• RSA encryption algorithm

Rivest-Shamir-Adleman encryption

public-key cryptography

allow one party to receive secret message from others

Alice : receiver

Bob, Charlie, ... : sender

Eve : third party

How it works

- Alice chooses (big) prime numbers p, q

  advertise $N = pq$ as the public key

  (and another e that is coprime to $\mathrm{lcm}(p-1, q-1)$)

- Bob wants to send a message to Alice,

  represented by an integer x ($\ll N$) copr. to p, q.

  he computes $y = x^3 \pmod N$ (or $y = x^e \bmod N$)

  sends y to Alice.

- Alice solves x from y : by finding d

  s.t. $3d = 1 \mod \mathrm{lcm}(p-1, q-1)$

  (or $ed = 1 \mod \mathrm{lcm}(p-1, q-1)$.)
  (can be $(p-1)(q-1)$.)

  then $x = y^d \bmod N$.

Point : only Alice knows p and q.

- d is easy to compute (polynom time in $\log N$) from p, q

- finding p and q from N is difficult.

  $\sim 2^{(1+o(1))\sqrt{\log N \log\log N}}$ time to compute.

  in known classical algorithms.

Eve can see N, y, but needs $O(N)$ time to know x

Why Alice can quickly compute $\mathrm{lcm}(p-1, q-1)$ and d : Euclidean algorithm.
(extended)

Problem : given a and b, compute x and y solving $ax + by = \gcd(a,b)$.

then $\begin{cases} \mathrm{lcm}(a,b) = ab / \gcd(a,b) \\ \text{if } a \text{ is copr. to } b, \quad ax = 1 \mod b \end{cases}$

Algorithm : recursively compute r_i, s_i, t_i

$r_0 = a, \; s_0 = 1, \; t_0 = 0$

$r_1 = b, \; s_1 = 0, \; t_1 = 1$.

$(i+1)$-th step :

find q_i s.t. $r_{i+1} = r_{i-1} - q_i r_i$ is between 0 and $r_i - 1$.

if $r_{i+1} = 0$, output $x = s_i$, $y = t_i$

otherwise $s_{i+1} = s_i - q_i s_i$, $t_{i+1} = t_{i-1} - q_i t_i$

go to next step.

Running time $\sim O(\log(\max(a,b))^2)$

Why Alice can get x from y and d.

"$x = y^d \mod N$" is a computation in the system $\mathbb{Z}/N\mathbb{Z} = \{ [k] : k \text{ int. } [k]=[k'] \Leftrightarrow N \text{ div. } k-k' \}$

integers modulo N.

this is a ring : sum and product make sense

$[k]+[k'] = [k+k']$ $\quad [k][k'] = [kk']$

$[1]$: multiplicative unit $\quad [1][k] = [k]$

$[0]$: $[0][k] = [0]$, $[0] + [k] = [k]$

its multiplicative group is $(\mathbb{Z}/N\mathbb{Z})^\times = \{ [k] : k \text{ copr. to } N \}$

$[k] \in (\mathbb{Z}/N\mathbb{Z})^\times \Leftrightarrow \exists\, l$ s.t. $kl = 1 \mod N$.

$(\mathbb{Z}/N\mathbb{Z})^\times$ is a finite group, with unit elem $[1]$.

in general : G finite group, $g \in G$

$\Rightarrow g^{|G|} = e$ unit element.

$\exists$ elems $g'_0, \cdots, g'_{m-1}$ s.t.

$$G = \coprod_{0 \le i < k} \{ g^i g'_0, \cdots g^i g'_{m-1} \}$$

k : first int. s.t. $g^k = e$.

for $G = (\mathbb{Z}/N\mathbb{Z})^\times$; $|G| = \varphi(N)$ Euler's totient function

when $N = pq$ p, q prime.

$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ direct prod. of rings.

$[k]_N \to ([k]_p, [k]_q)$

$\Rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \cong \underbrace{(\mathbb{Z}/p\mathbb{Z})^\times}_{\text{order } p-1} \times \underbrace{(\mathbb{Z}/q\mathbb{Z})^\times}_{\text{order } q-1}$.

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

Suppose $ed = 1 \mod (p-1)(q-1)$

i.e. $ed = 1 + k(p-1)(q-1)$

then $([x]^e)^d = [x]^{ed} = [x]^{1+k(p-1)(q-1)}$

$= [x] \cdot \underbrace{[x]^{\varphi(N) \cdot k}}_{= [1]} = [x]$ in $(\mathbb{Z}/N\mathbb{Z})^\times$

i.e. $y^d = x \mod N$.

- Replacing $(p-1)(q-1)$ by $\operatorname{lcm}(p-1, q-1)$

$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$

$p - 1 = p_1^{e_1} \cdots p_k^{e_k}$

allowing $e_i = 0$, write $q - 1 = p_1^{e'_1} \cdots p_k^{e'_k}$

then $(\mathbb{Z}/N\mathbb{Z})^\times \cong \prod \mathbb{Z}/p_i^{e_i}\mathbb{Z} \times \mathbb{Z}/p_i^{e'_i}\mathbb{Z}$

any elem has ord. dividing $\prod p_i^{\max(e_i, e'_i)} = \operatorname{lcm}(p-1, q-1)$

- Reduction to period problem.

Fix x coprime to N. Look at the function

$$f(r) = x^r \mod N$$

Obs. $f(r)$ is periodic: $\exists\, s$ s.t.

$$f(x) = f(y) \iff s \mid x - y.$$

s = order of $[x]$ in $(\mathbb{Z}/N\mathbb{Z})^\times$

$$[f(k + \ell s)] = [x]^{k+\ell s} = [x]^k ([x]^s)^\ell$$

if s is even: $0 = x^s - 1 = (x^{s/2} - 1)(x^{s/2} + 1) \mod N$

if moreover $N \nmid x^{s/2} + 1$, we get a factor of N (p or q) by $\gcd(x^{s/2} - 1, N)$.