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 $y^d \mod n$ direktno, najprej izračunamo

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

nato pa po CRT še

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

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

Algoritem RSA je cca. 150-krat počasnejši od
Uporablja se za prenos ključev simetričnega alg

(Za 512-bitno število n lahko dosežemo z R
bitrost 600 Kb na sekundo, medtem ko DES
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 $\frac{x}{\log x}$, ko gre $x \to \infty$.

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

Domnevo za PNT je prvi postavil leta 1
kot najstnik) **Frederic Gauss (177-185**
testiranje pa je kasneje uporabljal tudi tablice
Vege iz leta 1796:

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

Legendre pa jo je objavil v svoji knjigi iz let

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

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

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

vsebuje neskončno praštevil.

Pafnuti Lvovich Tchebysheff (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, D. Zagieru, ki je uporabil analitični izrek Tauberjevih izrekov. (Newman's Short Proo Prime Number Theorem, *American Mathe 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 Erdős** 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.dcst-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 praštevil

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

oziroma

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

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

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

oziroma ker gre $\log\log x / \log x \to 0$, 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)