8. cvičení – Binomické kongruence, primitivní kořeny

PKC
public-key
cryptography

RSA *Ron Rivest, Adi Shamir, Leonard Adleman* (1977; C. Cocks, GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
  provázanou (tajný)
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod n$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod n$ $\quad n = p \cdot q$

DÚ 7/1 Buď p prvočíslo. Dk, že $\forall a \in \mathbb{Z}: 0 \le a \le p-1$ platí:

$$\binom{p-1}{a} \equiv (-1)^a \pmod p$$

Řeš:

$$\binom{p-1}{a} = \frac{(p-1)!}{a!(p-1-a)!} = \frac{(p-1)(p-2)\cdots(p-1-a+1)}{a!} = \frac{(p-1)\cdots(p-a)}{a!}$$

Chceme dokázat, že $\frac{(p-1)\cdots(p-a)}{a!} \overset{?}{\equiv} (-1)^a \pmod p \quad / \cdot a!$

$$(p-1)\cdots(p-a) \overset{?}{\equiv} (-1)^a \cdot a! \pmod p \qquad (a!, p) = 1$$

$$(-1)(-2)\cdots(-a) \overset{?}{\equiv} (-1)^a a! \pmod p$$

$$(-1)^a \cdot (1 \cdot 2 \cdots a) \equiv (-1)^a \cdot a! \pmod p$$

Úpravy byly ekvivalentní, platí tedy dokazované tvrzení.

RSA: $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow \forall m \in \mathbb{Z} \quad (m,n)=1$ [tj. $p \nmid m \wedge q \nmid m$]

$$(m^e)^d \equiv m^1 \pmod{n}$$

② Příklad na RSA (zjednodušený)

$p=17,\ q=19 \to n=323$ — nevypočítáme bez rozkladu n na prvočísla

$\varphi(n) = 16\cdot 18 = 288$

$e=5$

Dopočítáme d tak, aby $d\cdot e \equiv 1 \pmod{\varphi(n)}$

$5d \equiv 1 \pmod{288}$ — POZOR: není to ekvivalentní soustavě $5d \equiv 1\ (16)$, $5d \equiv 1\ (18)$

$5d \equiv 1+3\cdot 288 \pmod{288}$

$5d \equiv 865\ (288) \quad |:5$

$\underline{\underline{d \equiv 173\ (288)}}$

Pošleme Alici zašifrovanou zprávu $M=13$

$C \equiv 13^5 \pmod{323}$

$C \equiv 13^3 \cdot 13^2 = 2197 \cdot 169 \equiv -64\cdot 169 \equiv -32\cdot(2\cdot 169) \equiv$

$\equiv -32\cdot 15 \equiv -320-160 \equiv -157 \equiv 166 \pmod{323}$

Eva: eavesdropper — odposlouchá $C \equiv 166$, zná e, n

„Stačilo" by vyřešit kongruenci $x^5 \equiv 166 \pmod{323}$

POZOR: nelze přímo použít V o binom. kongruencích (mod $p\cdot q$ neex. prim. kořeny)

Hypoteticky řešme tuto kongruenci kdybychom uměli modul rozložit na prvočísla:

$x^5 \equiv 166 \pmod{17\cdot 19}$

$x^5 \equiv 166\ (17) \qquad x^5 \equiv 166\ (19)$

$x^5 \equiv -4\ (17) \qquad x^5 \equiv -5\ (19)$

$(5,16)=1 \qquad (5,18)=1$

jediné řešení mod 17, mod 19 $\Rightarrow$ díky CRT i mod 323

řešme s využitím prim. kořenů.

mod 17 je p.k. $g=3$

mod 19 je p.k. $g=2$

a	1	2	3	4	5	6	7	8
$3^a\ (17)$	3	9	10	-4	5	-2	-6	-1

a	1	2	3	4	5	6	7	8	9	…
$2^a\ (19)$	2	4	8	-3	-6	7	-5	9	-1	

$x^5 \equiv -4 \ (17) \qquad x \equiv 3^y$

$3^{5y} \equiv 3^4 \ (17)$ 3 je p.k. mod 17

$5y \equiv 4 \ (16)$

$y \equiv 4 \ (16)$

$\Rightarrow x \equiv 3^4 \equiv -4 \ (17)$

$\equiv 13 \ (17)$

$x^5 \equiv -5 \ (19) \qquad x \equiv 2^y$

$2^{5y} \equiv 2^7 \ (19)$ 2 je p.k. mod 19

$5y \equiv 7 \ (18)$

$5y \equiv 25 \ (18) \quad |:5$

$y \equiv 5 \ (18)$

$\Rightarrow x \equiv 2^5 \equiv -6 \ (19)$

$\equiv 13 \ (19)$

Je tedy (např. s využitím Čínské zbytkové věty) vidět, že $x \equiv 13 \ (323)$.

POZN: efektivněji bychom se znalostí rozkladu $323 = 17 \cdot 19$ dosáhli třeba výpočtem d ($\varphi(n) = 16 \cdot 18$, $d \cdot e \equiv 1 \ (16 \cdot 18)$) a následným umocněním c^d mod n.

(3) Hledejme primitivní kořen(y) modulo 47, 47^2, $2 \cdot 47^2$

Řeš: $\varphi(47) = 46 = 2 \cdot 23 \Rightarrow$ možné řády jsou $1, 2, 23, 46$

$g^2 \not\equiv 1 \ (47) \wedge g^{23} \not\equiv 1 \ (47) \Rightarrow g$ je prim. kořen 47

$g = 2$: $2^2 \not\equiv 1$, $2^{23} = (2^5)^4 \cdot 2^3 \equiv (-3 \cdot 5)^4 \cdot 2^3 = 3^4 \cdot 5^4 \cdot 2^3 \equiv 34 \cdot (-16) \cdot 5 \cdot 8 \equiv$

$2^5 = 32 \equiv -15 \ (47)$

$\equiv (-13) \cdot (-16) \cdot (-7) \equiv$

$\equiv 208 \cdot (-7) \equiv 20 \cdot (-7) \equiv$

$\equiv -140 \equiv 1 \ (47)$

není p.k., má řád 23

muselo být $\pm 1 \ (47)$

$g = 3$: $3^2 \not\equiv 1 \ (47)$

$3^{23} \equiv (3^3)^7 \cdot 3^2 \equiv (-20)^7 \cdot 3^2 \equiv$

$\equiv -2^{14} \cdot 5^7 \cdot 3^2 \equiv -2^5 \cdot 2^5 \cdot 2^4 \cdot 5^7 \cdot 3^2 \equiv$

$\equiv -3^2 \cdot 5^2 \cdot 2^4 \cdot 5^7 \cdot 3^2 \equiv -2^4 \cdot 3^4 \cdot 5^9 \equiv -3^3 \cdot 5^9 \equiv$

$\equiv 20 \cdot 5^9 \equiv 20 (5^3)^3 \equiv 20 \cdot (-16)^3 \equiv$ $3 \cdot 16 = 48 \equiv 1 \ (47)$

$\equiv -20 \cdot 2^{12} \equiv -20 \cdot 2^6 \cdot 2^6 \equiv -20 \cdot 17^2 \equiv -20 \cdot 289 \equiv -140 \equiv 1 \ (47)$

není p.k. mod 47

muselo být ± 1

$g = 4$: nemůže být p.k. $4 = 2^2 \Rightarrow$ je řádu $\frac{23}{(23,2)} = 23$

$g = 5$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	…	23
$5^a\ (47)$	5	25	-16	14	23	21	11	8	-7	12	13	18	-4	…	

5 je p.k. mod 47

$5^{23} = 5^{13} \cdot 5^{10} \equiv (-4) \cdot 12 = -48 \equiv -1 \ (\text{mod } 47)$

Známe-li jeden prim. kořen, známe všechny:

5^a je p.k. mod 47 $\iff (a,46)=1$

(primitivních kořenů je $\varphi(\varphi(47))=\varphi(46)=22$)

Prim. kořen modulo 47^2 ... je to p.k. g mod 47, pro nějž $g^{46}\not\equiv 1\ (47^2)$

$\varphi(47^2)=46\cdot 47=2\cdot 23\cdot 47$ ($\downarrow$: $\tau(46\cdot 47)=8$ potenciálních řádů)

Stačí ověřit, zda $5^{46}\not\equiv 1\ (47^2)$

$5^4=625=13\cdot 47+14$

$5^{46}=(5^4)^{11}\cdot 5^2=(13\cdot 47+14)^{11}\cdot 5^2\equiv(14^{11}+14^{10}\cdot 11\cdot 13\cdot 47)\cdot 5^2\equiv$

$\equiv 14^{10}(14+11\cdot 13\cdot 47)\cdot 5^2\equiv(38\cdot 47+9)(11\cdot 13\cdot 47+14)\cdot 5^2\equiv$

$\shortparallel$

$1795\ (47^2)$

$\shortparallel$

$38\cdot 47+9$

$\equiv(-9\cdot 47+9)(2\cdot 47+14)\cdot 5^2\equiv$

$11\cdot 13\equiv 2\ (47)$

$\equiv(-108\cdot 47+126)\cdot 5^2$

$\equiv(-14\cdot 47+126)\cdot 5^2\equiv$

$\equiv -532\cdot 25\equiv 2163\not\equiv 1\ (\mathrm{mod}\ 2209)$

$2209 = 47^2$

$\Rightarrow g=5$ je prim. kořen i modulo 47^2 (a 47^α, $\alpha\geq 1$)

navíc 5 je liché číslo $\Rightarrow$ je 5 i p.k. mod $2\cdot 47^2$