

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

např. banka — chci dostávat kryptované zprávy

→ zvolím 2 prvočísla $p \neq q$

$$N = p \cdot q$$

$$\text{spočtu } \varphi(N) = (p-1)(q-1)$$

zvolím k nesoudělné s $\varphi(N)$

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

Veřejný klíč $(N, k) \leftarrow$ skládá se z N, k

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

$$\text{- počte se } b = a^k \pmod{N}$$

Soukromý klíč (N, s)

$$\text{dešifrování - } c = b^s \pmod{N}$$

$$\text{platí } c = a$$

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

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

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

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

pro a soudel s N
použij Č.V. o st., kde
 $N = \text{square-free}$

pro a nesoudel s N
~~jinak~~ také použij E.F.V

Bezpečnost RSA

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

\Rightarrow

= dělit všemi prvočísly do \sqrt{N}
 \rightarrow exponenciálně ~~velké~~ složitosti v závislosti na počtu cifer

POZN.

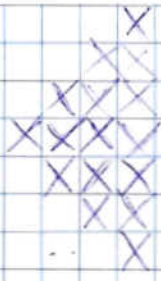
Šifrování používá opakovaní číselce
($k < \varphi(N)$)

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

+ opak. číselce

+ č.v. o.kb.

PR



RSA s veřejným klíčem ($N=221, k=4$)

Každý zná křivočku $b=45$.

Proveďte útok hrubou silou a dešifrujte.

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

→ dělit prvočísly $< \sqrt{N} \approx 15$

$$N = 13 \cdot 17$$

② Výpočet soukromého klíče

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

$$s = k^{-1} \text{ v } \mathbb{Z}_{\varphi(N)}$$

$$s = 4^{-1} \text{ v } \mathbb{Z}_{192} \quad \leftarrow \text{výpočet}$$

použijte rozšířený Eukl. alg. a ~~do~~ ~~ne~~ ~~u~~ ~~ž~~ ~~á~~ ~~d~~ ~~e~~ ~~ř~~ ~~í~~ ~~m~~ diofant. rovnici

$$4s = 1 \text{ v } \mathbb{Z}_{192}$$

$$7s + 192y = 1 \text{ v } \mathbb{Z}$$

$$192 = 24 \cdot 4 + 3$$

$$4 = 2 \cdot 3 + 1$$

$$1 = 4 - 2(192 - 24 \cdot 4) = -2 \cdot 192 + 55 \cdot 4$$

s

$$s = 55$$

③ Dešifrování

$$a = b^k \text{ v } \mathbb{Z}_N$$

$$a = 45^{55} \text{ v } \mathbb{Z}_{221}$$

opak. útok pro exp. 55

$$N = 13 \cdot 17$$

nesouditelná!

ke počítání reziduálně č.v.

$$\text{v } \mathbb{Z}_{13} \quad a = 45^{55} = 6^{55} = 6^4$$

$\text{GCD}(6, 13) = 1 \rightarrow$ ke E.-f.v.

\rightarrow v exp. mod $\varphi(13) = 12$

opakování útoků \leftarrow

opak. čísel $(4)_2 = \begin{matrix} 1 & 1 & 1 \\ \times & \times & \times \\ \times & \times & \times \\ \times & \times & \times \end{matrix}$

$$\mathbb{Z}_{13} \quad x \ 6$$

$$S \ 36 = (-3)$$

$$x \ -3 \cdot 6 = -18 = -5$$

$$S \ 25 = -1$$

$$x \ -1 \cdot 6 = -6 = 7$$

$$\pi \mathbb{Z}_{14} \quad a = 45^{55} = 11^{55} = 11^7 = \text{ryjole} = 3$$

\uparrow \uparrow
 $\varphi(17) = 16$ číslo

↳ č. v. o kb.

$$\pi \mathbb{Z}_{221} \quad a = 4 \cdot \varphi_{13} + 3 \varphi_{17}$$

$$\varphi_{13} = 14 \cdot k$$

$$\text{alg} = 1 \pi \mathbb{Z}_{13}$$

$$\varphi_{17} = 13 \cdot x$$

$$\text{alg} = 1 \pi \mathbb{Z}_{17}$$

$$14k + 13x = 1$$

pro 2 čísla je
možno sestavit
jen jednu

Diophant. rovnici

↓
1x Eukleid

$$14 = 13 + 1$$

$$13 = 3 \cdot 4 + 1$$

$$1 = 13 - 3(14 - 13) = \underbrace{(-3)}_{\varphi_{13}} \cdot 14 + \underbrace{4}_{\varphi_{17}} \cdot 13$$

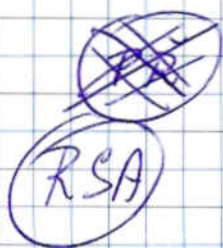
$$\varphi_{13} = (-3) \cdot 14 = -51$$

$$\varphi_{17} = 4 \cdot 13 = 52$$

dosadím

$$a \in \mathbb{Z}_{221} \quad a = 4 \cdot (-51) + 3 \cdot 52 = -204 = \underline{\underline{20}}$$

Poslaná zpráva je 20.



Útok outsidera - při sdílení N
a více veřejných klíčů a při zachycení
stejně zprávy zašifrované dvěma (nejlépe
nesouditelnými) klíči

mám 2 veřejné klíče (N, k_1) a (N, k_2)

N jsou stejná

Zachytilim zprávy $k_1 = a^{k_1}$
 $k_2 = a^{k_2}$

Chci najít a .

Bezout: $d = \text{GCD}(k_1, k_2) = k \cdot k_1 + l \cdot k_2$,
kde $k, l \in \mathbb{Z}$

použiji Eukleid. rozšířený algor.

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

Pokud jsou klíče k_1 a k_2 nesouditelné, pak

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

PR

zpráva a byla kóduována

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

$$(N = 1037, k_2 = 4) \rightarrow b_2 = a^{k_2} = 395$$

Mají a sítkem outsidera.

$$\text{GCD}(5, 4) = 1 \rightarrow \cancel{5 + 4} \quad k \cdot 5 + l \cdot 4 = 1$$

$$\text{Euklidem počtu nebo vhodnou} \quad 3 \cdot 5 + (-2) \cdot 4 = 1$$

$$3 \cdot 5 - 2 \cdot 4 = 1$$

$$a^1 = (a^5)^k \cdot (a^4)^l = 1016^3 \cdot 395^{-2} = 1016^3 \cdot (395^{-1})^2$$

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

musím najít inverzi $395^{-1} \pmod{1037}$

$$395x + 1037y = 1 \quad \pmod{1037}$$

$$\text{Euklid} \quad 1037 = \underline{\quad} \cdot 395 + \underline{\quad}$$

\vdots

$$= + \underline{1} \rightarrow \text{GCD}$$

$$\text{vyjde } x = -21$$

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

Pozn.

období inverze NEexistuje $\rightarrow \text{GCD}(b_2, N) > 1$

\rightarrow čísla jsou soudělná

Euklid alg. pro hledání $\text{GCD}(b_2, N) > 1$

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

$$\text{GCD} = p, \text{ kde } N = p \cdot q$$

\rightarrow znám prvočíselný rozklad N

\rightarrow dopočtu soukromý klíč

\rightarrow dešifruji