i za privatne ključeve. Njegova dužina koja je obično izražena u bitovima, je dužina ključa. Također, n je dio javnog ključa.
3. Izračuna se Ojlerova funkcija $\phi(n)= (p-1)(q-1)$.
    - $\phi(n)$ se čuva u tajnosti.
4. Odabere se cjelobrojna vrijednost e pri čemu $1 < e < \phi(n)$ takav da je $(e,\phi(n))=1$ tj. da je relativno prost sa $\phi(n)$.
    - Poželjno je odabrati što manji e kako bi se šifrovanje x^e mod n odvijalo brže. Kako broj operacija u šifrovanju zavisi od veličine broja e i broja jedinica u binarnom zapisu od e, jedan od čestih izbora jeste e = 3. Ali, s obzirom da upravo izbor malog broja e narušava sigurnost kriptosistema, najbolji izbor je broj $e = 2^{16} + 1 = 65537$. Taj broj je pogodan jer je prost te dovoljno velik za izbjegavanje napada malim eksponentom. A pritom se izbjegavaju dodatne operacije koje bi odužile proces šifrovanja. Također, e je dio javnog ključa.
5. Upotrebom proširenog Euklidovog algoritma izračunati jedinstveni cijeli broj d, $1 < d < \phi(n)$ takav da je $de \equiv 1 \pmod{\phi(n)}$ tj. $de = 1 + k\phi(n)$,
    - d se čuva u tajnosti.
    - inverzni element d od e se može odrediti iz Euklidovog algoritma, jer ima osobinu da postoji cijeli broj c za koji je $e \cdot d + c \cdot \phi(n) = 1$.
6. Javni ključ je par (n,e), a tajni ključ je d.

Distribucija ključeva

Bob želi da pošalje poruku Alice. Da bi to uradio on mora da zna njen javni ključ. Zato, Alice prenosi svoj javni ključ (n, e) Bobu putem rute koja ne mora nužno da bude tajna, kako bi joj on mogao poslati svoje šifrovane poruke. Privatni ključ (d) nikada se ne distribuira.

Šifrovanje poruke

Da bi osoba A šifrovala poruku x osobi B mora da:

1. Pristupi javnom ključu (n,e) osobe B.
2. Izračuna $e_K(x) = x^e \pmod n$.
3. Pošalje šifrat $e_K(x)$ osobi B.

Dešifrovanje poruke

Kako bi dobila otvoreni tekst x iz šifrata $e_K(x)$, osoba B treba da:

1. Upotrijebi tajni ključ d za dobijanje $x = (e_K(x))^d \pmod n$.

Primjer 2.1

Generisanje ključeva:

1. Osoba B odabere p = 23 i q = 31.
2. Izračuna $n = pq = 23 \cdot 31 = 713 \rightarrow$ **n = 713**
3. i $\phi(n) = (p-1)(q-1) = 22 \cdot 30 = 660 \rightarrow$ **ϕ(n) = 660**
4. Zatim odabere **e = 7** koji je relativno prost sa 160.
5. Pomoću proširenog Euklidovog algoritma računa d tako da je $de \equiv 1 \pmod{\phi(n)}$, tj. $d \cdot 7 \pmod{660} = 1$, slijedi da je **d = 283** jer je $1981 \pmod{660} = 1$.

B-ov javni ključ je (n = 713, e = 7), dok je tajni ključ d = 283.

Šifrovanje poruke:

1. Kako bi osoba A šifrovala otvoreni tekst x=123 potrebno je da izračuna:

$$e_K(x) = x^e \pmod n = 123^7 \pmod{713} = 495,$$

te šifrat $e_K(x)$ šalje osobi B.

Dešifrovanje poruke:

1. Za dešifrovanje $e_K(x)$, B računa:

$$(e_K(x))^d \pmod n = 495^{283} \pmod{713} = 123.$$

Primjer 2.2

Postupak slanja poruke INFORMATIKA.

- Alice preuzima Bobov javni ključ **(n, e) = (713, 7)** kako bi mogla šifrovati poruku INFORMATIKA. Slovima koji čine poruku redom pridruži brojevne vrijednosti koristeći se pravilom da slovima od A do Z redom odgovaraju brojevi od 01 do 26, dok se razmak označava sa 00. Na taj način dobija numerički ekvivalent prethodne poruke koji je **x = 09140615181301200911 01**. Pošto je x > n potrebno je x podijeliti u blokove od po 2 cifre. Slijedi da je x = (09, 14, 06, 15, 18, 13, 01, 20, 09, 11, 01).
- Pomoću Bobovog javnog ključa (n, e) Alice računa $y_i = x_i^e \mod n$ za sve i = 1, ...,11.

$y_1 = 09^7 \mod 713 = 165$
$y_2 = 14^7 \mod 713 = 19$
$y_3 = 06^7 \mod 713 = 440$
$y_4 = 15^7 \mod 713 = 333$
$y_5 = 18^7 \mod 713 = 443$
$y_6 = 13^7 \mod 713 = 239$
$y_7 = 01^7 \mod 713 = 1$
$y_8 = 20^7 \mod 713 = 297$
$y_9 = 09^7 \mod 713 = 165$
$y_{10} = 11^7 \mod 713 = 168$
$y_{11} = 01^7 \mod 713 = 1$

Alice formira šifrat tako što svaki y prikaže kroz 3 cifre, te dobija šifrat **y = 165019440333443239001297165168001**. Zatim ga šalje Bobu.

- Ponovo, šifrat y se dijeli na blokove od po 3 cifre, te Bob pomoću tajnog ključa d = 283 računa $x_i = y_i^d \mod n$ za sve i=1, ..., 11.

$x_1 = 165^{283} \mod 713 = 09$ => I
$x_2 = 19^{283} \mod 713 = 14$ => N
$x_3 = 440^{283} \mod 713 = 06$ => F
$x_4 = 333^{283} \mod 713 = 15$ => O
$x_5 = 443^{283} \mod 713 = 18$ => R
$x_6 = 239^{283} \mod 713 = 13$ => M
$x_7 = 1^{283} \mod 713 = 1$ => A
$x_8 = 297^{283} \mod 713 = 20$ => T
$x_9 = 165^{283} \mod 713 = 9$ => I
$x_{10} = 168^{283} \mod 713 = 11$ => K
$x_{11} = 1^{283} \mod 713 = 1$ => A

i dobija otvoreni tekst INFORMATIKA.

2.3 Efikasnost RSA kriptosistema

Prosti brojevi koji se koriste uglavnom sadrže nekoliko stotina cifara zbog sigurnosnih razloga, pa se javljaju određeni problemi vezani za efikasnost algoritma. Pošto se radi sa velikim brojevima potrebno je koristiti posebne algoritme pri računanju. Kao primjer možemo uzeti množenje velikih brojeva za koje je potreban poseban algoritam za množenje. Ali je za ovakve operacije potrebno više vremena, te nas to vodi do zaključka da su ovi algoritmi mnogo sporiji od simetričnih algoritama. Simetrični algoritam, DES, je do 1000 puta brži od RSA algoritma baš zbog operacija kao što su računanje modula i eksponenta, generisanja brojeva itd..
Neki od algoritama koji povećavaju efikasnost RSA kriptosistema su algoritam za generisanje prostih brojeva i algoritam za modularno potenciranje.

Modularno potenciranje
Brzina šifrovanja i dešifrovanja u RSA kriptosistemu zavisi od e i n. Te operacije mogu biti dugotrajne ako su eksponent i modul veliki. Složenost ovih operacija se može smanjiti tj. šifrat $e_K(x) = x^e \pmod n$ se može efikasno izračunati pomoću algoritma **„kvadriraj i množi”:**

1. Prikažemo e u bazi 2: $e = e_0 + 2e_1 + \cdots + 2^{s-1} e_{s-1}$.
2. Primijenimo sljedeći algoritam:

```
y=1
for (s-1 ≥ i ≥ 0)
        y = y^2 (mod n)
        if (e_i = 1)
                y = y · x (mod n)
```

Generisanje prostih brojeva
Potrebno je da algoritam za generisanje izgeneriše dva velika prosta broja koja su približno iste veličine. To je komplikovan posao jer je teško odrediti da li je broj koji ima na stotine cifara prost. Neki od algoritama koji se koriste za ispitivanje da li je broj prost su Miler-Rabinov test i Fermaov test za proste brojeve. Manje efektivan način jeste faktorizacija, jer se rastavljanjem na faktore može utvrditi da li je broj prost. Tu se izdvajaju Polardov rho algoritam, faktorizacija razlikom kvadrata, algoritam pokušaja dijeljenja, NFS algoritam itd.

3. Kriptoanaliza RSA kriptosistema

Napadi na RSA su uobičajena pojava, prvenstveno zato što se koristi za šifrovanje povjerljivih informacija. Postoje različite vrste napada. Jedan od njih je napad na fizičke komponente uređaja sa kog se vrši šifrovanje (napad na napajanje, napad bug-ovima, tajmirani napad koji omogućava da napadač pronađe ranjivosti uređaja i slično). Druga vrsta napada bazira se na manipulaciji i obmanjivanju korisnika. A treći, i najvažniji, jesu matematički napadi. Neki od njih će biti navedeni u nastavku.

3.1 Faktorizacija

Jedan od napada na RSA je faktorizacija od n gdje napadač pronalazi proste brojeve p i q čiji proizvod daje n. Ako napadač faktorizuje n onda može otkriti:

$$\varphi(n) = (p-1)(q-1),$$

ali i tajni ključ d pomoću Euklidovog algoritma:

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

Postoje mnogi algoritmi za faktorizaciju kao što su Polardov p-1 algoritam, Polardov rho algoritam, GNFS, QS, Fermaov metod itd., ali oni još uvijek ne predstavljaju opasnost po RSA kriptosistem ako se poštuju određena pravila. Čak i najbržem algoritmu za faktorizaciju (GNFS) treba dosta vremena da faktorizuje velike brojeve. Na primjer, potrebno je nekoliko mjeseci da se faktorizuje broj koji ima preko 140 cifri.
Zato se preporučuje da u RSA tajno izabrani parametri p i q budu veliki prosti brojevi od barem 100 cifara. Njih možemo izabrati na način da prvo generišemo broj x sa traženim brojem cifara, a potom pomoću testova prostosti pronađemo prvi prosti broj koji je veći od x. Tada n = pq ima oko 200 cifara, te se neće moći faktorizovati u razumnom vremenu. Ali treba da vodimo računa da p i q nisu vrlo blizu jer se mogu odrediti posmatranjem prostih brojeva koji su blizu $\sqrt{n}$. Takođe, brojevi p ± 1 i q ± 1 bi trebalo da imaju barem jedan veliki prosti faktor.

Primjer 3.1 (Polardov p-1 algoritam)
Neka je n = 713. Biramo B = 5 i definišemo M= $\prod_{q \le B} q^{\log_q B}$, s tim da su q isključivo prosti brojevi. Slijedi da je M = $2^2 \cdot 3^1 \cdot 5^1$. Izaberemo broj a koji je relativno prost sa n npr. a = 2 i tražimo NZD($a^M - 1$, n). Dobijamo da je NZD($2^{60} - 1$, 713) = 31. Pošto je $1 < 31 <$ 713 zaustavljamo se. Dalje računamo 713/31, te dobijamo 23 koji je takođe prost broj. Faktorizacija je uspješna: p = 23, q = 31.

3.2 Mali tajni eksponent

Da bi se skratilo vrijeme računanja često se bira mala vrijednost tajnog ključa d. Kanadski kriptolog Michael Wiener je pokazao da postoji efikasan algoritam koji može da razbije šifru kada je izabran mali tajni eksponent d. Ovaj napad se naziva Wienerov napad.

Teorema 3.1 (Wiener)
Neka je n = pq i p < q < 2p te neka je e < ϕ(n) i d < $\frac{1}{3}$ $n^{0.25}$. Tada postoji polinomijalni algoritam koji iz poznavanja javnog ključa (n,e) računa d.

Dokaz.
Kako je ed = 1 mod ϕ(n), postoji prirodan broj k takav da je ed − kϕ(n) = 1. Odavde je:

$$\left|\frac{e}{\phi(n)} - \frac{k}{d}\right| = \frac{1}{d\phi(n)}$$

Pošto je n=pq > q^2, slijedi da je q<$\sqrt{n}$, te da je n-ϕ(n) = p+q-1 < 2q+q-1 < $3\sqrt{n}$. Kako je ϕ(n) = n−p−q+1 i p+q−1 < $3\sqrt{n}$ slijedi da je |n−ϕ(n)| < $3\sqrt{n}$. Kada ϕ(n) zamijenimo sa n dobijamo:

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed-kn}{nd}\right| = \left|\frac{ed-k\phi(n)-kn+k\phi(n)}{nd}\right| = \left|\frac{1-k(n-\phi(n))}{nd}\right| < \left|\frac{3k\sqrt{n}}{nd}\right| < \frac{3k}{d\sqrt{n}}$$

Sada je kϕ(n) = ed − 1 < ed. Kako je e < ϕ(n), uočimo da je k < d. Slijedi da je 3k < 3d < $n^{1/4}$, pa dobijamo:

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{dn^{1/4}}$$

, pošto je 3d < $n^{1/4}$ slijedi da je:

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{3d^2}$$

Pošto je $\frac{k}{d}$ prema Legendreovom teoremu neka konvergenta razvoja u verižni razlomak od $\frac{e}{n}$, potrebno je da izračunamo sve konvergente od $\frac{e}{n}$, te da testiramo koja zadovoljava uslov $(x^e)^d \equiv x(\mod n)$ za nasumično odabrani x.

Primjer 3.2

Dat je modul n = 7064009 i javni eksponent e = 5773091, te pretpostavimo da tajni eksponent d zadovoljava $d < \frac{1}{3} \cdot n^{0.25} < 18$. Prvo računamo razvoj broja

$$\frac{e}{n} = \frac{5773091}{7064009}$$

u verižni razlomak (pomoću Euklidovog algoritma). Slijedi da je :

57730910 = 7064009 · **0** + 57730910,

7064009 = 5773091 · **1** + 1290918,

5773091 = 1290918 · **4** + 609419,

1290918 = 609419 · **2** + 72080 ...

Tada dobijamo: [0; 1, 4, 2, 8, 2, 5, 38, 1, 1, 2, 4, 2, 3]. Zatim računamo pripadne konvergente $\frac{k}{d}$:

$k_0 = \mathbf{0}$; $k_1 = 0 + 1 = \mathbf{1}$; $k_2 = 0 + \frac{1}{1+\frac{1}{4}} = \frac{1}{\frac{5}{4}} = \mathbf{\frac{4}{5}}$; $k_3 = 0 + \frac{1}{1+\frac{1}{4+\frac{1}{2}}} = \frac{1}{\frac{11}{9}} = \mathbf{\frac{9}{11}}$ ...

0, 1, $\frac{4}{5}$, $\frac{9}{11}$, $\frac{76}{93}$, $\frac{161}{197}$, $\frac{881}{1078}$, $\frac{33639}{41161}$, $\frac{34520}{42239}$, $\frac{68159}{83400}$, $\frac{170838}{209039}$, $\frac{751551}{919556}$, $\frac{1673860}{2048151}$, $\frac{5773091}{7064009}$. S obzirom da je d < 18, testiramo koji od imenioca 5 i 11 zadovoljava uslov $(x^e)^d \equiv x \pmod n$, za nasumično odabrani x, npr. x = 2. Tako dobijamo da je d = 11.

Da bi se izbjegao ovaj napad potrebno je koristiti veliki d (bar 256 bitni). Druga mogućnost je korištenje velikog javnog eksponenta e. Ako je $e > n^{1.5}$ napad se neće moći ostvariti bez obzira na veličinu tajnog eksponenta d. Međutim, velike vrijednosti eksponenta e dovode do smanjenja efikasnosti jer povećavaju vrijeme šifrovanja.

3.3 Mali javni eksponent

Često se koristi mali javni eksponent e jer značajno skraćuje vrijeme šifrovanja. Najmanji mogući javni eksponent koji se može koristiti jeste e = 3, ali izbor malog eksponenta e narušava sigurnost kriptosistema jer ga čini podložnim napadima. Baš zato, preporučena vrijednost za e je $2^{16} + 1$, koji je dovoljno velik da bi onemogućio sve poznate napade na RSA sa malim eksponentom.

Hastadov napad

Ovaj napad je opisao Hastad 1985. godine i po njemu je i dobio ime. Do njega dolazi kada se ista poruka m šifruje s nekoliko različitih javnih ključeva (n,e), a da pritom ključevi imaju isti javni eksponent e i različite module n koji su relativno prosti.

Pretpostavimo da postoje tri korisnika koji koriste isti javni eksponent e = 3, ali različite module n da šifruju poruku m. Napadač može da sazna šifrate:

$$c_1 \equiv m^3 \pmod{n_1},\ c_2 \equiv m^3 \pmod{n_2},\ c_3 \equiv m^3 \pmod{n_3}.$$

Dalje pomoću Kineske teoreme o ostacima pronalazi rješenje kongruencija:

$$x \equiv c_1 \pmod{n_1},\ x \equiv c_2 \pmod{n_2},\ x \equiv c3 \pmod{n_3}.$$

Pošto x ima osobinu da $x \equiv m^3 \pmod{n_1 \cdot n_2 \cdot n_3}$ i pošto je $m^3 < n_1 \cdot n_2 \cdot n_3$, slijedi da je $x = m^3$. Napadač dobija originalnu poruku m ukoliko izračuna $\sqrt[3]{x}$.

Primjer 3.3

Tri korisnika koriste različite module $n_1 = 329$, $n_2 = 341$, $n_3 = 377$, dok im je javni eksponent e=3. Sva tri korisnika šifruju poruku m=42, te dobijaju šifrate c_1=63, c_2=91, c_3=196. Napadač zna šifrate, te pokušava da sazna otvoreni tekst na osnovu njih.

Dobija sistem linearnih kongruencija:

$$x \equiv 63 \pmod{329},\ x \equiv 91 \pmod{341},\ x \equiv 196 \pmod{377}.$$

Pomoću Kineske teoreme o ostacima računa:

$n=n_1 \cdot n_2 \cdot n_3=329 \cdot 341 \cdot 377=42295253$,

$p_1= n/n_1=128557$, $p_2= n/n_2=124033$, $p_3=n/n_3=112189$,

slijedi da je:

$$p_1 \cdot x_1 \pmod{n1} = c_1$$
$$128557x \pmod{329} = 63 \Rightarrow x_1 = 252$$
$$p_2 \cdot x_2 \pmod{n2} = c_2$$
$$124033x \pmod{341} = 91 \Rightarrow x_2 = 340$$
$$p_3 \cdot x_3 \pmod{n3} = c_3$$
$$112189x \pmod{377} = 196 \Rightarrow x_3 = 90$$

,daljnjim rješavanjem:

$$x = p_1x_1 + p_2x_2 + p_3x_3$$
$$= 128557 \cdot 252 + 124033 \cdot 340 + 112189 \cdot 90$$
$$= 84664594 \pmod{329 \cdot 341 \cdot 377}$$
$$= 74088 \pmod{42295253}$$

dobija x = 74088, te ga uvrštava u formulu m = $\sqrt[3]{x}$. Odatle dobija da je m = 42.

3.4 Ciklični napadi

Ciklični napad je napad kod kog se otvoreni tekst uvijek dobija ponovljenim šifrovanjem njegovog šifrata, sve dok se ciklus ne vrati na izvorni šifrovani tekst.
Neka je $e_k(x) = x^e \pmod n$ šifrat. Potrebno je da napadač računa $e_k(x)^e \pmod n$, $e_k(x)^{e^2} \pmod n$, $e_k(x)^{e^3} \pmod n$, itd. sve dok ne dobije originalni šifrat. S obzirom da je $e_k(x)^{e^k} \pmod n$ jednak šifratu $e_k(x)$, onda je prethodni broj $e_k(x)^{e^{k-1}} \pmod n$ jednak otvorenom tekstu x.

Primjer 3.4
Alice šifruje poruku m = 11 pomoću Bobovog javnog ključa (3, 51) i tako dobija šifrat c = 5. Eve saznaje šifrat c i pokušava otkriti otvoreni tekst pomoću cikličnog napada.

$$e(5) = 5^3 \bmod 51 = 23$$
$$= 23^3 \bmod 51 = 29$$
$$= 29^3 \bmod 51 = 11$$
$$= 11^3 \bmod 51 = 5.$$

Nakon što Eve dobije izvornu vrijednost (c = 5) i izvrši prekid šifrovanja, vratiće se jedan korak nazad kako bi otkrila dešifrovanu poruku tj. x=11. Ona vrijednost koju je Eve šifrovala te dobila 5, mora biti jednaka onoj vrijednosti koju je Alice šifrovala i dobila šifrat c = 5.

Ciklični napad uvijek može da otkrije otvoreni tekst. Međutim, ovaj napad je nepraktičan i spor kada su parametri veliki. Kako bi se izbjegao potrebno je koristiti velike proste brojeve koji imaju velike proste faktore. Na ovaj način se povećava broj ciklusa.

4. Sigurnost RSA kriptosistema

RSA se može smatrati sigurnim kriptosistemom, pod uslovom da se ispravno koristi. Svi dosadašnji napadi nam daju mogućnost da uočimo greške pri implementaciji RSA i izboru parametara, te da ih u skladu sa tim izbjegavamo. Naglim napretkom današnjih računara javila se potreba za povećanjem sigurnosti, odnosno zaštite podataka. Takođe, činjenica da algoritmi za faktorizaciju brojeva postaju svakim danom sve bolji, ali i neumoljiv razvoj kompjutera učinili su da 512 bitni RSA algoritam nije više dovoljan za bezbjedno šifrovanje poruka. Međutim, ključeve dužine 512 bitova (155 cifara) nije moguće probiti na današnjim ličnim računarima. Za to se koriste složeni računarski sistemi, ali su oni skupi i teško dostupni. Dužina ključeva za RSA algoritam je uglavnom 1024 bita. Za njih se pretpostavlja da će biti bezbjedni barem još 15-tak godina. Ali za potpunu sigurnost preporučuje se korištenje ključeva koji su minimalno 2048 bita dugi.
Brojni informatičari čak smatraju da je praktično nemoguće faktorizovati brojeve koji su duži od 2048 bita na klasičnim računarima. Ali, sa razvojem tehnologije, pretpostavlja se da će problem faktorizacije biti lako rješiv u budućnosti. Kao primjer se mogu uzeti kvantni računari i Šorov algoritam. RSA je zasnovan na pretpostavci da je računarski neizvodljivo rastaviti veliki broj na proste činioce u polinomijalnom vremenu. Međutim, Šorov algoritam pokazuje da bi to moglo biti efikasno na idealnom kvantnom računaru, te da bi se sa lakoćom mogao faktorizovati broj duži od 2048 bita. Kako je time narušena i sigurnost RSA kriptosistema to je motivisalo naučnike da otpočnu istraživanje novih kriptosistema koji bi bili sigurni od kvantnih računara. Nazvani su post-kvantna kriptografija. Ipak, kvantni računari još ne postoje u obliku u kom bi ugrožavali sigurnost podataka. Samim tim, zaključujemo da je RSA još uvijek siguran algoritam za šifrovanje podataka.

Literatura

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

[2] A.Dujella, *Diskretna matematika*

[3] D.Boneh, *Twenty Years of Attacks on the RSA Cryptosystem.*

[4] B.Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list 5 (2005), 101-112.

[5] S.Robles, *The RSA Cryptosystem.*

[6] N. Smart, *Cryptography. An Introduction*, McGraw–Hill, New York, 2002.