Kriptoanaliza RSA kriptosustava i njegovih inačica

Alilović, Martina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martina Alilović

KRIPTOANALIZA RSA KRIPTOSUSTAVA I NJEGOVIH INAČICA

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, rujan, 2017.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

RSA kriptosustav je najkorišteniji kriptosustav s javnim ključem u svijetu, koristi se milijune puta svaki dan na Internetu. Dobio je ime po svojim stvarateljima: Ronu Rivestu, Adiu Shamiru i Leonardu Adlemanu. To je i prvi javno poznat kriptosustav sa javnim ključem u svijetu, objavljen 1977. u časopisu *Scientific American*. Uglavnom se RSA koristi za slanje ključa sesije za simetrični kriptosustav koji se onda koristi da osigura sigurnost komunikacije. Sve češće u upotrebi su i inačice RSA sustava koje su bazirane na RSA, ali su općenito efikasnije. Proučiti ćemo kriptoanalizu RSA kriptosustava i pet inačica RSA kriptosustava: CRT-RSA, RSA s više prostih faktora, RSA s višom potencijom, RSA sa zajedničkim prostim faktorom i dualni RSA.

U prvom poglavlju, gdje ćemo reći nešto općenito o RSA kriptosustavu, koristit ćemo se literaturom iz teorije brojeva i kriptografije [1], [2] i knjigom J. M. Hineka [3] koju ćemo najviše koristiti u radu. Kada navodimo matematičke tehnike, ponovno se koristimo s [1] i [3]. Kod ranih napada osim [3], koristimo knjigu S. Y. Yana [5], a kod napada baziranih na malom tajnom eksponentu i knjigu S. Katzenbeissera o posljednjim napretcima u kriptoanalizi RSA kriptosustava [4]. U trećem poglavlju, kod kriptoanalize RSA inačica, većina rada se oslanja na [3].

Poglavlje 1

RSA kriptosustav

1.1 Definicija i korektnost RSA kriptosustava

Poruku koju pošiljalac želi poslati primaocu zvat ćemo *otvoreni tekst*. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ*. Dobiveni rezultat nazivamo *šifrat*.

Definicija 1.1.1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

- $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;*
- $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
- $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
- *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_k \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_k \in \mathcal{D}$*. Pritom 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* $x \in \mathcal{P}$*.*

RSA je primjer kriptosustava s javnim ključem. Kod takvih kriptosustava funkcija šifriranja bit će javna, dok će funkcija dešifriranja biti tajna. Za obje funkcije mora vrijediti da se njihove vrijednosti mogu lako izračunati kako bi kriptosustav bio efikasan, ali se iz funkcije šifriranja ne smije moći lako izračunati funkcija dešifriranja kako bi kriptosustav bio siguran. Definirajmo sada RSA kriptosustav.

Definicija 1.1.2. *Neka je* $N = pq$ *produkt dva velika prosta broja* p *i* q*, neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$ *i definirajmo prostor ključeva kao:*

$$\mathcal{K} = \{(N, p, q, e, d) : ed \equiv 1 \pmod{\phi(N)}\}$$

gdje je $\phi(N) = (p-1)(q-1)$ *Eulerova funkcija. Za svaki ključ* $K \in \mathcal{K}$*, zadan s* $K = (N, p, q, e, d)$*, enkripcijsko pravilo* $enc_K : \mathbb{Z}_N \to \mathbb{Z}_N$ *definirano je s* $enc_K(x) = x^e \pmod{N}$*,*

a dekripcijsko pravilo $dec_K : \mathbb{Z}_N \to \mathbb{Z}_N$ *sa:* $dec_K(y) = y^d \pmod N$*, za svaki* $x,y \in \mathbb{Z}_N$*. Par* (e, N) *je RSA javni ključ, a trojika* (d, p, q) *je RSA tajni ključ.*

Produkt $N = pq$ zovemo RSA modul, faktore p i q RSA prosti faktori, e javni eksponent, a d tajni eksponent. Budući da vrijedi $ed \equiv 1 \pmod{\phi(N)}$ slijedi da je $ed = 1 + k\phi(N)$ za neki $k \in \mathbb{Z}$, ovu jednadžbu zovemo jednadžba ključa.

Da bi pokazali korektnost dekripcijskog pravila iskoristiti ćemo Eulerov teorem.

Teorem 1.1.3. *(Eulerov teorem). Ako je* $nzd(a, m) = 1$*, onda je* $a^{\phi(m)} \equiv 1 \pmod m$.

Budući da je $ed \equiv 1 \pmod{\phi(N)}$ slijedi da je $e = 1 + k\phi(N)$, za neki cijeli broj k. Sada dekriptiramo šifrat:

$$\begin{aligned} c^d &\equiv (m^e)^d \\ &\equiv m^{ed} \\ &\equiv m^{1+k\phi(N)} \\ &\equiv m(m^{\phi(N)^k}) \\ &\equiv m \pmod N. \end{aligned} \tag{1.1}$$

Za poruke koje nisu relativno proste sa modulom korektnost dekripcijskog pravila može se pokazati koristeći kineski teorem o ostacima, ali takve poruke treba izbjegavati jer one otkrivaju faktorizaciju modula.

Javne i tajne eksponente možemo definirati i modulo $\lambda(N)$ gdje je

$$\lambda(N) = nzv(p - 1, q - 1).$$

Vrijedi:

$$\phi(N) = (p - 1)(q - 1) = nzd(p - 1, q - 1)nzv(p - 1, q - 1) = nzd(p - 1, q - 1)\lambda(N).$$

Pokažimo da je dekripcijsko pravilo korektno i za eksponente definirane modulo $\lambda(N)$, odnosno da vrijedi ekvivalent Eulerovog teorema za $\lambda(N)$.

Budući da je $\lambda(N) = nzv(p - 1, q - 1) = nzv(\phi(p), \phi(q))$ slijedi da $\phi(p)|\lambda(N)$ i $\phi(q)|\lambda(N)$ pa je $p^{\lambda(N)} \equiv 1 \pmod p$ i $q^{\lambda(N)} \equiv 1 \pmod q$. Po kineskom teoremu o ostacima slijedi da je $a^{\lambda(N)} \equiv 1 \pmod N$ za a takav da $nzd(a, m) = 1$.

Pretpostavljat ćemo da su prosti faktori uvijek balansirani, tj. da vrijedi:

$$4 < \frac{1}{2}N^{\frac{1}{2}} < p < N^{\frac{1}{2}} < q < 2N^{\frac{1}{2}}.$$

Iz ovoga slijedi da

$$|N - \phi(N)| = |p + q - 1| < 3N^{\frac{1}{2}}.$$

Dakle N i $\phi(N)$ imati će otprilike jednakih $\frac{1}{2}$ najznačajnijih bitova. Sa s označavat ćemo $s = N - \phi(N)$. Kada je jedan eksponent izračunat kao inverz drugog očekivano je da će on biti pune veličine, odnosno otprilike iste veličine kao $\phi(N)$. Kako je N otprilike iste veličine kao i $\phi(N)$ i očekujemo da je $nzd(p-1, q-1)$ malen, očekujemo da će $\phi(N)$, $\lambda(N)$ i N biti otprilike iste veličine.

Dekripciju RSA kriptosustava poistovjećujemo s faktorizacijom modula. Do faktorizacije modula, osim poznatim metodama faktorizacije, možemo doći i računanjem tajnog eksponenta d ili vrijednosti od $\phi(N)$ ili $\lambda(N)$. Ukoliko nam je poznat $\phi(N)$ do faktorizacije dolazimo jednostavno rješavanjem sustava jednadžbi:

$$N = pq,$$

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

Ukoliko nam je pak poznat $\lambda(N)$ možemo doći do $\phi(N)$ množenjem lambde sa $nzd(p-1, q-1)$ do kojeg lako dolazimo jer vrijedi

$$\frac{N}{\lambda(N)} - 2 < nzd(p-1, q-1) < \frac{N}{\lambda(N)}.$$

Ako nam je poznat tajni eksponent d onda možemo izračunati $k\varphi(N) = ed - 1$ gdje je $\varphi(N)$ jednak $\lambda(N)$ ili $\phi(N)$. Postoji rezultat koji kaže da se N može (vjerojatnosno) faktorizirati u polinomijalnom vremenu ukoliko znamo višekratnik od $nzv(p-1, q-1)$, a znamo da $\varphi(N)$ to jest.

RSA ima svojstvo da je enkripcija produkta dvije poruke otvorenog teksta jednaka produktu enkripcije ta dva otvorena teksta.

Koristeći to svojstvo RSA nije otporan na napade koristeći odabrane šifrirane tekstove. Na primjer, pretpostavimo da je dani šifrat $c = m^e \pmod N$ i želimo izračunati m. Odaberemo nasumično $x \in \mathbb{Z}_N$, i tražimo dekripciju šifrata $c_0 \equiv cx^e \pmod N$. Budući da m_0 zadovoljava:

$$m_0 \equiv c_0^d \equiv (cx^e)^d \equiv c^d x^{ed} \equiv mx \pmod N$$

za dobiveni m_0 možemo lako izračunati $m \equiv m_0 x^{-1} \pmod N$ da bi došli do traženog otvorenog teksta.

Poglavlje 2

Kriptoanaliza RSA

2.1 Matematičke tehnike

Uz osnovne matematičke oznake i rezultate, u radu ćemo koristiti još neke matematičke tehnike. Ovdje ćemo samo navesti neke od tih tehnika i rezultata.

Zbog učestalosti korištenja kineskog teorema o ostacima ovdje ćemo samo navesti njegovu formulaciju.

Teorem 2.1.1. *(Kineski teorem o ostacima). Neka su $m_1, \ldots, m_n$ u parovima relativno prosti prirodni brojevi i $a_1, \ldots, a_n$ cijeli brojevi. Sustav kongruencija:*

$$x \equiv a_1 \pmod{m_1}$$

$$\ldots$$

$$x \equiv a_n \pmod{m_n}$$

ima jedinstveno rješenje modulo $M = \prod_{i=1}^{n} m_i$. Ako je $M_i = M/m_i$, za svaki $i = 1, \ldots, n$ rješenje je dano sa:

$$x = \sum_{i=1}^{n} a_i M_i (M_i^{-1} \pmod{m_i}) \pmod{M}.$$

U ovom radu često ćemo se baviti faktorizacijom velikog prirodnog broja, pa navedimo neke od poznatih algoritama.

NFS (Number Field Sieve) algoritam za faktorizaciju ima očekivanu heurističku brzinu pronalaženja faktora koja ovisi samo o veličini broja kojeg faktoriziramo i iznosi: $L[n] = e^{1.923(\log N)^{1/3}(\log\log n)^{2/3}}$.

ECM (Elliptic Curve Method) algoritam za faktorizaciju pak koristimo kada je jedan od faktora značajno manji od $n^{1/2}$. Tada je očekivana brzina $E[n, p] = (\log_2 n)^2 e^{\sqrt{2}(\log p)^{1/2}(\log\log p)^{1/2}}$.

Ovo su najpoznatije opće metode za faktorizaciju. Općenito, nije poznat efikasan (tj. polinomijalan) algoritam za problem faktorizacije.

U nekim od napada koristiti ćemo se teoremom o verižnim razlomcima.

Teorem 2.1.2. *Neka je $\alpha \in \mathbb{R}$ i za $c, d \in \mathbb{Z}$ vrijedi:*

$$\left|\alpha - \frac{c}{d}\right| < \frac{1}{2d^2}.$$

Tada je c/d jedna od konvergenti u razvoju od α u verižni razlomak.

Coppersmith je razvio jaku metodu za nalaženje svih malih rješenja modularnih polinomijalnih jednadžbi u jednoj ili dvije nepoznanice stupnja d koristeći LLL-algoritam za smanjenje dimenzije rešetke. Metoda se može proširiti na općeniti problem nalaženja malih rješenja jednadžbi s više nepoznanica u $\mathbb{Z}$ i $\mathbb{Z}_N$ ali su te proširene metode heurističke jer se oslanjaju na nedokazane pretpostavke. Ipak, u praksi se pokazalo da su pretpostavke točne u većini slučajeva. U napadima ćemo se često koristiti Coppersmithovom metodom i pretpostavljati da pretpostavke stoje. Prije nego navedemo spomenute pretpostavke uvesti ćemo neke definicije.

Definicija 2.1.3. *Rešetka je diskretna aditivna podgrupa od $\mathbb{R}^n$. Za danih $m \leq n$ linearno nezavisnih vektora $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$, skup*

$$\mathcal{L} = \mathcal{L}(b_1, \ldots, b_m) = \left\{ \sum_{i=0}^{m} \alpha_i b_i \mid \alpha_i \in \mathbb{Z} \right\}$$

je rešetka. Vektore b_i zovemo bazni vektori, a $\mathcal{B} = \{b_1, \ldots, b_m\}$ baza rešetke $\mathcal{L}$.

Rešetku ćemo prikazivati kao matricu baze $\mathcal{B}$ čiji su retci vektori baze.

Budući da su rešetke po definiciji diskretne, primijetimo da u svakoj rešetki postoji najmanji netrivijalni vektor, tj. barem 2 takva jer je za svaki $v \in \mathcal{L}$ i $-v \in \mathcal{L}$.

Definicija 2.1.4. *Dimenzija rešetke je broj vektora koji čine bazu rešetke.*

Definicija 2.1.5. *Volumen rešetke, $vol(\mathcal{L})$, je m-dimenzionalni volumen paralelopipeda razapetog bazom rešetke $\mathcal{L}$.*

Volumen je nezavisan od izbora baze. Ako je $\mathcal{B}$ neka baza rešetke, vrijedi:

$$vol(\mathcal{L}) = (det(\mathcal{B}\mathcal{B}^T))^{1/2}.$$

Svaka rešetka može imati više različitih baza, a posebno korisna biti će LLL-reducirana baza. Da bi je definirali prisjetimo se definicije Gram-Schmidtove ortoganalizacije.

Definicija 2.1.6. *Neka je dano m linearno nezavisnih vektora $b_1, \ldots, b_m \in \mathbb{R}^n$. Definiramo postupak Gram-Schmidtove ortogonalizacije kao rekurzivno definiranje vektora $b_1^*, \ldots, b_m^* \in \mathbb{R}^n$:*

$$b_1^* = b_1,$$

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \quad za\ 2 \leq i \leq m,$$

gdje su $\mu_{i,j} = \langle b_i, b_j^* \rangle / \|b_j^*\|^2$ Gram-Schmidtovi koeficijenti.

Definicija 2.1.7. *Za bazu kažemo da je LLL-reducirana ako njezini Gram-Schmidtovi koeficijenti zadovoljavaju $\mu_{i,j} < 1/2$ za $1 \leq j < i \leq n$ i*

$$\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \geq \frac{3}{4} \|b_{i-1}^*\|^2 \quad za\ 1 < i \leq n.$$

LLL-reducirane baze bit će nam korisne radi svojstva da je najmanji vektor u takvoj bazi, u najgorem slučaju, ne puno veći od najmanjeg vektora u rešetki.

Kada znamo da neka jednadžba s više nepoznanica ima malo rješenje, često je moguće pronaći to rješenje koristeći heurističke metode koje se oslanjaju na traženje najmanjeg vektora u rešetki.

Navedimo sada već spomenute pretpostavke koje ćemo koristiti u napadima:

Pretpostavka 2.1.8. *Polinomi s poznatim malim rješenjem, ili nad $\mathbb{Z}$ ili nad $\mathbb{Z}_N$, imaju samo jedno malo rješenje.*

Pretpostavka 2.1.9. *Polinomi dobiveni od vektora LLL-reducirene baze su algebarski nezavisni.*

Prisjetimo se da za polinome f_1 i f_2 kažemo da su algebarski nezavisni ako i samo ako su njihovi zajednički faktori konstante, odnosno $nzd(f_1, f_2) = konst$.

Često ćemo u kriptoanalizi koristiti sljedeće Coppersmithove rezultate.

Teorem 2.1.10. *Neka je N cijeli broj nepoznate faktorizacije s faktorom $b \geq N^\beta$. Neka je $f_b(x)$ normirani polinom s jednom varijablom stupnja d i neka je $c > 1$ neka konstanta. Svi x_0 koji zadovoljavaju $f_b(x_0) \equiv 0 \pmod{b}$ i $|x_0| \leq cN^{\beta^2/d}$ mogu se naći u vremenu polinomijalnom u $\log N$, c i broju rješenja.*

Korolar 2.1.11. *Neka je N cijeli broj nepoznate faktorizacije s faktorom $b \geq N^\beta$. Ako nam je poznata aproksimacija $\tilde{b}$ za kb, gdje je k bilo koji cijeli broj koji nije višekratnik od N/b, ako je $|kb - \tilde{b}| < N^{\beta^2}$ onda faktor b možemo izračunati u vremenu polinomijalnom u n.*

2.2 Rani napadi

Prvi napadi na RSA bazirali su se na ranim protokolarnim greškama kriptosustava. Navesti ćemo ih nekoliko.

Korištenje istog modula

Kada više korisnika koristi isti modul svaka se poruka koju šifriramo s dva različita javna ključa može lako dekriptirati. Neka su (e_1, N) i (e_2, N) dva različita javna ključa koji imaju relativno proste javne eksponente. Tada se, koristeći Euklidov algoritam, lako mogu izračunati brojevi a_1 i a_2 takvi da $a_1e_1 + a_2e_2 = 1$. Za svaku poruku m dobivamo šifrate $c_1 = m^{e_1} \pmod N$ i $c_2 = m^{e_2} \pmod N$. Sada otvoreni tekst poruke možemo lako izračunati množenjem $c_1^{a_1}c_2^{a_2}$ jer vrijedi:

$$c_1^{a_1}c_2^{a_2} = m^{a_1e_1}m^{e_2a_2} = m^{a_1e_1+a_2e_2} = m.$$

Pokazano je i da se poznavajući samo jedan par javnog i odgovarajućeg tajnog ključa može za svaki drugi javni ključ sa istim modulom efikasno izračunati odgovarajući tajni ključ.

Teorem 2.2.1. *Neka je (e, N) RSA javni ključ s odgovarajućim tajnim ključem d i neka je e_1 neki drugi javni ključ takav da je $e_1 \neq e$. Za dane e, d, N i e_1, tajni ključ koji odgovara ključu e_1 možemo izračunati kao*

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

Dokaz. Jednadžbu ključa možemo napisati kao $ed - 1 = k\lambda(N)$, gdje je $k \in \mathbb{N}$. Znamo da vrijedi $nzd(e_1, \lambda(N)) = 1$, pa $nzd(e_1, k\lambda(N)) = k'$, za neki k' takav da $k'|k$. Neka je $\tilde{k} = k/k'$. Imamo:

$$\frac{ed-1}{nzd(e_1, ed-1)} = \frac{k\lambda(N)}{k'} = \tilde{k}\lambda(N),$$

pa tajni eksponent $d_1 = e_1^{-1} \pmod{\frac{ed-1}{nzd(e_1,ed-1)}}$ zadovoljava:

$$e_1d_1 = 1 + k_1(\tilde{k}\lambda(N)),$$

za neki prirodni broj k_1. Slijedi da $e_1d_1 \equiv 1 \pmod{\lambda(N)}$m pa je d_1 valjani tajni eksponent za javni ključ (e_1, N). □

Dakle zaključujemo da bi svaki RSA modul trebao biti poznat samo jednom korisniku.

Korištenje bliskih prostih faktora

Kada koristimo bliske proste faktore, točnije, ako je $N = pq$ i $|p - q| < N^{\frac{1}{4}}$ tada N možemo efikasno faktorizirati Fermatovim algoritmom za faktorizaciju.

Neka je $N = pq$, definiramo $x = \frac{1}{2}(p + q)$ i $y = \frac{1}{2}(p - q)$. Vrijedi: $N = x^2 - y^2$ odnosno $y^2 = x^2 - N$, sada inicijaliziramo $x = \lfloor \sqrt{N} \rfloor + 1$, kvadriramo x, oduzmemo od njega N i provjeravamo jesmo li dobili kvadrat cijelog broja, iterativno povećavamo x za jedan i ponovno vršimo provjeru dok ne dođemo do kvadrata.

Primjer 2.2.2. *Neka je* $N = 20648509087$. *Dakle* $x = \lfloor \sqrt{N} \rfloor + 1 = 143696$.

$$143696^2 - 20648509087 = 31329 = 177^2$$

Kvadrat smo dobili iz prvog pokušaja. Za $y = 177$ *vrijedi* $x^2 = y^2 + N = 31329 + 20648509087 = 20648540416 = 143696^2$, *pa je* $x = 143696$. *Rješavamo sustav jednadžbi:*

$$143696 = \frac{1}{2}(p + q)$$

$$177 = \frac{1}{2}(p - q)$$

Dobivamo rješenja $p = 126481$ *i* $q = 126839$.

Håstadov napad prijenosom

Napad temeljen na jednakim otvorenim tekstovima

Napad otvorenim tekstom nastaje kada se ista poruka m šifrira s nekoliko javnih ključeva (e, N_i) koji svi imaju isti javni eksponent i različit modul. Tada se poruka može dekriptirati u polinomijalnom vremenu uz uvjet da je broj dostupnih javnih ključeva s istim javnim eksponentom i u parovima relativno prostim modulima veći ili jednak javnom eksponentu i da je tražena poruka manja od svih modula. Dekripciju vršimo koristeći kineski teorem o ostacima.

Napad temeljen na povezanim otvorenim tekstovima

Kada je više povezanih otvorenih tekstova kriptirano malim javnim eksponentom i različitim modulima provodimo ovaj tip napada. Otvorene tekstove m_i smatramo povezanim ako postoje poznati polinomi f_i takvi da $m_i = f_i(m)$. Tada dekripciju možemo izvršiti u polinomijalnom vremenu koristeći kineski teorem o ostacima i Coppersmithovu metodu za traženje korijena modularnih polinoma s jednom nepoznanicom. Naime, neka su f_i normirani polinomi i $\delta = \max_i\{e_i deg(f_i(x))\}$. Definiramo polinome:

$$g_i(x) = x^{h_i}(f_i(x)^{e_i} - c_i) \in \mathbb{Z}_{N_i}[x],$$

gdje je $h_i = \delta - deg(f_i(x)^{e_i})$. Oni zadovoljavaju kongruenciju: $g_i(m) \equiv 0 \pmod{N_i}$. Koristeći kineski teorem o ostacima računamo novi polinom $G(x) \in \mathbb{Z}_N[x]$ iz polinoma $g_i(x)$, on zadovoljava $G(m) \equiv 0 \pmod{N}$. Sada m računamo koristeći Coppersmithov rezultat.

Kružni napad

Svaki otvoreni tekst može se dekriptirati ako njegov šifrat opetovano kriptiramo. Za dani šifrat $c = m^e \pmod{N}$ i javni ključ (e, N), ako je nakon $l + 1$ reenkripcija šifrat ponovljen, tj. vrijedi $c^{e^{l+1}} \equiv c \pmod{N}$, tada slijedi da je $c^{e^l} \equiv m \pmod{N}$. Odnosno, originalan tekst je otkriven nakon l reenkripcija. Taj l nazivamo eksponent oporavka. Pokazat ćemo da za svaku poruku m eksponent oporavka dijeli $\lambda(\lambda(N))$. Iz toga slijedi da je najveći mogući eksponent oporavka upravo $\lambda(\lambda(N))$. No, ukoliko su odabrani sigurni prosti brojevi eksponent oporavka bit će za većinu poruka vrlo velik jer će tada i $\lambda(\lambda(N))$ biti velik i imat će velike proste faktore.

Teorem 2.2.3. *(Carmichaelov teorem) Za svaki $x \in \mathbb{Z}_N^*$ vrijedi*

$$x^{\lambda(N)} \equiv 1 \pmod{N}.$$

Teorem 2.2.4. *Za svaki $m \in \mathbb{Z}_N^*$ eksponent oporavka dijeli $\lambda(\lambda(N))$.*

Dokaz. Iz Carmichaelovog teorema slijedi:

$$c_i \equiv m^{e^i} \equiv m^{e^i \pmod{\lambda(N)}} \pmod{N}.$$

Na sličan način dolazimo do

$$e^i \equiv e^{i \pmod{\lambda(\lambda(N))}} \pmod{\lambda(N)}.$$

Budući da je $nzd(e, \lambda(N)) = 1$ slijedi da

$$c_i \equiv m^{e^{i \pmod{\lambda(\lambda(N))}} \pmod{\lambda(N)}} \pmod{N}.$$

Stavimo sada da je $i = \lambda(\lambda(N))$. Dobivamo

$$c_i \equiv m^{e^0 \pmod{\lambda(N)}} \equiv m \pmod{N}.$$

□

2.3 Napadi bazirani na malom javnom eksponentu

Svi napadi bazirani na malom javnom eksponentu koje ćemo proučiti nisu usmjereni na otkrivanje tajnog eksponenta niti na otkrivanje faktorizacije modula već samo na dekriptiranje dane poruke.

Korištenje malog javnog eksponenta može jako smanjiti cijenu šifriranja i zato se često koristi u praksi.

Vrlo mali tajni eksponent za jednake poruke

Promotrimo sljedeći napad za vrlo mali tajni eksponent, uzmimo za primjer $e = 3$.

Ako istu poruku m pošaljemo trima primateljima koristeći $\{(e, N_1), (e, N_2), (e, N_3)\}$, gdje je $nzd(N_i, N_j) = 1$, $\forall i, j \in \{1, 2, 3\}, i \neq j$ i $m < N_i$ tada lako dolazimo do originalne poruke rješavajući sustav kongruencija:

$$c_1 \equiv m^3 \pmod{N_1}, \quad c_2 \equiv m^3 \pmod{N_2}, \quad c_3 \equiv m^3 \pmod{N_3}.$$

Koristimo Kineski teorem o ostacima i dolazimo do x sa svojstvom $x \equiv m^3 \pmod{N_1N_2N_3}$. No kako je $m^3 < N_1N_2N_3$ vrijedi $x = m^3$, pa računamo poruku tako da izvadimo treći korijen od x.

Primijetimo da kad bi m bio manji od $N^{\frac{1}{3}}$ dovoljno bi bilo izvaditi treći korijen od originalne poruke.

Općenito, za $m < N^{\frac{1}{e}}$ za šifrat vrijedi $c = m^e \pmod{N} = m^e$, pa je za dekriptiranje bilo dovoljno izvaditi e-ti korijen od šifrata. U praksi se takve male poruke izbjegavaju nadopunjavanjem originalne poruke nasumičnim bitovima kako bi postigli željenu, sigurnu veličinu poruke.

Poruka poznatog formata

Ako nam je poznat samo dio poruke, moguće je efikasno izračunati čitav otvoreni tekst ukoliko su javni eksponent i veličina nepoznatog dijela poruke dovoljno mali.

Teorem 2.3.1. *Neka je (e, N) valjani RSA javni ključ i m neka poruka. Neka je $c = m^e \pmod{N}$ poznat. Ako su poznati svi osim najviše $1/e$ dio uzastopnih bitova otvorenog teksta, tada cijela m može biti izračunata u polinomijalnom vremenu u $\log N$ i e.*

Dokaz. $m = m_2 2^{k_2} + m_1 2^{k_1} + m_0$, gdje je nepoznato samo m_1 i $|m_1| < N^{\frac{1}{e}}$.

Tražimo rješenja od $f_N(x) \in \mathbb{Z}_N[x]$ gdje je

$$f_N(x) = 2^{-k_1 e}((m_2 2^{k_2} + x2^{k_1} + m_0)^e - c) \pmod{N}$$

budući je $f_N(m_1) = 2^{-k_1 e}(m^e - c) = 0 \pmod{N}$.

Kako je $|m_1| < N^{\frac{1}{e}}$ možemo koristiti Coppersmithovu metodu za pronalaženje malih rješenja za modularne jednadžbe s jednom nepoznanicom, odnosno Teorem 2.1.10. □

Primijetimo da je ova metoda primjenjiva samo na male javne eksponente jer čim je $e > \log_2 N$ svi bitovi otvorenog teksta moraju biti poznati. Također primijetimo da ukoliko nepoznati bitovi ukupne duljine manje od $1/e$ nisu uzastopni, opet je moguće pronaći rješenje koristeći Coppersmithovu heurističku metodu za pronalaženje malih rješenja modularne jednadžbe s više nepoznanica.

Povezane poruke

Ako imamo dva otvorena teksta povezana poznatom afinom vezom i mali javni eksponent, postoje poznati napadi kojima možemo otkriti ili pokušati otkriti tražene tekstove.

Ukoliko je javni eksponent $e = 3$ takve se poruke mogu dešifrirati u vremenu polinomijalnom u $\log N$ gdje je N modul.

Za općeniti polinom f takav da za dvije poruke vrijedi $m_2 = f(m_1)$ i proizvoljan javni eksponent e da bi izračunali m_1 i m_2 koristimo slijedeći postupak:

Uz dane uvjete vrijedi da je $x = m_1$ rješenje kongruencija:

$$x^e - c_1 \equiv 0 \pmod{N},$$

$$f(x)^e - c_2 \equiv 0 \pmod{N}.$$

Uzmimo $g(x) \in \mathbb{Z}_N[x]$ takav da $g(x) = nzd(x^e - c_1, f(x)^e - c_2) \pmod{N}$. Takav $g(x)$ je višekratnik od $x - m_1$. Ako je $g(x) = x - m_1$ tada je jednostavno $g(0) = -m_1$. Očekujemo da će biti $g(x) = x - m_1$ osim u nekim rijetkim slučajevima.

Primjer 2.3.2. *Neka je* $(e, N) = (3, 10084775329)$. *Dani su šifrati* $c_1 = 1860867$ *i* $c_2 = 2744000$ *za poruke povezane s* $m_2 = m_1 + 17$.

$$f_1(x) = x^3 - c_1 = x^3 - 1860867$$

$$f_2(x) = f(x)^3 - c_2 = (x + 17)^3 - 2744000 = x^3 + 51x^2 + 867x - 2739087$$

Računamo najveći zajednički djelitelj ta dva polinoma modulo N i dobivamo:

$$g(x) = nzd(f_1(x), f_2(x)) = x - 123 = x - m_1$$

Pa je rješenje $m_1 = 123$, *lako dobivamo i* $m_2 = m_1 + 17 = 123 + 17 = 140$.

Ukoliko su dvije poruke povezane afinom funkcijom $m_2 = m_1 + b$ gdje je b nepoznat i dovoljno mali postoje napadi kojima možemo doći do dekriptiranih poruka.

Za konkretan slučaj gdje je $e = 3$ i $|b| < N^{\frac{1}{9}}$ postoji algoritam za dekriptiranje poruka u vremenu $\log N$. Napad koristi Coppersmithovu metodu za pronalaženje malih rješenja modularnih jednadžbi s jednom nepoznanicom da bi pronašao b i zatim gore pojašnjen napad na povezane poruke da bi došao do m_1 i m_2.

Primijetimo da se od svih napada navedenih u ovom poglavlju možemo obraniti na način na našu poruku dodamo niz nasumičnih bitova. Kod poruka poznatog formata taj niz mora biti duljine barem $\frac{1}{e}$ od duljine poruke, a kod povezanih poruka dodajemo niz proizvoljne duljine kako bi razbili polinomijalnu vezu između poruka.

Izvlačenje informacija

Napadi bazirani na malom javnom eksponentu koje smo dosad spomenuli ne faktoriziraju modul već samo pokušavaju dekriptirati određenu poruku. Ipak, moguće je doznati i neke informacije o tajnom eksponentu.

Ako je $ed = 1 + k\phi(N)$ za neki poznati $k \in \mathbb{Z}$, možemo u polinomnom vremenu u $\log N$ izračunati d_1 takav da $|d_1 - d| < p + q$, gdje d_1 računamo kao $d_1 = \lceil \frac{1}{e}(1 + kN) \rfloor$.

Za balansirane proste faktore p i q vrijedi $p + q > \frac{3}{2}N^{\frac{1}{2}}$, pa možemo pronaći d_1 takav da $|d - d_1| < \frac{3}{2}N^{\frac{1}{2}}$, što znači da uz poznavanje konstante k možemo otkriti otprilike pola najznačajnijih znamenki od d. Vrijedi i obrat, ukoliko znamo pola najznačajnijih znamenki od d možemo dobiti informacije o k.

U slučaju kada je eksponent e malen moguće ga je i pogoditi iscrpnim pretraživanjem. U slučaju kada je $e = 3$ lako dolazimo do toga da mora biti $k = 2$. Dakle, kada koristimo javni eksponent $e = 3$ uvijek će otprilike pola najznačajnijih bitova tajnog eksponenta biti poznato.

Teorem 2.3.3. *Neka je $N = pq$ modul sa $p, q > 3$ i neka je (e, N) pripadni javni ključ. Ukoliko je $e = 3$, onda konstanta u jednadžbi ključa $ed = 1 + k\phi(N)$ mora biti $k = 2$.*

Dokaz. Iz jednadžbe ključa slijedi da je $0 < k < e$. Budući da je $e = 3$ znamo da je $nzd(3, p - 1) = 1$, pa $p - 1 \not\equiv 0 \pmod 3$. Kako je $p > 3$ slijedi da je $nzd(3, p) = 1$, pa $p - 1 \not\equiv 2 \pmod 3$. Dakle $p - 1 \equiv 1 \pmod 3$. Analogno dobivamo $q - 1 \equiv 1 \pmod 3$. Sada, ako jednadžbu ključa $3d = 1 + k\phi(N)$ reduciramo modulo 3, dobivamo $k \equiv -1 \equiv 2 \pmod 3$. Budući da je $0 < k < 3$ slijedi da je $k = 2$. □

2.4 Napadi bazirani na malom tajnom eksponentu

Napadi u ovom poglavlju uključuju otkrivanje tajnog eksponenta koji je veći od tajnog eksponenta koji se efikasno može pronaći iscrpnim pretraživanjem. Svi ovi napadi usmjereni su na faktorizaciju modula.

Wienerov napad

Wienerovim napadom možemo s dostupnim samo javnim ključem doći do faktorizacije modula koristeći informacije dobivene iz jedne od konvergenti verižnog razlomka od $\frac{e}{N}$.

Pogledajmo koja nam je ograda za d dovoljna za primijeniti napad. Ukoliko su eksponenti definirani modulo $\lambda(N)$ vrijedi:

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

gdje je $g = nzd(p-1, q-1)$. Jednadžbu ključa možemo zapisati kao:

$$ed = 1 + k\lambda(N) = 1 + \frac{k}{g}(N-s) = 1 + \frac{\frac{k}{nzd(k,g)}}{\frac{g}{nzd(k,g)}}(N-s) = 1 + \frac{k_0}{g_0}(N-s).$$

Slijedi:

$$\left|\frac{e}{N} - \frac{k_0}{dg_0}\right| = \left|\frac{1}{dN} - \frac{k_0 s}{dg_0 N}\right| < \frac{k_0 s}{dg_0 N}.$$

Primijetimo da ukoliko je

$$d < \frac{N}{2sg_0k_0}$$

vrijedi: $|\frac{e}{N} - \frac{k_0}{dg_0}| < \frac{1}{2(dg_0)^2}$, pa znamo da je $\frac{k_0}{dg_0}$ jedna od konvergenti u razvoju e/N u verižni razlomak, na primjer konvergenta c_j. Sada vrijedi:

$$\phi(N) = e\left(\frac{dg_0}{k_0}\right) - \frac{g_0}{k_0} = \left\lfloor e\frac{1}{c_j}\right\rfloor - \left\lfloor\frac{g_0}{k_0}\right\rfloor.$$

Dakle ako nam je poznata konvergenta c_j i vrijednost $\lfloor\frac{g_0}{k_0}\rfloor$ možemo lako faktorizirati modul. Složenost faktorizacije je polinomijalna u $\log N$ budući da je broj konvergenti od N/e polinomijalan u $\log N$ i g/k budući da je to maksimalan broj kandidata za $\lfloor\frac{g_0}{k_0}\rfloor$ za svaku od konvergenti.

Kada su p i q nasumično odabrani vrlo je vjerojatno da će i g biti jako mali, pa je $\lfloor\frac{g}{k}\rfloor = 0$ i jedna iteracija po kandidatima za traženu konvergentu će biti dovoljna.

Obrane od Wienerovog napada temelje se na smanjivanju ograde za d, tj. smanjivanje vrijednosti izraza $\frac{N}{2sg_0k_0}$:

1. Korištenjem nebalansiranih prostih brojeva tako da $s = p + q + 1$ postane velik.
2. Korištenjem prostih brojeva s velikim $g = nzd(p-1, q-1)$, pa g_0 postane velik.
3. Korištenjem $e > N$, pa $k = \frac{ed}{N}$ postane velik. (Za $e > N^{\frac{3}{2}}$ Wienerov napad postaje potpuno neefikasan.)

Kada je javni eksponent otprilike iste veličine kao i modul, prosti faktori su balansirani i g_0 je malen, tada je uobičajena ograda za uspjeh Wienerovog napada: $d < N^{1/4-\epsilon}$, za neki mali $\epsilon > 0$.

Primjer 2.4.1.

$$(e, N) = (41071493, 1020006797)$$

Odgovarajući verižni razlomak je $[0; 24, 1, 5, 17, 2, 5, 1, 9, 2, 2, 2, 4, 1, 2]$.

Odgovarajuće konvergente su: $1/24$, $1/25$, $6/149$, $103/2558$, $212/5625$, $1163/28883$, $1375/34148$,...

Testiramo svaku od konvergenti za $\left\lfloor \frac{g}{k} \right\rfloor = 0$. *Za treću konvergentu* $6/149$ *dobivamo* $\phi(N) = 1019942076$. *Nakon što to uvrstimo u sustav jednadžbi*

$$p \times q = 1020006797$$

$$(p-1) \times (q-1) = 1019942076$$

dobivamo $p = 27143$ *i* $q = 37579$ *i uspjeli smo faktorizirati modul. Sada je* $\lambda(N) = 509971038$ *i* $g = 2$, *pa vidimo da je* $d = 149$.

Napad Boneha i Durfeea

Neka je $N = pq$ n-bitni modul s balansiranim prostim faktorima, neka je (e, N) javni ključ d odgovarajući tajni ključ definiran modulo $\phi(N)$. Neka je $e = N^{\alpha}$ i $d = N^{\delta}$. Ako tajni eksponent zadovoljava ogradu

$$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{1 + 6\alpha} - \epsilon$$

onda modul N možemo faktorizirati u polinomijalnom vremenu u $\log N$ za dovoljno veliki n ukoliko vrijede Pretpostavka 2.1.8 i Pretpostavka 2.1.9.

Očekujemo da je $\alpha \approx 1$, pa ovaj napad može faktorizirati modul za tajne eksponente $d < N^{0.2847-\epsilon}$.

Ako jednadžbu ključa reduciramo modulo e dobivamo jednadžbu

$$-k(N - s) \equiv 1 \pmod{e}.$$

Problem faktorizacije u napadu Boneha i Durfeea svede se na problem traženja malih rješenja polinoma $f_e(x, y) \in \mathbb{Z}[x, y]$ s dvije nepoznanice

$$f_e(x, y) = Nx + xy + 1$$

budući da je $(x_0, y_0) = (k, -s)$ korijen od $f_e(x, y)$ modulo e.

Kako su faktori balansirani znamo da je $\phi(N) > \frac{1}{2}N$ i $s < 3N^{1/2}$, pa vrijedi:

$$|x_0| = k = \frac{ed - 1}{\phi(N)} < \frac{ed}{\frac{1}{2}N} = 2N^{\alpha+\delta-1} = X,$$

$$|y_0| = |-s| = p + q - 1 < 3N^{1/2} = Y.$$

Sada s postavljenim ogradama X i Y, koristeći polinom $f_e(x, y)$ tražimo rješenja konstrukcijom rešetke čiji svaki element odgovara polinomu s korijenom (x_0, y_0) modulo neka potencija od e.

Nakon toga pokrećemo LLL algoritam na retcima matrice i dobivamo LLL-reduciranu bazu te rešetke. Prvi vektor te baze, koji bi trebao odgovarati najmanjem vektoru rešetke, imati će malu normu, pa će i polinom koji mu odgovara imati malu normu, taj će polinom imati i korijen (x_0, y_0). Sada preostaje pronaći taj korijen.

2.5 Napadi bazirani na dijelom poznatom tajnom ključu

Napadi koje razmatramo koristit će neke informacije o tajnom ključu kako bi faktorizirali modul. Kada je poznato ϵ najznačajnijih znamenki od x pretpostavljati ćemo da znamo $\hat{x}$ takav da je $x = \hat{x} + x_0$ gdje za x_0 vrijedi $|x_0| = |x - \hat{x}| < x^{1-\epsilon}$. Kada je pak poznato ϵ najmanje značajnih znamenki od x pretpostavljati ćemo da znamo $\tilde{x}$ i $r \geq |x^{\epsilon}|$ takve da je $|\tilde{x}| < r$ i vrijedi

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

Teorem 2.5.1. *Neka je $N = pq$ RSA modul s balansiranim prostim faktorima. Ako je poznato barem $\frac{1}{2}$ najznačajnijih ili najmanje značajnih bitova jednog od faktora, tada se N može faktorizirati u polinomijalnom vremenu u* $\log N$.

Dokaz. Budući da su prosti faktori balansirani, znamo da vrijedi:

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

Pretpostavimo prvo da znamo barem $\frac{1}{2}$ najznačajnijih bitova od p, tj. znamo $\hat{p}$ takav da je $p = \hat{p} + p_0$, gdje za nepoznati p_0 vrijedi:

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

Vidimo da je p_0 korijen, modulo p, od polinoma s jednom nepoznanicom

$$f_{msb}(x) = x + \hat{p}.$$

Budući da je svaki korijen tog polinoma modulo p oblika $p_0 + \alpha p$ za neki $\alpha \in \mathbb{Z}$, vrijedi da je p_0 jedini korijen ograničen sa $\sqrt{2}N^{\frac{1}{4}}$. Neka je $\beta = 1/2 - \log_N(2)$ i $c = 2\sqrt{2}$. Vidimo da vrijedi

$$p > \frac{1}{2}N^{1/2} = N^{1/2-\log_N(2)} = N^{\beta},$$

pa za traženi korijen vrijedi

$$\begin{aligned} |p_0| &< \sqrt{2}N^{1/4} = \frac{2\sqrt{2}}{2}N^{1/4} = 2\sqrt{2}N^{1/4-\log_N(2)} \\ &< 2\sqrt{2}N^{1/4-\log_N(2)+\log_N^2(2)} = 2\sqrt{2}N^{(1/2-\log_N(2))^2} = cN^{\beta^2}. \end{aligned} \tag{2.1}$$

Iz Teorema 2.1.10 slijedi da možemo izračunati korijen p_0 odnosno faktorizirati modul u vremenu polinomijalnom u $\log N$.

Pretpostavimo sada da znamo barem $1/2$ najmanje značajnih znamenki faktora q. Odnosno, znamo $\tilde{q}$ i r takve da vrijedi $q = q_0 r + \tilde{q}$, gdje je $0 \leq \tilde{q} < r$, $q^{1/2} < r < q$, i za q_0 vrijedi

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

Definirajmo $R = r^{-1} \pmod N$ tako da $rR = 1 + kN$ za neki cijeli broj k. Sada polinom

$$f_{lsb}(x) = x + \tilde{q}R$$

ima korijen q_0 modulo q jer je

$$rf_{lsb}(q_0) = q_0 r + \tilde{q}Rr = q_0 r + \tilde{q} + \tilde{q}kN = q + \tilde{q}kpq \equiv 0 \pmod q.$$

Budući da nema djelitelja nule modulo q i budući da $q^{1/2} < r < q$ povlači da je $r \not\equiv 0 \pmod q$ slijedi da je $f_{lsb}(q_0) \equiv 0 \pmod q$. Kao i prije, q_0 može biti jedini korijen manji od $\sqrt{2}N^{1/4}$. Ograde za q_0 iste su kao i ograde za p_0 koje smo gore izveli, pa možemo primijeniti Teorem 2.1.10 s isto definiranim c i β kao i gore. □

Kada bi poznavali samo dio najznačajnijih ili najmanje značajnih znamenki tajnog eksponenta, postoje mnogobrojni napadi kojim bi mogli doći do faktorizacije modula.

Ukoliko nam je poznat određen broj najznačajnijih znamenki tajnog eksponenta, dakle znamo $\hat{d}$ takav da $|d - \hat{d}| < N^\delta$ nastupamo ovisno o veličinama javnog i tajnog eksponenta.

Kada su eksponenti proizvoljni označimo $e = N^\alpha$, $d = N^\beta$ i $|d - \hat{d}| < N^\delta$ gdje je $\hat{d}$ poznat. Uz uvjet da vrijede pretpostavke 2.1.8 i 2.1.9 postoje razni napadi kojima možemo doći do tajnog eksponenta tražeći korijene polinoma jednadžbe ključa. Napad koji ćemo primijeniti za određeni problem ovisi o ogradama koje imamo za δ u ovisnosti o α i β. Kada je javni odnosno tajni eksponent pune veličine koristimo iste napade uz $\alpha \approx 1$, odnosno $\beta \approx 1$.

Ako imamo RSA modul s balansiranim prostim faktorima i $e = N^\alpha$ javni eksponent takav da $0 < \alpha \leq \frac{1}{2}$ i poznato nam je α dio najznačajnijih znamenki tajnog eksponenta d definiranog modulo $\phi(N)$ tada možemo lako doći do konstante k iz jednadžbe ključa (do na malu aditivnu konstantu).

Naime, možemo staviti $\hat{k} = \left\lceil \frac{e\hat{d}-1}{N} \right\rfloor$.
Vidimo da vrijedi:

$$|k - \hat{k}| < \left| \frac{e(d-\hat{d})}{\phi(N)} \right| + \left| \frac{se\hat{d}}{N\phi(N)} \right| < 2N^{\alpha+(1-\alpha)-1} + 6N^{\alpha-1/2} + \frac{1}{2} < 9.$$

Dakle $k \in \{\hat{k} - 8, \hat{k} + 8\}$

Primjer 2.5.2. *Ako imamo* $e = 31913$, $N = 1020006797$, *dakle* $e = N^{0.4999}$, *i poznato je barem prvih* α *znamenki, npr. znamenke* 85374, *tj. možemo staviti* $\hat{d} = 853740000$. *Računamo* $\hat{k} = \lceil \frac{e\hat{d}-1}{N} \rfloor = 26711$. *Znači* $k \in \{\hat{k} - 8, \hat{k} + 8\} = \{26703, 26719\}$.

Sada možemo ovaj rezultat iskoristiti u napadu u slučaju da imamo javni eksponent manji od $N^{\frac{1}{2}}$.

Teorem 2.5.3. *Neka je* $e = N^{\alpha}$ *gdje je* $0 < \alpha \leq 1/2$ *i* d *odgovarajući tajni eksponent modulo* $\phi(N)$. *Neka je* k *konstanta u jednadžbi ključa i* $e = \gamma k$ *za neki* $\gamma > 1$. *Ako je dano* $(1 - \alpha)$ *najznačajnijih znamenki tajnog eksponenta možemo faktorizirati modul u vremenu polinomijalnom u* $\log N$ *i* γ.

Dokaz. Budući da je dano $(1 - \alpha)$ znamenki od d možemo konstruirati $\hat{d}$ takav da $|d - \hat{d}| < d^{\alpha} < N^{\alpha} = e$. Kako je $0 < \alpha \leq 1/2$ vrijedi da je $1 - \alpha \geq \alpha$, pa možemo doći do konstante $\hat{k}$ takve da vrijedi $k \in \{\hat{k} - 8, \hat{k} + 8\}$ za k iz jednadžbe ključa.

Ako znamo k, možemo izračunati $d_k = e^{-1} \pmod{k}$. Iz jednadžbe ključa slijedi da je $d_k \equiv d \pmod{k}$, pa možemo d prikazati kao $d = Dk + d_k$ za neki D.

Primijetimo da d možemo napisati kao:

$$d = \left(\frac{\hat{d} - d_k + d - \hat{d}}{k} \right) k + d_k = \left(\left\lceil \frac{\hat{d} - d_k}{k} \right\rceil + \left\lfloor \frac{d - \hat{d}}{k} \right\rfloor \right) k + d_k,$$

gdje je na desnoj strani sve poznato osim $v = \left\lfloor \frac{d-\hat{d}}{k} \right\rfloor$.

Budući da vrijedi

$$|v| = \left| \left\lfloor \frac{d - \hat{d}}{k} \right\rfloor \right| < \left| \frac{d - \hat{d}}{k} \right| < \frac{e}{k} = \gamma$$

postoji najviše $2\lfloor\gamma\rfloor + 1$ mogućih vrijednosti za v, pa i za D, odnosno d. Testiramo svaki od kandidata za v. Budući da k zapravo nije poznat, moramo ponoviti postupak za svaki od kandidata dok ne dođemo do faktorizacije, ima ih ukupno 17.

□

Primjer 2.5.4. *Neka je* $(e, N) = (31913, 1020006797)$ *kao i u prethodnom primjeru, dakle* $\alpha = 0.49996$*. Mora biti poznato* 0.5 *najznačajnijih znamenki, neka su to znamenke* 85374 *i neka preostaju još* 4 *nepoznate znamenke. Možemo staviti* $\hat{d} = 853740000$*. U prethodnom primjeru izračunali smo interval u kojem leži k, možemo nastaviti isprobavajući napad za svih* 17 *mogućnosti za k, no mi ćemo radi jednostavnosti pretpostaviti da smo k pogodili iz prve, dakle* $k = 26713$*. Sad računamo* $d_k = e^{-1} \pmod{k} = 31913^{-1} \pmod{26713} = 2173$.

U našem slučaju je $\gamma = 1.19$*, pa vrijedi* $|v| < 1.19$*, tj.* $v \in \{-1, 0, 1\}$*. Uvrštavanjem poznatih vrijednosti dobivamo:*

$$d = \left(\left\lfloor \frac{853740000 - 2173}{26713} \right\rfloor + v \right) 26713 + 2173 = (31959 + v)26713 + 2173$$

tj. $d \in \{853696227, 853722940, 853749653\}$*. Iz poznatih znamenki od d vidimo da samo* $d = 853749653$ *može biti rješenje.*

Primijetimo da ovaj napad ne možemo primijeniti ukoliko je javni eksponent jako mali jer bi tada morale biti poznate sve znamenke tajnog eksponenta.

Ukoliko je javni eksponent $e \leq N^{1/4}$ koristimo se alternativnim napadom za koji moramo poznavati $3/4$ najznačajnijih bitova tajnog eksponenta.

Teorem 2.5.5. *Neka je* $N = pq$ *RSA modul s balansiranim prostim faktorima. Neka je* $e = N^{\alpha}$ *javni eksponent takav da* $0 < \alpha \leq 1/4$ *i d odgovarajući tajni eksponent definiran modulo* $\phi(N)$*. Neka vrijedi* $|p - q| > \frac{1}{\lambda} N^{1/4}$ *za neki* $\lambda > 1$ *i* $e = \gamma k$ *za neki* $\gamma > 1$ *gdje je k konstanta iz jednadžbe ključa. Ako nam je poznato* $3/4$ *najznačajnijih bitova tajnog eksponenta d, N možemo faktorizirati u polinomijalnom vremenu u* $\log N$*,* γ *i* λ*.*

Objasnimo postupak. Budući da je $\alpha < 3/4$ možemo izračunati $\hat{k}$ takav da $k \in \{\hat{k} - 8, \hat{k} + 8\}$. Metodu možemo ponoviti za svaki mogući k, pretpostavimo radi jednostavnosti da je $k = \hat{k}$. Sada izračunamo $\hat{s_0} = N + 1 - \lceil \frac{e\hat{d}-1}{k} \rfloor$ što je dobra aproksimacija najznačajnijih bitova za $p + q$. Iz toga možemo izračunati dobru aproksimaciju najznačajnijih bitova većeg od prostih faktora budući da vrijedi

$$p = \frac{1}{2}((p + q) + \sqrt{(p + q)^2 - 4N}).$$

Dakle,

$$\hat{p} = \frac{1}{2}(\hat{s_0} + \sqrt{\hat{s_0}^2 - 4N}).$$

Pojednostavljivanjem i korištenjem nejednakosti $\hat{s_0} < 2(p + q)$ i $p + q < 3N^{1/2}$ dolazimo do toga da vrijedi $|\hat{p} - p| < 10\lambda\gamma N^{1/4}$.

Dakle, poznato nam je malo manje od $1/2$ najznačajnijih bitova od p. Sada možemo iskoristiti rezultat koji smo ranije naveli za slučaj kada nam je poznato barem pola bitova jednog od faktora. Kako nam zapravo nije poznato pola bitova koristimo metode kojima možemo proširiti broj poznatih bitova, jedna od najjednostavnijih je jednostavno pogađanje preostalih bitova.

Postoji i još jači napad za slučaj kada je $e = N^\alpha$ prost i $1/4 \leq \alpha \leq 1/2$.

Teorem 2.5.6. *Neka je $N = pq$ RSA modul s balansiranim prostim faktorima. Neka je $e = N^\alpha$ prost javni eksponent takav da $1/4 \leq \alpha \leq 1/2$ i d odgovarajući tajni eksponent definiran modulo $\phi(N)$. Ako je poznato α najznačajnijih bitova tajnog eksponenta, možemo faktorizirati modul u vremenu polinomijalnom u* $\log N$.

Na isti način kao u prethodnim napadima dolazimo do $\hat{k}$ takav da je $k \in \{\hat{k} - 8, \hat{k} + 8\}$. Pretpostavimo sada da znamo k. Primijetimo da vrijedi

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

a kada reduciramo modulo e dobivamo:

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

Budući da su k i e uvijek relativno prosti, inverz od k je dobro definiran. Dakle, možemo izračunati s_0 modulo e. Vrijedi da jednadžba

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

ima rješenja p i q, pa modularna jednadžba

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

ima rješenja $p_0 = p \pmod{e}$ i $q_0 = q \pmod{e}$. Budući da je e prost, to su i jedina rješenja te jednadžbe. Jednom kada znamo p_0 i q_0 možemo faktorizirati modul koristeći rezultat kada znamo barem pola najznačajnijih znamenaka od jednog prostog faktora (budući da $e > N^{1/4}$, a mi znamo $p \pmod{e}$).

Proučili smo nekoliko napada koji koriste poznavanje najznačajnijih bitova tajnog eksponenta. Spomenimo samo da postoje i napadi koji koriste poznavanje najmanje značajnih bitova, npr. kada imamo balansirane proste faktore, javni i tajni eksponent definiran modulo $\phi(N)$ i znamo $1/4$ najmanje značajnih bitova tajnog eksponenta očekuje se da možemo faktorizirati modul u vremenu polinomijalnom u $\log N$ i e.

Također, postoje i napadi koji koriste parcijalno poznavanje prostih faktora kako bi došli do što bolje aproksimacije od $\phi(N)$.

Poglavlje 3

Kriptoanaliza RSA inačica

3.1 CRT-RSA

CRT-RSA koristi faktorizaciju modula pri dekripciji kako bi se smanjila njezina cijena. Umjesto dekriptiranja na način: $m = c^d \pmod N$, poruka se dekriptira na način da se najprije izračunaju m_p i m_q:

$$m_p = c^d \bmod p,$$

$$m_q = c^d \bmod q.$$

I zatim pomoću kineskog teorema o ostacima izračuna originalna poruka:

$$m = m_p + p((m_q - m_p)p^{-1} \bmod q).$$

Enkripcija je ista kao kod klasičnog RSA. U dekripciji, ukoliko je tajni eksponent veći od $N^{1/2}$, možemo koristiti reducirane tajne eksponente:

$$d_p = d \bmod (p - 1),$$

$$d_q = d \bmod (q - 1).$$

Iz malog Fermatovog teorema slijedi da ih možemo koristiti umjesto d u parcijalnim dekripcijama. Slijedi da postoje k_pi k_q takvi da:

$$ed_p = 1 + k_p(p - 1),$$

$$ed_q = 1 + k_q(q - 1).$$

Ove jednadžbe zovemo CRT-jednadžbe.

Budući da je CRT-RSA inačica RSA kriptosustava, svi napadi na RSA se mogu primjeniti i na CRT-RSA.

No, za razbiti CRT-RSA dovoljno je i izračunati CRT eksponente jer tada množeći CRT-jednadžbe dobivamo $e(ed_pd_q - d_p - d_q) + 1 = k_pk_q(p-1)(q-1)$, dakle znamo višekratnik od $\phi(N)$, pa možemo faktorizirati modul.

Ukoliko nam je poznat samo jedan CRT-eksponent opet možemo lako faktorizirati modul. Naime, budući da je $m^{ed_p} \equiv m \pmod{p}$, dakle $m^{ed_p} - m = cp$, za neki $c \in \mathbb{Z}$. Neka je $M = (m^{ed_p} - m) \pmod{N}$. Kada c nije višekratnik od q tada vrijedi $gdc(M, N) = p$. Ukoliko je c višekratnik od q tada je $ed_p - 1$ višekratnik od $\phi(N)$ pa opet lako dolazimo do faktorizacije modula.

Primjer 3.1.1. *Neka je* $(e, N) = (3, 1735177)$ *i* $d_p = 1191$. *Uzmimo proizvoljnu poruku* $m \in \mathbb{Z}_p^*$, *npr.* $m = 2$. *Izračunajmo* $M = (m^{ed_p} - m) \bmod N = 1454558$. *Sada* $p = nzd(M, N) = 971$.

Kada imamo dovoljno male CRT eksponente modul možemo faktorizirati N u vremenu u kojem je dominantni faktor $\sqrt{d_p}$, gdje je d_p manji CRT eksponenat. Promatramo funkcije oblika:

$$G(X) = \prod_{y=0}^{2^{m/2}-1} (g^{e2^{m/2}y}X - g) \bmod N,$$

gdje je $g \in \mathbb{Z}_N^*$ i m je najmanji prirodni broj takav da je $d_p \leq 2^m$. Ako d_p zapišemo u obliku $d_p = A2^{m/2} + B$, gdje očito vrijedi $0 \leq A, B < 2^{m/2}$, tada $G(g^{eB})$ zadovoljava:

$$(g^{e2^{m/2}A}g^{eB} - g) \bmod N = (g^{ed_p} - g) \bmod N.$$

Vrijedi da je $g^{ed_p} - g$ neki višekratnik od p. Ako dodamo i uvjet da $d_p \not\equiv d_q \pmod{2^{m/2}}$ tada znamo da $G(g^{eB})$ nije višekratnik od q, pa $nzd(N, G(g^{eB}))$ daje p, odnosno otkriva faktorizaciju od N. Metodu provodimo na način da pogađamo B, odnosno tražimo $nzd(G(g^{ex}), N)$, za $x = 0, \ldots, 2^{m/2} - 1$ dokle ne dobijemo p.

Primjer 3.1.2. *Neka je* $(e, N) = (3, 1735177)$ *i pretpostavimo da znamo da je* $m = 10$ *(ukoliko ne znamo, možemo ponavljati postupak za različite veličine od m). Koristiti ćemo poruku* $g = 2$. *Računamo vrijednost funkcije* G *u* $2^5 = 32$ *točaka dok ne dobijemo faktorizaciju. Za* $x = 8$ *dobivamo* $p = nzd(G(g^{ex}), N) = nzd(G(2^{3\times 8}), 1735177) = nzd(1535151, 1735177) = 971$.

Postoje i napadi bazirani na dijelom poznatom CRT tajnom eksponentu.

Teorem 3.1.3. *Neka je* $N = pq$ *modul s balansiranim prostim faktorima za čiji javni eksponent vrijedi* $e = N^\alpha \leq N^{1/4}$ *i neka za CRT-eksponent* d_p *vrijedi* $ed_p \equiv 1 \pmod{p-1}$. *Ako imamo imamo* $\hat{d}_p$ *takav da*

$$|d_p - \hat{d}_p| \leq N^{\frac{1}{4}-\alpha},$$

tada možemo faktorizirati modul u polinomijalnom vremenu u $\log N$.

Dokaz. Neka je $d_p = \hat{d}_p + d_0$, za neki nepoznati d_0. Sada jednadžbu ključa:

$$e(\hat{d}_p + d_0) = 1 + k(p-1)$$

možemo napisati kao:

$$e\hat{d}_p - kp = 1 - k - ed_0 = -(ed_0 + k - 1).$$

Budući da je $|d_0| = |d_p - \hat{d}_p| < N^{1/4-\alpha}$ i $|k| < e \leq N^{1/4}$ slijedi:

$$|ed_0 + k - 1| < |ed_0 + k| < |ed_0| + |k| < N^{\alpha}N^{1/4-\alpha} + N^{1/4} = 2N^{1/4},$$

pa je $|e\hat{d}_p - kp| < 2N^{1/4}$. Slijedi da je $e\hat{d}_p$ dovoljno dobra aproksimacija za kp da možemo primijeniti Korolar 2.1.11 ukoliko $N \nmid kp$, a to vrijedi jer su p i q balansirani faktori, pa $kp < ep < N^{1/4}p < N$. □

Kada imamo jako mali javni eksponent, možemo faktorizirati modul ako je poznato dovoljno najznačajnijih ili najmanje značajnih bitova od jednog od CRT-eksponenata.

Teorem 3.1.4. *Neka je $N = pq$ RSA modul sa balansiranim prostim faktorima, neka je e javni eksponent takav da je $e < \frac{1}{2}N^{1/2}$ i neka d_p zadovoljava $ed_p \equiv 1 \pmod{p-1}$. Ako imamo dane $\tilde{d}_p$ i M takve da je $\tilde{d}_p = d_p \pmod{M}$ i*

$$M \geq N^{1/4}$$

ili $\hat{d}_p$ takav da

$$|d_p - \hat{d}_p| \leq N^{1/4}$$

tada modul možemo faktorizirati u polinomijalnom vremenu u $\log N$ *i e.*

Dati ćemo dokaz za slučaj kada su poznate najmanje značajne znamenke, odnosno kada je dan $\tilde{d}$. U slučaju kada su poznate najznačajnije znamenke od d postupak ćemo pokazati kroz primjer iza dokaza.

Dokaz. Kako vrijedi $k < e < \frac{1}{2}N^{1/2}$, k možemo pronaći iscrpnim pretraživanjem, pa za svaki $k' < e$ pokušati faktorizirati modul. Pretpostavimo sada da znamo k.

Neka je $d_p = \hat{d}_p M + \tilde{d}_p$ gdje za $\hat{d}$ vrijedi:

$$|\hat{d}| = \left|\frac{d_p - \tilde{d}_p}{M}\right| < \left|\frac{d_p}{M}\right| < 2N^{1/4},$$

jer je $M \geq N^{1/4}$ i $d_p < p < 2N^{1/2}$. Uvedimo supstituciju $d_p = \hat{d}_p M + \tilde{d}_p$ u CRT jednadžbu ključa, dobivamo

$$e\tilde{d}_p + k - 1 = kp - e\hat{d}M.$$

Neka je $E = (eM)^{-1} \pmod N$, pa je $EeM = 1 + cN$ za neki cijeli broj c. Gornju jednadžbu množimo sa E, dobivamo

$$E(e\tilde{d_p} + k - 1) = Ekp - (1 + cN)\hat{d} = (Ek - c\hat{d}q)p - \hat{d}.$$

Ovdje smo pretpostavili da E postoji, ukoliko inverz ne postoji to znači da je $nzd(eM, N) > 1$ pa će taj najveći zajednički djelitelj otkriti faktorizaciju od N (jer je $eM < N$) i postupak bi bio gotov.

Stavimo $K = Ek - c\hat{d}q$, dobivamo

$$|E(e\tilde{d_p} + k - 1) - Kp| = |-\hat{d}| < 2N^{1/4},$$

pa je $E(e\tilde{d_p} + k - 1)$ dovoljno dobra aproksimacija za Kp da bi primijenili Korolar 2.1.11 i faktorizirali modul. Prisjetimo se je za primjenu tog korolara nužan uvjet da Kp nije višekratnik od N, to vrijedi jer bi u suprotnome vrijedilo da $q|K$, odnosno $q|k$ što ne vrijedi jer je $k < e < \frac{1}{2}N^{1/2}$ i faktori su balansirani.

□

Primjer 3.1.5. *Neka je* $(e, N) = (3, 1735177)$ *i neka je* $\hat{d_p} = 1154911$. *Dakle* $d_p = \hat{d_p} + d_0$ *gdje je* $|d_0| < N^{1/4} = 36.29$. *Ubacujemo* $d_p = \hat{d_p} + d_0$ *u CRT jednadžbu i dobivamo:*

$$e\hat{d_p} + k - 1 = kp - ed_0.$$

Neka je sada $E = e^{-1} \pmod N = 1156785$, *pa je* $Ee = 1 + cN$. *Množimo gornju jednadžbu sa E i dobivamo:*

$$E(e\hat{d_p} + k - 1) = Ekp - (1 + cN)d_0 = (Ek - cd_0q)p - d_0.$$

Sada neka je $K = Ek - cd_0q$. *Vrijedi:*

$$|E(e\hat{d_p} + k - 1) - Kp| = |-d_0| < N^{1/4},$$

pa je $E(e\hat{d_p} + k - 1) = 1156785 \times (3 \times 1154911 + k - 1) = 1156785 \times (3464732 + k)$ *dovoljno dobra aproksimacija za Kp da bi primijenili Korolar 2.1.11. Sada još moramo izračunati k, ali znamo da vrijedi* $k < e$, *pa k možemo lako pronaći iscrpnim pretraživanjem, u našem slučaju* $k < 3$. *Uvrštavamo kandidate za k redom dok ne dobijemo faktorizaciju modula. U našem primjeru dobivamo* $k = 1$ *i zatim primjenom Korolara 2.1.11 dobivamo* $p = 971$.

3.2 RSA s više prostih faktora

RSA s više prostih faktora koristi modul koji ima tri ili više prostih faktora. On omogućuje brže generiranje ključeva i brže dekriptiranje pomoću kineskog teorema o ostacima. Koristimo balansirane proste faktore, što kod RSA s više prostih faktora znači da ako poredamo

proste faktore po veličini, $p_i < p_{i+1}$ za $i = 1, \ldots, r-1$ mora vrijediti

$$4 < \frac{1}{2}N^{1/r} < p_1 < N^{1/r} < p_r < 2N^{1/r}.$$

Iz izraza $\phi(N) = \prod_{i=1}^{r}(p_i - 1)$ i $s = N - \phi(N)$, zbog balansiranih faktora, dobivamo gornju ogradu za s, $|s| < (2r-1)N^{1-1/r}$ gdje je r broj prostih faktora modula, pa slijedi da $\phi(N)$ i N imaju otprilike $1/r$ jednakih najznačajnijih bitova. Enkripcija za RSA s više prostih faktora ista je kao i za RSA, za dekripciju pak možemo koristiti klasičnu RSA dekripciju ili dekripciju pomoću CRT tajnih eksponenata kao i kod CRT-RSA. Za razliku od prethodnih inačica, za RSA s više prostih faktora ne postoji deterministički algoritam za faktorizaciju modula ukoliko je poznata vrijednost od $\phi(N)$ ili od tajnog eksponenta d. No, ukoliko je poznat višekratnik od $\phi(N)$ (dakle, dovoljno i d budući da je $ed - 1 = k\phi(N)$) možemo probabilistički faktorizirati modul.

Ukoliko je poznato dovoljno najznačajnijih ili najmanje značajnih bitova od prostih faktora modul se može faktorizirati. Idući teorem je generalizacija Teorema 2.5.1.

Teorem 3.2.1. *Neka je N modul sa r balansiranih prostih faktora. Za bilo koji $s \in [2, r]$, ako je dano $r-s$ faktora od N, $(s-1)/s$ najznačajnijih ili najmanje značajnih bitova jednog od nepoznatih faktora, $(s-2)/(s-1)$ najznačajnijih ili najmanje značajnih bitova slijedećeg od nepoznatih faktora, $\ldots$, $2/3$ najznačajnijih ili najmanje značajnih bitova slijedećeg od nepoznatih faktora i $1/2$ najznačajnijih ili najmanje značajnih bitova jednog od 2 zadnja nepoznata faktora, onda se modul N može faktorizirati u vremenu polinomijalnom u r i* $\log N$.

Metoda se oslanja na uzastopnu primjenu Korolara 2.1.11 da izračunamo jedan po jedan prosti faktor.

Kada imamo mali tajni eksponent, točnije, eksponent mora poštivati ogradu:

$$d \leq \frac{N}{2ks} \leq \frac{N^{1/r}}{2k(2r-1)}$$

onda možemo za faktorizaciju modula koristiti proširenje Wienerovog napada, ponovo će jedna od konvergenti od proširenja e/N u verižni razlomak odgovarati k/d, što ćemo koristiti u računanju $\lfloor e(d/k) \rfloor = \phi(N)$.

Ako pak imamo poznate najznačajnije bitove tajnog eksponenta koristimo slijedeći napad.

Teorem 3.2.2. *Neka je N modul sa r faktora koji su balansirani, $e = N^{\alpha}$ javni eksponent takav da je $0 < \alpha \leq 1/r$ i d odgovarajući tajni eksponent. Neka je $e = \gamma k$ za neki $\gamma > 1$ i k koeficijent jednadžbe ključa. Ako je dano $1 - \alpha$ najznačajnijih bitova tajnog eksponenta, tada možemo faktorizirati modul u vremenu polinomijalnom u* $\log N$, *r i γ.*

Dokaz slijedi iz dokaza Teorema 2.5.3, samo što sada koristimo ogradu $|s| < (2r - 1)N^{1-1/r}$.

Može se pokazati da, slično kao kod klasičnog RSA, α najznačajnijih bitova tajnog eksponenta otkriva kontantu k iz jednadžbe ključa do na aditivnu grešku od $3 + 2(2r - 1)$.

Napomenimo da postoje i napadi koji koriste poznavanje najmanje značajnih bitova tajnog eksponenta.

Sada ćemo proučiti napad koji koristi poznavanje jednog ili više prostih faktora modula i koristi se za slučajeve kada je tajni eksponent dovoljno mali.

Ako označimo broj faktora sa r, broj poznatih faktora sa v, sa P produkt poznatih prostih faktora, a sa $Q = N/P$ produkt nepoznatih, primijetimo da vrijedi:

$$\phi(N) = \phi(PQ) = \phi(P)\phi(Q) = \phi(P)(Q - s_Q)$$

gdje je $|s_Q| = |Q - s\phi(Q)| < cN^{1-v/r-1/r}$.

Pretpostavljamo da su faktori balansirani i $d = N^\delta$, N je n-bitni modul. Ako je dano bilo kojih $1 \leq v \leq r - 2$ faktora i vrijedi $\delta < \frac{v}{r} - \epsilon$, onda možemo faktorizirati modul u polinomnom vremenu u n. Objasnit ćemo postupak sljedećim primjerom.

Primjer 3.2.3. *Neka je* $(e, N) = (60335741, 76728929)$*,* $r = 3$ *i neka je poznat prosti faktor* $p_1 = 379$*.*

Pišemo jednadžbu ključa u obliku: $ed = 1 + k\phi(Q)\phi(P)$*, gdje znamo da je* $\phi(P) = p_1 - 1 = 378$*. Kada je reduciramo modulo* $\phi(P)$ *dobivamo:* $d = e^{-1} \bmod \phi(P)$*, odnosno u našem primjeru:* $d = 60335741^{-1} \bmod 378 = 149$*. Ukoliko je* $d < \phi(N)$ *slijedi da je* $d = e^{-1} \bmod \phi(P) = 149$*. To će uvijek vrijediti zbog uvjeta da su faktori balansirani i zbog nejednakosti* $\delta < \frac{v}{r} - \epsilon$*. Sada kada znamo d možemo izračunati višekratnik od* $\phi(N)$ *i probabilistički faktorizirati modul. Dobivamo preostale faktore:* $p_2 = 443$ *i* $p_3 = 457$*.*

3.3 RSA s višom potencijom

RSA s višom potencijom koristi modul oblika $N = p^{b-1}q$, za neki $b \geq 3$. Promotriti ćemo inačicu u kojoj su tajni i javni eksponent definirani modulo

$$\lambda'(N) = nzv(p - 1, q - 1),$$

umjesto modulo $\phi(N) = p^{b-2}(p - 1)(q - 1)$. Ovdje ne možemo primijeniti standardnu dekripciju jer općenito $m^{ed} \not\equiv m \pmod N$, dakle moramo prvo napraviti parcijalnu dekripciju modulo p^{b-1} i modulo q i zatim rezultate kombinirati koristeći kineski teorem o ostacima. Enkripcija je ista kao i kod RSA. Javni eksponent biramo tako da je mali, tj. $e \ll N^{1/b}$ i

tako da je $nzd(e, p) = 1$. Zatim izračunamo tajni eksponent kao inverz od e modulo $\lambda'(N)$, i izračunamo parcijalne tajne eksponente:

$$d_p = d \bmod (p-1),$$

$$d_q = d \bmod (q-1).$$

Dekripciju vršimo na način da izračunamo:

$$m_q = c^{d_q} \bmod q = m \bmod q,$$

$$m_p = c^{d_p} \bmod p = m \bmod p.$$

Sada koristimo iterativno Henselovo podizanje da parcijalnu dekripciju m_p podignemo do parcijalne dekripcije modulo p^{b-1}, zatim dobivenu parcijalnu dekripciju pomoću kineskog teorema o ostacima kombiniramo s parcijalnom dekripcijom modulo q kako bi otkrili izvorni tekst modulo N. Kada se koristi mali javni eksponent, ovaj način dekripcije je najbrži od svih razmatranih inačica RSA kriptosustava. Prisjetimo se Henselove leme pomoću koje se radi Hanselovo podizanje.

Teorem 3.3.1. *(Henselova lema) Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \not\equiv 0 \pmod{p}$, onda postoji jedinstveni $t \in \{0, 1, 2, \ldots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

Ukoliko znamo višekratnik od $\lambda'(N)$ možemo probabilistički faktorizirati modul. Također, budući da je $ed - 1 = k\lambda'(N)$ za faktorizaciju modula dovoljno je znati tajni eksponent d. Bit će dovoljno i poznavanje bilo kojeg CRT tajnog eksponenta jer iz definicije za CRT eksponente očekuje se da za nasumičnu poruku $m \in \mathbb{Z}_N^*$ vrijedi:

$$nzd(m^{ed_p} - m, N) = p,$$

$$nzd(m^{ed_q} - m, N) = q.$$

Teorem 3.3.2. *Neka je $N = p^{b-1}q$ za neki poznati $b \geq 2$ gdje su p i q balansirani prosti faktori. Ako je poznato barem $1/b$ najznačajnijih ili najmanje značajnih bitova od p ili barem $(b-1)/b$ najznačajnijih ili najmanje značajnih bitova od q, tada N možemo faktorizirati u vremenu polinomijalnom u $\log N$.*

Metoda koju koristimo je generalizacija iste za obični RSA, odnosno Teorema 2.5.1 i dokaz slijedi direktno iz tog teorema.

Kada imamo djelomično poznate CRT tajne eksponente također možemo doći do faktorizacije modula.

Teorem 3.3.3. *Neka je $N = p^{b-1}q$ n-bitni modul s balansiranim faktorima. Ako je $e = N^{\alpha}$ gdje je $\alpha \leq (b-1)/b^2$ i CRT eksponenti zadovoljavaju $ed_p \equiv 1 \pmod{p-1}$ i $ed_q \equiv 1 \pmod{q-1}$, za dani $\hat{d}_p$ takav da vrijedi*

$$|d_p - \hat{d}_p| \leq N^{\frac{b-1}{b^2}-\alpha}$$

ili $\hat{d}_q$ takav da vrijedi

$$|d_q - \hat{d}_q| \leq N^{\frac{1}{b^2}-\alpha}$$

možemo doći do faktorizacije modula u vremenu polinomijalnom u n.

Ovaj napad je generalizacija Teorema 3.1.3.

3.4 RSA sa zajedničkim prostim faktorom

RSA sa zajedničkim prostim faktorom koristi proste faktore posebne strukture, točnije, biramo proste brojeve p i q takve da $p-1$ i $q-1$ imaju veliki zajednički djelitelj. Sada možemo koristiti tajne eksponente manje od $N^{1/4}$ bez straha od Wienerovog napada.

Za neki veliki prosti broj g, neka su $p = 2ga + 1$ i $q = 2gb + 1$ takvi da $nzd(a, b) = 1$ i $h = 2gab + a + b$ je prost. Sada je $\lambda(pq) = 2gab$ i $\phi(pq) = 2g\lambda(pq)$. Definiramo RSA sa zajedničkim prostim faktorom tako da koristi javni i tajni eksponent kao inverze s obzirom na $\lambda(N) = 2gab$. Vidimo da vrijedi i $N = pq = 2gh + 1$.

Pokažimo primjerom kako možemo efikasno faktorizirati modul ukoliko su nam poznati a i b.

Primjer 3.4.1. *Neka je $N = 12932234012219$, $a = 80$ i $b = 651$. Sada je u jednadžbi $N = 2g(2gab + a + b)$ samo g nepoznanica. Dobivamo kvadratnu jednadžbu:*

$$208320g^2 + 1462g - 12932234012218 = 0.$$

Dakle g je pozitivno rješenje jednadžbe, odnosno $g = 7879$. Sada lako izračunamo $p = 2ga + 1 = 1260641$ i $q = 2gb + 1 = 10258459$.

Ukoliko nam je poznat g i vrijedi $g < a+b$ (što je, budući da su prosti faktori balansirani, ekvivalentno tome da je $g \geq N^{1/4}$) opet možemo lako faktorizirati modul. Pokažimo to na istom primjeru.

Primjer 3.4.2. *Neka je $g = 7879$ i $N = 12932234012219$, pokušajmo samo pomoću tih informacija faktorizirati modul. Vrijedi $N = 2g(2gab + a + b) + 1$. Odnosno $(N-1)/(2g) = 2gab+a+b$. Budući da je $a+b < g$ reduciranjem jednadžbe modulo g dobivamo $a+b = 731$*

(mod 7879). *Dakle* $a + b = 731$. *Vraćamo* $b = 731 - a$ *u gornju jednadžbu, dobivamo kvadratnu jednadžbu*

$$2ga^2 - 2g(a + b)a + (N - 1)/(2g) - (a + b),$$

odnosno

$$15758a^2 - 11519098a + 820676640.$$

Rješavanjem dobivamo $a = 80$, $b = 651$ *i onda lako izračunamo proste faktore.*

Ukoliko nam je poznat g za koji vrijedi $g \leq N^{1/4}$ i za tajni eksponent vrijedi $d < g$ tada faktoriziramo modul na način prikazan u slijedećem primjeru.

Primjer 3.4.3. *Neka je* $N = 12645534754819$, $e = 835493367$ *i* $g = 1223$. *Ako reduciramo jednadžbu ključa* $ed = 1 + k2gab$ *modulo g dobivamo:*

$$ed \equiv 1 \pmod{1223}.$$

Odnosno $d \equiv e^{-1} \pmod{1223}$. *Budući je po pretpostavci* $d < g$ *slijedi da je* $d = e^{-1} \pmod{1223}$, *odnosno* $d = 1219$.

Iako je ova inačica RSA stvorena kako bi bila otpornija na napade bazirane na malom tajnom eksponentu, posebno Wienerov napad, ipak možemo iskoristiti posebnu strukturu prostih faktora i jednadžbu ključa kako bi primijenili inačicu istog napada.

Kada imamo mali tajni eksponent možemo koristiti Wienerov napad pod uvjetom da je zadovoljena ograda

$$\delta < \frac{3}{4} - \frac{\alpha}{2} - \gamma - \log_N \sqrt{12}$$

gdje je $g = N^\gamma$, $e = N^\alpha$ i $d = N^\delta$. Tada će e/N biti jedna od konvergenti za $\frac{k}{2gd}$. Budući da je g prost i $nzd(k, d) = 1$ slijedi da je nazivnik točne konvergente d, $2d$, gd ili $2gd$, pa lako dolazimo do d. Za svaku od konvergenti $c_i = a_i/b_i$ računamo $d_i = nzd(N - 1, b_i)$, kako je $N - 1 = 2gh$ gdje su g i h prosti, računanje najvećeg zajedničkog djelitelja od točne konvergente dati će nam d.

RSA sa zajedničkim prostim faktorom ipak je otporniji na Wienerov napad od klasičnog RSA u smislu ograde za tajni eksponent d.

3.5 Dualni RSA

Dualni RSA koristi se kada su nam potrebne dvije instance RSA, pa radi štednje na memoriji za obje koristimo iste javne i tajne eksponente, ali drugačiji modul.

Štednju na memoriji možemo postići i korištenjem drugih inačica RSA kriptosustava kao što je kompresirani RSA ili spareni RSA. Kod kompresiranog RSA koristimo dvije instance RSA s kompresiranim modulom. Postoji poznati algoritam kojim modul možemo kompresirati za faktor $2/3$, tj. dovoljno je spremiti $1/3$ bitova modula. Kod sparenog RSA ponovno koristimo dvije instance RSA, ali ovaj put s modulima koji imaju fiksnu razliku, pa je dovoljno pohraniti samo jedan od njih. Kada želimo koristiti RSA s malim javnim ili tajnim eksponentom koji ima dovoljno velike preostale parametre tako da bude otporan na sve poznate napade, pokazuje se da kompresiranim RSA dobivamo najveću uštedu na memoriji. Ako pak želimo koristiti RSA s malim CRT-eksponentima, pokazuje se da dualni RSA donosi najveću uštedu.

Proučimo dulani RSA. Javni i tajni eksponenti biti će inverzi modulo $\phi(N_1)$ odnosno modulo $\phi(N_2)$. Jednadžbe ključa dakle glase:

$$ed = 1 + k_1\phi(N_1) = 1 + k_1(N_1 - s_1),$$

$$ed = 1 + k_2\phi(N_2) = 1 + k_2(N_2 - s_2),$$

gdje su $k_1, k_2 \in \mathbb{Z}$. Kada se koriste CRT dekripcija, instance koriste i iste CRT eksponente, pa vrijedi:

$$\begin{aligned} ed_p &\equiv 1 \pmod{p_1 - 1},\\ ed_p &\equiv 1 \pmod{p_2 - 1},\\ ed_q &\equiv 1 \pmod{q_1 - 1},\\ ed_q &\equiv 1 \pmod{q_2 - 1}. \end{aligned}$$

U dualnom RSA imati mali javni eksponent može biti problem. Oduzimajući jednadžbe ključa dolazimo do jednadžbe:

$$k_1'(N_1 - s_1) = k_2'(N_2 - s_2),$$

gdje je $k_1' = k_1/nzd(k_1, k_2)$ i $k_2' = k_2/nzd(k_1, k_2)$. Za svaki n-bitni modul, gdje je $n > 14$ i javni eksponent $e = N^\alpha$ gdje je $\alpha < \frac{1}{4} - \frac{\log_N 18}{2}$ možemo lako doći do konstanta k_1' i k_2'. Naime, iz danih ograda slijedi da je

$$\left|\frac{N_1}{N_2} - \frac{k_2'}{k_1'}\right| < \frac{1}{2(k_1')^2},$$

pa je $k_1'/k_2' = k_1/k_2$ jedna od konvergenti u razvoju N_1/N_2 u verižni razlomak.

Ako pak imamo mali tajni eksponent, točnije $d = N^\delta$ gdje je $\delta < \frac{1}{3} - \log_N 6$, tada oba modula mogu biti faktorizirana u polinomijalnom vremenu u $\log N$.

Bibliografija

[1] Andrej Dujella, *Uvod u teoriju brojeva*, PMF-Matematički odjel, Sveučilište u Zagrebu (skripta) (2006).

[2] Andrej Dujella i Marcel Maretić, *Kriptografija*, Element, 2007.

[3] M. Jason Hinek, *Cryptanalysis of RSA and its variants*, CRC press, 2009.

[4] Stefan Katzenbeisser, *Recent advances in RSA cryptography*, sv. 3, Springer Science & Business Media, 2001.

[5] Song Y. Yan, *Cryptanalytic attacks on RSA*, Springer Science & Business Media, 2007.

Sažetak

Tema ovog diplomskog je RSA kriptosustav, njegove inačice i njihova kriptoanaliza. U prvom poglavlju opisujemo RSA općenito i navodimo definiciju i neka njegova svojstva. Slijedeća dva poglavlja čine glavninu rada.

U drugom poglavlju razrađujemo napade na RSA i proučavamo što kod implementacije treba izbjegavati. Kroz proučavanje raznih napada, u napadima baziranima na malom tajnom eksponentu utvrđujemo donju ogradu za tajni eksponent RSA instance kako bi kriptosustav bio siguran, a u napadima baziranima na dijelom poznatom ključu ističemo važnost čuvanja bitova tajnog ključa tajnima.

U trećem poglavlju bavimo se inačicama RSA sustava koje su efikasnije od običnog RSA. Veća efikasnost postiže se štednjom na cijeni dekripcije, cijeni generiranja ključeva i memoriji. Proučiti ćemo napade na te inačice, vidjeti koji se napadi na RSA mogu generalizirati na napad na inačicu, koji se mogu direktno primijeniti i koje nove napade možemo primijeniti. Novi napadi koristiti će specifična svojstva dane inačice.

Summary

The main topic of this work is cryptanalysis of RSA and its variants. In the first chapter we describe RSA in general and introduce some of its properties. Next two chapters contain the main work.

In the second chapter we analyze some attacks on RSA and explore what to avoid in RSA implementation. Through examining the attacks, in small private exponent attacks we determine the lower bound for RSA private exponent, and in partial key exposure attacks we highlight the importance of keeping bits of the secret key secret.

In the third chapter we introduce some of the RSA variants which are more effective then classic RSA in the sense of the decryption price, key generation price or memory. We explore the attacks on these variants and discover what classic RSA attacks can we use either directly or after generalization. We also explore some new attacks which use specific properties of the given variant.

Životopis

Moje ime je Martina Alilović. Rođena sam 15.8.1993. godine u Rijeci. Djetinjstvo vežem za Rabac u Istri gdje sam živjela, odlazila u vrtić i osnovnu školu i Humac u Hercegovini gdje sam provodila ljeta. Opću gimnaziju pohađala sam u Labinu, a 2012. upisala sam Prirodoslovno-matematički fakultet u Zagrebu, smjer Matematika. Godine 2015. stekla sam titulu sveučilišne prvostupnice i upisala diplomski studij Matematike i računarstva na istom fakultetu. Akademske godine 2016./2017. sudjelovala sam u vođenju Kluba studenata Istre "Mate Balota".