Opis in implementacija RSA

Generiranje ključev: najprej izberemo

- praštevili $\boldsymbol{p}$, $\boldsymbol{q}$ ter izračunamo *modul* $\boldsymbol{n} := pq$, in
- *šifrirni eksponent* $\boldsymbol{e}$, tako da je $D(e, \varphi(n))=1$,

nato pa izračunamo *odšifrirni eksponent* $\boldsymbol{d}$ iz kongruence

$$ed \equiv 1 \pmod{\varphi(n)}$$

z razširjenim Evklidovim algoritmom
(ali pa potenciranjem).

Javni ključ je $(\boldsymbol{e}, \boldsymbol{n})$, **zasebni ključ** pa $(\boldsymbol{d}, \boldsymbol{p}, \boldsymbol{q})$.

Šifriranje: $E(e,n)(x) = x^e \pmod{n}$.

Odšifriranje: $D(d,p,q)(y) = y^d \pmod{n}$.

Šifriranje in odšifriranje sta inverzni operaciji.
Za $x \in \mathbb{Z}_n^*$ to sledi iz Eulerjeve kongruence:

$$(x^e)^d \equiv x^{r\varphi(n)+1} \equiv (x^{\varphi(n)})^r x \equiv x \pmod{n},$$

za $x \in \mathbb{Z}_n \backslash \mathbb{Z}_n^*$ pa se prepričajte sami za DN.

Generiranje podpisa:
za podpis sporočila $m \in \{0,1\}^*$, Anita:

1. izračuna $M = H(m)$,
   kjer je H zgoščevalna funkcija (npr. SHA-1),
2. izračuna $s = M^d \bmod n$,
3. Anitin podpis za m je s.

Preverjanje podpisa:
Bojan preveri Anitin podpis s za m, tako da:

1. vzame overjeno kopijo Anitinega
   javnega ključa (n, e),
2. izračuna $M = H(m)$,
3. izračuna $M' = s^e \bmod n$,
4. sprejme (m, s) če in samo če je $M = M'$.

Potenciranje z redukcijo pri RSA je enosmerna funkcija z bližnjico.

Bližnjica: poznavanje števila d oziroma $\varphi(n)$ oziroma števil p in q.

RSA v praksi

- Modul $n = pq$ mora biti dovolj velik, da je njegova faktorizacija računsko prezahtevna.
- Implementacije RSA z dolžino ključev 512 bitov ne jamčijo več dolgoročne varnosti.

Časovna zahtevnost računskih operacij

Naj ima število n v binarni representaciji k bitov, tj.

$$k = \lfloor \log_2 n \rfloor + 1.$$

Potem je časovna zahtevnost

seštevanja $O(k)$,
Evklidovega algoritma $O(k^2)$,
modularne redukcije $O(k^2)$,
potenciranja pa $O(k^3)$.

Potenciranje opravimo učinkovito z metodo "**kvadriraj in množi**".

Izbira šifrirnega eksponenta

$$e = 5, 17, 2^{16} + 1$$

Pospešitev odšifriranja z uporabo kitajskega izreka o ostankih (CTR) za faktor 4:

namesto da računamo $y^d \bmod n$ direktno, najprej izračunamo

$C_p := y^{d \bmod (p-1)} \bmod p$ in $C_q := y^{d \bmod (q-1)} \bmod q$,

nato pa po CRT še

$$C := t_p C_p + t_q C_q \bmod n,$$

kjer $p \mid t_p - 1, t_q$ in $q \mid t_p, t_q - 1$.

Algoritem RSA je cca. 1500-krat počasnejši od DES-a. Uporablja se za prenos ključev simetričnega algoritma.

(Za 512-bitno število n lahko dosežemo z RSA-jem hitrost 600 Kb na sekundo, medtem ko DES zmore 1 Gb na sekundo.)

Nekaj lažjih nalog

1. Koliko množenj potrebujemo, da izračunamo m^d?
2. Prepričaj se, ali je dovolj, da pri RSA uporabimo le Fermatovo kongruenco.

3. Pokaži, da $p \mid \binom{p}{i}$, za $1 < i < p$.
4. Naj bo p praštevilo, potem za poljubni števili a in b velja
$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$
5. Naj bo p praštevilo, potem za poljubno število m velja $m^p \equiv m \pmod{p}$.

Gostota praštevil

Izrek o gostoti praštevil

[de la Vallée Poussin, Hadamard, 1896]

Funkcija $\pi(x)$ *je asimptotično enaka* $\dfrac{x}{\log x}$,

ko gre $x \to \infty$.

(angl. **Prime Number Theorem** oziroma PNT)

Domnevo za PNT je prvi postavil leta 1791 (še kot najstnik) **Frederic Gauss (1777-1855)**, za testiranje pa je kasneje uporabljal tudi tablice **Jurija Vege** iz leta 1796:

$$\pi(x) \approx \int_2^x \frac{1}{\log n} dn \ .$$

Legendre pa jo je objavil v svoji knjigi iz leta 1808:

$$\pi(x) \approx \frac{x}{\log x - 1.08366} \ .$$

Namesto da bi šteli praštevila, ki so manjša ali enaka številu n, raje poglejmo, kakšna je njihova *gostota*:

$$\pi(n)/n.$$

Primerjamo

$$\pi(10^{10})/10^{10} = .04550525$$

z

$$1/\ln(10^{10}) = .04342945.$$

To je bil **problem 19. stoletja.**

Peter Gustav Lejeune-Dirichlet (1805-1859) (začetki analitične teorije števil): za vsaki tuji si celi števili a in b aritmetično zaporedje

$$a, \quad a+b, \quad a+2b, \quad a+3b, \quad \ldots, a+nb, \quad \ldots$$

vsebuje neskončno praštevil.

Pafnuti Lvovich Chebyshev **(1821-1884)** je leta 1850 pokazal, da, če limita obstaja, potem leži na intervalu

$$[0.92129, 1.10555].$$

Leta 1859 je **Georg Friedrich Bernhard Riemann** **(1826-1866)** naredil briljanten napredek na področju analitične teorije števil s študijem Riemannove **zeta funkcije**.

Leta 1896 sta končno dokazala domnevo

Charles-Jean-Gustave-Nicholas de la Vallée-Poussin (1866-1962)

in

Jacques Hadamard (1865-1963).

V Prilogi A si lahko ogledate dokaz izreka, ki sledi D. Zagieru, ki je uporabil analitični izrek namesto Tauberjevih izrekov. (Newman's Short Proof of the Prime Number Theorem, *American Mathematical Monthly*, October 1997, strani 705-709).

Še nekaj zanimivih referenc:

J. Korevaar, On Newman's quick way to the prime number theorem, *Mathematical Intelligencer* 4, **3** 1982, 108-115.

P. Bateman and H. Diamond, A hundred years of prime numbers, *American Mathematical Monthly* **103** 1996, 729-741.

Elementarni dokaz izreka o gostoti praštevil

Prvi dokaz so poenostavili **Landau** in drugi v začetku 20. stoletja. Vsi so uporabljali zapletene metode realne in kompleksne analize.

Leta 1949 sta **Atle Selberg** in **Paul Erdös** odkrila neodvisno elementaren dokaz (brez kompleksne analize).

Leta 1956 je **Basil Gordon** dokazal izrek o gostoti praštevil s pomočjo Stirlingove formule za $n!$.

The Times London, sept. 25, 1996:

Selberg and Erdös agreed to publish their work in back-to-back papers in the same journal, explaining the work each had done and sharing the credit. But at the last minute Selberg ... raced ahead with his proof and published first. The following year Selberg won the Fields Medal for this work. Erdös was not much concerned with the competitive aspect of mathematics and was philosophical about the episode.

`http://www-groups.dcs.st-and.ac.uk/`
`~history/Mathematicians/Erdos.html`

Posledica: *Če je p_n n-to praštevilo, velja*

$$\lim_{n\to\infty} \frac{n\log n}{p_n} = 1.$$

Dokaz: Logaritmirajmo limito iz izreka o gostoti praštevil

$$\lim_{x\to\infty} (\log\pi(x) + \log\log x - \log x) = 0$$

oziroma

$$\lim_{x\to\infty} \left\{ \log x \left(\frac{\log\pi(x)}{\log x} + \frac{\log\log x}{\log x} - 1 \right) \right\} = 0 \,.$$

Ker gre $\log x \longrightarrow \infty$, velja

$$\lim_{x\to\infty} \left\{ \frac{\log \pi(x)}{\log x} + \frac{\log\log x}{\log x} - 1 \right\} = 0$$

oziroma ker gre $\log\log x / \log x \longrightarrow 0$, tudi

$$\lim_{x\to\infty} \frac{\log \pi(x)}{\log x} = 1.$$

Pomnožimo še z limito iz izreka o gostoti praštevil in dobimo

$$\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1,$$

kar pa je že želena limita, če vzamemo $x = p_n$ oziroma $\pi(x) = n$. ■

RSA sistem in faktorizacija

- Probabilistično testiranje praštevilčnosti (ponovitev Monte Carlo algoritem, Solovay-Strassen algoritem in Miller-Rabinov test)
- Napadi na RSA (odšifrirni eksponent, Las Vegas algoritem)
- Rabinov kriptosistem
- Algoritmi za faktorizacijo (naivna metoda, metoda $p-1$, Dixonov algoritem in kvadratno rešeto)

Generiranje praštevil

Za inicializacijo RSA kriptosistema potrebujemo velika (npr. 80-mestna) naključna praštevila.

V praksi generiramo veliko naključno število in testiramo, ali je praštevilo z Monte Carlo algoritmom (npr. Solovay-Stassen ali Miller-Rabin).

Ti algoritmi so hitri, vendar pa so probabilistični in ne deterministični. Po izreku o gostoti praštevil je verjetnost, da je naključno 512-bitno liho število praštevilo, približno $2/\log p \approx 2/177$.

S praštevili, ki so "osnovni gradniki" matematike, so se ukvarjali učenjaki vse od antičnih časov dalje.

Odločitveni problem `praštevilo`

Za dano število n ugotovi ali je praštevilo.

Leta **240 pr. n. št.** se je grški matematik in filozof **Eratostenes**, bibliotekar aleksandrijske knjižnice, domislil prve neoporečne metode (*čas. zahtev.* $O(n)$). V primeru zelo dolgih števil bi za rešitev tega problema potrebovali več časa kot je staro vesolje.

Od tedaj so matematiki poskušali najti algoritem, ki bi dal odgovor v smiselnem času.

Karl Frederich Gauss (1777-1855) je v svoji knjigi Disquisitiones Arithmeticae (1801) zapisal:

> *“Menim, da čast znanosti narekuje,*
> *da z vsemi sredstvi iščemo rešitev tako*
> *elegantnega in tako razvpitega problema.”*

Od prihoda računalnikov dalje poudarek ni več na iskanju matematične formule, ki bi dajala praštevila, ampak na iskanju učinkovitega algoritma za razpoznavanje praštevil.

Večji korak naprej je v 17. stoletju napravil **Fermat**, z že omenjenim **Fermatovim malim izrekom**:

$$a^{p-1} \equiv 1 \pmod{p}$$

za vsak $a \in \mathbb{N}$ in vsako praštevilo p, ki ne deli a.

Po zaslugi kriptografije so postale raziskave problema `praštevilo` v zadnjih desetletjih še intenzivnejše:

1976	**Miller**: deterministični algoritem polinomske časovne zahtevnosti (temelji na Riemannovi hipotezi)
1977	**Solovay in Strassen**: verjetnostni algoritem časovne zahtevnosti $O(\log^3 n)$.
1980	**Rabin**: modifikacija Millerjevega testa v verjetnostni alg. (pravilnost dokazana)
1983	**Adleman, Pomerance in Rumely**: det. alg. čas. zathev. $O(\log n^{O(\log\log\log n)})$
1986	**Golwasser in Kilian**: polinomski verj. alg. za skoraj vse podatke z uporabo eliptičnih krivulj
2002	**Agrawal, Kayal in Saxena (AKS)**: det. alg. s časovno zahtevnostjo $O(\log^{12} n)$ v praksi $O(\log^6 n)$, tudi $O(\log^3 n)$ a brez dokaza.

Naj bo p liho praštevilo, $0 \leq x \leq p-1$.
Potem je x **kvadratni ostanek** po modulu p,
tj. $x \in \mathbf{QR}(p)$, če ima kongruenca

$$y^2 \equiv x \pmod{p}$$

rešitev $y \in \mathbb{Z}_p$.

Eulerjev kriterij
Naj bo p liho praštevilo. Potem je

$$x \in \mathrm{QR}(p) \iff x^{(p-1)/2} \equiv 1 \pmod{p}.$$

Torej obstaja polinomski algoritem za odločitveni problem **kvadratnega ostanka**.

Naj bo p liho praštevilo in a nenegativno celo število. Potem je **Legendrov simbol** definiran z

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{če } p \mid a, \\ 1, & \text{če je } a \in \mathrm{QR}(p), \\ -1, & \text{sicer.} \end{cases}$$

Po Eulerjevem kriteriju velja

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

Legendrov simbol posplošimo v Jacobijev simbol. Število n naj bo celo liho število z naslednjo praštevilsko faktorizacijo $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

Za nenegativno celo število a definiramo **Jacobijev simbol** z

$$\left(\frac{a}{n}\right) \quad := \quad \Pi_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Eulerjevo psevdopraštevilo: $91 = 7 \cdot 13$, vseeno pa obstaja tak $a = 10$, da je

$$\left(\frac{10}{91}\right) = -1 = 10^{45} \mod 91.$$

DN: Pokaži, da je za poljubno sestavljeno število n, m Eulerjevo psevdopraštevilo glede na bazo a za največ polovico naravnih števil, ki so manjša od n (glej nalogo 4.14).