RSA Kriptosustav

Bernadin Ibrahimpašić*

Sažetak. *Osobama koje sudjeluju u komunikaciji nije uvijek dostupan siguran komunikacijski kanal pa razmjena ključeva može predstavljati veliki problem. Jedan od načina za rješenje ovog problema je korištenje kriptosustava javnog ključa. To su kriptosustavi kod kojih je iz poznavanja funkcije za šifriranje, praktički nemoguće, u nekom razumnom vremenu, izračunati funkciju za dešifriranje. Najpoznatiji kriptosustav s javnim ključem je RSA. Njegova sigurnost je zasnovana na teškoći faktorizacije velikih prirodnih brojeva.*

Ključne riječi: *RSA kriptosustav, verižni razlomci, diofantske aproksimacije, faktorizacija*

Abstract. *The persons involved in communication do not always have a secure communication channel and the exchange of the keys can be a big problem. One possible solution is the usage of public key cryptography. In these systems it is practically impossible to calculate the decryption function from the encryption function. The most popular public key cryptosystem in use today is the RSA. Its security is based on the difficulty of finding the prime factors of large integers.*

Key words: *RSA cryptosystem, continued fractions, Diophantine approximations, Factorization*

1. Uvod

Osnovni zadatak kriptografije je omogućiti dvjema osobama, od kojih je jedna *pošiljatelj*, tj. osoba koja želi priopćiti poruku, a druga *primatelj*, tj. osoba kojoj je poruka poslana, da komuniciraju preko nesigurnog komunikacijskog kanala (telefonska linija, radiovalovi, računalna mreža, itd.) na način da treća osoba (njihov protivnik, tzv. napadač) ne može razumjeti njihove poruke. Poruku koju pošiljatelj želi poslati primatelju zovemo *otvoreni tekst* (engl. *plaintext*). To može biti tekst na njihovom materinjem ili nekom drugom jeziku, numerički podaci ili bilo što drugo. Pošiljatelj transformira otvoreni tekst, koristeći unaprijed dogovoreni *ključ*. Taj postupak se zove *šifriranje (kriptiranje)*, a dobiveni rezultat *šifrat (šifrirana poruka, kriptogram, kriptat, kriptirana poruka)* (engl. *ciphertext*). Nakon toga pošiljatelj šalje šifrat putem nekog komunikacijskog kanala. Protivnik prisluškujući dozna

*Pedagoški fakultet, Džanica mahala, 36, BIH-77000 Bihać

sadržaj šifrata, ali ne može odrediti otvoreni tekst i razumjeti poruku. Za razliku od njega, primatelj, koji zna ključ kojim je poruka šifrirana, može dešifrirati (dekriptirati) šifrat i odrediti otvoreni tekst.

Šifra (kriptografski algoritam) je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, tu se radi o dvije funkcije od kojih je jedna za šifriranje, a druga za dešifriranje. Argumenti funkcije za šifriranje su ključ i otvoreni tekst, a argumenti funkcije za dešifriranje su ključ i šifrat. Skup svih mogućih vrijednosti ključeva zove se *prostor ključeva*. Kriptosustav se sastoji od šifre i svih mogućih otvorenih tekstova, šifrata i ključeva. Iz rečenog, dobijamo slijedeću formalnu definiciju.

Definicija 1. Kriptosustav *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih otvorenih tekstova.*
2. $\mathcal{C}$ *je konačan skup svih mogućih šifrata.*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva.*
4. *za svaki ključ* $K \in \mathcal{K}$ *postoji algoritam šifriranja* $e_K \in \mathcal{E}$ *i odgovarajući algoritam dešifriranja* $d_K \in \mathcal{D}$*, gdje su* $e_K \colon \mathcal{P} \to \mathcal{C}$ *i* $d_K \colon \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je*

$$d_K\left(e_K\left(x\right)\right) = x$$

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

S obzirom na tajnost ključa, kriptosustavi se dijele na:

1. *Simetrične kriptosustave* kod kojih se ključ za dešifriranje može izračunati poznajući ključ za šifriranje i obratno. Najčešće su ovi ključevi identični. Sigurnost im leži u tajnosti ključa. Zbog toga se oni i zovu **kriptosustavi s tajnim ključem**.
2. *Asimetrične kriptosustave* kod kojih se ključ za dešifriranje ne može (barem ne u nekom razumnom vremenu) odrediti iz ključa za šifriranje. Ovdje je ključ za šifriranje javni ključ. Točnije rečeno, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja poznaje odgovarajući ključ za dešifriranje (*privatni ili tajni ključ*) može dešifrirati tu poruku. Ideja javnog ključa se javila 1976. godine zbog potrebe razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala. Ovi sustavi se zovu i **kriptosustavi javnog ključa**.

Kod simetričnih kriptosustava, tj. kriptosustava s tajnim ključem, pošiljatelj i primatelj bi tajno izabrali ključ K pomoću kojeg su generirali funkcije e_K za šifriranje i d_K za dešifriranje. U ovom slučaju je d_K isti kao i e_K ili se iz njega može jednostavno izračunati. Iz tog razloga, sigurnost simetričnih kriptosustava leži u tajnosti ključa, što i predstavlja veliki nedostatak, jer pošiljatelj i primatelj prije šifriranja moraju biti u mogućnosti da razmjene tajni ključ preko nekog sigurnog komunikacijskog kanala, pomoću kurira ili se osobno sresti. To je nekada teško

izvodivo, naročito ako su oni na velikoj udaljenosti i ako su komunikacijski kanali, koji su im na raspolaganju, poprilično nesigurni. Pored toga, tajni ključ se mora često mijenjati, jer šifriranje više puta istim ključem smanjuje sigurnost.

Ideju jednog kriptosustava, potpuno drugačijeg tipa nego simetrični kriptosustav, iznijeli su 1976. godine *Whitfield Diffie* i *Martin Hellman*. Nazvali su ga ***kriptosustav javnog ključa***. Ideja se sastojala u tome da se koriste funkcije za šifriranje e_K iz kojih je praktički nemoguće, u nekom razumnom vremenu, izračunati funkciju za dešifriranje d_K. U tom slučaju bi funkcija za šifriranje e_K mogla biti javna.

U svrhu realizacije ideje kriptosustava s javnim ključem, koriste se osobne jednosmjerne funkcije. Za funkciju $f\colon X \to Y$ kažemo da je **jednosmjerna funkcija** (one-way function), ako je $f(x)$ lako izračunati za svaki $x \in X$, ali je $f^{-1}(y)$ jako teško izračunati. Ako je f^{-1} lako izračunati ukoliko nam je poznat neki dodatni podatak (*trapdoor* - tajni ulaz), onda za funkciju f kažemo da je **osobna jednosmjerna funkcija** (trapdoor one-way function).

Kriptosustav s javnim ključem se sastoji od dva skupa funkcija. Funkcija za šifriranje e_K i funkcija za dešifriranje d_K, gdje K prolazi skupom svih mogućih korisnika, sa svojstvom:

1. Za svaki K je d_K inverz od e_K
2. Za svaki K je e_K javan, ali je d_K poznat samo osobi K
3. Za svaki K je e_K osobna jednosmjerna funkcija.

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

Ako Alice (A) želi poslati poruku x Bobu (B), onda Bob prvo pošalje, potpuno otvoreno, Alice svoj javni ključ e_B. Pomoću e_B, Alice šifrira svoju poruku i Bobu pošalje šifrat $y = e_B(x)$. Na kraju, Bob dešifrira šifrat pomoću svog tajnog ključa d_B i dobije otvoreni tekst $x = d_B(y) = d_B(e_B(x))$.

Ukoliko imamo grupu korisnika koji svi žele međusobno komunicirati na ovaj način, onda se svi javni ključevi stave u neku javnu, svima dostupnu, datoteku, koja se formira u obliku telefonskog imenika. Datoteka mora biti jedino takva da nitko ne može promijeniti ničiji javni ključ. Sada, ako Alice želi poslati poruku Bobu, dovoljno je da iz datoteke pročita njegov javni ključ e_B i izvrši šifriranje. Međutim, postavlja se pitanje, kako Bob može biti siguran da mu je baš Alice poslala poruku, a ne netko drugi. Taj problem *autentičnosti* (vjerodostojnosti) se vrlo lako rješava. Neka je P potpis od Alice, koji možda uključuje JMBG, ime kućnog ljubimca ili djevojačko prezime majke. Kako svi znaju e_B, nije dovoljno da Alice pošalje poruku $e_B(P)$ jer to mogu svi. Zbog toga ona na početku ili kraju poruke koju mu šalje, dopiše $e_B d_A(P)$. Primljeni šifrat, koji se sastoji od poruke i dijela $e_B d_A(P)$, Bob dešifrira pomoću d_B i dobije tekst poruke i nerazumljivi dio koji je $d_A(P)$. Kako Bob zna da bi ta poruka trebala biti od Alice, on koristi njen javni ključ e_A i dešifrira $d_A(P)$ i dobije P. Zbog nepoznavanja d_A, niko drugi, osim Alice, nije mogao poruku potpisati na taj način.

Pored toga, što u kriptosustavima s javnim ključem nema potrebe za sigurnim komunikacijskim kanalom, kao što je to kod simetričnih kriptosustava, vidimo da im je prednost i mogućnost potpisa poruke. Prednost je, također, i smanjeni broj

potrebnih ključeva za komunikaciju grupe od n ljudi. Dok je kod simetričnog sustava potrebno $n(n-1)/2$ ključeva, kod kriptosustava s javnim ključem potrebno je samo n javnih i n tajnih ključeva. Unatoč tim prednostima, kriptosustavi s javnim ključem nisu, niti potisli niti zamijenili, simetrične kriptosustave. Osnovni razlog je što su algoritmi s javnim ključem puno sporiji (oko 1000 puta) od modernih simetričnih algoritama (DES, AES). Zbog toga se kriptosustavi s javnim ključem ne koriste za šifriranje poruka nego za šifriranje ključeva. Takav kriptosustav, gdje se komunikacija obavlja pomoću simetričnog kriptosustava, s ključem kojeg su osobe razmijenile pomoću kriptosustava s javnim ključem, zove se ***hibridni kriptosustav***.

2. Definicija RSA kriptosustava

Ideju koju su iznijeli Diffie i Hellman, iskoristili su Ronald Rivest, Adi Shamir i Leonard Adleman i 1977. godine izumili prvi i najšire korišteni kriptosustav s javnim ključem. Nazvan je po svojim izumiteljima (prva slova njihovih prezimena) RSA kriptosustav, a sigurnost mu leži u činjenici da je faktorizacija velikih prirodnih brojeva na produkt dva prosta broja izuzetno teška.

U skladu s definicijom 1, možemo preciznije definirati RSA kriptosustav.

Neka je $n = pq$, gdje su p i q prosti. Neka je $\mathcal{P} = \mathcal{C} = \mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ i neka je

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

gdje je $\varphi(n)$ Eulerova funkcija, koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n, koji su relativno prosti s n.

Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \bmod n \qquad\qquad d_K(y) = y^d \bmod n$$

gdje su $x, y \in \mathbf{Z}_n$.

Vrijednosti n i e su javne, dok su vrijednosti p, q i d tajne.

Ovdje je $x^e \bmod n$ jednosmjerna funkcija, a *trapdoor* je poznavanje faktorizacije $n = pq$.

Još nam ostaje provjeriti jesu li funkcije e_K i d_K jedna drugoj inverzne. Prije toga iskažimo i dokažimo Eulerov teorem.

Definicija 2. *Za prirodan broj n, skup od $\varphi(n)$ cijelih brojeva $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ se zove* **reducirani sustav ostataka modulo n** *ako sadrži točno po jedan element svake klase ostataka modulo n koji je relativno prost sa n.*

Teorem 1 [Euler]. *Ako je $M(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

DOKAZ: Neka je $\{r_1, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m. Kako je $M(a, m) = 1$, imamo da je $M(ar_i, m) = 1$, za sve $i = 1, \ldots, \varphi(m)$. Nadalje, za svaki $i \in \{1, \ldots, \varphi(m)\}$ postoji $\sigma(i) \in \{1, \ldots, \varphi(m)\}$ takav da je

$$ar_i \equiv r_{\sigma(i)} \pmod{m}.$$

Šta više, $ar_i \equiv ar_j \pmod{m}$ ako i samo ako je $i = j$, pa je σ neka permutacija skupa $\{1, \ldots, \varphi(m)\}$, a skup $\{ar_1, \ldots, ar_{\varphi(m)}\}$ je također reducirani sustav ostataka modulo m. Sada je

$$\begin{aligned} a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} &\equiv (ar_1) \cdot (ar_2) \cdot \ldots \cdot \left(ar_{\varphi(m)}\right) \pmod{m} \\ &\equiv r_{\sigma(1)} \cdot r_{\sigma(2)} \cdot \ldots \cdot r_{\sigma(\varphi(m))} \pmod{m} \\ &\equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \pmod{m}. \end{aligned}$$

Podijelimo li obje strane ove kongruencije sa $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}$, što smijemo jer su brojevi r_i relativno prosti s m, dobivamo da je

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

■

Provjerimo sada jesu li funkcije e_K i d_K jedna drugoj inverzne.

$$d_K(e_K(x)) \equiv (e_K(x))^d \equiv (x^e)^d \equiv x^{de} \pmod{n}$$

Kako je $de \equiv 1 \pmod{\varphi(n)}$, to znači da postoji prirodan broj t takav da je $de = t \cdot \varphi(n) + 1$ pa imamo

$$x^{de} = x^{t \cdot \varphi(n)+1} = x^{t \cdot \varphi(n)} \cdot x = \left[x^{\varphi(n)}\right]^t \cdot x.$$

U zavisnosti od n i x imamo 2 slučaja:

1. $M(x, n) = 1$

   Kako je tada, prema Eulerovom teoremu, $x^{\varphi(n)} \equiv 1 \pmod{n}$, to je

   $$x^{de} \equiv 1^t \cdot x \equiv x \pmod{n}.$$

2. $M(x, n) \neq 1$

   Ako je $M(x, n) = n$, tada je $x = 0$ pa je kongruencija trivijalno zadovoljena. Neka je $M(x, n) = p$ ili $M(x, n) = q$. Bez smanjenja općenitosti uzmimo da je $M(x, n) = p$, pa je $x^{de} \equiv 0 \equiv x \pmod{p}$. Kako je $M(x, pq) = p$, gdje su p i q prosti, to je $M(x, q) = 1$ pa je prema Eulerovom teoremu

   $$x^{\varphi(q)} \equiv 1 \pmod{q} \quad \Rightarrow \quad x^{q-1} \equiv 1 \pmod{q}.$$

   Sada je

   $$x^{de} = \left(x^{q-1}\right)^{(p-1) \cdot t} \cdot x \equiv x \pmod{q}.$$

   Konačno je $x^{de} \equiv x \pmod{pq}$, tj. $x^{de} \equiv x \pmod{n}$.

3. Implementacija RSA kriptosustava

Opišimo sada kako se primjenjuje RSA.

1. Bob tajno odabere dva različita prosta broja p i q, od kojih svaki ima oko 100 znamenki. Obično se odaberu tako da jedan od njih ima nekoliko znamenki više od drugog. Odabir se izvrši tako da se, pomoću nekog generatora slučajnih brojeva, generira dovoljno velik prirodan broj k, a zatim se korištenjem nekog testa za testiranje prostosti, traži prvi prosti broj koji je veći ili jednak k.

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

3. Bob bira na slučajan način broj e takav da je $e < \varphi(n)$ i $M(e, \varphi(n)) = 1$.

4. Bob računa d takav da je $de \equiv 1 \pmod{\varphi(n)}$, tj. $d \equiv e^{-1} \pmod{\varphi(n)}$. Izračunavanje d se vrši pomoću *proširenog Euklidovog algoritma*, koji za dane a i b računa $b^{-1} \bmod a$.

Postupak šifriranja poruke, tj. računanja šifrata $y = x^e \bmod n$, se naziva *modularno potenciranje*. Za efikasnost RSA kriptosustava je bitno da se računanje $x^e \bmod n$ može vrlo efikasno provesti pomoću algoritma "*kvadriraj i množi*":

$y = 1$
za $i = l-1, \ldots, 1, 0$ radi
$y = y^2 \bmod n$
ako je $e_i = 1$ tada je $y = y \cdot x \bmod n$

gdje je $e = \sum_{i=0}^{l-1} e_i 2^i$ binarni zapis broja e.

Primjer 1. *Simulirajmo kako Alice šalje poruku* OSIJEK NA DRAVI *Bobu i kako je on dešifrira.*

Bob bira $p = 47$ i $q = 59$ i računa

$$n = pq = 2773$$
$$\varphi(n) = (p-1)(q-1) = 2668.$$

Zatim odabere $e = 17$ i pomoću proširenog Euklidovog algoritma računa d takav da je $de \equiv 1 \pmod{\varphi(n)}$ i dobija da je $d = 157$.

Vrijednosti p, q, d zadržava za sebe, a n i e šalje Alice ili ih jednostavno upisuje u javni direktorij.

Alice želi poslati poruku *OSIJEK NA DRAVI*, čiji je numerički ekvivalent

$$x = 15190910051100140100041801220 9,$$

jer je $(razmak = 00, A = 01, B = 02, \ldots, Y = 25, Z = 26)$.

Kako je $x > n$ to se x razbija u četveroznamenkaste blokove, krećući sa lijeve strane. Zadnji blok, ukoliko mu nedostaje znamenki, se dopuni nulama. Sada je:

$$\begin{aligned} x &= (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \\ &= (1519, 0910, 0511, 0014, 0100, 0418, 0122, 0900). \end{aligned}$$

Poznavajući Bobove javne $n = 273$ i $e = 17$, Alice računa

$$\begin{aligned}
y_1 &= 1519^{17} \bmod 2773 = 1204\\
y_2 &= 910^{17} \bmod 2773 = 883\\
y_1 &= 511^{17} \bmod 2773 = 680\\
y_1 &= 14^{17} \bmod 2773 = 2049\\
y_1 &= 100^{17} \bmod 2773 = 1952\\
y_1 &= 418^{17} \bmod 2773 = 1983\\
y_1 &= 122^{17} \bmod 2773 = 1384\\
y_1 &= 900^{17} \bmod 2773 = 1510
\end{aligned}$$

Dobijeni šifrat

$$\begin{aligned}
y &= (yx_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)\\
&= (1204, 0883, 0680, 2049, 1952, 1983, 1384, 1510)\\
&= 120408830680204919521983138415 10
\end{aligned}$$

šalje Bobu. Bob pomoću $d = 157$, koji je samo njemu poznat, računa, na isti način dijeleći y na blokove,

$$x_i = y_i^{157} \bmod 2773, \quad i = 1, 2, \ldots, 8$$

i dobija originalnu poruku *OSIJEK NA DRAVI.*

■

4. Napadi na RSA

Kao što smo vidjeli, implementacija RSA je vrlo jednostavna. Analogno tome, i napad na RSA se može jednostavno provesti ako je poznat eksponent d. Očigledno je da je jedan od napada na RSA faktorizacija od $n = pq$, jer ako napadač faktorizira n, on može jednostavno otkriti i $\varphi(n) = (p-1)(q-1)$, te odrediti tajni eksponent d iz $de \equiv 1 \pmod{\varphi(n)}$ pomoću Euklidovog algoritma. Postavlja se pitanje, u čemu je onda sigurnost RSA.

Kako mi u RSA uzimamo p i q takve da svaki ima oko 100 znamenki, to naš $n = pq$ ima oko 200 znamenki, pa bi za njegovu faktorizaciju, primitivnom metodom dijeljenja sa svim prostim brojevima manjim od $\sqrt{n}$, uz pomoć računara koji može u sekundi izvršiti 10^9 takvih dijeljenja, trebalo otprilike 10^{81} godina. Iako postoje mnogo brži algoritmi za faktorizaciju ipak su brojevi od preko 200 znamenki sigurni od takvih napada. Trenutno najbrži algoritmi za faktorizaciju trebaju $O\left(e^{c(\log n)^{1/3}(\log\log n)^{2/3}}\right)$ operacija, što znači da nije poznat niti jedan polinomijalni algoritam za faktorizaciju.

Treba još napomenuti da postoje i slučajevi kada je n lakše faktorizirati nego inače. To je kada su p i q jako blizu jedan drugoga, ili ako $p-1$ i $q-1$ imaju samo male proste faktore. Takve slučajeve treba izbjegavati pri izboru parametara za RSA kriptosustav.

Kao što smo rekli, podaci n i e su javni, pa uz tajnost p, q i d, RSA je dosta siguran. Pogledajmo sada, šta se dešava ako napadač uspije saznati još neki podatak.

Lema 1. *Poznavanje tajnog eksponenta d, koji odgovara javnima n i e, može omogućiti faktorizaciju od n.*

DOKAZ: Pretpostavimo da znamo broj d takav da je $x^{de} \equiv x \pmod{n}$ za sve x relativno proste s n, tj. za koje je $M(x,n) = 1$.
Neka je $m = ed - 1$. Sada je $x^m \equiv 1 \pmod{n}$ za sve x takve da je $M(x,n) = 1$.

Pošto je grupa svih reduciranih ostataka modulo p ciklička, $x^m \equiv 1 \pmod{n}$ je ekvivalentno činjenici da je m neki zajednički višekratnik od $p-1$ i $q-1$. Iz toga slijedi da je poznavanje broja $m = ed - 1$ slabije od poznavanja broja $\varphi(n) = (p-1)(q-1)$. Međutim, vidjet ćemo sada kako poznavajući $m = ed - 1$ možemo s velikom vjerojatnošću faktorizirati n. To je jedan vjerojatnosni algoritam iz klase Las Vegas algoritama, koji imaju osobinu da nikad ne vraćaju netočan odgovor, ali ponekad ne pronađu rješenje. U slučaju da algoritam ne pronađe rješenje, potrebno mu je omogućiti drugu nezavisnu šansu nalaženja rješenja. Na taj način se sveukupna vjerojatnost uspjeha povećava s količinom raspoloživog vremena.

Uzmimo da mi znamo n, koji je produkt dva prosta broja p i q, i neka je m takav da je $x^m \equiv 1 \pmod{n}$, za sve x koji su relativno prosti s n. Uzimajući $x = -1$, vidimo da je m paran. Sada, provjerimo je li $m/2$ ima isto svojstvo kao i m. Ako ima, onda m zamijenimo s $m/2$. U slučaju da postoji x za koji vrijedi $x^{m/2} \not\equiv 1 \pmod{n}$, tada u $\mathbf{Z}_n$ postoji bar 50% takvih brojeva, jer svakom broju w koji zadovoljava kongruenciju $w^{m/2} \equiv 1 \pmod{n}$ odgovara broj xw koji tu kongruenciju ne zadovoljava. Sada, ako testiramo nekoliko desetina x–ova i ako oni zadovoljavaju kongruenciju $x^{m/2} \equiv 1 \pmod{n}$, onda s velikom vjerojatnošću možemo reći da je kongruencija $x^{m/2} \equiv 1 \pmod{n}$ ispunjena za sve x za koje je $M(x,n) = 1$, pa možemo zamijeniti m sa $m/2$. Postupak dijeljenja sa 2 nastavljamo sve dok je to moguće. Na kraju imamo jednu od dvije mogućnosti:

1. $m/2$ je djelitelj točno jednog od brojeva $p-1$ i $q-1$. Neka je to $p-1$. U tom slučaju je $x^{m/2} \equiv 1 \pmod{p}$ za sve x, ali je $x^{m/2} \equiv -1 \pmod{q}$ u točno 50% slučajeva.

2. $m/2$ nije djelitelj ni od $p-1$ ni od $q-1$. Tada može biti $x^{m/2} \equiv \pm 1 \pmod{p}$ ili $x^{m/2} \equiv \pm 1 \pmod{q}$. Svaka od 4 moguće kombinacije nastupa u točno 25% slučajeva.

Znači da za proizvoljan x imamo vjerojatnost $1/2$ da je $x^{m/2} - 1$ djeljiv s točno jednim od brojeva p i q. Dakle, uzimajući slučajno nekoliko desetaka x–ova, možemo s velikom vjerojatnošću očekivati da ćemo pronaći x sa svojstvom da je $x^{m/2} - 1$ djeljiv s točno jednim od brojeva p i q. Neka je to p, tj. neka je x takav da je $x^{m/2} - 1$ djeljiv s p, ali ne i sa q. Tada je $M\left(n, x^{m/2} - 1\right) = p$ pa smo uspjeli faktorizirati n.

■

Ideja da se izabere jedan n za sve, a da se korisnicima tajno dodijele parovi e_K i d_K, nije dobra iz dva razloga. Jedan je taj što bi korisnik A, na osnovu svojih e_A i d_A, pomoću algoritma iz Leme 1, mogao faktorizirati n i odrediti p i q, pa bi zbog posjedovanja e_B i poznavanja faktorizacije od n, a samim tim i vrijednosti $\varphi(n)$, mogao otkriti i d_B za svakog drugog korisnika. Drugi razlog je taj, što bi napadač

otkrivanjem jednog d_K došao u poziciju tog korisnika, pa bi se mogao postaviti u ulogu korisnika A i otkriti sve tajne eksponente d_K.

Lema 2. *Neka je $n = pq$ produkt dva različita prosta broja. Ako znamo n i $\varphi(n)$, tada možemo brzo naći p i q.*

Dokaz: Kako je $\varphi(n) = (p-1)(q-1)$, imamo da je

$$\varphi(n) = pq - p - q + 1 = n - p - q + 1 = n - (p+q) + 1.$$

Sada je

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

pa nam je pored produkta pq poznata i suma $p+q$. Definiramo polinom

$$f(X) = (X-p)(X-q) = X^2 - (p+q)X + pq$$

$$f(X) = X^2 - (n - \varphi(n) + 1)X + n$$

Sada p i q računamo pomoću formule za rješavanje kvadratne jednadžbe:

$$p, q = \frac{(n - \varphi(n) + 1) \pm \sqrt{(n - \varphi(n) + 1)^2 - 4n}}{2}$$

■

Primjer 2. *Neka je $n = 25397$ i $\varphi(n) = 25056$. Odredimo p i q tako da je $n = pq$.*

Imamo da je $n - \varphi(n) + 1 = 25397 - 25056 + 1 = 342$, pa je

$$f(X) = X^2 - 342X + 25397$$

$$p, q = \frac{342 \pm \sqrt{342^2 - 4 \cdot 25397}}{2} = \frac{342 \pm 124}{2} \Longrightarrow p = 223, q = 109$$

■

Za sigurnost RSA kriptosustava treba izbjegavati mali tajni eksponent d. Wiener je 1990. godine opisao polinomijalan algoritam za razbijanje standardnog RSA kriptosustava ukoliko je izabran mali tajni eksponent d. Taj algoritam, poznat kao Wienerov napad na RSA, je opisan slijedećim teoremom.

Teorem 2. *Neka je $n = pq$ i $p < q < 2p$, te neka je $d < \frac{1}{3}n^{0,25}$. Tada postoji polinomijalni algoritam, koji iz poznavanja n i e, izračunava d.*

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

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

Dakle, $\frac{k}{d}$ je dobra aproksimacija od $\frac{e}{\varphi(n)}$. Međutim, mi ne znamo $\varphi(n)$, pa ćemo $\varphi(n)$ zamijeniti sa n. Kako je

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

to slijedi da je $|n-\varphi(n)|<3\sqrt{n}$, pa nakon zamjene imamo:

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

Sada je $k\varphi(n)=ed-1<ed$, pa iz $e<\varphi(n)$ slijedi da je $k<d<\frac{1}{3}n^{0,25}$, pa dobijamo

$$\left|\frac{e}{n}-\frac{k}{d}\right|\leq\frac{1}{dn^{0,25}}<\frac{1}{2d^2}. \tag{1}$$

Prema Legendreovom teoremu iz teorije diofantskih aproksimacija, slijedi da relacija (1) povlači da je $\frac{k}{d}$ neka konvergenta razvoja u verižni razlomak od $\frac{e}{n}$.

Napomenimo da razvoj u verižni razlomak racionalnog broja $\frac{b}{c}$ izgleda ovako:

$$\frac{b}{c}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots_{a_{n-1}+\frac{1}{a_n}}}}}=[a_0;a_1,a_2,\ldots,a_n],$$

gdje su $a_0,\ldots,a_n$ kvocijenti iz Euklidovog algoritma primijenjenog na b i c. Razlomke $\frac{p_k}{q_k}=[a_0;a_1,a_2,\ldots,a_k]$, za $k\leq n$, nazivamo konvergente verižnog razvoja.

Vrijedi:

$$p_0=a_0,\qquad q_0=1,\qquad p_1=a_0a_1+1,\qquad q_1=a_1$$

$$p_k=a_kp_{k-1}+p_{k-2},\qquad q_k=a_kq_{k-1}+q_{k-2}.$$

Odavde odmah slijedi da je $q_k\geq F_k$, gdje je F_k k–ti Fibonaccijev broj. To znači da nazivnici konvergenti rastu eksponencijalno.

U našem slučaju to povlači da ima $O(\log n)$ konvergenti od $\frac{e}{n}$. Jedna od njih je $\frac{k}{d}$. To daje polinomijalni algoritam za otkrivanje tajnog ključa d.

■

Wiener je predložio slijedeću metodu za testiranje konvergenti. Neka je $\frac{a}{b}$ konvergenta od $\frac{e}{n}$. Ako je to korektna konvergenta, tada $\varphi(n)$ možemo izračunati iz

$$\varphi(n)=(p-1)(q-1)=\frac{be-1}{a}.$$

Sada računamo:

$$\begin{aligned}\frac{p+q}{2}&=\frac{pq-(p-1)(q-1)+1}{2}=\frac{an-be+1+a}{2a}\\ \left(\frac{q-p}{2}\right)^2&=\left(\frac{p+q}{2}\right)^2-pq=\left(\frac{p+q}{2}\right)^2-n\end{aligned}$$

Ako su $\frac{p+q}{2}$ i $\frac{q-p}{2}$, određeni pomoću navedenih relacija, prirodni brojevi, tada je $\frac{a}{b}$ odgovarajuća konvergenta od $\frac{e}{n}$. Sada je iz toga jednostavno odrediti p i q.

Primjer 3. *Neka je* $n = 14462477761$ *i* $e = 13456168555$. *Uz pretpostavku da je* $d < \frac{1}{3}n^{0,25} \approx 115.5$, *faktorizirajmo* n.

Rješenje: Razvoj u verižni razlomak od $\frac{e}{n}$ je:

$$\frac{e}{n} = [0; 1, 13, 2, 1, 2, 4, 1, 1, 19, 2, 3, 1, 1, 5041, 1, 7],$$

a konvergente su:

$$0, 1, \frac{13}{14}, \frac{27}{29}, \frac{40}{43}, \frac{107}{115}, \frac{468}{503}, \frac{575}{618}, \ldots$$

Ispitujući konvergente redom, dobijamo da je za $\frac{a}{b} = \frac{107}{115}$

$$\begin{aligned} \frac{p+q}{2} &= \frac{107 \cdot 14462477761 - 115 \cdot 13456168555 + 1 + 107}{2 \cdot 107} = 120265 \\ \left(\frac{q-p}{2}\right)^2 &= 120265^2 - 14462477761 = 1092^2 \end{aligned}$$

Sada je

$$\begin{aligned} p + q &= 240530 \\ q - p &= 2184 \end{aligned}$$

pa dobijamo da je

$$\begin{aligned} p &= 119173 \\ q &= 121357 \end{aligned}$$

tako da smo faktorizirali $n = 119173 \cdot 121357$ i dobili tajni eksponent kao nazivnik pete konvergente $d = 115$.

■

Kako postoje napadi na RSA s malim e, to i takav izbor parametara $\left(e < 10^5\right)$ treba izbjegavati.

Na kraju još napomenimo, da unatoč intenzivnom proučavanju, još uvijek nije pronađena metoda kojom bi se u potpunosti razbio RSA kriptosustav. Sve se svodi na to da se samo otkrije pojedina slabost i time da upozorenje kako treba birati parametre za implementaciju RSA. Sve to nam omogućuje da RSA, za sada, smatramo sigurnim kriptosustavom.

Literatura

[1] D. Boneh, *Twenty Years of Attacs on the RSA Cryptosystem*, Notices of the AMS, Vol. 46 (2), 203–213, 1999.

[2] J. A. Buchmann, *Introduction to Cryptography*, Springer–Verlag, New York, 2001.

[3] W. DIFFIE, M. E. HELLMAN, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT–22: 644–654, 1976.

[4] A. DUJELLA, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ., 29, 101–112, 2004.

[5] A. DUJELLA, *Kriptografija*, PMF–Matematički odjel, Sveučilište u Zagrebu `http://www.math.hr/∼duje/kript.html`

[6] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Springer–Verlag, New York, 1994.

[7] A. J. MENEZES, P. C. OORSHOT, S. A. VANSTONE, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.

[8] N. SMART, *Cryptography. An Introduction*, McGraw–Hill, New York, 2002.

[9] D. R. STINSON, *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 1996.

[10] W. TRAPPE, L. C. WASHINGTON, *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Sadle River, 2002.

[11] S. Y. YAN, *Number Theory for Computing*, Springer–Verlag, Berlin, 2002.