Napadi s djelomičnim poznavanjem ključa

Erceg, Erika

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij matematike
modul: financijska matematika i statistika

Napadi s djelomičnim poznavanjem ključa

Diplomski rad

Mentor:
prof. dr. sc. Ivan Matić

Student:
Erika Erceg

Osijek, 2024

Sadržaj

1 | Uvod

Sigurnost kriptografskih sustava najvažnija je u zaštiti osjetljivih informacija od neovlaštenog pristupa i zlonamjernih napada. Među raznim kriptografskim mehanizmima, RSA kriptosustav je jedan od najčešće primjenjivanih i proučavanih zbog svoje čvrste osnove u teoriji brojeva i praktične učinkovitosti. Unatoč svojoj snazi, RSA nije otporan na sve napade, osobito u scenarijima gdje dolazi do djelomičnog poznavanja ključa.

Kroz cijeli rad ćemo koristiti RSA kriptosustav tako da ćemo se u drugom poglavlju upoznati s njime. U trećem poglavlju ćemo pokazati da je otprilike polovina značajnih bitova potrebna da bi se modul mogao učinkovito faktorizirati. Nakon toga ćemo, u poglavlju četiri za MSB, a u poglavlju pet za LSB, otkriti koje informacije o privatnom eksponentu moramo znati da bi RSA kriptosustav bio ugrožen. Na kraju ćemo, u šestom poglavlju otkriti koje informacije o prostim brojevima p i q, za koje vrijedi $N = pq$, moramo znati da bi RSA kriptosustav bio ugrožen.

2 | RSA kriptosustav

Ovaj kriptosustav spada pod asimetrične šifre, a nastao je 1977. i dobio je naziv prema trojici njegovih tvoraca, matematičarima Ronu Rivestu, Adiu Shamiru i Lenu Adlemanu. Definirajmo prvo osnovne sastavnice RSA kriptosustava, a to su Eulerova funkcija, Eulerov teorem te multiplikativni inverzi modulo neki prirodan broj čiju primjenu možemo vidjeti u Wilsonovom teoremu.

Neka je N prirodan broj. Broj prirodnih brojeva u nizu $1, 2, ..., N$ koji su relativno prosti s N označavamo s $\varphi(N)$; ovim je definirana funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ koju nazivamo Eulerova funkcija. Sada možemo iskazati Eulerov teorem:

Teorem 1 ([4, Teorem 2.2.3.]). *Neka je a cijeli broj te N prirodan broj. Ako su brojevi a i N relativno prosti, tada je*

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

Neka je p prost broj i $a < p$ prirodan broj. Tada postoji prirodan broj b za koji vrijedi $a \cdot b \equiv 1 \pmod{p}$ i takav broj b nazivamo multiplikativni inverz od a modulo p. Iskažimo sada Wilsonov teorem:

Teorem 2 ([4, Teorem 2.3.1.]). *Ako je p prost broj tada je*

$$(p-1)! \equiv -1 \pmod{p}.$$

Opišimo sada postupak šifriranja. Alfabet otvorenog teksta sastoji se od slova engleske abecede te ćemo u ovome radu uzeti da se postupak šifriranja i dešifriranja radi nad prirodnim brojevima te možemo smatrati kako se od njih sastoji i polazni alfabet. Neka su p i q što veći prosti brojevi te neka je $p \cdot q = N$. Pošto je Eulerova funkcija multiplikativna znamo da vrijedi:

$$\varphi(N) = (p-1)(q-1).$$

Korisnik odabire enkripcijski eksponent $e \in \mathbb{N}$ koji je relativno prost s $\varphi(N)$. Zato što su e i $\varphi(N)$ relativno prosti, postoji multiplikativni inverz d od e modulo $\varphi(N)$, tj.

$$d \cdot e \equiv 1 \pmod{\varphi(N)}.$$

Iz Euklidova algoritma možemo odrediti d jer postoji neki cijeli broj k za koji je

$$ed + k\varphi(N) = 1,$$

te prethodnu jednadžbu nazivamo fundamentalnom jednadžbom, a broj d dekripcijskim eksponentom. Parametar (e, N) je svima poznat i nazivamo ga javni ključ, a (d, p, q) nazivamo tajni ključ i poznat je samo pošiljatelju i primatelju poruke.

Neka je sada x dio otvorenog teksta koji treba šifrirati, gdje uzimamo da je $x < N$. Tada pomoću $f_t(x) = x^e \bmod N$, gdje je $t = (N, e)$, dobivamo odgovarajući dio šifrata. Ako je y dio šifrata, dekripcija se obavlja pomoću $g_t(x) = y^d \bmod N$, gdje je $t = (N, e)$. Sljedeći teorem nam potvrđuje da su funkcije f_t i g_t jedna drugoj inverzne na skupu prirodnih brojeva.

Teorem 3 ([4, Teorem 3.6.1.]). *Za $1 \leq x < N$ vrijedi $g_t(f_t(x)) = x$ gdje je $t = (N, e)$, uz uvjet $(e, \varphi(N)) = 1$.*

Promatrat ćemo slučajeve kada je poznat neki broj najznačajnijih bitova (MSB = most significant bits) ili najmanje značajnih bitova (LSB = least significant bits) privatnog eksponenta ili nekog od prostih parametara p i q. Neka je $0 \leq \epsilon \leq 1$ udio poznatih bitova. Kada je poznato ϵ MSB od x, pretpostavljamo da znamo $\hat{x}$ takav da vrijedi $x = \hat{x} + x_0$, gdje je x_0 nepoznat i zadovoljava $|x| = |x - \hat{x}| < x^{1-\epsilon}$. Kada je poznato ϵ LSB od x, pretpostavljamo da znamo $\tilde{x}$ i $r \geq |x^\epsilon|$ takav da vrijedi $x = x_0 r + \tilde{x}$, gdje je $|\tilde{x}| < r$ i nepoznati x_0 zadovoljava

$$|x_0| = \left|\frac{x - \tilde{x}}{r}\right| < \left|\frac{x}{r}\right| < x^{1-\epsilon}.$$

Kroz cijeli rad ćemo koristiti RSA kriptosustav i svi napadi koje ćemo obraditi koriste neku informaciju o tajnom ključu, koja općenito nije poznata, da bi mogli faktorizirati modul N.

3 | Faktoriziranje s poznatom polovinom značajnih bitova

Teorem 4 ([3, Theorem 6.1.]). *Neka je $N = pq$ modul RSA kriptosustava s balansiranim prostim brojevima*[1]*. Ako znamo barem jednu polovinu MSB ili LSB od p ili q, onda se N može faktorizirati u polinomijalnom vremenu* $\log N$.

Dokaz. Pošto su p i q uzastopni prosti brojevi, znamo da vrijedi

$$\frac{1}{2}N^{\frac{1}{2}} < p, q < 2N^{\frac{1}{2}},$$

bez smanjenja općenitosti smo uzeli da nije bitno koji je od brojeva p i q veći. Ideja napada, kada znamo MSB ili LSB od p ili q, je konstruirati polinom (s vodećim koeficijentom 1) koji ima poznatu malu nultočku. Kada znamo tu nultočku onda znamo i ostatak nepoznatih bitova od tog prostog broja pa je i faktorizacija modula N otkrivena.

Prvo pretpostavimo da znamo barem jednu polovinu MSB od p. Stoga znamo $\hat{p}$ takav da je $p = \hat{p} + p_0$, gdje je p_0 nepoznat i zadovoljava

$$|p_0| = |p - \hat{p}| < p^{\frac{1}{2}} < \sqrt{2}N^{\frac{1}{4}}.$$

Primijetimo da je p_0 nultočka modulo p polinoma

$$f_{MSB}(x) = x + \hat{p},$$

pošto je $f_{MSB}(p_0) = p_0 + \hat{p} = p \equiv 0 \pmod{p}$. Uočimo da zato što je vodeći koeficijent od f_{MSB} jednak 1, svaka nultočka polinoma modulo p je oblika $p_0 + \alpha p$, za neki $\alpha \in \mathbb{Z}$. Od svih tih nultočki p_0 je jedina koja je omeđena s $\sqrt{2}N^{\frac{1}{4}}$. Sada ćemo koristiti Coppersmithovu metodu za pronalaženje malih nultočki polinoma koja kaže:

Lema 1 ([3, Theorem 2.8.]). *Neka je $N \in \mathbb{Z}$ čija je faktorizacija nepoznata i njegov djelitelj je $b \geq N^{\beta}$. Neka je $f_b(x)$ polinom jedne varijable s vodećim koeficijentom 1 i stupnja d, te neka je $c > 0$ konstanta. Svi x_0 koji zadovoljavaju $f_b(x_0) \equiv 0 \pmod{b}$ i $|x_0| \leq cN^{\frac{\beta^2}{d}}$ mogu biti izračunati u polinomijalnom vremenu u ovisnosti o* $\log N$, *c i broju nultočki.*

[1] n-ti prost broj p_n je balansiran prost broj ako zadovoljava $p_n = \frac{p_{n-1}+p_{n+1}}{2}$.

Označimo sada $\beta = \frac{1}{2} - \log_N(2)$ i $c = 2\sqrt{2}$ i primijetimo da p zadovoljava sljedeće

$$\begin{aligned} p &> \frac{1}{2}N^{\frac{1}{2}} \\ &= N^{\frac{1}{2}-\log_N(2)} \\ &= N^{\beta}, \end{aligned}$$

te da nultočka p_0 zadovoljava

$$\begin{aligned} |p_0| &< \sqrt{2}N^{\frac{1}{4}} \\ &= 2\sqrt{2}N^{\frac{1}{4}-\log_N(2)} \\ &< 2\sqrt{2}N^{\frac{1}{4}-\log_N(2)+\log_N^2(2)} \\ &= 2\sqrt{2}N^{\left(\frac{1}{2}-\log_N(2)\right)^2} \\ &= cN^{\beta^2}. \end{aligned}$$

Sada, uzimajući u obzir tako definirane β i c, iz Coppersmithove metode slijedi da možemo izračunati p_0. Pošto znamo p_0 znamo i $p = p_0 + \hat{p}$, a s time i faktorizirati modul N u polinomijalnom vremenu $\log N$.

Nadalje, pretpostavimo da znamo barem jednu polovinu LSB od q. Stoga znamo $\tilde{q}$ i r takav da je $q = q_0 r + \tilde{q}$, gdje je $0 \leq \tilde{q} < r$, $q^{\frac{1}{2}} < r < q$, a q_0 je nepoznat i zadovoljava

$$|q_0| = \left|\frac{q-\tilde{q}}{r}\right| \leq \left|\frac{q}{r}\right| < q^{\frac{1}{2}} < \sqrt{2}N^{\frac{1}{4}}.$$

Kada je r potencija broja 2 tada se $\tilde{q}$ podudara sa LSB od q. Neka je $R = r^{-1} \pmod N$, takav da je $rR = 1 + kN$ za neki $k \in \mathbb{Z}$. Uočimo da polinom

$$f_{LSB} = x + \tilde{q}R$$

ima za nultočku q_0 modulo q. Objasnit ćemo zašto to vrijedi tako što ćemo pokazati da je $rf_{LSB}(q_0) \equiv 0 \pmod q$, a pošto je $q^{\frac{1}{2}} < r < q$ znamo da $r \not\equiv 0 \pmod q$ pa slijedi da je $f_{LSB}(q_0) \equiv 0 \pmod q$.

$$\begin{aligned} rf_{LSB}(q_0) &= q_0 r + \tilde{q}Rr \\ &= q_0 r + \tilde{q} + \tilde{q}kN \\ &= q + \tilde{q}kpq \\ &\equiv 0 \pmod q \end{aligned}$$

Sada kao i u prošlom slučaju, zato što je $f_{LSB}(x)$ linearni polinom s vodećim koeficijentom 1, nultočka q_0 je jedina nultočka modulo q za koju vrijedi $q_0 < \sqrt{2}N^{\frac{1}{4}}$. Pošto su q_0 i q omeđeni s istim granicama kao p_0 i p u prošlom slučaju, slijedi iz Coppersmithove metode, da možemo izračunati nultočku q_0 u polinomijalnom

vremenu $\log(N)$. Kada znamo q_0 znamo i $q = q_0 r + \tilde{q}$, a onda znamo i faktorizaciju modula N.

Uočimo da se N može faktorizirati u polinomijalnom vremenu $\log(N)$ i ako znamo barem jednu polovinu MSB od q ili barem jednu polovinu LSB od p, zato što tijekom dokaza nismo imali potrebu definirati koji faktor od N je veći. □

Ovim teoremom smo pokazali da je potrebno poznavati barem jednu polovinu MSB ili LSB od p ili q, ali možemo malo relaksirati tu tvrdnju, tako da je potrebno poznavati nešto manje bitova. Iz Coppersmithove metode znamo da nepoznati dio prostog broja možemo odrediti ako je manji od $cN^{\frac{1}{4}}$. Konstanta c nam dopušta da je potrebno nešto manje bitova na račun povećanog vremena izvođenja. Ako je poznato $\frac{1}{2} - \epsilon$ bitova i $\epsilon \in O(\log(\log(N)))$, tada će ukupno vrijeme izvođenja i dalje biti u polinomijalnom vremenu $\log(N)$. Alternativno, možemo napraviti iscrpnu pretragu nad nepoznatih ϵ bitova i pokušati faktorizirati modul za svaki kandidat od jedne polovine poznatih bitova, sve dok ne dobijemo faktorizaciju. Koristeći bilo koju od ove dvije tehnike slijedi da ako je poznata otprilike jedna polovina MSB ili LSB od p ili q, onda se modul može učinkovito faktorizirati.

4 | Djelomično poznavanje privatnog eksponenta: MSB

U ovom poglavlju ćemo pretpostaviti da suparnik zna neki broj MSB od privatnog eksponenta $d = N^{\beta}$. Za dani javni ključ (e, N) pretpostavimo da suparnik zna $\hat{d}$ takav da

$$|d - \hat{d}| < N^{\delta},$$

za neki $0 \leq \delta \leq \beta$. Napade ćemo razdvojiti obzirom na veličinu privatnog i javnog eksponenta. Počet ćemo s nekim općim rezultatima za proizvoljnu veličinu eksponenta, a zatim nastaviti s napadima kada jedan od eksponenata bude pune veličine.

4.1 Proizvoljni eksponent

Počinjemo s dva napada s djelomičnim poznavanjem privatnog ključa te s proizvoljnim veličinama javnog i privatnog eksponenta. Ali prije toga moramo spomenuti dvije pretpostavke koje će morati biti zadovoljene u svim napadima.

Pretpostavka 1 ([3, Assumption 2.14.]). *Polinomi s poznatim malim nultočkama nad $\mathbb{Z}$ ili $\mathbb{N}$ imaju samo jednu malu nultočku.*

Definirajmo sada pojmove čije poznavanje nam je potrebno prije nego što napravimo drugu pretpostavku.

Definicija 1 ([3, str. 26]). *Neka je $b_1, \ldots, b_m$ baza za rešetku L i neka je $b_1^*, \ldots, b_m^*$ odgovarajuća baza dobivena Gram-Schmidtovim postupkom ortogonalizacije. Baza $b_1, \ldots, b_m$ se nazima Lovászova reducirana baza ili LLL reducirana baza, ako Gram-Schmidthov koeficijent zadovoljava $|\mu_{i,j}| \leq \frac{1}{2}$ za $1 \leq j < i \leq n$ i*

$$||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \frac{3}{4} ||b_{i-1}^*||^2$$

za $1 < i \leq n$, ili ekvivalentno

$$||b_i^*||^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) ||b_{i-1}^*||^2$$

za $1 < i \leq n$. Uočimo da su vektori $b_i^* + \mu_{i,i-1} b_{i-1}^*$ i b_{i-1}^* projekcije od b_i i b_{i-1}, na ortogonalnom komplementu od $span(\{b_1, \ldots, b_{i-2}\})$[1].

[1] $span(S)$ definiran je kao skup svih linearnih kombinacija vektora u S.

Definicija 2 ([6]). *Kažemo da su $x_1, \ldots, x_n \in \mathbb{C}$ algebarski nezavisni, ako za svaki polinom $P(x_1, \ldots, x_n)$ s algebarskim koeficijentima koji nisu svi jednaki nuli vrijedi $P(x_1, \ldots, x_n) \neq 0$. Ako je $P(x_1, \ldots, x_n) = 0$, tada su brojevi $x_1, \ldots, x_n$ algebarski zavisni.*

Pretpostavka 2 ([3, Assumption 2.15.]). *Polinomi dobiveni iz LLL reducirane baze su algebarski nezavisni.*

Sada kada znamo bitne pretpostavke možemo navesti napad:

Napad 1 ([3, Attack 6.2.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N RSA modul s balansiranim prostim brojevima p i q. Neka je $e = N^\alpha$ javni eksponent i neka je $d = N^\beta$ privatni eksponent definiran modulo $\varphi(N)$. Ako nam je poznat javni ključ (e, N) i $\hat{d}$ zadovoljava $|d - \hat{d}| < N^\delta$, ako je $\delta < \frac{1}{2}$ i*

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\alpha + 6\beta - 5} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Dokaz. Neka je $d = \hat{d} + d_0$ i

$$\begin{aligned} \varphi(N) &= (p-1)(q-1) \\ &= pq - p - q + 1 \\ &= N - s. \end{aligned}$$

Započnimo s jednakostima

$$\begin{aligned} ed - k\varphi(N) &= 1 \\ e(\hat{d} + d_0) - k(N - s) - 1 &= 0, \end{aligned}$$

gdje su jedino d_0, k i s nepoznanice. Znači želimo pronaći nultočku funkcije

$$f(x, y, z) = ex - Ny + yz + e\hat{d} - 1,$$

jer je $(x_0, y_0, z_0) = (d_0, k, s)$ nultočka od $f(x, y, z)$. Definirajmo $X = N^\delta$, $Y = 2N^{\alpha+\beta-1}$ i $Z = 3N^{\frac{1}{2}}$ te primijetimo

$$\begin{aligned} |x_0| = |d_0| = |\hat{d} - d| &< N^\delta = X \\ |y_0| = |k| = \frac{ed-1}{\varphi(N)} &< \frac{ed}{\varphi(N)} < \frac{2ed}{N} = 2N^{\alpha+\beta-1} = Y \\ |z_0| = |s| = |p + q - 1| &< \frac{3}{\sqrt{2}}N^{\frac{1}{2}} - 1 < 3N^{\frac{1}{2}} = Z \end{aligned}$$

te da je $W = ||f(xX, yY, zZ)||_\infty \geq 2N^{\alpha+\beta}$ jer je

$$W = \max\{eX, NY, YZ, e\hat{d} - 1\} \geq NY = 2N^{\alpha+\beta}.$$

Sada nam je potrebno poznavanje proširene Coppersmithove metode za cjelobrojne polinome u dvije varijable, ali ćemo ju iskazati samo za dvije funkcije koje koristimo u ovom i sljedećem dokazu.

Teorem 5 ([3, Theorem 2.13.]). *Za svaki $\epsilon > 0$ postoji W_0 takav da za neki $W > W_0$ vrijedi sljedeće: Neka je ili $f_1(x_1, x_2, x_3) = a_0 + a_1x_1 + a_2x_2 + a_3x_2x_3$ uz uvjet*

$$X_1^{1+3\tau} X_2^{2+3\tau} X_3^{1+3\tau+3\tau^2} < W^{1+3\tau-\epsilon} \tag{4.1}$$

ili $f_2(x_1, x_2, x_3) = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_4x_2x_3$ uz uvjet

$$X_1^{2+3\tau} X_2^{3+6\tau+3\tau^2} X_3^{3+3\tau} < W^{2+3\tau-\epsilon}. \tag{4.2}$$

Neka je $f = f_1$ ili $f = f_2$ i $X_1, X_2, X_3 > 0$ zadovoljavaju jedan od uvjeta (4.1) ili (4.2) te neka je $W = \|f(x_1X_1, x_2X_2, x_3X_3)\|_\infty$. Skup od tri linearno nezavisna polinoma $g_1, g_2, g_3 \in \mathbb{Z}[x_1, x_2, x_3]$ može biti konstruiran u polinomijalnom vremenu $\log(W)$ tako da je $g_i(y_1, y_2, y_3) = 0$ za svaki $1 \leq i \leq 3$, za svaki (y_1, y_2, y_3) koji zadovoljava $f(y_1, y_2, y_3) = 0$ i $|y_i| < X_i$ za svaki $i = 1, 2, 3$.

Vidimo da u ovom slučaju vrijedi $f(x, y, z) = f_1(x_1, x_2, x_3)$ te iz teorema slijedi da za dovoljno velik N možemo pronaći dva linearno nezavisna polinoma, svaki algebarski nezavisan s $f(x, y, z)$, s nultočkom (x_0, y_0, z_0) nad cijelim brojevima, ako je zadovoljen uvjet (4.1) za $\tau > 0$. Kada uvrstimo vrijednosti od X, Y, Z i W, malo sredimo izraz, ignoriramo sve male konstante i gledamo samo potencije od N dobijemo

$$3\tau^2 + 3\tau(2\delta - 1) + 2\alpha + 2\beta + 2\delta - 3 < 0.$$

Kada deriviramo tu nejednakost po τ dobijemo

$$\tau_{min} = \frac{1}{2} - \delta.$$

Uvrštavanjem te optimalne vrijednosti za τ imamo

$$-3\delta^2 + 5\delta + 2\alpha + 2\beta - \frac{15}{4} < 0,$$

gdje je $\delta < \frac{1}{2}$ da bi bilo zadovoljeno $\tau_{min} > 0$. Rješavanjem te nejednakosti po δ imamo

$$\delta \leq \frac{5}{6} \pm \frac{-1}{3}\sqrt{6\alpha + 6\beta - 5} - \epsilon,$$

gdje je $\epsilon > 0$ dodan zbog ignoriranih konstanti s početka. Pretpostavljajući da su dva dobivena polinoma algebarski nezavisna, što je Pretpostavka 2, te da postoji samo jedna nultočka od $f(x, y, z)$ omeđena s X, Y i Z, što je Pretpostavka 1, onda možemo izračunati nultočku $(x_0, y_0, z_0) = (d_0, k, s)$. Pošto znamo da je $z_0 = s$ možemo izračunati $\varphi(N) = N - s$ i jednostavno napraviti faktorizaciju od N. Svi izračuni mogu biti obavljeni u polinomijalnom vremenu $\log(N)$, stoga slijedi tvrdnja teorema. □

U sljedećem napadu ćemo koristiti istu ideju kao i u prvom, osim što ćemo ovdje uz MSB od privatnog eksponenta koristiti i MSB od konstante k iz fundamentalne jednadžbe. Definirajmo prvo funkcju $\lfloor x \rceil$, koja svakom realnom broju x pridružuje cijeli broj koji je najbliži broju x. Također definirajmo funkciju najveće cijelo od x, tj. $\lfloor x \rfloor$ koja svakom realnom broju x pridružuje najveći cijeli broj

ne veći od x i funkciju najmanje cijelo od x, tj. $\lceil x \rceil$ koja svakom realnom broju x pridružuje najmanji cijeli broj ne manji od x. Nadalje, neka je N RSA modul, $e = N^\alpha$ javni eksponent i neka je $d = N^\beta$ privatni eksponent definirani modulo $\varphi(N)$. Poznat nam je $\hat{d}$ takav da je $|d - \hat{d}| < N^\delta$, za neki $0 < \delta < \beta$ i onda $\hat{k}$ dan s

$$\hat{k} = \left\lfloor \frac{e\hat{d} - 1}{N} \right\rceil = \frac{e\hat{d} - 1}{N} + \epsilon, \tag{4.3}$$

za neki $|\epsilon| \leq \frac{1}{2}$, otkriva neke MSB od k. Primijetimo da vrijedi

$$\begin{aligned} |k - \hat{k}| &= \left| \frac{ed - 1}{\varphi(N)} - \left\lfloor \frac{e\hat{d} - 1}{N} \right\rceil \right| \\ &= \left| \frac{ed - 1}{\varphi(N)} - \frac{e\hat{d} - 1}{N} + \epsilon \right| \\ &= \left| \frac{N(ed - 1)}{N\varphi(N)} - \frac{\varphi(N)(e\hat{d} - 1)}{N\varphi(N)} + \epsilon \right| \\ &= \left| \frac{Ne(d - \hat{d})}{N\varphi(N)} + \frac{s(e\hat{d} - 1)}{N\varphi(N)} + \epsilon \right| \\ &< \left| \frac{e(d - \hat{d})}{\varphi(N)} \right| + \left| \frac{se\hat{d}}{N\varphi(N)} \right| + \frac{1}{2}. \end{aligned} \tag{4.4}$$

Pošto je $e < \varphi(N)$ i $\hat{d} < N$ slijedi da $\hat{k}$ uvijek zadovoljava

$$\begin{aligned} |k - \hat{k}| &< \left| \frac{e(d - \hat{d})}{\varphi(N)} \right| + \left| \frac{se\hat{d}}{N\varphi(N)} \right| + \frac{1}{2} \\ &< N^\delta + 3N^{\frac{1}{2}} + \frac{1}{2}, \end{aligned}$$

iako se bolje granice mogu dobiti ovisno o stvarnim RSA parametrima. Korištenje znanja o $\hat{d}$ i $\hat{k}$ rezultira jačim napadom za određene veličine javnih i privatnih eksponenata. Taj rezultat je dan u sljedećem napadu.

Napad 2 ([3, Attack 6.3.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^\alpha$ javni eksponent i neka je $d = N^\beta$ privatni eksponent. Poznat nam je javni ključ (e, N) i $\hat{d}$ zadovoljava $|d - \hat{d}| < N^\delta$, ako je zadovoljen bilo koji od slučajeva*

$$\begin{aligned} &1. \quad \delta \geq \beta - \frac{1}{2}, \ \delta > 1 - \alpha, \ \delta < \frac{3 - 2\alpha}{4} \quad i \\ &\qquad \beta - \frac{1}{2} \leq \delta \leq \frac{3 + 4\alpha - 4\alpha^2}{16\alpha} - \epsilon, \\ &2. \quad \delta \leq \beta - \frac{1}{2}, \ \delta < 2 - \alpha - \beta, \ \alpha + \beta > \frac{3}{2} \quad i \end{aligned} \tag{4.5}$$

$$\delta \leq \frac{\alpha+\beta}{3} - \frac{1}{3}\sqrt{(2\alpha+2\beta-3)(2\alpha+2\beta)} - \epsilon, \tag{4.6}$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$*, ako su zadovoljene Pretpostavke 1 i 2.*

Dokaz. Neka je $\hat{k} = \left\lfloor \frac{e\hat{d}-1}{N} \right\rceil$ te primijetimo da fundamentalnu jednadžbu možemo zapisati na sljedeći način:

$$e(\hat{d}+d_0) - (\hat{k}+k_0)(M-s) - 1 = 0,$$

gdje su $d_0 = d - \hat{d}$, $k_0 = k - \hat{k}$ i s jedine nepoznanice. To nam sugerira da tražimo male nultočke od polinoma

$$g(x,y,z) = ex - Ny + \hat{k}z + yz + (e\hat{d} - \hat{k}N - 1) \in \mathbb{Z}[x,y,z],$$

jer je $(x_0, y_0, z_0) = (d_0, k_0, s)$ nultočka od $g(x,y,z)$ nad skupom cijelih brojeva. Definirajmo $X = N^{\delta}$, $Y = 15N^{\gamma}$ i $Z = 3N^{\frac{1}{2}}$ te primijetimo

$$\begin{aligned}
|x_0| &= |d_0| = |d - \hat{d}| < N^{\delta} = X \\
|y_0| &= |k_0| < \left|\frac{e(d-\hat{d})}{\varphi(N)}\right| + \left|\frac{se\hat{d}}{N\varphi(N)}\right| + \frac{1}{2} \\
&< 2N^{\alpha+\delta-1} + 12N^{\alpha+\beta-\frac{3}{2}} + \frac{1}{2} \\
&< \max\{15N^{\alpha+\delta-1}, 15N^{\alpha+\beta-\frac{3}{2}}\} = Y \\
|z_0| &= |s| < 3N^{\frac{1}{2}} = Z,
\end{aligned}$$

kada je $\gamma = \max\{\alpha+\delta-1, \alpha+\beta-\frac{3}{2}\}$. Granica za y_0 slijedi iz jednakosti (4.4) i iz nejednakosti $2\varphi(N) > N$, $|s| < 3N^{\frac{1}{2}}$ i $\hat{d} < 2d < 2N^{\beta}$. Primijetimo sada da $W = \|g(xX, yY, zZ)\|_{\infty}$ zadovoljava

$$W = \max\{eX, NY, \hat{k}Y, YZ, |e\hat{d} - \hat{k}N - 1|\} \geq NY = 15N^{\gamma+1}.$$

Vidimo da u ovom slučaju vrijedi $f(x,y,z) = f_2(x_1, x_2, x_3)$ te iz Teorema 5 slijedi da za dovoljno velik N možemo pronaći dva linearno nezavisna polinoma, svaki algebarski nezavisan s $f(x,y,z)$, s nultočkom (x_0, y_0, z_0) nad cijelim brojevima, ako je zadovoljen uvjet (4.2) za $\tau > 0$. Kada uvrstimo vrijednosti od X, Y, Z i W, malo sredimo izraz, ignoriramo sve male konstante i gledamo samo potencije od N dobijemo

$$3\gamma\tau^2 + 3\tau\left(\gamma + \delta - \frac{1}{2}\right) + \gamma + 2\delta - \frac{1}{2} < 0.$$

Kada deriviramo tu nejednakost po τ, uz uvjet $\gamma > 0$ dobijemo

$$\tau_{min} = \frac{1 - 2\gamma - 2\delta}{4\gamma}.$$

Uvrštavanjem te optimalne vrijednosti za τ dobijemo da je uvjet zadovoljen kada je

$$4\gamma^2 + 4\gamma + 8\delta\gamma - 3 + 12\delta - 12\delta^2 < 0. \tag{4.7}$$

Nadalje moramo uzeti u obzir dva slučaja. Prvo neka je $\delta \geq \beta - \frac{1}{2}$ pa je $\gamma = \alpha + \delta - 1$. Uvrstimo sada γ u nejednakost (4.7) i rješavanjem te nejednakosti po δ imamo

$$\delta \leq \frac{3 + 4\alpha - 4\alpha^2}{16\alpha} - \epsilon,$$

gdje je $\epsilon > 0$ dodan zbog ignoriranih konstanti s početka. Da osiguramo da je τ_{min} optimalan izbor za τ, uvjet $\gamma > 0$ zahtijeva $\alpha + \delta - 1 > 0$, a pošto mora biti zadovoljeno $\tau_{min} > 0$ slijedi i da je $\delta < \frac{3-2\alpha}{4}$. S time smo izveli granicu (4.5) i sve potrebne uvjete.

Neka je sada $\delta \leq \beta - \frac{1}{2}$ pa je $\gamma = \alpha + \beta - \frac{3}{2}$. Uvrstimo sada γ u nejednakost (4.7) i rješavanjem te nejednakosti po δ imamo

$$\delta \leq \frac{\alpha + \beta}{3} - \frac{1}{3}\sqrt{(2\alpha + 2\beta - 3)(2\alpha + 2\beta)} - \epsilon$$

gdje je $\epsilon > 0$ dodan zbog ignoriranih konstanti s početka. Da osiguramo da je τ_{min} optimalan izbor za τ, uvjet $\gamma > 0$ zahtijeva da je $\alpha + \delta > \frac{3}{2}$, a pošto mora biti zadovoljeno $\tau_{min} > 0$ slijedi i da je $\delta < 2 - \alpha - \beta$. S time smo izveli granicu (4.6) i sve potrebne uvjete. □

Ta dva napada se koriste za proizvoljne veličine javnog i privatnog eksponenta. U praksi se očekuje da će barem jedan od eksponenata biti pune veličine pa ćemo u nastavku razmatrati takve slučajeve.

4.2 Javni eksponent u punoj veličini

Kada je javni eksponent u punoj veličini postoje napadi s djelomičnim poznavanjem ključa koji mogu dešifrirati RSA za bilo koju veličinu privatnog eksponenta, pod uvjetom da je poznato dovoljno MSB privatnog eksponenta.

Za male privatne eksponente koristimo napade u kojima nam nije potreban niti jedan MSB od privatnog eksponenta. Navesti ćemo sada Wienerov napad koji učinkovito faktorizira modulus.

Teorem 6 ([3, Theorem 5.1.]). *Neka je $N = pq$ RSA modul, neka je e javni eksponent i d privatni eksponent definiran modulo $\varphi(N)$. Neka $k \in \mathbb{Z}$ zadovoljava $ed = 1 + k\varphi(N)$, $g = NZD(p-1, q-1)$, $g_0 = \frac{g}{NZD(g,k)}$ i $k_0 = \frac{k}{NZD(k,g)}$. Ako privatni eksponent zadovoljava*

$$d < \frac{pq}{2(p+q-1)g_0k_0} = \frac{N}{2sg_0k_0}, \tag{4.8}$$

onda N može biti faktoriziran u polinomijalnom vremenu u ovisnoti o $\log(N)$ i $\frac{g}{k}$.

Inače ne povezujemo sa Wienerovim napadom dovoljan uvjet (4.8) iz Teorema 6, nego uvjet

$$d < \frac{1}{c} N^{\frac{1}{4}},$$

za neku malu konstantu $c > 1$. Taj uvjet se dobiva pretpostavkom da je javni eksponent otprilike iste veličine kao i modul, da su prosti brojevi balansirani te da je g_0 mali. U tipičnom primjeru RSA s nasumično generiranim prostim brojevima i malim privatnim eksponentom, te su pretpostavke valjane. Ova granica, grubo govoreći $d < N^{\frac{1}{4}}$, je referentna točka za Wienerov napad i ponekad se naziva Wienerova granica.

Za privatne eksponente veličine najviše $N^{0.2929}$ imamo sljedeći napad:

Napad 3 ([3, Attack 5.4.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je $N = pq$ RSA modul s balansiranim prostim brojevima p i q. Neka je $e = N^{\alpha}$ javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definirani modulo $\varphi(N)$. Poznat nam je javni ključ (e, N) i ako privatni eksponent zadovoljava*

$$\beta < \frac{2 - \sqrt{2\alpha}}{2} - \epsilon, \tag{4.9}$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Pošto u ovom poglavlju radimo s javnim eksponentima koji su u punoj veličini ($\alpha = 1$), iz nejednakosti (4.9) imamo

$$\begin{aligned} \beta &< \frac{2 - \sqrt{2 \cdot 1}}{2} - \epsilon \\ &< 0.2929. \end{aligned}$$

Sada, za veće privatne eksponente, najbolji poznati napadi su Napad 1 i 2. Kada uvrstimo u njih $\alpha = 1$ dobijemo sljedeće:

Napad 4 ([3, Attack 6.4.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q. Neka je e javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definirani modulo $\varphi(N)$. Poznat nam je javni ključ (e, N) i $\hat{d}$ zadovoljava $|d - \hat{d}| < N^{\delta}$, ako vrijedi*

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\alpha + 6\beta - 5} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Napad 5 ([3, Attack 6.5.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je e javni eksponent i neka je $d = N^{\beta}$ privatni eksponent. Poznat nam je javni ključ (e, N) i $\hat{d}$ zadovoljava $|d - \hat{d}| < N^{\delta}$, ako je zadovoljen bilo koji od slučajeva*

1. $\beta \leq \frac{11}{16} = 0.687$ *i*

$$\delta < \frac{3}{16} - \epsilon, \tag{4.10}$$

2. $\beta \geq \frac{11}{16} = 0.687$ *i*

$$\delta < \frac{1}{3} + \frac{\beta}{3} - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2} - \epsilon, \tag{4.11}$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$*, ako su zadovoljene Pretpostavke 1 i 2.*

Primijetimo da se granice za Napade 4 i 5 podudaraju kada je

$$\beta = \frac{235}{512} \approx 0.459,$$

s time da je Napad 4 jači za manje privatne eksponente, a Napad 5 jači za veće privatne eksponente.

4.3 Privatni eksponent u punoj veličini

Kada je privatni eksponent u punoj veličini, postoje napadi s djelomičnim poznavanjem ključa koji mogu dešifrirati RSA za bilo koju veličinu javnog eksponenta, pod uvjetom da je poznato dovoljno MSB privatnog eksponenta.

Kada je javni eksponent manji od $N^{\frac{1}{2}}$ postoji nekoliko napada, svi se ti napadi oslanjaju na sljedeći rezultat koji im omogućuje da znaju konstantu iz fundamentalne jednadžbe.

Lema 2 ([3, Lemma 6.6.])**.** *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je* $e = N^{\alpha}$ *javni eksponent, gdje je* $0 < \alpha \leq \frac{1}{2}$ *i d privatni eksponent definiran modulo* $\varphi(N)$*. Ako je poznato* α *MSB od privatnog eksponenta, onda konstanta k iz fundamentalne jednadžbe može biti izračunata, do na malu grešku, u polinomijalnom vremenu* $\log(N)$*.*

Dokaz. Kada imamo α MSB od privatnog eksponenta možemo konstruirati $\hat{d}$ takav da je $|d - \hat{d}| < d^{1-\alpha} < N^{1-\alpha}$ i $\hat{d} < N$. Iz jednakosti (4.3) imamo formulu

$$\hat{k} = \left\lfloor \frac{e\hat{d} - 1}{N} \right\rceil = \frac{e\hat{d} - 1}{N} + \epsilon,$$

gdje je $|\epsilon| \leq \frac{1}{2}$, a onda iz jednakosti (4.4), uzimajući u obzir da vrijedi $2\varphi(N) > N$, $|s| < 3N^{\frac{1}{2}}$, $\hat{d} < N$ i $\alpha \leq \frac{1}{2}$ slijedi

$$\begin{aligned} |k - \hat{k}| &< \left| \frac{e(d - \hat{d})}{\varphi(N)} \right| + \left| \frac{se\hat{d}}{N\varphi(N)} \right| + \frac{1}{2} \\ &< 2N^{\alpha + (1-\alpha) - 1} + 6N^{\alpha - \frac{1}{2}} + \frac{1}{2} \\ &< 9. \end{aligned}$$

Stoga se konstanta k iz fundamentalne jednadžbe nalazi u intervalu $\langle \hat{k} - 9, \hat{k} + 9 \rangle$ i može se izračunati u vremenskom polinomu $\log(N)$ pa rezultat slijedi. □

Prvo obradimo slučaj javnog eksponenta manjeg od $N^{\frac{1}{2}}$.

Teorem 7 ([3, Theorem 6.7.]). *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent, gdje je $0 < \alpha \leq \frac{1}{2}$ i d privatni eksponent definiran modulo $\varphi(N)$. Neka je k konstanta iz fundamentalne jednadžbe i neka je $e = \gamma k$ za neki $\gamma > 1$. Ako je poznato $1 - \alpha$ MSB privatnog eksponenta, onda modul N može biti faktorizirian u polinomijalnom vremenu $\log(N)$ i γ.*

Dokaz. Poznato je $(1 - \alpha)$ MSB privatnog eksponenta, konstruirajmo $\hat{d}$ tako da je $|d - \hat{d}| < d^{\alpha} < N^{\alpha} = e$. Pošto je $0 < \alpha \leq \frac{1}{2}$ slijedi da za dio poznatih bitova vrijedi $1 - \alpha \geq \alpha$ pa iz Leme 2 znamo da možemo konstruirati $\hat{k}$ takav da konstanta iz fundamentalne jednadžbe zadovoljava $k \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$.

Za sada pretpostavimo da znamo k pa možemo, iz fundamentalne jednadžbe $ed = 1 + k\varphi(N)$, izračunati $d_k = e^{-1} \pmod{k}$ (e i k su relativno prosti). Također iz fundamentalne jednadžbe vidimo da vrijedi i $d_k = d \pmod{k}$ pa privatni eksponent možemo zapisati na način $d = Dk + d_k$ za neki nepoznati D. Iz toga imamo da je $D = \frac{d - d_k}{k}$, a pošto je $\hat{d}$ $(1 - \alpha)$ MSB privatnog eksponenta i k dovoljno velik, možemo gotovo potpuno odrediti D s $\frac{\hat{d}}{k}$. Primijetimo da privatni eksponent može biti zapisan u obliku

$$\begin{aligned} d &= \left(\frac{\hat{d} - d_1 + d - \hat{d}}{k} \right) k + d_1 \\ &= \left(\left\lceil \frac{\hat{d} - d_1}{k} \right\rceil + \left\lfloor \frac{d - \hat{d}}{k} \right\rfloor \right) k + d_1, \end{aligned}$$

gdje znamo sve s desne strane jednakosti osim $v = \left\lfloor \frac{d - \hat{d}}{k} \right\rfloor$. Pošto v zadovoljava sljedeću nejednakost

$$\begin{aligned} |v| &= \left| \left\lfloor \frac{d - \hat{d}}{k} \right\rfloor \right| \\ &< \left| \frac{d - \hat{d}}{k} \right| \\ &< \frac{e}{k} = \gamma, \end{aligned}$$

znamo da postoji najviše $2\lfloor \gamma \rfloor + 1$ cijelih brojeva koji mogu biti jednaki v. Za svaki cijeli broj $|v'| < \gamma$ možemo izračunati kandidata za D pa s time i privatni eksponent

$$d' = \left(\left\lceil \frac{\hat{d} - d_1}{k} \right\rceil + v' \right) k + d_1.$$

Kada je $v' = v$ onda je i $d' = d$ te smo pronašli privatni eksponent. Nakon toga se modulus N može lagano faktorizirati pošto znamo $\varphi(N) = \frac{ed - 1}{k}$. Iz toga vidimo da kada znamo k, samo je $2\lfloor \gamma \rfloor + 1 = 2\lfloor \frac{e}{k} \rfloor + 1$ kandidata potrebno testirati prije

nego što otkrijemo faktorizaciju modula. Pošto na početku ne znamo k, možemo jednostavno ponoviti korištenu metodu za svaki $k' \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$ koji je relativno prost s javnim eksponentom. Da osiguramo da nema više od $2\lfloor \gamma \rfloor + 1$ kandidata za testiranje privatnog eksponenta, možemo testirati kandidate tako što povećavamo vrijednost od v'. To znači da fiksiramo $v' = 0$ i isprobamo taj kandidat za svaku vrijednost od k', onda fiksiramo $v' = \pm 1$ i isprobamo svaki od tih kandidata za svaku vrijednost od k' te tako nastavimo dok ne dobijemo $k' = k$ i $v' = v$, što nam otkriva d i faktorizira modul. Na ovaj način imamo najviše $19(2\lfloor \gamma \rfloor + 1)$ kandidata za privatni eksponent koji moraju biti konstruirani i testirani. Pošto svi izračuni mogu biti odrađeni u vremenskom polinomu $\log(N)$, rezultat slijedi. □

Primijetimo da Teorem 8 zahtjeva, kada je javni eksponent jako mal, da nam je poznat skoro cijeli privatni eksponent. Postoji i drugi rezultat, u kojem je javni eksponent manji od $N^{\frac{1}{4}}$ i koji je bolji od prethodnog teorema jer zahtjeva da znamo samo $\frac{3}{4}$ MSB privatnog eksponenta.

Prije nego što iskažemo i dokažemo teorem, izvest ćemo formulu koja će nam trebati u njegovu dokazu. Označimo da je $s_0 = p + q$ te uočimo da veći broj između p i q možemo izraziti u ovisnosti s_0 i N kao

$$p = \frac{s_0 + \sqrt{s_0^2 - 4N}}{2},$$

gdje je

$$s_0^2 - 4N = (p+q)^2 - 4pq = p^2 - 2pq + q^2 = (p-q)^2.$$

Teorem 8 ([3, Theorem 6.8.]). *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent, gdje je $0 < \alpha \leq \frac{1}{4}$ i d privatni eksponent definiran modulo $\varphi(N)$. Neka je zadovoljena nejednakost $|p - q| > \frac{1}{\lambda} N^{\frac{1}{4}}$ za neki $\lambda > 1$, neka je k konstanta iz fundamentalne jednadžbe i neka je $e = \gamma k$ za neki $\gamma > 1$. Ako je poznato $\frac{3}{4}$ MSB privatnog eksponenta, onda modul N može biti faktorizirian u polinomijalnom vremenu $\log(N)$, λ i γ.*

Dokaz. Kada je poznato $\frac{3}{4}$ MSB privatnog eksponenta, onda znamo $\hat{d}$ takav da je $|d - \hat{d}| < d^{\frac{1}{4}} < N^{\frac{1}{4}}$. Pošto je $\frac{3}{4} > \alpha$, možemo koristiti $\hat{d}$ i Lemu 2 da konstruiramo $\hat{k}$ takav da konstanta iz fundamentalne jednadžbe zadovoljava $k \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$. Za svaki $k' \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$, izračunajmo

$$\begin{aligned} \hat{s}_0 &= N + 1 - \left\lceil \frac{e\hat{d} - 1}{k'} \right\rceil \\ &= N + 1 - \frac{e\hat{d} - 1}{k'} + \epsilon', \end{aligned}$$

za neki $|\epsilon'| \leq \frac{1}{2}$. Primijetimo da kada je $k' = k$ imamo

$$|\hat{s}_0 - s_0| = \left| \left(N + 1 - \frac{e\hat{d} - 1}{k} + \epsilon \right) - \left(N + 1 - \frac{ed - 1}{k} \right) \right|$$

$$
\begin{aligned}
&= \left|\frac{e}{k}(d-\hat{d}) + \epsilon\right| \\
&< \gamma N^{\frac{1}{4}} + \frac{1}{2} \\
&< 2\gamma N^{\frac{1}{4}}.
\end{aligned}
$$

Vidimo da je $\hat{s}_0$ dobra aproksimacija za MSB od $s_0 = p + q$. Koristeći taj podatak možemo konstruirati dobru aproksimaciju za MSB od p (uz pretpostavku da je $p > q$) na sljedeći način

$$\hat{p} = \frac{\hat{s}_0 + \sqrt{\hat{s}_0^2 - 4N}}{2},$$

te primijetimo da pošto je

$$(\hat{s}_0 + s_0)(\hat{s}_0 - s_0) = \left(\sqrt{\hat{s}_0^2 - 4N} - \sqrt{s_0^2 - 4N}\right)\left(\sqrt{\hat{s}_0^2 - 4N} + \sqrt{s_0^2 - 4N}\right)$$

imamo

$$
\begin{aligned}
|\hat{p} - p| &= \left|\frac{\hat{s}_0 + \sqrt{\hat{s}_0^2 - 4N}}{2} - \frac{s_0 + \sqrt{s_0^2 - 4N}}{2}\right| \\
&= \left|\frac{\hat{s}_0 - s_0}{2} + \frac{\sqrt{\hat{s}_0^2 - 4N} - \sqrt{s_0^2 - 4N}}{2}\right| \\
&= \left|\frac{\hat{s}_0 - s_0}{2} + \frac{1}{2}\frac{(\hat{s}_0 + s_0)(\hat{s}_0 - s_0)}{\sqrt{\hat{s}_0^2 - 4N} + \sqrt{s_0^2 - 4N}}\right| \\
&\leq \frac{1}{2}|(\hat{s}_0 - s_0)| + \frac{1}{2}\left|\frac{\hat{s}_0 + s_0}{\sqrt{\hat{s}_0^2 - 4N} + \sqrt{s_0^2 - 4N}}\right||(\hat{s}_0 - s_0)|.
\end{aligned}
$$

Prethodnu nejednakost možemo pojednostaviti, jer je $\hat{s}_0 < 2s_0$ i $s_0 = p + q < 3N^{\frac{1}{2}}$ iz čega slijedi

$$
\begin{aligned}
\left|\frac{\hat{s}_0 + s_0}{\sqrt{\hat{s}_0^2 - 4N} + \sqrt{s_0^2 - 4N}}\right| &< \left|\frac{\hat{s}_0 + s_0}{\sqrt{s^2 - 4N}}\right| \\
&< \left|\frac{3s_0}{\sqrt{s_0^2 - 4N}}\right| \\
&= 3\left|\frac{p+q}{p-q}\right| \\
&< \left|\frac{3N^{\frac{1}{2}}}{\frac{1}{\lambda}N^{\frac{1}{2}}}\right| \\
&= 9\lambda
\end{aligned}
$$

pa imamo

$$\begin{aligned}|\hat{p} - p| &< \frac{1}{2}(1 + 9\lambda)|(\hat{s}_0 - s_0)| \\ &< \frac{1}{2}(1 + 9\lambda)2\gamma N^{\frac{1}{4}} \\ &< 10\lambda\gamma N^{\frac{1}{4}}.\end{aligned}$$

Stoga znamo oko jednu polovinu MSB od p pa iz Teorema 4, uzimajući da je dovoljno da znamo malo manje od jedne polovine MSB, možemo izračunati p i otuda faktorizirati modul u vremenskom polinomu $\log(N)$, λ i γ. Posebno, možemo tražiti male nultočke linearnog polinoma $f(x) = x + \hat{p}$ koji ima samo jednu malu nultočku $p_0 = p - \hat{p}$, modulo p. Koristeći Coppersmithovu metodu za $c = 10\lambda\gamma$ i $\beta = \frac{1}{2}$ možemo izračunati tu nultočku, time dobivamo faktorizaciju modula. □

Ovaj teorem je poboljšanje prethodnog teorema za javni eksponent manji od $N^{\frac{1}{4}}$, ali postoji još jači teorem za javni eksponent kada je $N^{\frac{1}{4}} \leq e \leq N^{\frac{1}{2}}$, pod uvjetom da je e prost. Time smo došli do najjačeg poznatog napada kada su poznati neki MSB od privatnog eksponenta, koji ćemo sada dokazati i iskazati.

Teorem 9 ([1, Theorem 4.3]). *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent koji je ujedno i prost broj, gdje je $\frac{1}{4} < \alpha \leq \frac{1}{2}$ i d privatni eksponent definiran modulo $\varphi(N)$. Ako je poznato α MSB privatnog eksponenta, onda modul N može biti faktoriziran u polinomijalnom vremenu* $\log(N)$.

Dokaz. Pošto znamo α MSB privatnog eksponenta, iz Leme 2 znamo da možemo konstruirati $\hat{k}$ takav da konstanta iz fundamentalne jednadžbe zadovoljava $k \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$. Pretpostavimo sada da znamo k te primijetimo da je

$$s_0 = p + q = N + 1 + \frac{1 - ed}{k},$$

te, modulo e,

$$s_0 \equiv p + q \equiv N + 1 + k^{-1} \pmod{e}.$$

Inverz od k je dobro definiran jer su e i k relativno prosti, a pošto znamo k možemo izračunati s_0 modulo e. Također znamo da je $s_0 = p + q$ i $N = pq$ te primijetimo da

$$x^2 - s_0 x + N = x^2 - (p + q)x + pq = 0,$$

ima nultočke p i q, a iz toga slijedi da

$$x^2 - s_0 x + N \equiv 0 \pmod{e}, \tag{4.12}$$

također ima nultočke $p_0 = p \pmod{e}$ i $q_0 = q \pmod{e}$. Zato što je e prost broj, p_0 i q_0 su jedine nultočke jednadžbe i možemo ih izračunati u polinomijalnom vremenu $\log(N)$. Kada su nam poznati p_0 i q_0, možemo izračunati modul pomoću Teorema 4 jer znamo jednu polovinu LSB od p i q. Vidimo da kada znamo konstantu k možemo faktorizirati modul. Pošto mi ne znamo k možemo ponoviti provedeni postupak za svaki $k' \in \langle \hat{k} - 9, \hat{k} + 9 \rangle$ sve dok ne dobijemo $k' = k$, time slijedi i faktorizacija modula. Sve možemo izračunati u polinomijalnom vremenu $\log(N)$ pa rezultat slijedi. □

Ovaj napad je jak jer je potrebna samo jedna četvrtina bitova za faktorizaciju modula, ali je problem što javni eksponent mora biti prost broj. Taj uvjet je potreban da bi osigurali da jednadžba (4.12) ima samo dvije nultočke i da ih možemo efikasno izračunati. Napad može biti konstruiran i kada javni eksponent nije prost broj, samo što onda mora biti poznata faktorizacija javnog eksponenta, ili se mora moći izračunati faktorizacija. Ako javni eksponent ima r prostih faktora $e_1, \ldots, e_r$, s potencijama redom $\gamma_1, \ldots, \gamma_r$, onda će jednadžba

$$x^2 - s_0 x + N \equiv 0 \pmod{e_i},$$

imati nultočke $p \pmod{e_i}$ i $q \pmod{e_i}$ za svaki i. Ako je potencija od e_i veća od jedan, onda dobivamo nultočke p i q modulo $e_i^{\gamma_i}$. Kada imamo sve $p \pmod{e_i^{\gamma_i}}$ možemo izračunati $p \pmod{e}$ pomoću Kineskog teorema o ostatcima koji glasi ovako:

Teorem 10 ([3, Theorem 2.1.]). *Neka su $m_1, \ldots, m_r$ u parovima relativno prosti prirodni brojevi te neka su $a_1, \ldots, a_r$ cijeli brojevi. Tada sustav od r kongruencija $x = a_i \pmod{m_i}$, za $1 \leq i \leq r$ ima jedinstvenu nultočku modulo $M = m_1 \cdots m_r$, koja je dana s*

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod{M},$$

gdje je $M_i = \frac{M}{m_i}$ i $y_i = M_i^{-1} \pmod{m_i}$, za $1 \leq i \leq r$.

Pošto imamo dva kandidata za $p \pmod{e_i^{\gamma_i}}$, za svaki i, morat ćemo isprobati 2^r mogućih kombinacija prije nego što uspijemo izračunati $p \pmod{e}$. Idući korolar nam govori baš o tome.

Korolar 1 ([3, Corollary 6.10.]). *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^\alpha$ javni eksponent, gdje je $\frac{1}{4} < \alpha \leq \frac{1}{2}$ i d privatni eksponent definirani modulo $\varphi(N)$. Ako je poznato α MSB privatnog eksponenta, javni eksponent ima r različitih prostih faktora i faktorizacija javnog eksponenta je poznata, onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$ i 2^r.*

Kada je javni eksponent veći od $N^{\frac{1}{2}}$, možemo koristiti napade za proizvoljnu veličinu eksponenta ako je poznato dovoljno MSB od d. Najjači rezultat se dobiva kada stavimo da je $\beta \approx 1$ u Napadu 2.

Napad 6 ([2, Theorem 2]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^\alpha \geq N^{\frac{1}{2}}$ javni eksponent i neka je d privatni eksponent definiran modulo $\varphi(N)$. Poznat nam je javni ključ (e, N) i $\hat{d}$ zadovoljava $|d - \hat{d}| < N^\delta$, ako je*

$$\delta \leq \frac{1}{3} + \frac{\alpha}{3} - \frac{1}{3}\sqrt{4\alpha^2 + 2\alpha - 2} - \epsilon, \tag{4.13}$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

5 | Djelomično poznavanje privatnog eksponenta: LSB

U ovom poglavlju ćemo razmatrati napade u kojima suparnik zna neki broj LSB od privatnog eksponenta. Stoga ćemo pretpostaviti da suparnik zna $\tilde{d}$ i neki M takav da vrijedi $\tilde{d} = d \pmod{M}$. Dakle privatni eksponent možemo zapisati kao $d = d_0 M + \tilde{d}$, gdje je d_0 jedina nepoznanica. Neka je $d = N^{\beta}$ i $M = N^{\beta-\delta}$, tada d_0 zadovoljava

$$|d_0| = \left|\frac{d - \tilde{d}}{M}\right| < \left|\frac{d}{M}\right| < N^{\delta},$$

pa vidimo da se δ još uvijek koristi za predstavljanje veličine nepoznatog dijela privatnog eksponenta. Kao što smo radili kod slučaja za MSB, tako ćemo i ovdje početi s napadom za proizvoljnu veličinu javnog i privatnog eksponenta, a zatim ćemo nastaviti sa slučajevima kada je jedan od eksponenata pune veličine.

5.1 Proizvoljni eksponent

Postoji jedan napad s djelomičnim poznavanjem ključa, te s poznatim LSB privatnog eksponenta, koji se odnosi na proizvoljne javne i privatne eksponente.

Napad 7 ([3, Attack 6.12.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definiran modulo $\varphi(N)$. Neka je $M = N^{\beta-\delta}$ za neke $0 \leq \delta \leq \beta$. Ukoliko su nam poznati javni ključ (e, N), M i $\tilde{d} = d \pmod{M}$, i vrijedi*

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\beta + 6\alpha - 5} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Dokaz. Neka je $d = Md_0 + \tilde{d}$, te primijetimo da fundamentalnu jednadžbu možemo zapisati u obliku

$$eMd_0 + e\tilde{d} = 1 + kN - ks,$$

gdje su d_0, k i s jedine nepoznanice. To nam sugerira da tražimo male nultočke polinoma

$$f(x, y, z) = (eM)x - Ny + yz + e\tilde{d} - 1 \in \mathbb{Z}[x, y, z],$$

jer je $(x_0, y_0, z_0) = (d_0, k, s)$ nultočka od $f(x, y, z)$ nad skupom cijelih brojeva. Definirajmo $X = N^{\delta}$, $Y = 2N^{\alpha+\beta-1}$ i $Z = 3N^{\frac{1}{2}}$ te primijetimo

$$|x_0| = |d_0| = \left|\frac{d - \tilde{d}}{M}\right| < \left|\frac{d}{M}\right| = N^{\delta} = X$$

$$|y_0| = |k| = \left|\frac{ed - 1}{\varphi(N)}\right| < 2N^{\alpha+\beta-1} = Y$$

$$|z_0| = |s| = |N - \varphi(N)| < 3N^{\frac{1}{2}} = Z,$$

a $W = ||f(xX, yY, zZ)||_{\infty}$ je dano s

$$W = max\{eMX, NY, y + YZ, e\tilde{d} - 1\} = NY = 2N^{\alpha+\beta}.$$

Vidimo da polinom $f(x, y, z)$ ima slične ili iste monome kao polinom u dokazu Napada 1. Također su i granice za X, Y, Z i W iste. Prema tome, iz dokaza Napada 1 možemo zaključiti da za dovoljno velik N, nultočka (x_0, y_0, z_0) može biti izračunata u polinomijalnom vremenu $\log(N)$ kada je

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\beta + 6\alpha - 5} - \epsilon,$$

i zadovoljene su Pretpostavke 1 i 2. Tada je lako dobiti faktorizaciju modula N jer kada znamo $z_0 = s$, znamo i $\varphi(N) = N - s$. □

5.2 Javni eksponent u punoj veličini

Kada je javni eksponent u punoj veličini postoje napadi s djelomičnim poznavanjem ključa kada god je privatni eksponent manji od $N^{0.875}$, pod uvjetom da je poznato dovoljno LSB privatnog eksponenta.

Za male privatne eksponente koristimo napade u kojima nam nije potreban niti jedan LSB od privatnog eksponenta. Jedan od tih napada je Wienerov napad, koji smo iskazali u Teoremu 6, koji učinkovito faktorizira modul kada je privatni eksponent manji od $N^{\frac{1}{4}}$. Drugi je Napad 3 koji kaže da se RSA smatra nesigurnim kada je privatni eksponent manji od $N^{0.2929}$.

Za veće privatne eksponente je najbolji poznati napad upravo Napad 7. Kada uvrstimo u njega $\alpha \approx 1$ dobijemo sljedeće:

Napad 8 ([3, Attack 6.13.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je e javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definiran modulo $\varphi(N)$. Neka je $M = N^{\beta-\delta}$ za neke $0 \leq \delta \leq \beta$. Ako su nam poznati javni ključ (e, N), M i $\tilde{d} = d \pmod{M}$, i vrijedi*

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\beta + 1} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Primijetimo da kada je $\beta \geq \frac{21}{24} = 0.875$, dovoljan uvjet za napad je $\delta \leq 0$. Pošto je to samo dovoljan uvjet, ništa ne možemo reći o napadima za privatan eksponent koji je veći od $N^{0.875}$.

5.3 Privatni eksponent u punoj veličini

Kada je privatni eksponent u punoj veličini, postoje dva napada u slučaju kada je javni eksponent manji od $N^{0.875}$, pod uvjetom da je poznato dovoljno LSB privatnog eksponenta.

Kada je javni eksponent vrlo mali, postoji napad koji zahtjeva da znamo samo jednu četvrtinu LSB privatnog eksponenta. To je najjači napad s poznatim LSB i donekle je sličan najjačem napadu s poznatim MSB koji smo iskazali u Teoremu 9. Ovdje ćemo iskazati modifikaciju tog rezultata u sljedećem napadu.

Napad 9 ([3, Attack 6.14.]). *Neka je N RSA modul s balansiranim prostim brojevima p i q, neka je e javni eksponent i d privatni eksponent definiran modulo $\varphi(N)$. Ako je poznata jedna četvrtina LSB privatnog eksponenta, onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$ i e.*

Napad se oslanja na računanje nultočki kongruencijske jednadžbe

$$x^2 - (p+q)x + N \equiv 0 \pmod{2^\gamma}, \tag{5.1}$$

za neki prirodan broj $\gamma > 1$. Pošto 2^γ nije prost broj, može postojati puno nultočki te jednadžbe. Sljedeća lema u potpunosti karakterizira tražene nultočke. U nastavku ćemo označiti t_x kao najveći cijeli broj takav da 2^{t_x} dijeli x.

Lema 3 ([3, lemma 6.15.]). *Neka je $N = pq$ n-bitni RSA modul i neka je S_l skup nultočki jednadžbe*

$$x^2 - (p+q)x + pq \equiv 0 \pmod{2^{\frac{n}{4}-l}},$$

za neki prirodan broj $0 \leq l \leq \frac{n}{4}$. Onda je veličina od S_l dana s

$$|S_l| = \begin{cases} 2^{t_{p-q}+v}, & l < \frac{n}{4} - 2(t_{p-q}-1) \\ 2^{\left\lfloor \frac{\frac{n}{4}-l}{2} \right\rfloor}, & l \geq \frac{n}{4} - 2(t_{p-q}-1), \end{cases}$$

gdje je $v = 1$ kada je $l \leq \frac{n}{4} - 2(t_{p-q}-1) - 3$, $v = 0$ kada je $l = \frac{n}{4} - 2(t_{p-q}-1) - 2$, i $v = -1$ kada je $l = \frac{n}{4} - 2(t_{p-q}-1) - 1$. Nadalje, neka je $\eta = \frac{n}{4} - l$, tada su sve nultočke oblika

$$x_0 \equiv \begin{cases} (\{p,q\} \pmod{2^{\eta - t_{p-q}}}) + r2^{\eta - t_{p-q}} \pmod{2^\eta}, & l < \frac{n}{4} - 2(t_{p-q}-1) \\ \left(p \pmod{2^{\left\lfloor \frac{\eta}{2} \right\rfloor}}\right) + r2^{\left\lceil \frac{\eta}{2} \right\rceil} \pmod{2^\eta}, & l \geq \frac{n}{4} - 2(t_{p-q}-1), \end{cases}$$

gdje je r cijeli broj.

Broj nultočki jednadžbe (5.1) ovisi o l i t_{p-q}. Uočimo da je t_{p-q} broj LSB koji su zajednički p i q. Prema tome, kada god je l mali te p i q nemaju puno zajedničkih LSB, tada će broj nultočki biti mali. Kada bi se p i q ponašali kao nasumični neparni cijeli brojevi, tada bi imali sljedeću vjerojatnost $P[t_{p-q} = m] = 2^{-m}$ i očekivanje $E[t_{p-q}] \leq 2$. U praksi je uočeno da nasumično generirani RSA prosti parovi zadovoljavaju $P[t_{p-q} = m] \approx 2^{-m}$. Stoga se u praksi očekuje da će postojati najviše osam nultočaka jednadžbe (5.1), kada je l mali. Sada možemo dati opravdanje za napad.

Dokaz. Neka je N n-bitni RSA modul, neka je $\tilde{d} = d \pmod{2^{\frac{n}{4}}}$ jedna četvrtina poznatih LSB privatnog eksponenta i neka je $k = m2^{t_k}$ konstanta iz fundamentalne jednadžbe, gdje je $m = \frac{k}{2^{t_k}}$ neparan broj. Za sada pretpostavimo da znamo k. Iz fundamentalne jednadžbe, $ed = 1 + k(N + 1 - s_0)$, uočimo da vrijedi

$$ks_0 = k(N+1) - (ed-1) = k(N+1) - k\left(\frac{ed-1}{k}\right),$$

gdje je $\frac{ed-1}{k} = \varphi(N)$ cijeli broj. Supstituiramo li $k = m2^{t_k}$ u tu jednadžbu imamo

$$m2^{t_k}s_0 = m2^{t_k}(N+1) - 2^{t_k}\left(\frac{ed-1}{2^{t_k}}\right),$$

te, modulo $2^{\frac{n}{4}-t_k}$,

$$ms_0 \equiv m(N+1) - \left(\frac{e\tilde{d}-1}{2^{t_k}}\right) \pmod{2^{\frac{n}{4}-t_k}},$$

gdje je desna strana jednadžbe poznata. Podijelimo sada cijelu jednadžbu s m te dobivamo

$$s_0 \equiv (N+1) - m^{-1}\left(\frac{e\tilde{d}-1}{2^{t_k}}\right) \pmod{2^{\frac{n}{4}-t_k}}.$$

Pošto znamo $s_0 \pmod{2^{\frac{n}{4}-t_k}}$, onda možemo riješiti jednadžbu

$$x^2 - s_0x + N \equiv 0 \pmod{2^{\frac{n}{4}-t_k}},$$

za koju znamo da ima nultočke $p_0 = p \pmod{2^{\frac{n}{4}-t_k}}$, i $q_0 = q \pmod{2^{\frac{n}{4}-t_k}}$. Ako znamo jednu od nultočki, na primjer p_0, onda možemo konstruirati $p \pmod{2^{\frac{n}{4}}}$ tako da napravimo iscrpnu pretragu nad nepoznatih t_k bitova i faktorizirati modul koristeći Teorem 4 pošto je jedna polovina LSB od p ili q poznata. Stoga, kada znamo k ili p_0 možemo faktorizirati modul primjenjujući Coppersmithovu metodu najviše 2^{t_k} puta.

Pošto ne znamo k, radimo iscrpnu pretragu da ga pronađemo. Za svaki $2 \leq k' < e$, koji je relativno prost s e, računamo

$$\tilde{s}_0' = (N+1) - m^{-1}\left(\frac{e\tilde{d}-1}{2^{t_{k'}}}\right) \pmod{2^{\frac{n}{4}-t_{k'}}},$$

ako postoji, i rješavamo jednadžbu

$$x^2 - \tilde{s}'_0 x + N \equiv 0 \pmod{2^{\frac{n}{4}-t_{k'}}}.$$

Ako pretpostavimo da vrijedi $t_k < \frac{n}{4} - 2(t_{p-q} - 1)$, tada će prema Lemi 3, postojati najviše $2^{t_{p-q}+1}$ nultočaka prethodne jednadžbe. Ukoliko ih dobivamo više, odbacujemo k' i pokušavamo s drugom vrijednosti za k'. Kada jednadžba ima najviše $2^{t_{p-q}+1}$ nultočki, svaka nultočka je kandidat za $p_0 = p \pmod{2^{\frac{n}{4}-t_k}}$, ili $q_0 = q \pmod{2^{\frac{n}{4}-t_k}}$. Svaki od tih kandidata onda možemo iskoristiti da bi konstruirali 2^{t_k} kandidata za $p \pmod{2^{\frac{n}{4}}}$, ili $q \pmod{2^{\frac{n}{4}}}$, pogađanjem dodatnih t_k bitova. Kada je $k' = k$, onda smo pronašli pravog kandidata i modul će biti faktoriziran. Pošto svaki k' dovodi do najviše $2^{t_{p-q}+1}2^{t_{k'}}$ kandidata i uzimamo u obzir svaki $k' \in [2, e\rangle$, slijedi da je granica za ukupan broj kandidata za $p \pmod{2^{\frac{n}{4}}}$ dana s $2^{t_{p-q}+1}e\lceil\log_2(e)\rceil$. Označimo $\gamma = t_{p-q} + 1$ i uočimo sljedeće

$$\sum_{k'=2}^{e} 2^{\gamma+t_{k'}} \leq \sum_{c=0}^{\lceil\log_2(e)\rceil} 2^{\gamma+c} H(c) < \sum_{c=0}^{\lceil\log_2(e)\rceil} 2^{\gamma+c} \left\lfloor \frac{e}{2^c} \right\rfloor \leq 2^{\gamma} e \lceil\log_2(e)\rceil,$$

gdje je $H(c)$ broj onih k' koji zadovoljavaju $t_{k'} = c$. U najboljem slučaju ($t_{p-q} = 1$) imamo najviše $4e\lceil\log_2(e)\rceil$ kandidata koja trebamo testirati. U najgorem slučaju, kada je t_{p-q} jako velik i $t_{k'} \geq \frac{n}{4} - 2(t_{p-q} - 1)$, imat ćemo eksponencijalni broj nultočki jednadžbe.

Pod pretpostavkom da se p i q ponašaju kao nasumični neparni cijeli brojevi, očekivana vrijednost od t_{p-q} je otprilike 2. Uzimajući to u obzir, onda očekujemo faktoriziranje modula testiranjem najviše $8\lceil\log_2(e)\rceil$ kandidata. Pošto svi izračuni mogu biti odrađeni u vremenu polinomijalnom u $\log(N)$, rezultat slijedi. □

U praksi se može smanjiti broj kandidata koje je potrebno testirati, tako da zanemarimo neke vrijednosti za k prije rješavanja odgovarajuće jednadžbe. Na primjer, budući da je $(e, k) = 1$, sve vrijednosti od k' takve da je $(e, k') > 1$ mogu biti zanemarene. Također, kada je $k' = k$ znamo da su $p_0 = p \pmod{2^{\frac{n}{4}-t_k}}$ i $q_0 = q \pmod{2^{\frac{n}{4}-t_k}}$ nultočke jednadžbe. Također, pošto znamo $s_0 = (p + q) \pmod{2^{\frac{n}{4}-t_k}}$, slijedi da dvije od najviše $2^{t_{p-q}+1+t_k}$ nultočki, označimo ih s x_1 i x_2, trebaju zadovoljavati $s_0 \equiv x_1 + x_2 \pmod{2^{\frac{n}{4}-t_k}}$. Ako ne postoje dvije nultočke, tada se trenutna vrijednost k' može odbaciti. Dodatno, kada je broj nultočki mali, samo nultočke koje zadovoljavaju $s_0 \equiv x_1 + x_2 \pmod{2^{\frac{n}{4}-t_k}}$ treba uzeti u obzir kao kandidate.

Budući da vrijeme izvođenja napada ovisi o veličini javnog eksponenta, napad se može izvesti samo za vrlo male javne eksponente. Doista, da bi se održala ukupna složenost koja je polinomijalna u $\log(N)$, veličina javnog eksponenta također treba biti polinomijalna u $\log(N)$.

Kada je javni eksponent veći pa ne možemo koristiti Napad 9, može se koristiti Napad 7 tako da uvrstimo aproksimaciju $\beta \approx 1$ i onda dobivamo sljedeći napad.

Napad 10 ([3, Attack 6.16.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je*

$e = N^{\alpha}$ javni eksponent i neka je d privatni eksponent definiran modulo $\varphi(N)$. Neka je $M = N^{1-\delta}$ za neke $0 \leq \delta \leq 1$. Ukoliko su nam poznati javni ključ (e, N), M i $\tilde{d} = d \pmod{M}$, te

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{6\alpha + 1} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Primijetimo da je za $\alpha \geq \frac{21}{24} = 0.875$ dovoljan uvjet za napad $\delta \leq 0$. Zato, slično kao i u slučaju privatnog eksponenta u punoj veličini, ništa ne možemo reći o napadima za javni eksponent koji je veći od $N^{0.875}$.

6 | Djelomično poznavanje bitova prostih brojeva p i q

Za većinu napada s djelomičnim poznavanjem ključa u ovom radu koristili smo fundamentalnu jednadžbu

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

te se oslanjali na činjenicu da je modul N dobra aproksimacija za $\varphi(N)$. Konkretno, granice za svaki od napada ovise o $|N - \varphi(N)| = |s| < 3N^{\frac{1}{2}}$ pa napadi mogu biti poboljšani ako imamo bolju aproksimaciju za $\varphi(N)$.

Kada je poznat neki broj MSB od jednog ili oba prosta broja p i q, možemo konstruirati bolju aproksimaciju za $\varphi(N)$. Neka je $\hat{p}$ aproksimacija za p koja zadovoljava

$$|p - \hat{p}| < N^{\gamma},$$

za neki $\frac{1}{4} < \gamma \leq \frac{1}{2}$. Stoga kada znamo $\hat{p}$, znamo i $\frac{\gamma}{2}$ MSB od p, pri čemu kao i inače pretpostavljamo da su p i q balansirani prosti brojevi. Nema potrebe razmatrati slučaj kada je $\gamma \leq \frac{1}{4}$ jer zbog Teorema 4 znamo da u tom slučaju možemo dobiti faktorizaciju modula pošto znamo jednu polovinu MSB od p. Kada znamo $\hat{p}$ možemo izračunati i $\hat{q} = \frac{N}{\hat{p}}$, što je MSB od q i zadovoljava

$$|q - \hat{q}| = \left|\frac{N}{p} - \frac{N}{\hat{p}}\right| = \left|\frac{N(\hat{p} - p)}{\hat{p}p}\right| < 4N^{\gamma},$$

gdje smo pretpostavili da su $p, \hat{p} > \frac{1}{2}N^{\frac{1}{2}}$. Kada je $p > q$, možemo pretpostaviti da su $p, \hat{p} > N^{\frac{1}{2}}$ iz čega slijedi $|q - \hat{q}| < N^{\gamma}$. Primijetimo da koristeći MSB od p i q možemo izračunati aproksimaciju N' za $\varphi(N)$ koja je dana s $N' = N - \hat{p} - \hat{q} + 1$ i zadovoljava

$$|\varphi(N) - N'| = |N - p - q + 1 - (N - \hat{p} - \hat{q} + 1)| = |p - \hat{p} + q - \hat{q}| < 5N^{\gamma}.$$

Inače smo koristili N kao aproksimaciju za $\varphi(N)$, a pošto je

$$|\varphi(N) - N| = |s| \geq \frac{3}{2}N^{\frac{1}{2}},$$

vidimo da je N' bolja aproksimacija za $\varphi(N)$ ako je $\gamma < \frac{1}{2} - \log_N(\frac{3}{10})$. Neka je $s' = N' - \varphi(N)$, možemo fundamentalnu jednadžbu napisati u obliku

$$ed = 1 + k\varphi(N) = 1 + k(N' - s'), \tag{6.1}$$

i to koristiti kao početnu točku za sve poznate napade na RSA. U nastavku ćemo navesti glavne rezultate za napade kada je privatni eksponent mali i napade s djelomičnim poznavanjem ključa, ali ćemo sada koristiti jednakost (6.1) kao polazište.

6.1 Napadi kada je privatni eksponent mali

U sljedećem teoremu ćemo iskazati generalizaciju Wienerovog napada za male privatne eksponente (Teorem 6), kada su poznati MSB jednog od prostih brojeva p ili q.

Teorem 11 ([3, Theorem 6.17.]). *Neka je $N = pq$ RSA modul s balansiranim prostim brojevima, neka je e javni eksponent i d privatni eksponent definiran modulo $\varphi(N)$. Neka $k \in \mathbb{Z}$ zadovoljava $ed = 1 + k\varphi(N)$, $g = NZD(p-1, q-1)$, $g_0 = \frac{g}{NZD(g,k)}$ i $k_0 = \frac{k}{NZD(k,g)}$. Ako nam je poznat $\hat{p}$ takav da $|p - \hat{p}| < N^{\gamma}$, te privatni eksponent zadovoljava*

$$d < \frac{N'}{2s'g_0k_0} = \frac{N^{1-\gamma}}{10g_0k_0}, \tag{6.2}$$

gdje je $N' = N - \hat{p} - \frac{N}{\hat{q}} + 1$ i $s' = N' - \varphi(N)$, onda N može biti faktoriziran u polinomijalnom vremenu u ovisnosti o $\log(N)$ i $\frac{g}{k}$.

Neka je $d = N^{\delta}$ i ako pretpostavimo da je g_0 mali, uvjet (6.2) možemo pojednostaviti na sljedeći način

$$\delta \leq \begin{cases} \frac{3}{4} - \frac{\alpha}{2} - \epsilon, & \gamma = \frac{1}{2} \\ 1 - \frac{\alpha}{2} - \frac{\gamma}{2} - \epsilon, & \gamma < \frac{1}{2}, \end{cases}$$

za javne eksponente proizvoljne veličine i

$$\delta \leq \begin{cases} \frac{1}{4} - \epsilon, & \gamma = \frac{1}{2}, \alpha = 1 \\ \frac{1}{2} - \frac{\gamma}{2} - \epsilon, & \gamma < \frac{1}{2}, \alpha = 1, \end{cases}$$

za javne eksponente u punoj veličini. Kao što vidimo, kada je $\gamma = \frac{1}{2}$ granica odgovara Wienerovoj granici.

Dalje ćemo navesti generalizirani rezultat jakog napada za male privatne eksponente.

Napad 11 ([5, Theorem 5]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je e javni eksponent i neka je $d = N^{\delta}$ privatni eksponent definiran modulo $\varphi(N)$. Ako nam je poznat javni ključ (e, N) i γ MSB od p ili q, pri čemu je $\frac{1}{4} < \gamma \leq \frac{1}{2}$ i vrijedi*

$$\delta \leq \frac{2}{5} - \frac{6}{5}\gamma + \frac{2}{5}\sqrt{4\gamma^2 - \gamma + 1} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Idući napad je generalizacija Napada 3.

Napad 12 ([5, Theorem 4]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je e javni eksponent i neka je $d = N^{\delta}$ privatni eksponent definiran modulo $\varphi(N)$. Ako nam je poznat javni ključ (e, N) i γ MSB od p ili q, pri čemu je $\frac{1}{4} < \gamma \leq \frac{1}{2}$ i vrijedi*

$$1 - 2\gamma < \delta \leq 1 - \sqrt{\gamma} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

6.2 Napadi s djelomičnim poznavanjem ključa

U sljedećem napadu ćemo navesti kombiniranu generalizaciju Napada 1 i 7, tj. napad za proizvoljnu veličinu javnog eksponenta s poznatim MSB i LSB privatnog eksponenta.

Napad 13 ([3, Attack 6.20.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definiran modulo $\varphi(N)$. Ako nam je poznat $\hat{p}$ takav da je $|p - \hat{p}| < N^{\gamma}$, i barem $\frac{\beta - \delta}{\beta}$ MSB ili LSB privatnog eksponenta, te δ zadovoljava*

$$\delta \leq 1 - \frac{\gamma}{3} - \frac{2}{3}\sqrt{\gamma(\gamma + 3\beta + 3\alpha - 3)} - \epsilon,$$

onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Generalizacija Napada 2, tj. napad za proizvoljnu veličinu javnog eksponenta s poznatim MSB privatnog eksponenta dan je u nastavku.

Napad 14 ([3, Attack 6.21.]). *Za svaki $\epsilon > 0$ postoji n_0 takav da za svaki $n > n_0$ vrijedi sljedeće: Neka je N n-bitni RSA modul s balansiranim prostim brojevima p i q, neka je $e = N^{\alpha}$ javni eksponent i neka je $d = N^{\beta}$ privatni eksponent definiran modulo $\varphi(N)$. Ako su nam poznati $\hat{p}$ i $\hat{d}$ takvi da je $|p - \hat{p}| < N^{\gamma}$ i $|d - \hat{d}| < N^{\delta}$, ako δ zadovoljava*

$$\delta \leq 1 - \gamma + \frac{\lambda}{3} - \frac{2}{3}\sqrt{\lambda(\lambda + 3\gamma)} - \epsilon,$$

gdje je $\lambda = \max\{\delta + \alpha - 1, \beta + \alpha - \frac{3}{2}\}$, onda modul N može biti faktoriziran u polinomijalnom vremenu $\log(N)$, ako su zadovoljene Pretpostavke 1 i 2.

Ono što je prilično zanimljivo kod ovih kombiniranih napada s djelomičnim poznavanjem ključa je da, kada su neki bitovi prostih brojeva p ili q poznati, ukupan broj bitova potrebnih u kombinaciji prostih brojeva i privatnog eksponenta je manji nego ukupan broj potrebnih bitova kada su dostupni samo bitovi iz privatnog eksponenta.

7 | Zaključak

U ovom diplomskom radu smo istražili ranjivost RSA kriptosustava pokazujući kako kompromitacija djelomičnih informacija o privatnom ključu ili prostim brojevima p i q može značajno oslabiti sigurnost RSA. Ispitali smo kako faktoriziranje s poznatom polovinom značajnih bitova omogućuje napadačima da iskoriste djelomično poznavanje prostih brojeva p ili q kako bi olakšali faktorizaciju RSA modula, narušavajući sigurnost sustava. Zatim smo se pozabavili napadima u kojima je privatni eksponent djelomično poznat. Analiza MSB i LSB privatnog ključa pokazala je kako čak i ograničena izloženost bilo kojeg segmenta može dovesti do potpunog oporavka ključa korištenjem naprednih kriptoanalitičkih tehnika. Naposljetku, u djelomičnom poznavanju bitova prostih brojeva raspravljali smo o tome kako napadači mogu iskoristiti nepotpune informacije o p ili q da dođu do faktorizacije RSA modula, ugrožavajući kriptosustav. Iz ovog rada možemo vidjeti važnost zaštite svih komponenti RSA ključa, jer čak i manje curenje može rezultirati potpunim slomom sigurnosti. Jačanje zaštitnih mjera protiv djelomičnog izlaganja ključa presudno je za održavanje integriteta RSA u praksi.

Literatura

[1] D. Boneh, G. Durfee, Y. Frankel, *Exposing an RSA Private Key Given a Small Fration of its Bits*, Stanford University, 2001.

[2] M. Ernst, E. Jochemsz, A. May, B. de Weger, *Partial key exposure attacks on RSA up to full size exponents*, Lecture Notes in Computer Science, Vol. 3494, 371-386, Springer, 2005.

[3] M. Hinek, *Cryptanalysis of RSA and Its Variants*, CRC Press, Boca Raton, 2010.

[4] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, 2014

[5] S. Sarkar, S. Maitra, S. Sarkar, *RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension*, Cryptology ePrint Archive, Report 2008/315, 2008.

[6] Hrvatska enciklopedija dostupna na https://www.enciklopedija.hr/

Sažetak

U ovom diplomskom radu ćemo prvo objasniti što je RSA kriptosustav, zatim ćemo krenuvši od općenitijih teorema i napada doći do glavnih, najbitnijih teorema i napada s djelomičnim poznavanjem ključa. Napadi koje ćemo iskazati i dokazati koriste djelomične informacije o privatnom ključu ili o prostim brojevima p i q, za koje vrijedi $N = pq$, kako bi ugrozili sigurnost RSA kriptosustava. U radu ćemo vidjeti koje su najmanje informacije koje moramo znati o tajnom ključu te o prostim brojevima p i q da bi mogli faktorizirati modul N.

Ključne riječi

RSA kriptosustav, Eulerov teorem, Wilsonov teorem, fundamentalna jednadžba, privatni i javni eksponenti, javni i tajni ključ, MSB, LSB, Kineski teorem o ostatcima, Coppersmithova metoda, Wienerov napad

Partial key exposure attacks

Summary

In this final paper, we will first explain what the RSA cryptosystem is, then, starting from more general theorems and attacks, we will get to the main, most important theorems and attacks with partial key exposure. The attacks that we will present and prove use partial information about the private key or about the prime numbers p and q, for which $N = pq$ holds, to compromise the security of the RSA cryptosystem. In the paper, we will see what is the minimum information that we need to know about the private key and about the prime numbers p and q in order to be able to factorize the module N.

Keywords

RSA cryptosystem, Euler's theorem, Wilson's theorem, key equation, private and public exponents, public and private key, MSB, LSB, Chinese remainder theorem, Coppersmith's method, Wiener's attack

Životopis

Rođena sam 11. siječnja 1998. godine u Osijeku. Pohađala sam Osnovnu školu Ljudevita Gaja u Osijeku te III. gimnaziju Osijek, svoje srednjoškolsko obrazovanje završavam 2016. godine. Iste godine upisujem preddiplomski studij matematike na Sveučilištu J.J. Strossmayera u Osijeku na Odjelu za matematiku (sadašnji Fakultet primijenjene matematike i informatike) koji završavam 2020. godine. Na jesen iste godine, na istom fakultetu upisujem i diplomski studij, smjer Financijska matematika i statistika.