Neki kriptosustavi zasnovani na problemu faktorizacije

Stojaković, Helena

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Helena Stojaković

Neki kriptosustavi zasnovani na problemu faktorizacije

Završni rad

Osijek, 2020.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Helena Stojaković

Neki kriptosustavi zasnovani na problemu faktorizacije

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2020.

Sažetak

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku u kojem ih može razumijeti samo osoba kojoj su te poruke namijenjene. Kriptosustavi s javnim ključem imaju javan ključ za šifriranje poruke, ali tajan ključ za njezino dešifriranje. Koriste se za prijenos ključeva modernih simetričnih kriptosustava i u digitalnim potpisima. Neki od njih temelje se na problemu faktorizacije velikih prirodnih brojeva. U radu su objašnjeni RSA i Rabinov kriptosustav. RSA kriptosustav svoju sigurnost zasniva na problemu faktorizacije, a Rabinov kriptosustav na problemu kvadratnog korijena po složenom modulu koji je ekvivalentan problemu faktorizacije tog modula. Kriptoanaliza oba kriptosustava ističe njihove slabosti, ali time i mogućnosti te potrebne promjene za sprječavanje poznatih napada i jačanje njihove sigurnosti.

Ključne riječi

kriptosustavi s javnim ključem, RSA kriptosustav, Rabinov kriptosustav, problem faktorizacije, problem kvadratnog korijena, kripoanaliza, Hastadov napad, Wienerov napad, Rabin - Williamsov kriptosustav

Some cryptosystems based on the factorization problem

Summary

Cryptography is a scientific discipline that studies methods for sending messages in a form in which they can only be understood by the person to whom they are intended. Public key cryptosystems have a public key to encrypt the message, but a private key to decrypt it. They are used to transfer the keys of modern symmetric cryptosystems and in digital signatures. Some of them are based on the problem factorization of positive integers. The paper explains RSA and Rabin's cryptosystem. The RSA cryptosystem bases its security on the factorization problem while the Rabin cryptosystem on the square root of the composite modulus problem that is equivalent to the factorization problem of that modulus. Cryptanalysis of both cryptosystems emphasizes their weaknesses, but also possibilities and necessary changes to prevent known attacks and strengthen their security.

Key words

public key cryptosystems, RSA cryptosystem, Rabin cryptosystem, integer factorization problem, the square root problem, cryptanalysis, Hastad's attack, Wiener's attack, Rabin - Williams cryptosystem

Sadržaj

Uvod

Potreba za sigurnim komuniciranjem postojala je oduvijek. Tijekom povijesti mijenjali su se načini sigurne komunikacije, ali glavni problem ostao je uvijek isti, odnosno kako onemogućiti treću osobu da sazna poruku. Tim se problemom bavi kriptografija.

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku da ih može pročitati osoba kojoj su namijenjene. Osnovni zadatak je omogućiti dvijema osobama koje ćemo zvati *pošiljatelj* i *primatelj* (poznati kao Alice i Bob) komunikaciju u kojoj treća osoba koju zovemo *protivnik* (poznat kao Eva ili Oscar) ne može razumjeti njihove poruke. Poruku koju pošiljatelj šalje primatelju nazivamo *otvoreni tekst*. Poruka koja se dobiva šifriranjem otvorenog teksta naziva se *šifrat*.

Kriptoanaliza je znanstvena disciplina koja se bavi proučavanjem postupaka za otkrivanje poruka bez poznavanja ključa. Grana znanosti koja obuhvaća kriptografiju i kriptoanalizu naziva se *kriptologija*.

Šifra je matematička funkcija koja služi za šifriranje i dešifriranje. Zapravo, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. One preslikavaju osnovne elemente otvorenog teksta u osnovne elemente šifrata te obratno. Biramo ih iz određene familije funkcija u ovisnosti o ključu. *Prostor ključeva* je skup svih mogućih vrijednosti ključeva. Sada možemo definirati *kriptosustav*.

Definicija 1. *Neka je $\mathcal{P}$ konačan skup svih mogućih elemenata otvorenog teksta, $\mathcal{C}$ konačan skup svih mogućih elemenata šifrata, $\mathcal{K}$ konačan skup svih mogućih ključeva, $\mathcal{E}$ skup svih mogućih funkcija šifriranja i $\mathcal{D}$ skup svih mogućih funkcija dešifriranja. Za svaki $K \in \mathcal{K}$ neka postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$, odnosno funkcije $e_K : \mathcal{P} \to \mathcal{C}$ i $e_K : \mathcal{C} \to \mathcal{P}$ sa svojstvom $d_K(e_K(x)) = x$, za svaki $x \in \mathcal{P}$. Tada se uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ naziva kriptosustav.*

Svojstvo $d_K(e_K(x)) = x$, za svaki $x \in \mathcal{P}$ nam zapravo govori kako bi funkcije e_K trebale biti injekcije da bi primatelj mogao jasno odrediti pošiljateljevu poruku.

Kriptosustave dijelimo prema:

1. tipu operacija koje koriste za šifriranje
    - supstitucijske šifre - zamjena svakog elementa otvorenog teksta s nekim drugim elementom
    - transpozicijske šifre - permutiranje elemenata otvorenog teksta
2. načinu obrade teksta
    - blokovne šifre - obrađivanje jednog po jednog bloka otvorenog teksta primjenjujući isti ključ
    - protočne šifre - obrađivanje jednog po jednog bloka otvorenog teksta primjenjujući paralelno generirani niz ključeva

3. (ne)tajnosti ključa

    - simetrični ili kriptosustavi s tajnim ključem - ključ za dešifriranje može se izračunati poznavajući ključ za šifriranje, pa je važna tajnost ključa za šifriranje
    - asimetrični ili kriptosustavi s javnim ključem - ključ za dešifriranje se ne može izračunati poznavajući ključ za šifriranje u nekom razumnom vremenu, pa ključ za šifriranje je javan, a ključ za dešifriranje tajan

U ovome radu posvetit ćemo se nekim kriptosustavima zasnovanim na problemu faktorizacije. Ovi kriptosustavi koriste težinu faktorizacije velikih brojeva kao dio svoje sigurnosti jer od njihova nastanka nemoguće je u razumnom vremenu rastavljanje na faktore broja od barem 250 znamenaka. Kako kriptosustavi zasnovani na problemu faktorizacije pripadaju asimetričnim kriptosustavima, u prvom poglavlju upoznajemo se s osnovama kriptografije javnoga ključa koja su nam potrebna za daljnje razumijevanje ovih kriptosustava. U drugom i trećem poglavlju upoznajemo se sa RSA i Rabinovim kriptosustavom i njihovom kriptoanalizom koja nam pomaže uočiti poželjne karakteristike ovih kriptosustava.

1 Uvod u kriptografiju javnoga ključa

Whitfield Diffie i Martin Hellman smatraju su začetnicima kriptografije javnoga ključa koji su 1976. godine objavili u svome radu mogućnost objavljivanja ključeva javno uz osiguranu privatnost pošiljatelja i primatelja što je velika prednost naspram simetričnih kriptosustava. Ideja javnog ključa je stvaranje kriptosustava iz kojih je nemoguće u razumnom vremenu saznati funkciju dešifriranja d_K iz poznate funkcije šifriranja e_K. Zato ovdje važnu ulogu imaju osobne jednosmjerne funkcije.

Definicija 2. *Za funkciju f kažemo da je jednosmjerna ako je f lako izračunati, a f^{-1} teško. Ukoliko koristimo neki dodatan podatak koji omogućava lako izračunavanje f^{-1}, onda f nazivamo osobna jednosmjerna funkcija.*

Primjerice, modularno potenciranje je jednosmjerna funkcija. Sada možemo definirati kriptosustave s javnim ključem.

Definicija 3. *Kriptosustav s javnim ključem sastoji se od dviju familija funkcija šifriranja $\{e_K\}$ i funkcija dešifriranja $\{d_K\}$ sa svojstvima koja vrijede za svaki ključ K:*

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

Ovdje e_K nazivamo javnim ključem, a d_K tajnim ključem.

Primatelj B šalje pošiljatelju A svoj javni ključ e_B. Pošiljatelj A šifrira svoj otvoreni tekst x i šalje B pripadni šifrat $y = e_B(x)$. Kako bi B saznao poruku x pošiljatelja A dešifrira šifrat pomoću svoga tajnoga ključa d_B,

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

Ako se komunikacija odvija između više korisnika, svi korisnici stavljaju svoje javne ključeve u neku javnu datoteku, pa pojedinačno slanje ključeva pošiljatelju nije potrebno.

Glavne prednosti ovih kriptosustava naspram simetričnih su što se ne mora koristiti sigurni komunikacijski kanal, korištenje manjeg broja ključeva i mogućnost potpisa poruke.

U primjeni, kriptografija javnoga ključa ne zamjenjuje simetrične kriptosustave, nego se koristi za šifriranje njihovih ključeva. Moderni sustavi ne koriste kriptosustave s javnim ključem za šifriranje otvorenih tekstova jer su znatno sporiji od novih simetričnih kriptosustava. Dodatni nedostatak ovih kriptosustava je što su podložni na napad na "odabrani otvoreni tekst". Neka je x otvoreni tekst koji može poprimiti jednu od n vrijednosti i $y = e(x)$. Kako je funkcija e javna, možemo šifrirati svih n mogućih vrijednosti i usporediti rezultat s y te otkrivamo x.

Ovi kriptosustavi imaju veliku ulogu u komercijalnome svijetu zbog digitalnih potpisa koji osiguravaju autentičnost i povjerljivost prilikom razmjene, tj. B zna da poruku koju je

zaprimio je mogao poslati samo pošiljatelj A i samo B je zna pročitati. Objasnimo dodatno uz pretpostavku $\mathcal{P} = \mathcal{C}$. Pošiljatelj potpisuje poruku x tako da pošalje B šifrat $z = d_A(y) = d_A(e_B(x))$. Sada B primjenjuje javan ključ e_A i svoj tajni ključ d_B, odnosno $d_B(e_A(z)) = d_B(e_A(d_A(e_B(x)))) = x$. Primatelj B zna da je poruku mogao poslati samo A jer je A jedina osoba koja je mogla primjeniti funkciju d_A.

2 RSA kriptosustav

RSA kriptosustav je jedan od prvih kriptosustava s javnim ključem. Osmislili su ga Ronald L. Rivest, Adi Shamir i Leonard M. Adleman 1977. godine po kojima je i nazvan. Sigurnost mu se temelji na težini faktorizacije velikih prirodnih brojeva. Jedan je od najkorištenijih kriptosustava sa širokom primjenom.

U definiranju ovog kriptosustava koristit ćemo i Eulerovu funkciju φ koja predstavlja broj brojeva u nizu $1, \ldots, n$ koji su relativno prosti s n.

Definicija 4. *Neka je $n = pq$, pri čemu su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Neka je*

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

Za $K \in \mathcal{K}$ definiramo funkciju šifriranja

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

i funkciju dešifriranja

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

Javni ključ je (n, e), a tajni ključ je (p, q, d).

Složeni broj $n = pq$ naziva se *modul*. Broj e je poznat kao *enkripcijski* ili *javni eksponent*, a d kao *dekripcijski* ili *tajni eksponent*.

Pokažimo da su funkcije e_K i d_K međusobno inverzne. Koristit ćemo Eulerov teorem i multiplikativnost Eulerove funkcije:

Teorem 1 (Eulerov teorem, vidjeti [3, Teorem 3.9.])**.** *Ako su $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da je $(a, n) = 1$, tada vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Teorem 2 (vidjeti [3, Teorem 3.11.])**.** *Neka su $m, n \in \mathbb{N}$ takvi da je $(m, n) = 1$. Tada vrijedi $\varphi(mn) = \varphi(m)\varphi(n)$, tj. Eulerova funkcija je multiplikativna.*

Dokazi Teorema 1 i 2 se nalaze u [3].
Iz uvjeta $de \equiv 1 \pmod{\varphi(n)}$ prema definiciji kongruencije slijedi $\varphi(n) \mid de - 1$, a znamo da po definiciji djeljivosti postoji cijeli broj k takav da vrijedi $de - 1 = k\varphi(n)$. Uočimo da je $d_K(e_K(x)) = x^{de} \pmod{n}$.
Sada razlikujemo četiri slučaja:

1° $(x, n) = 1$: Kako je $(x, n) = 1$, primjenom Teorema 1 dobivamo $x^{\varphi(n)} \equiv 1 \pmod{n}$. Iz $x^{de} = x^{k\varphi(n)+1} = x^{k\varphi(n)}x$ slijedi da je $x^{de} \equiv x \pmod{n}$.

2° $(x, n) = n$: Lako je vidljivo da vrijedi $x^{de} \equiv 0 \equiv x \pmod{n}$.

3° $(x, n) = p$: Budući da je $n = pq$, gdje su p i q prosti brojevi, zbog $p \mid x$ slijedi $(x, q) = 1$. Tada Teorem 1 implicira $x^{\varphi(q)} = x^{q-1} \equiv 1 \pmod{q}$. Zatim opet primjenom Teorema 1 i 2 imamo $x^{de} = x^{k\varphi(pq)+1} = (x^{q-1})^{k(p-1)} \cdot x \equiv x \pmod{q}$. Množeći s p dobivamo $px^{de} \equiv px \pmod{n}$, pa prema definiciji kongruencije slijedi $n \mid p(x^{de} - x)$. Znamo da je $n \nmid p$, pa imamo $n \mid x^{de} - x$, odnosno $x^{de} \equiv x \pmod{n}$.

4° $(x, n) = p$: Analogno prethodnom slučaju.

U svakom slučaju dobili smo $x^{de} \equiv x \pmod{n}$. Dakle, dokazali smo da vrijedi $d_K(e_K(x)) = x$, što je osnovno svojstvo kriptosustava. Primijetimo također da javni eksponent treba biti relativno prost s $\varphi(n)$ zbog egzistencije tajnog eksponenta d koji će sigurno postojati zbog Eulerova teorema.

Objasnimo sada RSA na postupku koji je potreban napraviti za uspješno skrivanje otvorenog teksta.
Generiranje ključa:
Alice treba učiniti sljedeće:

1. Odabrati dva različita prosta broja p i q.
2. Izračunati $n = pq$ i $\varphi(n) = (p-1)(q-1)$.
3. Odabrati enkripcijski eksponent e, $1 < e < \varphi(n)$, takav da je $(e, \varphi(n)) = 1$.
4. Primjenom Euklidova algoritma izračunati pripadni dekripcijski eksponent d iz $ed - k\varphi(n) = 1$ za neki cijeli broj k. Metode Euklidova algoritma mogu se vidjeti u [7].

Tada je javni ključ (n, e), a (p, q, d) je tajni ključ.

Šifriranje:
Bob primitkom zadanog javnog ključa radi sljedeće korake:

1. Koristeći zadani javni ključ šifrirati otvoreni tekst $x \in \mathbb{Z}_n$, stvarajući šifrat y pomoću izraza $y = x^e \bmod n$.
2. Šifrat y poslati Alice.

Dešifriranje:
Kako bi Alice saznala Bobovu poruku x, rješava $y = x^d \bmod n$ primjenjujući svoj tajni eksponent d.

Pokažimo sada kako to funkcionira na primjeru.

Primjer 1. *Alice odabire proste brojeve* $p = 17$ *i* $q = 23$ *te dobiva* $n = 17 \cdot 23 = 391$.
Računa $\varphi(n)$

$$\varphi(n) = (p-1)(q-1) = 16 \cdot 22 = 352$$

te bira javni eksponent e *takav da vrijedi* $(e, \varphi(n)) = 1$, *odnosno uzima primjerice* $e = 15$.
Tada je javni ključ $(391, 15)$.

Tajni eksponent dobiva iz $ed - k\varphi(n) = 1$ *primjenom Euklidova algoritma. Vrijednost eksponenta* d *je* 47.
Bob želi poslati poruku $x = 101$. *Treba izračunati šifrat* $y = 101^{15} \pmod{391}$. *Dobiva*

$$101^{15} \equiv (101^3)^5 \equiv 16^5 \equiv 305 \pmod{391}$$

te je traženi šifrat $y = 305$. *Svoj šifrat* y *šalje Alice.*
Alice dešifrira poruku pomoću svog tajnog eksponenta $d = 47$, *odnosno računa* $x = 305^{47} \bmod 391$. *Dobiva*

$$\begin{aligned} 305^{47} &\equiv (305^5)^9 \cdot 305^2 \equiv (-86^5)^9(-86)^2 \equiv (-205^3)^3 \cdot 358 \\ &\equiv (-222)^3 \cdot 358 \equiv -86 \cdot 358 \equiv 101 \pmod{391} \end{aligned}$$

i Bobova poruka je $x = 101$.

Ukoliko je otvoreni tekst $x \geq n$, x rastavljamo na blokove koji su manji od n.

Primjer 2. *Šifrirajmo poruku KONGRUENCIJA. Odaberemo primjerice* $p = 241$ *i* $q = 421$ *te dobivamo* $n = 101461$.
$\varphi(n)$ *iznosi*

$$\varphi(n) = (p-1)(q-1) = 240 \cdot 420 = 100800.$$

Biramo takav e *da vrijedi* $(e, \varphi(n)) = 1$, *pa uzimamo primjerice* $e = 13$.
Svakom slovu engleske abecede pridružujemo dvoznamenkasti broj na način $A = 00, B = 01, C = 02, \ldots Z = 25$. *Sada je numerički ekvivalent poruke KONGRUENCIJA jednak* $x = 10141306172004130208090 0$. *Našu poruku* x *želimo podijeliti na blokove jednake duljine koji su manji od* n. *Imamo*

$$\begin{aligned} x_1 &= KON = 101413 \\ x_2 &= GRU = 061720 \\ x_3 &= ENC = 041302 \\ x_4 &= IJA = 080900. \end{aligned}$$

Šaljemo pripadne šifrate:

$$y_1 = 101413^{15} \bmod 101461.$$

Imamo

$$101413^{15} \equiv (-48^5)^3 \equiv (-35397)^2(-35397) \equiv 5720(-35397) \equiv 45316 \pmod{101461},$$

tj. $y_1 = 45316$. *Analogno dobivamo*

$$\begin{aligned} y_2 &= 61720^{15} \pmod{101461} = 4580, \\ y_3 &= 41302^{15} \pmod{101461} = 66517, \\ y_4 &= 80900^{15} \pmod{101461} = 3022. \end{aligned}$$

Kako je polazna poruka bila podijeljenja na blokove duljine 3*, tada bi i šifrati trebali biti te duljine. Zbog toga ispred svakog šifrata dodajemo nule jer se šifrat mora sastojati od* 6 *znamenaka. Imamo šifrate*

$$y_1 = 045316, \quad y_2 = 004580, \quad y_3 = 066517, \quad y_4 = 003022.$$

Sada blokovima pridružemo slova (ukoliko je dvoznamenkasti broj veći od 26, uzimamo njegov ostatak pri dijeljenju s 26) i slijedi

$$y_1 = EBQ, \quad y_2 = ATC, \quad y_3 = GNQ, \quad y_4 = AEW$$

te šaljemo šifrat $y = EBQATCGNQAEW$*.*

2.1 Sigurnost i kriptoanaliza RSA kriptosustava

Sigurnost ovog kriptosustava ovisi o težini rješavanja tzv. RSA problema. RSA problem je dobivanje otvorenog teksta x iz danog javnog ključa (n, e) i šifrata $y = x^e \pmod{n}$. To je zapravo problem računanja e-tog korijena modulo n ili računanje inverza. RSA pretpostavka je pretpostavka da je RSA problem težak za slučajno odabrani otvoreni tekst x, znatno veliki n i znatno velike slučajno generirane proste brojeve p i q. Otkako je RSA osmišljen, pretpostavka se nije pokazala neispravnom.

Navedimo moguće probleme i napade na RSA kriptosustav te što će nam pomoći u njihovom spriječavanju.

2.1.1 Faktorizacija modula

Ako napadač uspije faktorizirati $n = pq$, izračunat će $\varphi(n) = (p-1)(q-1)$, pa iz $de \equiv 1 \pmod{\varphi(n)}$ primjenom Euklidovog algoritma saznaje i tajni eksponent d. Time je za sigurnost važan odabir prostih brojeva p i q. Lako je vidljivo da mali prosti brojevi p i q uzrokuju razbijanje sustava, pa poželjno odabrati velike p i q tako da svaki ima barem 100 znamenaka. Međutim, veličina p i q nije dovoljna. Ako su p i q veliki prosti brojevi čija je apsolutna razlika jako mala također narušavamo sigurnost RSA jer se tada $n = pq$ lako faktorizira korištenjem Fermatovog algoritma, odnosno traženjem prostih brojeva koji su blizu $\sqrt{n}$. Kako bi se osiguralo da se faktorizacija n ne sazna nekim poznatim algoritmima, p i q biramo tako da $p-1, p+1, q-1$ i $q+1$ imaju barem jedan veliki prost faktor. Neki poznati algoritmi faktorizacije mogu se pronaći u [1].

Opasnost za poznavanje faktorizacije predstavlja nam i poznavanje $\varphi(n)$. Ukoliko je $\varphi(n)$ poznat, n možemo faktorizirati rješavanjem sustava

$$n = pq \tag{1}$$

$$\varphi(n) = (p-1)(q-1) \tag{2}$$

odnosno iz $\varphi(n) = n - p - q + 1$ slijedi

$$p + q = n + 1 - \varphi(n). \tag{3}$$

Sada iz Vietovih formula (1) i (3) slijedi da su p i q nultočke kvadratne funkcije $x^2 - (n + 1 - \varphi(n))x + n$.

Ukoliko je poznat tajni eksponent d, onda se faktorizacija broja n može saznati iz tzv. vjerojatnosnog algoritma. Opišimo jedan takav algoritam prikazan u [2] koji pripada Las Vegas algoritmima koji ne daju uvijek odgovor, ali kada ga daju on je sigurno točan. Za sve cijele brojeve a, $(a, n) = 1$, iz $a^{ed} \equiv a \pmod{n}$ vrijedi $a^m \equiv 1 \pmod{n}$, pri čemu je $m = ed - 1$. Budući da vrijedi $de - k\varphi(n) = 1$, $k \in \mathbb{N}$ slijedi $\varphi(n)|m$, tj. m je zajednički djelitelj od $p - 1$ i $q - 1$. Broj m je paran što možemo zaključiti uvrštavanjem $a = -1$ u $a^m \equiv 1 \pmod{n}$. Pogledajmo za cijeli broj $\frac{m}{2}$ vrijedi li također ovo svojstvo. Brojeva a, $(a, n) = 1$, koji ne zadovoljavaju $a^{\frac{m}{2}} \equiv 1 \pmod{n}$, ima barem 50% jer svakom broju c za koji vrijedi $c^{\frac{m}{2}} \equiv 1 \pmod{n}$ možemo pridružiti broj a, ac, koji takvu kongruenciju ne zadovoljava. Nastavljamo dijeljenje s 2 dok god je ono moguće te dobivamo tri mogućnosti:

1. $\frac{m}{2}$ je višekratnik od $p - 1$, ali ne i od $q - 1$ te tada $a^{\frac{m}{2}} \equiv 1 \pmod{p}$ vrijedi uvijek, a $a^{\frac{m}{2}} \equiv -1 \pmod{q}$ u 50% slučajeva

2. $\frac{m}{2}$ je višekratnik od $q - 1$, ali ne i od $p - 1$, pa je to analogno slučaju 1.

3. $\frac{m}{2}$ nije višekratnik od $p-1$, ali ni od $q-1$, pa slijedi $a^{\frac{m}{2}} \equiv \pm 1 \pmod{p}$ i $a^{\frac{m}{2}} \equiv \pm 1 \pmod{q}$ pri čemu svaka mogućnost nastupa u 25% slučajeva

Stoga dobivamo vjerojatnost 50% da je a djeljiv ili sa p ili q. Ako je $a^{\frac{m}{2}} - 1$ djeljiv sa p, tada je $(a^{\frac{m}{2}} - 1, n) = p$, pa smo uspjeli faktorizirati n. Analogno u slučaju kada je $a^{\frac{m}{2}} - 1$ djeljiv sa q.
Prikažimo na sljedećem jednostavnom primjeru ideju ovakvog algoritma.

Primjer 3. *Pokušajmo pomoću javnog ključa* $(259, 5)$ *i poznatog tajnog eksponenta* $d = 173$ *otkriti faktorizaciju modula* $n = 259$.
Izračunamo $m = ed - 1 = 5 \cdot 173 - 1 = 864$, *pa time iz* $a^{ed} \equiv a \pmod{n}$ *slijedi* $a^{864} \equiv 1 \pmod{259}$ *za svaki cijeli broj* a, $(a, 259) = 1$. *Uzmimo primjerice* $a = 25$.
Broj m *je paran, pa pogledajmo vrijedi li kongruencija ako bismo zamijenili* m *s* $\frac{m}{2}$,

$$25^{432} \equiv (25^4)^{108} \equiv 1^{108} \equiv 1 \pmod{259},$$

pa nastavljamo dalje s dijeljenjem broja m *s* 2. *Tada imamo*

$$\begin{aligned} 25^{216} &\equiv (25^{18})^{24} \equiv 1^{24} \equiv 1 \pmod{259}, \\ 25^{108} &\equiv (25^{18})^{6} \equiv 1^{6} \equiv 1 \pmod{259}, \\ 25^{54} &\equiv (25^{18})^{3} \equiv 1^{3} \equiv 1 \pmod{259}, \\ 25^{27} &\equiv 25^{18} \cdot 25^{9} \equiv 36 \pmod{259}. \end{aligned}$$

Sada iz $(25^{54} - 1, 259) = 7$ *slijedi da je jedan od faktora broja* n *jednak* 7. *Dakle, drugi faktor je jednak* 37, *pa smo uspješno faktorizirali modul* 259.

2.1.2 Napad na zajednički modul

Vrlo važno je da se uvijek koristi različit broj n za različite primatelje kako bi se spriječio sljedeći napad.

Pošiljatelj koristi isti n pri slanju poruke primateljima $P_1, P_2, \ldots, P_k$ uz različite odgovarajuće eksponente e_i, d_i, $i \in \{1, \ldots, k\}$. Gustavus J. Simmons je 1983. uočio pad protokola pri slanju jednakog otvorenog teksta već kada je $k = 2$. Neka su (n, e_1) i (n, e_2) javni ključevi i x otvoreni tekst koji želimo poslati korisnicima P_1 i P_2. Pretpostavimo da su e_1 i e_2 relativno prosti. Tada računamo cijele brojeve u i v, koji zadovoljavaju $ue_1 + ve_2 = 1$, pomoću Euklidova algoritma. Poruku x možemo lako dobiti iz šifrata $y_1 = x^{e_1} \bmod n$ i $y_2 = x^{e_2} \bmod n$ računanjem $y_1^u y_2^v \pmod n$ jer vrijedi

$$y_1^u y_2^v = x^{ue_1} x^{ve_2} = x^{ue_1 + ve_2} = x.$$

Primjer 4. *Alice želi poslati poruku $x = 63$ primateljima P_1 i P_2.*
P_1 je kreirao svoj javni ključ birajući proste brojeve $p = 19$ i $q = 47$ te je dobio $n_1 = 893$. $\varphi(n_1) = (p_1 - 1)(q_1 - 1) = 18 \cdot 46 = 828$, pa za e_1 uzima primjerice $e_1 = 5$, $(e_1, \varphi(n_1)) = 1$. Javni ključ je $(893, 5)$.
P_2 bira iste proste brojeve te dobiva isti n. Za e_2 uzima $e_2 = 11$, $(e_2, \varphi(n_2)) = 1$. Javni ključ je $(893, 11)$.
Alice računa odgovarajuće šifrate za svoju poruku:

$$y_1 = 63^5 \bmod 893 = 100$$
$$y_2 = 63^{11} \bmod 893 = 435.$$

Primijetimo da su e_1 i e_2 relativno prosti, pa se iz Euklidova algoritma dobivaju cijeli brojevi $u = -2$ i $v = 1$ koji zadovoljavaju $ue_1 + ve_2 = 1$.
Eva nakon što je saznala šifrate y_1 i y_2 i izračunala u i v otkriva poruku x iz

$$y_1^u y_2^v \equiv 100^{-2} \cdot 435 \equiv 384^2 \cdot 435 \equiv 63 \pmod{89}.$$

2.1.3 Ciklički napadi

Gustavus J. Simmons i Michael J. Norris su 1977. godine uočili da se otvoreni tekst može otkriti iz ponovljenog šifriranja samog šifrata otvorenog teksta. Neka je x otvoreni tekst i $y = x^e \bmod n$ pripadni šifrat. Neka je k prirodan broj za koji vrijedi $y^{e^{k+1}} \equiv y \pmod n$, tj. nakon $k + 1$ šifriranja dobivamo polazni šifrat y. Tada slijedi $y^{e^k} \equiv x \pmod n$. Cilj ovog cikličkog napada je pronaći najmanji k za koji se pronalazi poruka x. Napad se može spriječiti korištenjem dovoljno velikog javnog eksponenta e i velikih prostih broja.

Općeniti oblik cikličkog napada kojeg su osmislili Hugh C. Williams i B. K. Schmid 1979. godine traži najmanji pozitivni cijeli broj l tako da je $(y^{e^l} - y, n) > 1$.
Ukoliko je $y^{e^l} \equiv y \pmod n$, tada je problem jednak prethodnom opisanom napadu. Ako je $y^{e^l} \equiv y \pmod p$, ali $y^{e^l} \not\equiv y \pmod q$, onda je $(y^{e^l} - y, n) = p$ i n je faktoriziran. Primijetimo da ako vrijedi $y^{e^l} \not\equiv y \pmod p$, ali $y^{e^l} \equiv y \pmod q$, također je otkrivena faktorizacija broja n jer je sada $(y^{e^l} - y, n) = q$.

Primjer 5. *Bob želi poslati Alice poruku* $x = 20$. *Alice bira proste brojeve* $p = 11$ *i* $q = 29$ *te dobiva* $n = 319$. *Računa* $\varphi(n) = 10 \cdot 28 = 280$ *te odabere primjerice* $e = 3$ *kako bi ispunila uvjet* $(e, \varphi(n)) = 1$. *Javni ključ je* $(319, 3)$. *Sada Bob može izračunati šifrat*

$$y = 20^3 \bmod 319 = 25.$$

Oscar želi saznati poruku x *iz poznatog šifrata* y. *Potrebno je da otkrije najmanji prirodan broj* k *za koji vrijedi* $25^{3^{k+1}} \equiv 25 \pmod{391}$. *Nakon* $k + 1 = 12$ *ponovnog šifriranja dobiva odgovarajući šifrat:*

$$\begin{aligned}
25^3 \bmod 319 &= 313 \\
313^3 \bmod 319 &= 103 \\
103^3 \bmod 319 &= 152 \\
152^3 \bmod 319 &= 256 \\
256^3 \bmod 319 &= 49 \\
49^3 \bmod 319 &= 257 \\
257^3 \bmod 319 &= 284 \\
284^3 \bmod 319 &= 190 \\
190^3 \bmod 319 &= 181 \\
181^3 \bmod 319 &= 169 \\
169^3 \bmod 319 &= 20 \\
20^3 \bmod 319 &= 25.
\end{aligned}$$

Sada Oscar za $k = 11$ *iz* $25^{3^9} \equiv x \pmod{391}$ *dobiva traženi otvoreni tekst* $x = 20$.
Ukoliko bi Oscar tražio najmanji pozitivan cijeli broj l *za koji je* $(25^{3^l} - 25, 391) > 1$, *dobio bi da za* $l = 6$ *je* $(25^{3^6} - 25, 391) = 29$ *te je time otkrio jedan prosti faktor javnog modula* n, *pa lako dobiva da je drugi prosti faktor jednak* 11. *Poznavajući faktorizaciju broja* n, *saznaje da je* $\varphi(n) = 280$. *Sada iz uvjeta* $de \equiv 1 \pmod{\varphi(n)}$, *Oscar saznaje da tajni eksponent iznosi* $d = 187$. *Time je sigurnost kriptosustava u potpunosti ugrožena.*

2.1.4 Napadi na mali enkripcijski eksponent

Korištenje malog enkripcijskog eksponenta e ima prednost u smanjenju broja koraka u šifriranju, ali RSA kriptosustav s vrlo malim enkripcijskim eksponentom je podložniji napadima. Dva takva napada objasnio je Johan Håstad 1985. godine.

Napad na zajednički otvoreni tekst

RSA je ugrožen kada pošiljatelj želi poslati otvoreni tekst x primateljima $P_1, P_2, \ldots, P_k$, pri čemu svaki primalac ima odgovarajući javni ključ (n_i, e), za $i \in \{1, \ldots k\}$ i $k \geq e$, pri čemu je e male vrijednosti. Sada ćemo navesti teorem koji nam govori da se u ovakvom slučaju poruka otkriva u polinomijalnom vremenu.

Teorem 3 (vidjeti [5, Teorem 3.2.]). *Neka su (n_i, e) javni ključevi za $i \in \{1, \dots k\}$, $k \geq e$. Neka su moduli u parovima relativno prosti. Svaki otvoreni tekst $x < n_i$, za svaki $i \in \{1, \dots, k\}$ uz poznate $y_i = x^e \bmod n_i$ i (n_i, e) za $i = 1 \dots k$, može se izračunati u polinomijalnom vremenu $\log(n_1 n_2 \cdot \ldots \cdot n_k)$.*

Za dokazivanje Teorema 3 potreban nam je Kineski teorem o ostacima čiji se dokaz nalazi u [3].

Teorem 4 (Kineski teorem o ostacima, vidjeti [3, Teorem 3.7.]). *Neka su $n_1, n_2, \dots n_k \in \mathbb{N}$ u parovima relativno prosti brojevi i neka su $a_1, a_2, \dots a_k \in \mathbb{Z}$. Tada sustav kongruencija $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $\dots$, $x \equiv a_k \pmod{n_k}$ ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja tog sustava jednaka $x \equiv x_0 \pmod{n_1 n_2 \dots n_k}$.*

Dokaz Teorema 3: Poznati su nam (n_i, e) i y_i za $i \in \{1, \dots k\}$. Budući da su moduli u parovima relativno prosti, primjenjujemo Kineski teorem o ostacima nad modulima n_i i šifratima y_i da izračunamo rješenje $y_0 \equiv x^e \pmod{n_1 n_2 \cdot \ldots \cdot n_k}$ sustava određenog kongruencijama

$$\begin{aligned} y &\equiv y_1 \pmod{n_1} \\ y &\equiv y_2 \pmod{n_2} \\ &\vdots \\ y &\equiv y_k \pmod{n_k}. \end{aligned}$$

Pretpostavka $x < n_i$, za svaki $i \in \{1, \dots, k\}$ povlači $x^e < n_1 n_2 \cdot \ldots \cdot n_k$. Tada je $y_0 = x^e$, pa se otkrivanje otvorenog teksta x svodi na računanje e-tog korijena iz $y_0 = x^e$.
Polinomijalno vrijeme $\log(n_1 n_2 \cdot \ldots \cdot n_k)$ potrebno nam je za sve izračune. □

Dokaz Teorema 3 opisuje potreban račun koji napadač mora provesti. Prikažimo ovaj napad na jednostavnom primjeru za $k = e = 3$.

Primjer 6. *Bob želi poslati poruku $m = 70$ primateljima P_1, P_2 i P_3 koristeći javni eksponent $e = 3$.*
Javni ključ i šifrat za P_1: Uzmimo $p_1 = 11$ i $q_1 = 23$, pa n_1 iznosi 253. Sada je $\varphi(n_1) = 10 \cdot 22 = 220$ te smo zadovoljili uvjet $(\varphi(n_1), e) = 1$. Time dobivamo javni ključ $(253, 3)$.
Šifrat c_1 koji Bob šalje je jednak

$$c_1 = 70^3 \pmod{253} = 185.$$

Analogno, za P_2 javni ključ je $(1927, 3)$ i šifrat c_2 iznosi 1921, a za P_3 javni ključ je $(4897, 3)$ i pripadni šifrat je $c_3 = 210$.
Pretpostavimo da je protivnik uspio nabaviti sva tri šifrata c_1, c_2 i c_3. Kako su moduli u parovima relativno prosti, protivnik primjenjuje Kineski teorem o ostacima na sustav:

$$x \equiv 185 \pmod{253} \tag{4}$$
$$x \equiv 1921 \pmod{1927} \tag{5}$$
$$x \equiv 210 \pmod{4897}. \tag{6}$$

Obzirom na kongruenciju (4) *rješava linearnu kongruenciju* $9436519x_1 \equiv 185 \pmod{253}$, *odnosno* $125x_1 \equiv 185 \pmod{253}$. *Budući da je* $(125, 253) = 1$, *postoje* $u, v \in \mathbb{Z}$ *takvi da je* $125u + 253v = 1$. *Primjenom Euklidova algoritma dobiva* $u = -85$ *i* $v = 42$, *pa je rješenje* $x_1 \equiv -85 \cdot 185 \equiv 168 \cdot 185 \equiv 31080 \equiv 214 \pmod{253}$.
Uzimajući u obzir (5) *i* (6) *dobiva* $x_2 \equiv 1638 \pmod{1927}$ *i* $x_3 \equiv 1490 \pmod{4897}$.
Dobiva se

$$\begin{aligned} x &\equiv 9436519 \cdot 214 + 1238941 \cdot 1638 + 487531 \cdot 1490 \\ &\equiv 4775221614 \equiv 343000 \pmod{2387439307}, \end{aligned}$$

odnosno $x = 343000$, *pa protivnik poruku dobiva iz* $m = \sqrt[3]{x} = 70$.

Opisani napad možemo onemogućiti tako da se otvorenom tekstu prije šifriranja doda zalihost, odnosno "slučajni dodatak" koji osigurava da različitim primateljima nikada ne šaljemo iste poruke. Međutim idući napad pokazuje da je dodavanjem zalihosti RSA kriptosustav s vrlo malim javnim eksponentom e i dalje nesiguran.

Napad na povezane poruke

Ovaj napad temelji se na jednom od Coppersmithovih rezultata koji nam govori o pronalasku malih rješenja po modulu. Iskažimo općeniti oblik tog rezultata.

Teorem 5 (Coppersmith, vidjeti [3, Teorem 9.3.]). *Neka je* $m \in \mathbb{N}$ *i neka je* $f(x) \in \mathbb{Z}[x]$ *normirani polinom stupnja* d *i s nultočkom* x_0 *modulo* m *koja zadovoljava uvjet* $|x_0| \leq m^{\frac{1}{d}-\epsilon}$. *Tada se* x_0 *može pronaći u vremenu koje je polinomijalno u* $\frac{1}{\epsilon}$ *i* $\log(m)$.

Pretpostavimo da u ovom napadu svi primatelji $P_1, P_2, \ldots, P_k$ imaju različite pripadne javne ključeve (n_i, e_i) za $i \in \{1, \ldots, k\}$ s malim ne nužno različitim eksponentima e_i. Pošiljatelj želi poslati otvoreni tekst x, ali primjenjujući zalihost šalje povezane poruke x_i, tj. poruke za koje vrijedi $x_i = f_i(x)$ za neki polinom f_i. Idući teorem govori nam kako je u tom slučaju moguće saznati otvoreni tekst x.

Teorem 6 (vidjeti [5, Teorem 3.3.]). *Neka su* (n_i, e_i) *javni ključevi za* $i \in \{1, \ldots k\}$. *Neka su moduli u parovima relativno prosti. Nadalje, neka su poznati polinomi* $f_i(x) \in \mathbb{Z}_{n_i}[x]$. *Ako je* $k \geq \max_i\{e_i \deg(f_i)\}$, *tada iz danih* $c_i = f_i(m)^{e_i} \pmod{n_i}$ *i* (n_i, e_i) *za* $i \in \{1, \ldots k\}$ *može se svaki otvoreni tekst* $m < n_i$, *za sve* $i \in \{1, \ldots, k\}$ *izračunati u polinomijalnom vremenu* $\log(n_1 n_2 \cdot \ldots \cdot n_k)$.

Dokaz. Pretpostavimo da je f_i normirani polinom, u suprotnom množimo polinom inverzom vodećeg koeficijenta modulo n_i. Ako ne postoji takav inverz, tada je poznata faktorizacija modula n_i, pa se lako saznaje tajni eksponent te dešifriramo c_i i dobivamo m.
Neka je $a = \max_i\{e_i \deg(f_i)\}$ i $b_i = a - \deg(f_i(x)^{e_i})$. Definirajmo normirane polinome $g \in \mathbb{Z}_{n_i}[x]$ stupnja a za $i \in \{1, \ldots k\}$ kao

$$g_i(x) = x^{b_i}(f_i(x)^{e_i} - c_i).$$

Ukoliko uvrstimo m u polinom g_i, imamo $g_i(m) = m^{b_i}(f_i(m)^{e_i} - c_i) = m^{b_i}(c_i - c_i) = 0$, odnosno za svaki $i \in \{1, \ldots, k\}$ $g_i(m) \equiv 0 \pmod{n_i}$.
Kako su moduli u parovima relativno prosti, primjenjuje se Kineski teorem o ostacima nad sustavom

$$\begin{aligned} y &\equiv g_1(x) \pmod{n_1} \\ y &\equiv g_2(x) \pmod{n_2} \\ &\vdots \\ y &\equiv g_k(x) \pmod{n_k}, \end{aligned}$$

pomoću kojega se dobiva novi polinom $G(x) \in \mathbb{Z}_{n_1 n_2 \cdot \ldots \cdot n_k}[x]$ stupnja a. Polinom G zadovoljava

$$G(m) \equiv 0 \pmod{n_1 n_2 \cdot \ldots \cdot n_k}, \tag{7}$$

odnosno m je nultočka toga polinoma.
Najmanji n_i označimo s n_{min}. Budući da je $k \geq a$, poruku m možemo omeđiti s $m < n_{min} < (n_1 n_2 \cdot \ldots \cdot n_k)^{\frac{1}{k}} < (n_1 n_2 \cdot \ldots \cdot n_k)^{\frac{1}{a}}$.
Sada iz Teorema 5 slijedi da možemo odrediti poruku m. Potrebno vrijeme za sve izračune je polinomijalno u $\log(n_1 n_2 \cdot \ldots \cdot n_k)$.

□

Dokaz Teorema 6 također kao i u prethodnom napadu opisuje potreban račun koji je potreban za otkrivanje otvorenog teksta. Otvoreni tekst m iz dokaza se određuje pomoću Coppersmithovih metoda za pronalazak rješenja koje se mogu pronaći u literaturi [5].

Primjer 7. *Otvoreni tekst $m = 15$ Alice želi poslati primateljima P_1, P_2, P_3, P_4, P_5 i P_6 čiji su javni ključevi redom $(355, 3), (583, 3), (1189, 3), (629, 5), (161, 5)$ i $(141, 5)$. Zbog veće sigurnosti, Alice će iskoristiti iduće polinome kako ne bi svim primateljima slala jednaku poruku:*

$$\begin{aligned} f_1(x) &= x^2 - 1, \\ f_2(x) &= x^2 - 7, \\ f_3(x) &= x^2 - 11, \\ f_4(x) &= x - 3, \\ f_5(x) &= x - 5, \\ f_6(x) &= x - 13. \end{aligned}$$

Sada uvrštavanjem svoje poruke $m = 15$ u odgovarajuće polinome dobiva povezane poruke,

$$f_1(m) = 224, \quad f_2(m) = 218, \quad f_3(m) = 214, \quad f_4(m) = 12, \quad f_5(m) = 10, \quad f_6(m) = 2,$$

za koje sada računa pripadne šifrate koje šalje odgovarajućem primatelju

$$\begin{aligned} c_1 &= 224^3 \bmod 355 = 124, \\ c_2 &= 218^3 \bmod 583 = 322, \\ c_3 &= 214^3 \bmod 1189 = 606, \\ c_4 &= 12^5 \bmod 629 = 377, \\ c_5 &= 10^5 \bmod 161 = 19, \\ c_6 &= 2^5 \bmod 141 = 32. \end{aligned}$$

Protivnik nakon što je saznao javne ključeve, pripadne polinome $f_1(x), \ldots, f_6(x)$ *i šifrate* $c_1, \ldots, c_6$*, računa* $a = \max_i\{e_i \deg(f_i)\} = 6$ *za* $i = 1, \ldots, 6$*. Sada računa* $b_i = a - \deg(f_i(x)^{e_i})$ *za* $i = 1, \ldots, 6$ *te dobiva*

$$b_1 = 0, \quad b_2 = 0, \quad b_3 = 0, \quad b_4 = 1, \quad b_5 = 1, \quad b_6 = 1.$$

Definira polinome oblika $g_i(x) = x^{b_i}(f_i(x)^{e_i} - c_i)$ *za* $i = 1, \ldots, 6$*, tj.*

$$\begin{aligned} g_1(x) &= x^0(x^2-1)^3 - 124) = x^6 - 3x^4 + 3x^2 - 125, \\ g_2(x) &= x^0(x^2-7)^3 - 322) = x^6 - 21x^4 + 147x^2 - 665, \\ g_3(x) &= x^0(x^2-11)^3 - 606) = x^6 - 33x^4 + 363x^2 - 1937, \\ g_4(x) &= x((x-3)^5 - 377) = x^6 - 15x^5 + 90x^4 - 270x^3 + 405x^2 - 620x, \\ g_5(x) &= x((x-5)^5 - 19) = x^6 - 25x^5 + 250x^4 - 1250x^3 + 3125x^2 - 3144x, \\ g_6(x) &= x((x-13)^5 - 32) = x^6 - 65x^5 + 1690x^4 - 21970x^3 + 142805x^2 - 371312x. \end{aligned}$$

Kako su moduli u parovima relativno prosti, protivnik rješava pripadni sustav koristeći Kineski teorem o ostacima:

$$y = x^6 - 3x^4 + 3x^2 - 125 \pmod{355} \tag{8}$$
$$y = x^6 - 21x^4 + 147x^2 - 82 \pmod{583} \tag{9}$$
$$y = x^6 - 33x^4 + 363x^2 - 748 \pmod{1189} \tag{10}$$
$$y = x^6 - 15x^5 + 90x^4 - 270x^3 + 405x^2 - 620x \pmod{629} \tag{11}$$
$$y = x^6 - 25x^5 + 89x^4 - 123x^3 + 66x^2 - 85x \pmod{161} \tag{12}$$
$$y = x^6 - 65x^5 + 139x^4 - 115x^3 + 113x^2 - 72x \pmod{141}. \tag{13}$$

Obzirom na kongrueciju (8)*, rješava kongruenciju* $9897967956723y_1 \equiv x^6 - 3x^4 + 3x^2 - 125 \pmod{355}$ *odnosno* $33y_1 \equiv x^6 - 3x^4 + 3x^2 - 125 \pmod{355}$*. Kako je* $(33, 355) = 1$*, tj.* $33u + 355v = 1$ *za neke cijele brojeve* u *i* v*, koristi Euklidov algoritam za pronalazak brojeva* $u = -43$ *i* $v = 67$ *te dobiva rješenje* $y_1 \equiv -43(x^6 - 3x^4 + 3x^2 - 125) \equiv -43x^6 - 129x^4 + 129x^2 + 50 \pmod{355}$*. Analogno dobiva rješenja preostalih kongruencija,* $y_2 \equiv -140x^6 + 25x^4 - 175x^2 + 403 \pmod{583}$*,* $y_3 \equiv -309x^6 + 685x^4 - 401x^2 + 466 \pmod{1189}$*,* $y_4 \equiv -173x^6 + 79x^5 - 474x^4 + 164x^3 - 246x^2 + 330x \pmod{629}$*,* $y_5 \equiv -72x^6 + 29x^5 - 129x^4 +$

$x^3 - 83x^2 + 2x \pmod{161}$ *i* $y_6 \equiv 13x^6 - 140x^5 + 115x^4 - 85x^3 + 59x^2 - 90x \pmod{141}$. *Sada koristeći program Wolfram Mathematica dobiva polinom stupnja* 6,

$$\begin{aligned} G(x) \equiv\ & 9897967956723(-43x^6 - 129x^4 + 129x^2 + 50) \\ & + 6027064536255(-140x^6 + 25x^4 - 175x^2 + 403) \\ & + 2955238540485(-309x^6 + 685x^4 - 401x^2 + 466) \\ & + 5586293520885(-173x^6 + 79x^5 - 474x^4 + 164x^3 - 246x^2 + 330x) \\ & + 21824711954265(-72x^6 + 29x^5 - 129x^4 + x^3 - 83x^2 + 2x) \\ & + 24920415777565(13x^6 - 140x^5 + 115x^4 - 85x^3 + 59x^2 - 90x) \\ \equiv\ & 2631144248336836x^6 + 1099154250601165x^5 + 854409723476167x^4 \\ & + 2333520132923045x^3 + 1795557666811583x^2 + 3158067490456395x \\ & + 787167941176260 \pmod{3513778624636665}, \end{aligned}$$

takav da za $x = 15$ *je* $G(15) \equiv 0 \pmod{3513778624636665}$, *odnosno poruka* m *je nultočka ovoga polinoma. Time je protivnik otkrio traženu poruku.*

Napomena 1. *Primijetimo da ukoliko moduli nisu u parovima relativno prosti u ova dva napada, protivnik će prije primjene Kineskog teorema o ostacima iskoristiti pravila djeljivosti i grupirati kongruencije čiji su moduli potencije istoga prostog broja.*

Ostali poznati napadi koji se temelje na Coppersmithovim rezultatima mogu se pogledati u [5]. Moderni sustavi uz "slučajne dodatke" koriste najčešće $e = 65537$ jer onemogućuje poznate napade na mali enkripcijski eksponent uz prednost brzog šifriranja jer u binarnom zapisu sadrži malo jedinica $65537 = 2^{16} + 1$.

2.1.5 Napad na mali dekripcijski eksponent

Iako je možda poželjno u nekim situacijama koristiti mali broj d kako bi postupak dešifriranja bio najmanji mogući, ugrožavamo sigurnost našeg kriptosustava. Objasnimo nesigurnost na Wienerovom napadu.

Michael J. Wiener je 1990. godine objavio rezultat koji nam govori o postojanju algoritma za razbijanje šifrata ukoliko je d relativno mali u odnosu na n.

Teorem 7 (Wiener, vidjeti [2, Teorem 3.1.])**.** *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.

Prije dokazivanja ovog teorema prisjetimo se verižnih razlomaka i Legendreova teorema.

Definicija 5. *Neka je* α *racionalan broj. Ako je* $a_0 \in \mathbb{Z}$ *i* $a_1, \ldots, a_n \in \mathbb{N}$ *te ako je* $\alpha = [a_0; a_1, \ldots, a_n]$, *onda ovaj izraz nazivamo razvoj broja* α *u konačni jednostavni verižni (neprekidni) razlomak. Broj* $\frac{p_i}{q_i}$ *predstavlja* i*-tu konvergentu od* α, a_i *predstavlja* i*-ti parcijalni kvocijent, a* $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ *je* i*-ti potpuni kvocijent od* α.

Razvoj od α u verižni razlomak tada izgleda:

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

Napomena 2. *Za nazivnike q_n u konvergentama razvoja verižnog razlomka α vrijedi $q_n \leq F_n$, gdje je F_n n-ti Fibonaccijev broj, što znači da je rast nazvnika konvergenti eksponencijalan.*

Teorem 8 (Legendre, vidjeti [3, Teorem 8.26])**.** *Neka su $p, q \in \mathbb{Z}$ takvi da je $q \geq 1$ i*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ neka konvergenta od α.

Dokaz Legendreova teorema može se pronaći u [3]. Pokažimo sada tvrdnju Teorema 7.

Dokaz Teorema 7: Uvjet $de \equiv 1 \pmod{n}$ povlači da postoji $k \in \mathbb{N}$ takav da je $de - k\varphi(n) = 1$, pa iz tog izraza slijedi

$$\left|\frac{e}{\varphi(n)} - \frac{k}{d}\right| = \left|\frac{de - k\varphi(n)}{d\varphi(n)}\right| = \frac{1}{d\varphi(n)}. \tag{14}$$

Time $\frac{k}{d}$ predstavlja dobru aproksimaciju od $\frac{e}{\varphi(n)}$, no $\varphi(n)$ nam je nepoznat, pa ga možemo aproksimirati s n. Kako je $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ i $0 < p + q - 1 < 3\sqrt{n}$, slijedi

$$|n - \varphi(n)| = |n - n + p + q - 1| = |p + q - 1| = p + q - 1 < 3\sqrt{n}.$$

Uvrstimo n umjesto $\varphi(n)$ u jednakost (14) te dobivamo:

$$\begin{aligned}\left|\frac{e}{n} - \frac{k}{d}\right| &= \left|\frac{ed - kn}{dn}\right| = \left|\frac{ed - k\varphi(n) - kn + k\varphi(n)}{dn}\right| \\ &= \left|\frac{1 - k(n - \varphi(n))}{dn}\right| \leq \frac{3k\sqrt{n}}{dn} = \frac{3k}{d\sqrt{n}}.\end{aligned} \tag{15}$$

Koristeći pretpostavke teorema $e < \varphi(n)$ i $d < \frac{1}{3}n^{\frac{1}{4}}$ iz izraza $de - k\varphi(n) = 1$, dobivamo $k\varphi(n) = ed - 1 < ed < d\varphi(n)$, pa slijedi $k < d < \frac{1}{3}n^{\frac{1}{4}}$. Sada (15) možemo ograničiti s

$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{1}{dn^{\frac{1}{4}}} < \frac{1}{2d^2},$$

pa iz Teorema 8 možemo zaključiti da je $\frac{k}{d}$ neka konvergenta razvoja u verižni razlomak od $\frac{e}{n}$. Prema Napomeni 2, imamo $O(\log(n))$ konvergenti od $\frac{e}{n}$ od kojih je jedna $\frac{k}{d}$. Kada izračunamo sve konvergente od $\frac{e}{n}$, provjeravamo koja konvergenta zadovoljava $x^{ed} \equiv x \pmod{n}$ za slučajno odabrani broj x što nam daje polinomijalni algoritam za otkrivanje dekripcijskog eksponenta d. □

Pogledajmo kako to funkcionira na sljedećem jednostavnom primjeru.

Primjer 8. *Neka je modul* $n = 770681$ *i javni eksponent* $e = 307565$. *Neka za tajni eksponent vrijedi* $d < \frac{1}{3}n^{\frac{1}{4}} < 9$.
Odredimo razvoj broja $\frac{e}{n} = \frac{307565}{770681}$ *u verižni razlomak:*

$$\frac{307565}{770681} = [0; 2, 1, 1, 42, 1, 44, 1, 14, 2, 2].$$

Izračunamo prvih nekoliko konvergenti:

$$\frac{p_1}{q_1} = \frac{1}{2}, \quad \frac{p_2}{q_2} = \frac{1}{3}, \quad \frac{p_3}{q_3} = \frac{2}{5}, \quad \frac{p_4}{q_4} = \frac{85}{212}, \quad \frac{p_5}{q_5} = \frac{87}{217}, \ldots$$

Budući da je $d < 9$, *vrijednost od* d *određujemo provjerom koji od nazivnika* $2, 3$ *i* 5 *zadovoljava* $(x^e)^d \equiv x \pmod{n}$ *za neki proizvoljan* x. *Dobiva se* $d = 5$.

Ostali poznati napadi na mali dekripcijski eksponent mogu se pronaći u [5].

3 Rabinov kriptosustav

Michael O. Rabin je 1979. osmislio kriptosustav koji se temelji na težini računanja kvadratnog korijena u $\mathbb{Z}_n$. Za Rabinov kriptosustav je dokazano da je njegovo razbijanje ekvivalentno rješavanju problema kvadratnog korijena po modulu n, pa time i problema faktorizacije broja n što mu daje jednu određenu teorijsku prednost naspram RSA kriptosustava za koji još nije dokazano da je razbijanje ekvivalentno problemu faktorizacije broja n.

Prikažimo postupak računanja kvadratnog korijena koji nam je potreban za definiciju funkcije dešifriranja u Rabinovom kriptosustavu. Podsjetimo se kvadratnog ostatka, Legendreova simbola i Eulerova kriterija koji će nam biti potrebni.

Definicija 6. *Neka su a i n relativno prosti cijeli brojevi i $n \geq 1$. Ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, onda kažemo da je a kvadratni ostatak modulo n. Ako kongruencija $x^2 \equiv a \pmod{n}$ nema rješenja, onda kažemo da je a kvadratni neostatak modulo n.*

Definicija 7. *Neka je a cijeli broj i p neparan prost broj. Definiramo Legendreov simbol $\left(\frac{a}{p}\right)$ na sljedeći način*

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{ako je } a \text{ kvadratni neostatak modulo } p \\ 0, & \text{ako } p \mid a \\ 1, & \text{ako je } a \text{ kvadratni ostatak modulo } p. \end{cases}$$

Primjer 9. *Kvadratni ostaci modulo 7 su $1, 2, 4$, a kvadratni neostaci modulo 7 su $3, 5, 6$. Pripadni Legendreovi simboli su*

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Za sve brojeve oblika $7k$ za neki cijeli broj k Legendreov simbol iznosi $\left(\frac{7k}{7}\right) = 0$.

Teorem 9 (Eulerov kriterij, vidjeti [3, Teorem 4.2.])**.** *Za svaki cijeli broj a i neparan prost broj p vrijedi*

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

Dokaz Eulerova kriterija može se naći u [3]. Sada možemo objasniti računanje kvadratnog korijena po modulu n.

Neka je $n = pq$, pri čemu su p i q prosti brojevi. Treba pronaći $x \in \mathbb{Z}$ (ukoliko postoji) takav da je $x^2 \equiv a \pmod{n}$ za $1 \leq a \leq n-1$, tj. da je a kvadratni ostatak modulo n. Pretpostavimo da je p neparan prost broj te da vrijedi $\left(\frac{a}{p}\right) = 1$. Tada pokušavamo efikasno pronaći x iz $x^2 \equiv a \pmod{p}$. Za male brojeve p možemo ispitati sve njegove kvadratne ostatke, no za veće brojeve p ovo nije učinkovita metoda. Međutim, za broj p oblika $p \equiv 3 \pmod{4}$, pronalazak rješenja je mnogo jednostavniji, a to je navedeno u sljedećoj propoziciji:

Propozicija 1 (vidjeti [2, Propozicija 5.6.])**.** *Ako je p prost broj sa svojstvom $p \equiv 3 \pmod{4}$ i a cijeli broj takav da $p \nmid a$, onda ako kongruencija $x^2 \equiv a \pmod{p}$ ima rješenja, ona su oblika $x^2 \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$.*

Dokaz: Budući da je a kvadratni ostatak modulo p, tj. $\left(\frac{a}{p}\right) = 1$, primjenom Eulerovog kriterija dobivamo $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, pa slijedi $x^2 \equiv (\pm a^{\frac{p+1}{4}})^2 \equiv a^{\frac{p+1}{2}} \equiv a a^{\frac{p-1}{2}} \equiv a \pmod{p}$. □

Analogno za q sa svojstvom $q \equiv 3 \pmod 4$ – ukoliko kongruencija $x^2 \equiv a \pmod{q}$ ima rješenja, ona su oblika $x \equiv \pm a^{\frac{q+1}{4}} \pmod{q}$.
Označimo s

$$\begin{aligned} r &= a^{\frac{p+1}{4}} \bmod p \\ s &= a^{\frac{q+1}{4}} \bmod q. \end{aligned} \tag{16}$$

Primjenom Kineskog teorema o ostacima na kombinaciju dva rješenja $\pm r$ kongruencije $x^2 \equiv a \pmod{p}$ i dva rješenja $\pm s$ kongruencije $x^2 \equiv a \pmod{q}$ dobivamo četiri rješenja kongruencije $x^2 \equiv a \pmod{n}$. Rješenja su oblika

$$\begin{aligned} x &= (ups + vqr) \bmod n \\ y &= (ups - vqr) \bmod n, \end{aligned} \tag{17}$$

odnosno $x, -x, y, -y$ su sva rješenja kvadratne kongruencije $x^2 \equiv a \pmod{n}$ pri čemu su u i v cijeli brojevi koji se dobiju iz $up + vq = 1$ korištenjem Euklidova algoritma.
Sada možemo definirati Rabinov kriptosustav.

Definicija 8. *Neka je $n = pq$, pri čemu su p i q prosti brojevi takvi da je $p \equiv q \equiv 3 \pmod 4$. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Neka je*

$$\mathcal{K} = \{(n, p, q) : n = pq\}.$$

Za $K \in \mathcal{K}$ definiramo funkciju šifriranja

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

i funkciju dešifriranja

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

Javni ključ je n, a tajni ključ je (p, q).

Svojstvo $p \equiv q \equiv 3 \pmod 4$ koje zadovoljavaju prosti brojevi p i q osigurava jednostavnije dešifriranje. Rabinov kriptosustav je brži nasparam RSA kriptosustava zbog korištenja kvadriranja i kvadratnog korijena. Napišimo ukratko korake kojih se potrebno pridržavati pri korištenju Rabinova kriptosustva.

Generiranje ključa:
Alice za formiranje ključeva treba učiniti sljedeće:

1. Odabrati različite proste brojeve p i q sa svojstvom $p \equiv q \equiv 3 \pmod 4$.
2. Izračunati $n = pq$.

Javni ključ je n, a tajni ključ (p, q).

Šifriranje:
Kad Bob sazna javni ključ n, on izvršava sljedeće korake nad svojim otvorenim tekstom $m \in \mathbb{Z}_n$:

1. Riješiti $c = m^2 \bmod n$ kako bi se dobio odgovarajući šifrat c.
2. Šifrat c poslati Alice.

Dešifriranje:
Za otkrivanje Bobove poruke, Alice čini sljedeće:

1. Primjenom Euklidova algoritma pronaći cijele brojeve u i v takve da vrijedi $up+vq = 1$ jer su $(p, q) = 1$.
2. Izračunati $r = c^{\frac{p+1}{4}} \bmod p$ i $s = c^{\frac{q+1}{4}} \bmod q$.
3. Izračunati $x = (ups + vqr) \bmod n$ i $y = (ups - vqr) \bmod n$.
4. Od četiri rješenja $x, -x, y, -y$ kongruencije $m^2 = c \pmod{n}$ izabrati koje rješenje predstavlja Bobov otvoreni tekst m.

Pogledajmo sada kako to funkcionira na primjeru.

Primjer 10. *Alice bira proste brojeve $p = 31$ i $q = 59$ koji zadovoljavaju $p \equiv q \equiv 3 \pmod 4$ te dobiva $n = 1829$.*
Bob želi poslati otvoreni tekst $m = 80$ Alice. Računa šifrat,

$$c = x^2 = 80^2 \bmod 1829 = 913,$$

koji šalje Alice.
Za dešifriranje poruke, Alice prvo računa cijele brojeve u i v za koje vrijedi $up + vq = 1$ te Euklidovim algoritmom dobiva $u = -19$ i $v = 10$. Primjenom formula (16) računa

$$r = c^{\frac{p+1}{4}} = 913^8 \bmod 31$$
$$s = c^{\frac{q+1}{4}} = 913^{15} \bmod 59,$$

odnosno

$$913^8 \equiv (913^2)^4 \equiv 10^4 \equiv 18 \pmod{31}$$
$$913^{15} \equiv (913^3)^5 \equiv 4^5 \equiv 21 \pmod{59}$$

i dobiva $r = 18$ i $s = 21$. Iz (17) računa x i y, tj.

$$x = (ups + vqr) = (-19 \cdot 31 \cdot 21 + 10 \cdot 59 \cdot 18) \bmod 1829 = 80$$
$$y = (ups - vqr) = (-19 \cdot 31 \cdot 21 - 10 \cdot 59 \cdot 18) \bmod 1829 = 788.$$

Sva rješenja dekripcije su 80, 1749, 788 i 1041 od kojih Alice trea na neki način odabrati Bobovu poruku.

Primijetimo da funkcija e_K nije injekcija. Dobivamo četiri kvadratna korijena modulo n, pa se dešifriranje ne može provesti na jednoznačni način ako otvoreni tekst nije smislen. Osoba bi morala sama izabrati traženi otvoreni tekst. U cilju da dešifriranjem dobijemo točan polazni otvoreni tekst, u otvoreni tekst unosimo na umjetan način određenu pravilnost, odnosno zalihost poput dodavanja dodatnih bitova informacije za rješenje.

Hugh C. Williams je 1980. dao drukčiji pristup problemu injekcije uz modifikaciju Rabinovog kriptosustava. Podsjetimo se definicije Jacobijeva simbola i njegovih svojstava.

Definicija 9. *Neka je a cijeli broj i neka je $n = \prod_{i=1}^{n} p_i^{\alpha_i}$ neparan prirodan broj, pri čemu su p_i neparni prosti brojevi i $\alpha_i \in \mathbb{N}$. Tada definiramo Jacobijev simbol $\left(\frac{a}{n}\right)$ kao produkt Legendreovih simbola, tj.*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{n} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

Navedimo sada najbitnija svojstva Jacobijeva simbola.

Propozicija 2 (vidjeti [7, Teorem 1.24.])**.** *Neka su n_1 i n_2 neparni prirodni brojevi i $a_1, a_2 \in \mathbb{Z}$. Tada vrijedi:*

a) $\left(\frac{a}{n_1}\right) = \left(\frac{a \pmod{n_1}}{n_1}\right)$;

b) $\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right)$;

c) $\left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$;

d) $\left(\frac{-1}{n_1}\right) = (-1)^{\frac{n_1-1}{2}}$;

e) $\left(\frac{2}{n_1}\right) = (-1)^{\frac{n_1^2-1}{8}}$;

f) Ako je $(n_1, n_2) = 1$, onda $\left(\frac{n_1}{n_2}\right) = (-1)^{\frac{(n_1^2-1)(n_2^2-1)}{4}} \left(\frac{n_2}{n_1}\right)$.

Dokaz Propozicije 2 može se pronaći u [7].

Sada možemo konstruirati postupak opisan u [4]. Umjesto $p \equiv q \equiv 3 \pmod 4$ odaberimo p i q takve da je zadovoljeno $p \equiv 3 \pmod 8$ i $q \equiv 7 \pmod 8$. Otvoreni tekst $1 \leq m < \frac{n}{8} - 1$ možemo zamijeniti s parnim cijelim brojem x za koji je Jacobijev simbol jednak $\left(\frac{x}{n}\right) = 1$ ako je:

$$x = \begin{cases} 4(2m+1), & \text{ako vrijedi } \left(\frac{2m+1}{n}\right) = 1 \\ 2(2m+1), & \text{ako vrijedi } \left(\frac{2m+1}{n}\right) = -1. \end{cases}$$

Sada šifrat računamo iz $c = x^2 \mod n$. U dešifriranju pri rješavanju kvadratnih korijena tražimo paran broj $1 < x < n$ koji zadovoljava $\left(\frac{x}{n}\right) = 1$ i $x^2 \equiv c \pmod n$. Dešifriranjem dobivamo:

$$m = \frac{\frac{x}{2} - 1}{2}, \text{ za } x \equiv 2 \pmod 4$$
$$m = \frac{\frac{x}{4} - 1}{2}, \text{ za } x \equiv 0 \pmod 4.$$

Ovim postupkom uvodi se dodatan račun za izračunavanje Jacobijeva simbola zbog čega gubimo na brzini, ali osigurava se ispravan odabir otvorenog teksta. Rabinov kriptosustav uz Williamsove modifikacije naziva se *Rabin – Williamsov kriptosustav.* Objasnimo ga na sljedećem primjeru:

Primjer 11. *Alice bira proste brojeve $p = 19$ i $q = 23$ koji zadovoljavaju uvjete $p \equiv 3 \pmod 8$ i $q \equiv 7 \pmod 8$. Tada je $n = 437$ i šalje ga Bobu.*
Bob želi poslati svoju poruku $m = 32$ za koju vrijedi $1 \leq 32 < \frac{437}{8} - 1$. Primjenjujući svojstva Jacobijeva simbola, Bob dobiva da je

$$\left(\frac{2m+1}{n}\right) = \left(\frac{65}{437}\right) = \left(\frac{65}{19}\right)\left(\frac{65}{23}\right) = \left(\frac{5}{19}\right)\left(\frac{13}{19}\right)\left(\frac{5}{23}\right)\left(\frac{13}{23}\right) = 1(-1)(-1)1 = 1,$$

pa je $x = 4(2m+1) = 4 \cdot 65 = 260$. Odgovarajući šifrat dobiva iz $c = x^2 \bmod n$, odnosno

$$c = x^2 = 260^2 \bmod 437 = 302$$

koji šalje Alice.
Kako bi otkrila poruku, Alice traži cijele brojeve u i v koji zadovoljavaju uvjet $up + vq = 1$. Uz pomoć Euklidova algoritma dobiva da je $u = -6$ i $v = 5$. Sada računa r i s primjenom formula (16) i dobiva

$$r = c^{\frac{p+1}{4}} = 302^5 \bmod 19$$
$$s = c^{\frac{q+1}{4}} = 302^6 \bmod 23,$$

odnosno

$$302^5 \equiv (2 \cdot 151)^5 \equiv 2^5 \cdot (151^2)^2 \cdot 151 \equiv 13 \cdot 1 \cdot 151 \equiv 6 \pmod{19}$$
$$302^6 \equiv (2 \cdot 151)^6 \equiv 2^6 \cdot (151^2)^3 \equiv 18 \cdot 8^3 \equiv 18 \cdot 6 \equiv 16 \pmod{23},$$

tj. $r = 6$, a $s = 16$. Može izračunati x i y iz formula (17), tj.

$$x = (ups + vqr) = (-6 \cdot 19 \cdot 16 + 5 \cdot 23 \cdot 6) \bmod 437 = 260$$
$$y = (ups - vqr) = (-6 \cdot 19 \cdot 16 - 5 \cdot 23 \cdot 6) \bmod 437 = 788.$$

Sva rješenja dešifriranja su 260, 177, 329 i 108.
Alice primjećuje da jedini paran za koji je Jacobijev simbol jednak jedan iznosi 260. Budući da je $260 \equiv 0 \pmod 4$, Bobov otvoreni tekst je

$$m = \frac{\frac{260}{4} - 1}{2} = \frac{64}{2} = 32.$$

3.1 Sigurnost i kriptoanaliza Rabinova kriptosustava

Spomenuli smo kako se Rabinova sigurnost temelji na problemu rješavanja kvadratnog korijena modulo n. Očito je da poznavanje faktorizacije broja n rješava i problem kvadratnog korijena.

Biranjem velikih prostih brojeva p i q za koje ne možemo primijeniti poznate algoritme faktorizacije (kao i u RSA kriptosustavu) osiguravamo da je faktorizacija njihovog produkta $n = pq$ gotovo nemoguća u razumnom vremenu.

Ovaj kriptosustav je također podložan napadima na mali eksponent (najčešće $e = 2$) opisanih u RSA kriptosustavu, no istaknimo jedan napad koji značajno narušava sigurnost ovog kriptosustava. To je napad na odabrani šifrat opisan u [6] na sljedeći način.

Neka protivnik za svoj otvoreni tekst m_1, takav da zadovoljava $(m_1, n) = 1$, izračuna šifrat $c_1 = m_1^2 \bmod n$. Pretpostavimo da je protivnik uspio na neki način nagovoriti pošiljatelja da dešifrira šifrat c_1 sa svojim tajnim ključem te dešifriranjem dobiva neki otvoreni tekst m_2. Ukoliko je $m_2 \not\equiv \pm m_1 \pmod{n}$ bira se novi m_1 i ponavlja se postupak. Ako je $m_2 \equiv \pm m_1 \pmod{n}$, onda se iz $n \mid (m_1 - m_2)(m_1 + m_2)$ dobiva da je $(m_1 - m_2, n)$ jedan od prostih faktora broja n. Vjerojatnost faktorizacije n je $\frac{1}{2}$ jer postoje četiri kvadratna korijena c_1 modulo n. Općenito, vjerojatnost da će protivnik uspješno faktorizirati n nakon što uspije nagovoriti pošiljatelja za dešifriranje k šifrata iznosi $1 - \frac{1}{2^k}$. Ovim postupkom pokazali smo i da iz problema kvadratnog korijena modulo n možemo doći do faktorizacije n, pa je poznavanje faktorizacije n ekvivalentno problemu kvadratnog korijena modulo n.

Primijetimo da je RSA također osjetljiv na ovakav napad. Kako bi dešifrirao šifrat c, protivnik će izračunati $c_1 = cm_1^e \bmod n$ za svoj odabrani otvoreni tekst m_1 te nagovoriti pošiljatelja da dešifrira c_1. Dobiva se mm_1 iz kojeg se lagano izračuna otvoreni tekst m šifrata c. Protivnik napadom na RSA kriptosustav dobiva samo jednu poruku, ali tajni ključ ostaje i dalje nepoznat što je u Rabinovom kriptosustavu ugroženo.

Napad se ipak može spriječiti upotrebom već spomenute određene zalihosti koja omogućuje dobivanje traženog otvorenog teksta. Ukoliko protivnik da svoj šifrat $c = m^2 \bmod n$ pošiljatelju, pri čemu je m poruka s potrebnom zalihosti, dešifriranjem će dobiti s velikom vjerojatnošću svoj polazni otvoreni tekst m jer preostala tri rješenja najvjerojatnije ne sadrže određenu zalihost. Šifriranje otvorenog teksta m bez zalihosti rezultirat će također neuspjehom jer s velikom vjerojatnoću nijedan od četiri korijena neće sadržavati potrebnu zalihost. Time u oba slučaja protivnik neće moći saznati neku novu informaciju koja bi mu pomogla u razbijanju kriptosustava.

Literatura

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

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

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[4] S. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, Cambridge, 2012.

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

[6] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.

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