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

**Juro Ivančić**

# Napadi na RSA kriptosustav

Završni rad

Osijek, 2015.

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

**Juro Ivančić**

# Napadi na RSA kriptosustav

Završni rad

Mentor: doc. dr. sc. Ivan Matić

Osijek, 2015.

# Sadržaj

# Sažetak

Problem uspostave sigurne komunikacije preko nesigurnog komunikacijskog kanala je predmet istraživanja kriptografije, a danas najpoznatiji kriptosustav je RSA. RSA kriptosustav je kriptosustav s javnim ključem, što znači da biramo javne i tajne parametre, koje koristimo za šifriranje i dešifriranje. Sustav je dosta siguran sve do trenutka kada protivnik, koji je u stanju presresti šifriranu poruku i želi saznati izvorni tekst, otkrije tajne parametre. Brojni su napadi na RSA kriptosustav, a oni mogu biti posljedica klasičnih pogrešaka korištenja RSA, pa sve do pogrešnog odabira parametara. Poznato je kako korištenje zajedničkog modula ili potpisivanje protivnikove nasumične „slijepe“ poruke može dovesti do razbijanja RSA. Isto tako i pogrešan odabir parametara može dovesti do razbijanja RSA kriptosustava, što je Wiener pokazao u slučaju odabira malog tajnog ključa i Hastad, uz pomoć Coppersmithovog rezultata i LLL algoritma, u slučaju odabira malog javnog ključa.



**Ključne riječi:** *Kriptografija, RSA kriptosustav, Elementarni napadi, Wienerov napad, Hastadov napad*



# Abstract

The problem of establishing safe communication through an unsecure communication channel is cryptography's subject of study. Today's most famous cryptosystem is RSA. The RSA is a cryptosystem with a public key, which means that we are the ones who choose public and private parameters used for coding and decoding. The system is fairly secure up until when the adversary, who is capable of intercepting an encrypted message and wants to find out the original text, discovers secret parameters. There are numerous attacks on RSA cryptosystem, and they can be anything, from a result of typical mistakes while using the RSA, to a wrong choice of parameters. It is known how using a common modulus or signing the adversary's random „blind“ message can result in breaking the RSA system. Equally, a wrong choice of parameters can also lead to breaking of the RSA, as Wiener showed in case of using a low private key and Hastad, with help of Coppersmith's results and the LLL algorythm, in case of using a low public key.



**Keywords:** *Cryptography, RSA Cryptosystem, Elementary Attacks, Wiener's Attack, Hastad's Attack*

# 1 Uvod

Kriptografija je znanstvena disciplina čiji je temeljni zadatak omogućiti dvjema osobama, od kojih je jedna pošiljatelj (osoba koja želi poslati poruku), a druga primatelj (osoba kojoj se poruka šalje), da komuniciraju preko nesigurnog komunikacijskog kanala. Komunikacija se treba odigrati na način da treća osoba (njihov protivnik) ne može razumjeti poruku. Poruku koju pošiljatelj želi poslati nazivamo otvoreni tekst. Pošiljatelj transformira otvoreni tekst uz pomoć unaprijed dogovorenog ključa, a postupak transformiranja otvorenog teksta se naziva šifriranje (kriptiranje), dok se dobiveni rezultat naziva šifrat (kriptirana poruka). Šifrat se šalje preko komunikacijskog kanala, te protivnik može doznati šifrat, ali mu sadržaj otvorenog teksta ostaje nepoznat, jer ne poznaje ključ. Međutim, primatelj, koji poznaje ključ, može dešifrirati šifrat i odrediti otvoreni tekst.

**Definicija 1.1** *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \varepsilon, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih elemenata otvorenog teksta.*
2. $\mathcal{C}$ *je konačan skup svih elemenata šifrata.*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva.*
4. *Za svaki ključ* $K \in \mathcal{K}$ *postoji algoritam šifriranja* $e_K \in \varepsilon$ *i odgovarajući algoritam 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 da je*

$$d_K(e_K(x)) = x$$

*za svaki otvoreni tekst* $x \in \mathcal{P}$*.*

S obzirom na tajnost ključa, kriptosustave možemo podijeliti na:

1. *Simetrične kriptosustave* koji se još nazivaju i **kriptosustavi s tajnim ključem**, jer im sigurnost leži u tajnosti ključa, a ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno.
2. *Asimetrične kriptosustave* koji se još nazivaju i **kriptosustavi s javnim ključem**, jer je ključ za šifriranje svima poznat i bilo tko može šifrirati poruku, ali samo osoba koja poznaje ključ za dešifriranje može dešifrirati poruku. Bitna razlika asimetričnih kriptosustava je da se ključ za dešifriranje ne može izračunati iz poznatog ključa za šifriranje, što je bio slučaj kod simetričnih kriptosustava.

Nedostatak simetričnih kriptosustava je nemogućnost razmjene tajnog ključa u slučajima kada su pošiljatelj i primatelj na velikoj udaljenosti, a komunikacijski kanali s kojima raspolažu su dosta nesigurni. Isto tako, tajni ključ se mora često mijenjati, jer često šifriranje istim tajnim ključem smanjuje sigurnost.

Whitfield Diffie i Martin Hellman su 1976. godine iznijeli ideju kriptosustava s tajnim ključem. Njihova ideja se temeljila na činjenici da za kriptiranje otvorenog teksta koriste

funkciju $e_K$, iz koje se iz praktičnih razloga i u nekom razumnom vremenu, ne može izračunati funkcija $d_K$ (funkcija za dešifriranje). Korištenje funkcije $e_K$ bi moglo imati značajnu prednost u odnosu na simetrične kriptosustave, jer bi ona mogla biti javna i razmjena ključa za šifriranje bi bila olakšana.

U kriptosustavu s javnim ključem se koriste osobne jednosmjerne funkcije. Za funkciju $f\colon X \to Y$ kažemo da je jednosmjerna funkcija, ako je $f(x)$ lako izračunati za svaki $x \in X$, ali je $f^{-1}(x)$ jako teško izračunati. Ako je $f^{-1}$ lako izračunati ako nam je poznat neki dodatni podatak, onda za funkciju $f$ kažemo da je osobna jednosmjerna funkcija.

Kriptosustav s javnim ključem se realizira upotrebom funkcije za šifriranje $e_K$ i funkcije za dešifriranje $d_K$, gdje je $K$ skup svih mogućih korisnika. Vrijede sljedeća svojstva:

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

Ključ $e_K$ se zove javni ključ, a $d_K$ se zove tajni ili vlastiti ključ.

Ako pošiljatelj (A) želi poslati poruku $x$ primatelju (B) potrebno je napraviti sljedeće:

1. primatelj pošalje pošiljatelju svoj javni ključ $e_B$
2. pošiljatelj pomoću $e_B$ šifrira otvoreni tekst i primatelju pošalje šifrat $y = e_B(x)$
3. primatelj dešifrira šifrat pomoću svog tajnog ključa $d_B$ i dobije otvoreni tekst:

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

Ideju koju su iznijeli Whitfield Diffie i Martin Hellman su iskoristili Ronald Rivest, Adi Shamir i Leonard Adleman, te su 1977. godine izumili prvi i najšire korišteni kriptosustav s javnim ključem.

# 2 RSA kriptosustav

RSA kriptosustav je prvi i najšire korišteni kriptosustav s javnim ključem, koji je dobio ime prema svojim izumiteljima (Rivest, Shamir, Adleman). Parametri kojima se realizira RSA kriptosustav su modul $n$, koji je produkt dva velika prosta broja $p$ i $q$, te eksponenti $e$ i $d$, koji se koriste za šifriranje i dešifriranje.

**Definicija 2.1** *Neka je n=pq gdje su p i q prosti brojevi. Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n = 0, 1, ..., n-1$, *te*

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

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

$$e_K(x) = x^e \bmod n, \quad d_K(x) = y^d \bmod n.$$

Broj $e$ se zove enkripcijski, a $d$ dekripcijski eksponent. Vrijednosti $n$ i $e$ su javne, a vrijednosti $p$, $q$ i $d$ su tajne, pa zbog toga ($n$,$e$) nazivamo javni, a ($p$,$q$,$d$) tajni ključ. $\varphi(n) = (p-1)(q-1)$ je Eulerova funkcija, a kako za Eulerovu funkciju vrijedi da je $a^{\varphi(n)} \equiv 1 \pmod{n}$ za (a,n)=1, slijedi da su funkcije $e_K$ i $d_K$ jedna drugoj inverzne. U standardnom RSA kriptosustavu dodatno još pretpostavljamo da $p$ i $q$ imaju približno jednaki broj bitova (što se naziva balansirani RSA), te da je $e < n$.

## 2.1 Implementacija RSA kriptosustava

1. Tajno biramo dva prirodna prosta broja $p$ i $q$. Brojevi bi trebali imati oko 100 znamenaka (oko 512 bitova) i jedan od njih bi trebao imati nekoliko znamenaka više od drugog. $p$ i $q$ biramo tako da pomoću nekog generatora slučajnih brojeva generiramo dovoljno velik prirodan broj $m$, a zatim korištenjem nekog testa prostosti (npr. Miller-Rabinov test prostosti (vidjeti [5])) tražimo prvi prost broj koji je veći ili jednak od $m$.

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

3. Izaberemo broj $e$ takav da je $e < \varphi(n)$ i $(\varphi(n), e) = 1$. Zatim se pomoću Euklidovog algoritma izračuna $d$ takav da je $de \equiv 1 \pmod{\varphi(n)}$.

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

Računanje šifrata $e_k(x) = x^e \bmod n$ se naziva modularno potenciranje. Modularno potenciranje se može vrlo efikasno računati pomoću algoritma "kvadriraj i množi". Broj $e$ se prikaže u bazi 2:

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

a zatim se primijeni algoritam.

**Kvadriraj i množi**
$y = 1$
for $(s - 1 \geq i \geq 0)\{$
$y = y^2 \bmod n$
if $(e_i = 1)$ then $y = y \cdot x \bmod n$ $\}$

Ukupan broj množenja $\leq 2s$, pa je ukupan broj operacija $O(\log e \cdot \log^2 n)$, što će značiti da je ovaj algoritam polinomijalan.

**Primjer 2.2** *U RSA kriptosustavu s javnim ključem* $(2047, 411)$ *treba dešifrirati poruku "BP" u engleskom alfabetu.*

Faktorizacijom $n = 2047$ i $e = 411$, dobivamo $n = 23 \cdot 89$, $e = 3 \cdot 137$, pa je $\varphi(n) = \varphi(23 \cdot 89) = 1936$. Iz $(e, \varphi(n)) = (411, 1936) = 1$ slijedi kako postoje $d, l \in \mathbb{Z}$ takvi da je $411d + 1936l = 1$. Zatim primjenimo Euklidov algoritam:

$$\begin{aligned} 1936 &= 411 \cdot 4 + 292 \\ 411 &= 292 \cdot 1 + 119 \\ 292 &= 119 \cdot 2 + 54 \\ 119 &= 54 \cdot 2 + 11 \\ 54 &= 11 \cdot 4 + 10 \\ 11 &= 10 \cdot 1 + 1 \\ 10 &= 1 \cdot 10 + 0. \end{aligned}$$

| $i$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ |
|---|---|---|---|---|---|---|---|---|
| $q_i$ | | | $4$ | $1$ | $2$ | $2$ | $4$ | $1$ |
| $d_i$ | $0$ | $1$ | $-4$ | $5$ | $-14$ | $33$ | $-146$ | $179$ |

Iz tablice vidimo da je $d = 179$. Šifratu "BP" pridružujemo numerički eksponent

$$2 \quad 16$$

i dešifriramo pomoću funkcije

$$d_K(y) = y^{179} \,(\text{mod } 2047), \quad za\ y = 2, 16.$$

Dobivamo

$$d_K(2) = 2^{179} \,(\text{mod } 2047) = 8$$

$$d_K(16) = 16^{179} \,(\text{mod } 2047)) = 2,$$

pa je otvoreni tekst jedna "HB".

Ako bi željeli provesti inverzan postupak, šifrirali bi funkcijom

$$x_K = x^{411} \,(\text{mod } 2047), \quad za\ x = 8, 2.$$

Dobivamo

$$e_K(8) = 8^{411} \pmod{2047} = 2$$
$$e_K(2) = 2^{411} \pmod{2047}) = 16,$$

pa je šifrat jednak "BP".

## 2.2 Sigurnost i nedostatci RSA kriptosustava

Iako je prethodno opisana implementacija RSA kriptosustava prilično jednostavna, RSA kriptosustav je dosta siguran. Sigurnost RSA kriptosustava se temelji na teškoći faktorizacije velikih prirodnih brojeva, te na pretpostavci da je funkcija $e_K(x) = x^e \pmod{n}$ jednosmjerna (kao što smo već rekli jednosmjerna funkcija $f$ je ona kod koje je relativno lagano odrediti $y = f(x)$, ali je vrlo teško odrediti $x = f^{-1}(y)$).

Napad na RSA će omogućiti poznavanje faktorizacije broja $n$. Kada protivnik faktorizira $n$, on može lako otkriti i $\varphi(n) = (p-1)(q-1)$, te na kraju izračunati $d$ iz $de \equiv 1 \pmod{\varphi(n)}$ pomoću proširenog Euklidovog algoritma.

Međutim, sigurnost RSA se temelji na tome da brojeve $p$ i $q$ koje uzimamo imaju oko 100 znamenaka, a to znači da $n = pq$ ima oko 200 znamenaka. Za faktorizaciju takvog $n$, primitivnom metodom dijeljenja sa svim prostim brojevima manjim od $\sqrt{n}$, uz pomoć računala koje može u sekundi izvršiti $10^9$ takvih dijeljenja, trebalo bi otprilike $10^{81}$ godina. Postoje i mnogo brži algoritmi za faktorizaciju, ali su brojevi od oko 200 znamenki ipak sigurni od takvih napada. Trenutno najbrži algoritmi za faktorizaciju trebaju $O(e^{c(\log(n))^{1/3}(\log(\log(n))^{2/3}})$ operacija, što znači da nije poznat niti jedan polinomijalan algoritam za faktorizaciju.

Postoje i slučajevi kada je $n$ lakše faktorizirati nego inače, uz odabir $p$ i $q$ specijalnog oblika. Treba paziti da brojevi $p \pm 1$ i $q \pm 1$ imaju barem jedan veliki prosti faktor, jer postoje metode za faktorizaciju brojeva koji imaju prosti faktor $p$ takav da je jedan od brojeva $p+1$, $p-1$ "gladak", tj. ima samo male proste faktore. Isto tako, brojevi $p$ i $q$ ne smiju biti jako blizu jedan drugom, jer ih se onda može naći koristeći činjenicu da su približno jednaki $\sqrt{n}$. Takve slučajeve treba izbjegavati pri izboru parametara za RSA kriptosustav.

Poznato je da je broj operacija za modularno potenciranje linearna funkcija u broju bitova eksponenta. Zbog toga se dobrom idejom čini izabrati parametre RSA kriptosustava tako da jedan od eksponenata $e$ ili $d$ bude mali. Odabir malog javnog eksponenta $e$ bi mogao bitno smanjiti vrijeme potrebno za šifriranje, a odabir malog tajnog eksponenta $d$ bi mogao bitno smanjiti vrijeme potrebno za dešifriranje. No, u sljedećim poglavljima ćemo vidjeti da takav izbor eksponenata predstavlja opasnost za sigurnost RSA kriptosustava.

RSA kriptosustav je dosta siguran uz javne podatke $n$ i $e$, ali uz tajnost podataka $p$, $q$ i $d$. Sada ćemo prikazati neke od napada na RSA kriptosustav, što će protivniku omogućiti da sazna neke od tajnih podataka.

# 3 Elementarni napadi

Elementarni napadi su stariji napadi na RSA kriptosustav, te ilustriraju neke od klasičnih pogrešaka u javnom korištenju RSA kriptosustava. Brojni su takvi napadi, a ovdje ćemo navesti dva primjera.

## 3.1 Zajednički modul

Da bi izbjegli generiranje različitih modula $n = pq$, bilo bi poželjno da se izabere jedan "dobar" $n$, koji će se koristiti cijelo vrijeme. Izabrani $n$ bi koristili svi korisnici. Korisnik $i$ bi definirao jedinstvene brojeve $d_i, e_i$ pomoću kojih bi formirao javni ključ $(n, e_i)$ i tajni ključ $(n, d_i)$.

Na prvi pogled ovo se ne čini lošom idejom: šifrat $C = M^{e_a} \bmod n$, koji je namijenjen primatelju, ne može biti dešifriran od strane protivnika, jer protivnik ne posjeduje $d_a$. Međutim, ovo je netočno i sustav je nesiguran.

**Lema 3.1** *Poznavanje tajnog eksponenta d, koji odgovara javnim n i e, može omogućiti faktorizaciju od n.*

Poznato je da, ako je zadan javni ključ $(n, e)$, iz zadanog privatnog ključa $d$ može se učinkovito faktorizirati modul $n = pq$. Isto tako vrijedi i obrat, iz zadane faktorizacije od $n$, može se učinkovito otkriti $d$.

Zbog toga ideja da se izabere jedan $n$ za sve, a da se korisnicima tajno dodijele parovi $e_k$ i $d_k$, nije dobra iz dva razloga. Jedan razlog je taj što bi korisnik A, na osnovu svojih $e_a$ i $d_a$, mogao faktorizirati $n$ i odrediti $p$ i $q$, pa bi zbog posjedovanja $e_b$ i poznavanja faktorizacije od $n$, a samim tim i vrijednosti $\varphi(n)$, mogao otkriti i $d_b$ za svakog drugog korisnika. Drugi razlog je da bi protivnik otkrivanjem jednog $d_k$ došao u poziciju tog korisnika, pa bi se mogao postaviti u ulogu korisnika A i otkriti sve tajne eksponente $d_k$. Ovo objašnjenje pokazuje da RSA modul ne bi smjelo koristiti više korisnika.

## 3.2 Blinding

Pored toga što u kriptosustavima s javnim ključem nema potrebe za sigurnim komunikacijskim kanalom, jedna od prednosti im je i mogućnost potpisa poruke. Ukoliko imamo grupu korisnika i svi žele međusobno komunicirati pomoću RSA kriptsustava, onda se svi javni ključevi stave u neku javnu datoteku, koja je svima dostupna, te datoteka mora biti takva da nitko ne može promijeniti ničiji javni ključ. Ako pošiljatelj želi poslati poruku primatelju dovoljno je da iz datoteke pročita javni ključ primatelja $e_b$ i izvrši šifriranje. Problem autentičnosti poruke, tj. problem na koji će način primatelj (B) znati da mu je poruka stigla od nekog određenog pošiljatelja (A), se vrlo lako rješava korištenjem potpisa $P$. Neka je $P$ potpis pošiljatelja, koji može sadržavati ime, JMBG, ili neki drugi podatak. Budući da svi korisnici zajedničke datoteke javnih ključeva znaju $e_B$, nije dovoljno da

pošiljatelj pošalje poruku $e_B(P)$. Zbog toga, pošiljatelj na početku ili na kraju poruke dopiše $e_B d_A(P)$. Primatelj šifrat dešifrira pomoću $d_B$ i dobije tekst poruke i dio $d_A(P)$. Kako primatelj zna da bi ta poruka trebala biti od pošiljatelja koji koristi $d_A$, on koristi njegov javni ključ $e_A$ i dešifrira $d_A(P)$, te dobije $P$. Kako nijedan drugi korisnik osim korisnika A ne poznaje $d_A$, nitko drugi nije mogao poruku potpisati na taj način.

Neka je $(n, d)$ pošiljateljev tajni ključ i $(n, e)$ njegov odgovarajući javni ključ. Pretpostavimo da protivnik želi pošiljateljev potpis na poruci $M \in \mathbb{Z}_n^*$. Pošiljatelj naravno odbija. Protivnik može pokušati sljedeće: izabrat će bilo koji $r \in \mathbb{Z}_n^*$ i postaviti $M' = r^e M \bmod n$. Zatim zamoli pošiljatelja da potiše poruku $M'$. Pošiljatelj je možda voljan dati svoj potpis $S'$ u ovom slučaju, ali znamo da vrijedi $S' = (M')^d \bmod n$. Protivnik sada jednostavno može izračunati $S = S'/r \bmod n$ i tako dobiti pošiljateljev potpis $S$ za orginalni $M$. Doista,

$$S^e = (S')^e/r^e = (M')^{ed}/r^e \equiv M'/r^e \equiv M \pmod{n}.$$

Ovaj postupak, nazvan *blinding*, omogućuje protivniku da dobije važeći potpis na poruku svog izbora preko nasumične "slijepe" poruke. Pošiljatelj zapravo ne zna koju poruku potpisuje. Iako smo ovdje *blinding* predstavili kao napad na RSA kriptosustav, ovo je zapravo jedno korisno svojstvo RSA kriptosustava provedeno kod digitalnog novca (novac koji se može koristiti za kupnju, ali ne otkriva identitet osobe pri kupnji).

# 4 Napadi na RSA s malim tajnim eksponentom

Kao što smo već rekli, broj operacija za modularno potenciranje je linearna funkcija u broju bitova eksponenta, pa bi zbog toga odabir malog javnog ili tajnog eksponenta mogao bitno smanjiti vrijeme potrebno za šifriranje, odnosno dešifriranje. To je posebno značajno kada u komunikaciji sudjeluju dva uređaja koji se bitno razlikuju u snazi, npr. "pametna kartica" i centralno računalo. U ovom slučaju bi bilo dobro dodijeliti kartici mali tajni eksponent, a računalu mali javni eksponent i na taj način bi se minimizirao dio računanja koje treba provesti kartica. Međutim, takav izbor parametara je nesiguran i može dovesti do razbijanja RSA kriptosustava.

Wiener je 1990. godine pokazao da za sigurnost RSA kriptosustava treba izbjegavati mali tajni eksponent $d$. Opisao je polinomijalan algoritam za razbijanje standardnog RSA kriptosustava ukoliko je izabran mali tajni eksponent $d$. Taj algoritam, poznat kao Wienerov napad na RSA kriptosustav, je opisan sljedećim teoremom.

## 4.1 Wienerov napad na RSA kriptosustav

**Teorem 4.1** *Neka je $n = pq$ i $n < q < 2p$, te neka je $e < \varphi(n)$ i $d < \frac{1}{3}n^{0.25}$. Tada postoji polinomijalni algoritam koji iz poznavanja $n$ i $e$ izračunava $d$.*

*Dokaz* : Iz $ed \equiv 1 \pmod{\varphi(n)}$ slijedi da postoji prirodan broj $k$ takav da je $ed - k\varphi(n) = 1$. Odavde je

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

Dakle, $\frac{k}{d}$ je dobra aproksimacija od $\frac{e}{\varphi(n)}$. Međutim, $\varphi(n)$ je nepoznat. Stoga ćemo $\varphi(n)$ aproksimirati s $n$. Iz $\varphi(n) = n - p - q + 1$ i $p + q - 1 < 3\sqrt{n}$ slijedi $|n - \varphi(n)| < 3\sqrt{n}$. Zamijenimo $\varphi(n)$ s $n$ u (1), pa dobivamo

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

$$\leq \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}.$$

Sada je $k\varphi(n) = ed - 1 < ed$, pa iz $e < \varphi(n)$ (standardna pretpostavka u RSA kriptosustavu), slijedi $k < d < \frac{1}{3}n^{0.25}$, te dobivamo

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

Nadalje će nam u dokazu trebati sljedeći rezultat.

**Teorem 4.2 (Legendre)** *Neka su p,q cijeli brojevi takvi da je $q \geq 1$ i*

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

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

Iz Legenderovog teorema slijedi da relacija (2) povlači 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 slijedi da imamo $O(\log n)$ 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 $(x^e)^d \equiv x \pmod{n}$ za slučajno odabran broj $x$. To daje polinomijalni algoritam za otkrivanje tajnog ključa $d$.

Drugi način za testiranje točnosti pretpostavke da je neka konkretna konvergenta jednaka $\frac{k}{d}$, jest da se, uz tu pretpostavku, izračuna $\varphi(n) = (p-1)(q-1) = (ed-1)/k$. Tada se može izračunati $\frac{p+q}{2}$ iz identiteta:

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

te $\frac{q-p}{2}$ iz identiteta:

$$\left(\frac{p+q}{2}\right)^2 - pq = \left(\frac{q-p}{2}\right)^2.$$

Ako se na ovaj način dobije da su brojevi $\frac{p+q}{2}$ i $\frac{q-p}{2}$ cijeli, onda zaključujemo da je promatrana konvergenta stvarno jednaka $\frac{k}{d}$. Tada iz $\frac{p+q}{2}$ i $\frac{q-p}{2}$ možemo lako dobiti faktorizaciju modula $n = pq$. □

## 4.2 Numerički primjeri Wienerovog napada

**Primjer 4.3** *Neka je u RSA kriptosustavu zadan modul* $n = 2989234739$ *i javni eksponent* $e = 2501103889$*, te neka je poznato da tajni eksponent* $d$ *zadovoljava* $d < \frac{1}{3}n^{0.25} < 80$*. Razvoj od* $\frac{e}{n}$ *u verižni razlomak je:*

$$[0, 1, 5, 8, 13, 3, 2505, 1, 7, 3, 1, 5, 3].$$

*Zatim računamo pripadne konvergente:*

$$0, 1, \frac{5}{6}, \frac{41}{49}, \frac{538}{643}, \cdots$$

*Sada ćemo provjeravati za koje konvergente* $\frac{k_i}{d_i}$*,* $i \geq 2$*, vrijedi da je* $\varphi(n) = (p-1)(q-1) = (ed-1)/k$ *cijeli broj i da li se* $n$ *može faktorizirati iz* $\varphi(n)$*.*
*Za* $k_3 = 5$ *i* $d_3 = 6$ *slijedi:*

$$\varphi(n) = \frac{ed_3 - 1}{k_3} = \frac{2501103889 \cdot 6 - 1}{5} = \frac{15006623333}{5} = 3001324666,6.$$

*Za* $k_4 = 41$ *i* $d_4 = 49$ *slijedi:*

$$\varphi(n) = \frac{ed_4 - 1}{k_4} = \frac{2501103889 \cdot 49 - 1}{41} = \frac{122554090560}{41} = 2989124160.$$

*Iz* $\varphi(n) = 2989124160$ *dobivamo i odgovarajuće faktore od* $n$ *(*$p = 47059$ *i* $q = 63521$*), što će značiti da je traženi tajni ključ* $d = 49$*.*

**Primjer 4.4** *Pretpostavimo da su u RSA kriptosustavu zadani modul* $n = 7978886869909$ *i javni eksponent* $e = 3594320245477$*, te da je poznato da tajni eksponent* $d$ *zadovoljava* $d < \frac{1}{3}n^{0.25} < 561$*. Računamo razvoj broja* $\frac{e}{n}$ *u verižni razlomak. Dobivamo:*

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

*Potom računamo pripadne konvergente:*

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

*Na kraju provjeravamo koji od nazivnika* $2, 9, 11, 20, 91, 111, 313$ *zadovoljava kongruenciju* $(x^e)^d \equiv x \pmod{n}$ *za npr.* $x = 2$*. Tako dobivamo da je tajni eksponent* $d = 313$*.*

U zadnjem primjeru je prava konvergenta bila upravo zadnja koja je zadovoljavala uvjet $d < 561$. Iz toga vidimo da možda nije nužno testirati sve konvergente u zadanom rasponu, već da bi moglo biti moguće karakterizirati pravu konvergentu. Preciznijom ocjenom za $\varphi(n)$ i uz razumnu pretpostavku da je $n > 10^8$ dobije se da je $\frac{k}{d}$ jedinstvena konvergenta koja zadovoljava nejednakost

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

Verheul i van Tilborg (1997.), te Dujella (2004.) prikazali su dvije varijante Wienerovog napada na RSA u kojem je tajni ključ veći od $\sqrt[4]{n}$. Neka je $d = D\sqrt[4]{n}$. Ako $D$ nije jako velik, $\frac{k}{d}$ bi mogli 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 $\frac{e}{n}$. Broj mogućih parova $(r, s)$ u Verheul - van Tilborgovom napadu je $O(D^2A^2)$, gdje je $A = \max\{a_i : i = m+1, m+2, m+3\}$, dok je u Dujellinoj varijanti $O(D^2 \log(A))$ ($a_i$ su parcijalni kvocijenti u razvoju u verižni razlomak).

**Primjer 4.5** *Neka je* $n = 7978886869909$*,* $e = 4603830998027$*, 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*

$$0, 1, \frac{1}{2}, \frac{3}{5}, \frac{4}{7}, \frac{11}{9}, \frac{15}{26}, \frac{281}{487}, \frac{2825}{4896}, \dots$$

*Tražimo dvije susjedne neparne konvergente između kojih se nalazi* $\frac{e}{n} + \frac{2.122e}{n\sqrt{n}}$*. Dobivamo:*

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

*Tajni eksponent tražimo među brojevima nekog od oblika* $26r + 19s$ *ili* $487s - 26t$ *ili* $4896r' + 487s'$*. Primjenjujući kriterij za testiranje kandidata za razlomak* $\frac{k}{d}$*, nalazimo da je* $d = 5936963$*, što se dobiva za* $s = 12195$*,* $t = 77$*.*

# 5 Napadi na RSA s malim javnim eksponentom

Osim napada na RSA kriptosustav s malim tajnim eksponentom, postoje i napadi na RSA uz pretpostavku da je javni eksponent $e$ mali, pa bi i to trebalo izbjegavati. U trećem koraku implementacije RSA kriptosustava broj $e$ se može izabrati slučajno, a smisleno je izabrati ga što manjim, tako da bi šifriranje $x^e \bmod n$ (modularno potenciranje) bilo što brže. Broj operacija u šifriranju ovisi o veličini javnog eksponenta $e$, te o broju jedinica u binarnom zapisu od $e$. Zbog toga se dugo vremena $e = 3$ smatrao dobrim izborom. No, pokazalo se da je RSA kriptosustav s malim javnim eksponentom $e$ prilično nesiguran.

Pretpostavimo da pošiljatelj šalje identičnu poruku $m$ trima korisnicima. Svaki od tri korisnika koristi isti javni eksponent $e = 3$, dok su vrijednosti javnih modula $n_1$, $n_2$, $n_3$ različite. U tom slučaju njihov protivnik može saznati sljedeće šifrate:

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

Nakon što protivnik dozna šifrate može naći i rješenje sustava linearnih kongruencija pomoću Kineskog teorema o ostatcima:

$$x \equiv c_1 \pmod{n_1}, \quad x \equiv c_2 \pmod{n_2}, \quad x \equiv c_3 \pmod{n_3}.$$

Rješenje sustava linearnih kongruencija je broj $x$ sa svojstvom $x \equiv m^3 \pmod{n_1 n_2 n_3}$. Kako je $m^3 < n_1 n_2 n_3$, vrijedi da je $x = m^3$. Protivnik sada može jednostavno otkriti orginalnu poruku $m$ tako da nađe treći korijen iz $x$.

Da bi izbjegli ovakav napad porukama prije šifriranja se može dodati neki "slučajni dodatak" i na taj način će svaki od primatelja dobiti različitu poruku. Ali, ni to nije obećavajuće, jer danas postoje napadi zasnovani na Coppersmithovu rezultatu i LLL algoritmu, koji uspješno razbijaju RSA kriptosustav s malim eksponentom $e$ i "slučajnim dodatkom" u porukama. Takvi napadi za nalaženje rješenja polinomijalnih kongruencija koriste Coppersmithovu metodu (vidjeti [1]).

Neka je zadan polinom $f(x) \in \mathbb{Z}[x]$ stupnja $d$ i neka je poznato da postoji "malo" rješenje kongruencije $f(x) \equiv 0 \pmod{N}$, tj. rješenje $x_0$ za koje vrijedi $|x_0| < N^{1/d}$. Coppersmith je pokazao da se učinkovito može naći $x_0$. Osnovna ideja Coppersmithove metode je konstrukcija novog polinoma $h(x) = h_0 + h_1 x + \cdots + h_n x^n \in \mathbb{Z}[x]$, tako da će također vrijediti $h(x_0) \equiv 0 \pmod{N}$, ali će ovako definirani polinom imati male koeficijente. Bolje rečeno, traži se da "norma" $||h(x)|| := (\sum_{i=0}^{n} h_i^2)^{1/2}$ bude mala. U tom slučaju se koristi činjenica da ako za prirodan broj $X$ vrijedi

$$||h(xX)|| < \frac{N}{\sqrt{n+1}}$$

i $|x_0| < X$ zadovoljava kongruenciju $h(x_0) \equiv 0 \pmod{N}$, onda je $x_0$ nultočka polinoma $h$, tj. vrijedi ne samo kongruencija, već i jednakost $h(x_0) = 0$.

Polinom $h_x$ s traženim svojstvom se može naći pomoću LLL algoritma (vidjeti [6]). Koeficijenti polinoma $h(x)$ mogu se dobiti kao komponente prvog vektora LLL-reducirane

baze određene rešetke koja se dobije pomoću koeficijenata polaznog polinoma $f(x)$. Jedan od napada zasnovan na Coppersmithovu rezultatu i LLL algoritmu je Hastadov napad (1985.), koji ćemo sada prikazati.

## 5.1 Hastadov napad

Pretpostavimo da je, prije šifriranja, na početku svake poruke dodan neki podatak ovisan o korisniku. Npr.

$$c_i = (i \cdot 2^h + m)^e \bmod n_i, \quad i = 1, ..., k.$$

Dakle, imamo $k$ polinoma $g_i(x) = (i \cdot 2^h + x)^e - c_i$, te tražimo $m$ sa svojstvom da je

$$g_i(m) \equiv 0 \,(\text{mod } n_i).$$

Neka je $n = n_1 n_2 \cdots n_k$. Pomoću Kineskog teorema o ostacima možemo naći $t_i$ tako da je

$$g(x) = \sum_{i=1}^{k} t_i g_i(x) \quad \text{i} \quad g(m) \equiv 0 \,(\text{mod } n)$$

($t_i \equiv 1 \pmod{n_i}$, $t_i \equiv 0 \pmod{n_j}$ za $j \neq i$). Polinom $g$ je normiran i stupnja $e$. Ako je $k > e$, tj. imamo više korisnika (presretnutih šifrata) nego što je javni eksponent, onda je $m < min_i n_i < n^{1/k} < n^{1/e}$, pa se $m$ može efikasno naći primjenom Coppersmithovog rezultata.

Za odabir eksponenta $e$, može se preporučiti $e = 65537$, jer je on dovoljno velik da bi onemogućio sve poznate napade na RSA s malim eksponentom. Prednost mu je i vrlo brzo šifriranje jer ima malo jedinica u binarnom zapisu, $65537 = 2^{16} + 1$.

## 5.2 Numerički primjeri

Prikazat ćemo primjer napada na RSA s malim javnim eksponentom $e$ kada protivnik otkriva orginalnu poruku, koju je pošiljatelj poslao trima korisnicima, od kojih svaki koristi isti javni eksponent $e = 3$ uz različite javne module $n_1$, $n_2$, $n_3$.

**Primjer 5.1** *Pretpostavimo da tri korisnika koriste različite module $n_1 = 329$, $n_2 = 341$, $n_3 = 377$, dok im je javni eksponent $e = 3$ svima isti. Pošiljatelj šifrira identičnu poruku $m$ za svakog od tri korisnika i dobije sljedeće šifrate $c_1 = 43$, $c_2 = 30$, $c_3 = 372$. Nadalje, neka je protivnik saznao odgovarajuće šifrate, te sada želi saznati i orginalnu poruku. Protivnik za početak rješava sustav linearnih kongruencija*

$$x \equiv 43 \,(\text{mod } 329), \quad x \equiv 30 \,(\text{mod } 341), \quad x \equiv 372 \,(\text{mod } 377),$$

*koristeći Kineski teorem o ostatcima. Na taj način dobije sljedeće kongruencije:*

$$128557x \equiv 43 \pmod{329}, \tag{1}$$

$$124033x \equiv 30 \pmod{341}, \tag{2}$$

$$112189x \equiv 372 \pmod{377}. \tag{3}$$

*Kako je* $128557 \equiv 247 \pmod{329}$ *rješenje kongruencije* (1) *se dobije iz* $247x \equiv 43 \pmod{329}$. *Iz* $(247, 329) = 1$ *slijedi da postoje* $u, v \in \mathbb{Z}$ *takvi da je* $247u + 329v = 1$. *Pomoću Euklidovog algoritma dobijemo* $u = 4$, $v = -1$, *pa su sva rješenja kongruencije* (1) *dana sa* $x_1 \equiv 172 \pmod{329}$.
*Kako je* $124033 \equiv 250 \pmod{341}$ *rješenje kongruencije* (2) *se dobije iz* $250x \equiv 30 \pmod{341}$. *Iz* $(250, 341) = 1$ *slijedi da postoje* $u, v \in \mathbb{Z}$ *takvi da je* $250u + 341v = 1$. *Pomoću Euklidovog algoritma dobijemo* $u = -15$, $v = -1$, *pa su sva rješenja kongruencije* (2) *dana sa* $x_2 \equiv 232 \pmod{341}$.
*Kako je* $112189 \equiv 220 \pmod{377}$ *rješenje kongruencije* (3) *se dobije iz* $220x \equiv 372 \pmod{377}$. *Iz* $(220, 377) = 1$ *slijedi da postoje* $u, v \in \mathbb{Z}$ *takvi da je* $220u + 377v = 1$. *Pomoću Euklidovog algoritma dobijemo* $u = 12$, $v = -7$, *pa su sva rješenja kongruencije* (3) *dana sa* $x_3 \equiv 317 \pmod{377}$.
*Dakle, sva rješenja sustava kongruencija* (1), (2), (3) *su dana sa:*

$$x \equiv 128557 \cdot 172 + 124033 \cdot 232 + 112189 \cdot 317 \equiv 86451373 \equiv 1860867 \pmod{329 \cdot 341 \cdot 377}.$$

*Slijedi da je* $x = 1860867$ *i* $m = \sqrt[3]{x} = 123$.

# Literatura


[1] D. Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*, Stanford University, February 1999

[2] F. da Costa Boucinha, *A Survey of Cryptanalytic Attacks on RSA*, Instituto superior técnico, Universidade Técnica de Lisboa, October 2011

[3] A. Dujella, *Diofantske aproksimacije i primjene*, Matematički odjel, Sveučilište u Zagrebu, Poslijediplomski kolegij 2011/2012

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

[5] B. Kleinberg, *Introduction to Algorithms: The Miller-Rabin Randomized Primality test*, Cornell University, Lecture notes, May 2010

[6] D. Micciancio, *Lattice Algorithms and Applications, The LLL Algorithm*, Lecture notes 2012