RSA ŠIFROVÁNÍ → ŠIFROVÁNÍ S VEŘEJNÝM KLÍČEM (~~RE~~)

např. Banka — chci dostávat zašifrované zprávy

→ zvolím 2 prvočísla $p \neq q$

$N = p \cdot q$

spočtu $\varphi(N) = (p-1)(q-1)$

zvolím k nesoudělné s $\varphi(N)$

dopočtu $s = k^{-1} \pmod{\varphi(N)}$

Veřejný klíč (N, k) ⟵ skládá se z N, k

šifrování - zprávy $a < N$ (větší zprávy se rozsekají po k cifrách, kde $10^k < N$)

- pošle se $b = a^k \pmod{N}$

Soukromý klíč (N, s)

dešifrování - $c = b^s \pmod{N}$

platí $c = a$

(DK) $c = (b^s) = (a^k)^s = a^{k \cdot s}$

$k \cdot s = 1 \pmod{\varphi(N)}$

$= 1 + k \cdot \varphi(N) \pmod{N}$

$a^{k \cdot s} = a^{1 + k \cdot \varphi(N)} = a^1 \pmod{N}$

pro a soudělné s N použij Č.V. o zb., kde N = square-free

pro a nesoud s N ~~jinak~~ tak použij E.F.V

Bezpečnost RSA

- pro soukromý klíč je potřeba $\varphi(N)$
- znalost $\varphi(N)$ je ekvivalentní prvočíselnému rozkladu N

⇒

= dělit všemi prvočísly do $\sqrt{N}$

→ exponenciálně ~~(roste s počtem)~~ složité v závislosti na počtu cifer

POZN.

Šifrování používá opakované dvojce $(k < \varphi(N))$

Dešifrování - kdo dešifruje, zná p a q, tzn. může počítat reziduálně v $\mathbb{Z}_p$, $\mathbb{Z}_q$ a lze použít E.-F.V. $(k > \varphi(p))$ $\varphi(q)$

+ opak. dvojce
+ Č.V. o zb.

PŘ

RSA s veřejným klíčem $(N = 221, k = 7)$

Zachycená zpráva $b = 45$.

Proveďte útok hrubou silou a dešifrujte.

---

① ~~Útěm~~ Hrubou silou rozložit N na $N = p \cdot q$

→ dělit prvočísly $< \sqrt{N} \doteq 25$

$N = 13 \cdot 17$

② Výpočet soukromého klíče

$\varphi(N) = 12 \cdot 16 = 192$

$s = k^{-1} \pmod{\varphi(N)}$

$s = 7^{-1} \pmod{192}$ ~~vypočti~~

použijí rozšířený Eukl. alg. a ~~dio~~ řeším diofant. rovnici

$7s = 1 \pmod{192}$

$7s + 192y = 1 \pmod{Z}$

$192 = 27 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

$1 = 7 - 2(192 - 27 \cdot 7)$

$= -2 \cdot 192 + 55 \cdot 7$

s

$s = 55$

③ Dešifrování

$a = b^s \pmod{Z_N}$

$a = 45^{55} \pmod{Z_{221}}$

→ rozk. čísla pro exp. 55

→ $N = \underbrace{13 \cdot 17}_{\text{nesoudělná}}$

lze počítat reziduální č. V.

$\pmod{Z_{13}}$ $a = 45^{55\,55} = 6^{55} = 6^{4}$

$GCD(6, 13) = 1$ → lze E.-F. V.

→ $\pmod{\text{exp. mod } \varphi(13) = 12}$

opakované čtverce

opak. čísla $(7)_2 = 1\ 1\ 1$
$\times 3 \times 3 \times$

Z_{13} x 6
3 36 = (-3)
x -3 . 6 = -18 = -5
3 25 = -1
x -1 . 6 = -6 = 7

$r \in Z_{17}$ $a = 45^{-55} = 11^{55} = 11^7 =$ nyjde $= 3$
$\varphi(17) = 16$ čísla

↳ Č. V. o zb:

$r \in Z_{221}$ $a = 7 \cdot q_{13} + 3 q_{17}$
$q_{13} = 17 \cdot l$
$alg = 1 r \in Z_{13}$
$q_{17} = 13 \cdot x$
$alg = 1 r \in Z_{17}$

$17l + 13x = 1$
pro 2 čísla je možno sestavit jen jednu Diofant. rovnici
↓
1x Euklid

$17 = 13 + 4$
$13 = 3 \cdot 4 + 1$ l x
$1 = 13 - 3(17 - 13) = \underbrace{(-3) \cdot 17}_{q_{13}} + \underbrace{4 \cdot 13}_{q_{17}}$

$q_{13} = (-3) \cdot 17 = -51$
$q_{17} = 4 \cdot 13 = 52$

dosadím

v Z_{221} $a = 7 \cdot (-51) + 3 \cdot 52 = -201 = \underline{\underline{20}}$

Hledaná zpráva je 20.

RSA

útok opakováním - při sdíleném N a více veřejných klíčů a při zachycení stejné zprávy zašifrované dvěma (nejlépe nesoudělnými) klíči

mám 2 veřejné klíče (N, k_1) a (N, k_2) → N jsou stejná

Zachytím zprávy $b_1 = a^{k_1}$

$b_2 = a^{k_2}$

Chci najít $\underline{\underline{a}}$.

Bezout: $d = GCD(k_1, k_2) = k \cdot k_1 + l \cdot k_2$,

kde $k, l \in \mathbb{Z}$

použiji Eukleid. rozšířený algor.

Pak $a^d = a^{k k_1 + l k_2} = b_1^k \cdot b_2^l$

Pokud jsou klíče k_1 a k_2 nesoudělné, pak

$d = 1 \rightarrow a^d = a$

(PŘ) Zpráva $\underline{a}$ byla kašifrována

$(N = 1037,\ k_1 = 5) \rightarrow b_1 = a^{k_1} = 1016$

$(N = 1037,\ k_2 = 7) \rightarrow b_2 = a^{k_2} = 395$

Najít $\underline{a}$ pěkem eukleidova.

$GCD(5,7) = 1 \rightarrow$ ~~$k \cdot 5 + l \cdot 7$~~ $k \cdot 5 + l \cdot 7 = 1$

Eukleidem spočtu nebo uhodnu $3 \cdot 5 + (-2) \cdot 7 = 1$

$3 \cdot 5 - 2 \cdot 7 = 1$

$a^1 = (a^5)^k \cdot (a^7)^l = 1016^3 \cdot 395^{-2} = 1016^3 \cdot (395^{-1})^2$

$395^{-2} = (395^{-1})^2$

musím najít inverzi 395^{-1} v $\mathbb{Z}_{1037}$

$395x + 1037y = 1 \quad v\ \mathbb{Z}$

Eukleid $1037 = \square \cdot 395 + \square$

$\vdots$

$= +\boxed{1} \rightarrow GCD$

vyjde $x = -21$

$a = 1016^3 \cdot (-21)^2 = 642$

Pozn. Pokud inverze NEexistuje $\rightarrow$ GCD ~~$(b_2, N) > 1$~~ $(b_2, N) > 1$

$\rightarrow$ čísla jsou soudělná

Eukleid alg. pro hledání $GCD(b_2, N) > 1$

poskytne prvočíselný rozklad ~~$N = p \cdot q$~~

$GCD = p$, kde $N = p \cdot q$

$\rightarrow$ znám prvočíselný rozklad N

$\rightarrow$ dopočtu soukromý klíč

$\rightarrow$ dešifruji