Kamil Zvelý

(4.1) Řešte v $\mathbb{Z}$ soustavu

$$x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 8, \quad x \equiv 5 \pmod{11}$$

$M = 5 \cdot 8 \cdot 11 = 440$

Nejdříve vypočítáme $q_i$

v $\mathbb{Z}_{440}$:

$q_5 = 8 \cdot 11 \cdot 1$

[ v $\mathbb{Z}_5$ $\quad 8 \cdot 11 \cdot 1 = 1$

$3 \cdot 1 = 1$

$3 1 = 1$

$1 = 2$ ]

v $\mathbb{Z}_{440}$:

$q_{11} = 5 \cdot 8 \cdot 1$

[ v $\mathbb{Z}_{11}$ $\quad 5 \cdot 8 \cdot 1 = 1$

$7 1 = 1$

$1 = 8$ ]

v $\mathbb{Z}_{440}$:

$q_8 = 5 \cdot 11 \cdot 1$

[ v $\mathbb{Z}_8$ $\quad 5 \cdot 11 \cdot 1 = 1$

$5 \cdot 3 \cdot 1 = 1$

$15 1 = 1$

$7 1 = 1$

$1 = 7$ ]

v $\mathbb{Z}_{440}$:

$$x = 3 \cdot q_5 + 2 \cdot q_8 + 5 \cdot q_{11} = 3 \cdot 8 \cdot 11 \cdot 2 + 2 \cdot 5 \cdot 11 \cdot 7 + 5 \cdot 5 \cdot 8 \cdot 8 =$$

$$= 528 + 770 + 1600 = 2898 = 258$$

v $\mathbb{Z}$:

$x = 258 + k \cdot 440 \quad k \in \mathbb{Z}$

Kamil Dareby

(4.2) Spočtěte reziduální AB a $A^B$ v $\mathbb{Z}_{440}$ pro $A = 21754$ a $B = 1213$.

$440 = 2^3 \cdot 5 \cdot 8$

z příkladu 4.1

$q_8 = 385 \qquad q_5 = 176 \qquad q_{11} = 320$

a) $A \cdot B$

v $\mathbb{Z}_5$ $A.B = 21754 . 1213 = 4 . 3 = 2$

v $\mathbb{Z}_8$ $A.B = 21754 . 1213 = 2 . 5 = 2$

v $\mathbb{Z}_{11}$ $A.B = 21754 . 1213 = (4 - 5 + 7 - 1 + 2) . (3 - 1 + 2 - 1) = 7 . 3 = 10$

v $\mathbb{Z}_{440}$ $A.B = 2 \cdot q_5 + 2 \cdot q_8 + 10 \cdot q_{11} = 2 . 176 + 2 . 385 + 10 . 320$

$= 352 + 330 + 120 = \underline{\underline{362}}$

b) $A^B$

v $\mathbb{Z}_5$ $A^B = 21754^{1213} = 4^{1213}$

$\gcd(5, 4) = 1$

$5 = 1 \cdot 4 + 1$

$4 = 4 . 1 + 0$

musíme použít Euler-Fermatova věta

$\varphi(5) = 4$

tedy $4^4 = 1$ v $\mathbb{Z}_{11}$

$4^{1213} = 4^{4 . 303 + 1} = 4$ v $\mathbb{Z}_5$

(4.2) pokračování

v $\mathbb{Z}_8$ $A^B = 21754^{1213} = 2^{1213}$

$gcd(8,2) = 2$ nelze použít Euler-Fermatovu větu

použijeme algoritmus opakovaných čtverců

1213 : 2 = 606 1
606 : 2 = 303 0
303 : 2 = 151 1
151 : 2 = 75 1
75 : 2 = 37 1
37 : 2 = 18 1
18 : 2 = 9 0
9 : 2 = 4 1
4 : 2 = 2 0
2 : 2 = 1 0
1 : 2 = 1 1

$(1213)_2 = 10010111101$

1 $a = 2$

x 1.2 = 2
s 2.2 = 4
s $4^2 = 16 = 0$
s $0^2 = 0$
x 0.2 = 0
s $0^2 = 0$
s $0^2 = 0$
x 0.2 = 0
s $0^2 = 0$
x 0.2 = 0
s $0^2 = 0$
x 0.2 = 0
s $0^2 = 0$
s $0^2 = 0$
x 0.2 = 0

$2^{1213} = 0$ v $\mathbb{Z}_8$

Kamil Dareby

(4.2) pokračování

$v\ Z_{11} \quad 21754^{1213} = 7^{1213}$

$gcd(11, 7) = 1$

$11 = 1 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

Můžeme použít Euler-Fermatovu větu

$\varphi(11) = 10$

$7^{10} = 1 \quad v\ Z_{11}$

$7^{1213} = 7^3 = 343 = 2$

$v\ Z_{440} \quad A^B = 21754^{1213} = 4 \cdot q_5 + 0 \cdot q_8 + 2 \cdot q_{11} =$

$4 \cdot 176 + 0 + 2 \cdot 320 = 24$

Kamil Dareby

(4.3) Pro RSA šifrování je dáno $N = 247$ a veřejný klíč $A = 11$.

Spočtěte soukromý klíč a dešifrujte zprávu $b = 147$.

Pro ~~dešifrování~~ dešifrování použijte čínskou větu o zbytcích.

hledáme rozklad 247 na prvočísla

$\sqrt{247} \leq 16$

Můžeme vyzkoušet tato prvočísla

2, 3, 5, 7, 11, 13

$247 = 13 \cdot 19$

$\varphi(247) = \varphi(13) \cdot \varphi(19) = 12 \cdot 18 = 216$

dopočteme $11^{-1}$ v $\mathbb{Z}_{216}$

gcd(216, 11)  $n = 216$  $a = 11$

$216 = 19 \cdot 11 + 7$  $7 = n - 19a$

$11 = 1 \cdot 7 + 4$  $4 = 11 - 1 \cdot 7 = a - n + 19a = 20a - n$

$7 = 1 \cdot 4 + 3$  $3 = 7 - 1 \cdot 4 = n - 19a - 20a + n = 2n - 39a$

$4 = 1 \cdot 3 + 1$  $1 = 4 - 1 \cdot 3 = 20a - n - 2n + 39a = -3n + 59a$

$1 = -3 \cdot 216 + 59 \cdot 11$

$11^{-1} = 59$ v $\mathbb{Z}_{216}$

soukromý klíč je (247, 59)

pro dešifrování je potřeba spočítat

$147^{59}$ v $\mathbb{Z}_{247}$

(4.3) pokračování

pro výpočtání použijeme Čínskou větu o zbytcích a algoritmus opakovaných čtverců.

$59 : 2 = 29$ 1

$29 : 2 = 14$ 1

$14 : 2 = 7$ 0

$7 : 2 = 3$ 1

$3 : 2 = 1$ 1

$1 : 2 = 0$ 1

$(59)_2 = 111011$

1) $147^{59} \mod 13$

$147^{59} = 4^{59}$

$\times 4$

$\downarrow 4^2 = 16 = 3$

$\times 3 \cdot 4 = 12$

$\downarrow 12^2 = 144 = 1$

$\times 1 \cdot 4 = 4$

$\downarrow 4^2 = 16 = 3$

$\downarrow 3^2 = 9$

$\times 9 \cdot 4 = 36 = 10$

$\downarrow 10^2 = 100 = 9$

$\times 9 \cdot 4 = 36 = 10$

2) $\mod 19 \quad 147^{59} = 14^{59}$

$\times 14$

$\downarrow 14^2 = 196 = 6$

$\times 6 \cdot 14 = 84 = 8$

$\downarrow 8^2 = 64 = 7$

$\times 7 \cdot 14 = 98 = 3$

$\downarrow 3^2 = 9$

$\downarrow 9^2 = 81 = 5$

$\times 5 \cdot 14 = 70 = 13$

$\downarrow 13^2 = 169 = 17$

$\times 17 \cdot 14 = 238 = 10$

Kamil Zarebský

(4.3) pokračování

připomínám koeficienty pro Šifrovou větu o zbytcích

a) $13^{-1}$ v $\mathbb{Z}_{19}$

gcd(19, 13) $\quad n = 19 \quad a = 13$

$19 = 1 \cdot 13 + 6 \quad 6 = 19 - 1 \cdot 13 = n - a$

$13 = 2 \cdot 6 + 1 \quad 1 = 13 - 2 \cdot 6 = a - 2n + 2a = 3a - 2n$

$1 = 3 \cdot 13 - 2 \cdot 19$

$13^{-1} = 3$ v $\mathbb{Z}_{19}$

b) $19^{-1}$ v $\mathbb{Z}_{13}$

$6^{-1}$ v $\mathbb{Z}_{13}$

gcd(13, 1)

$13 = 2 \cdot 6 + 1 \quad 1 = 13 - 2 \cdot 6$

$19^{-1} = 11$ v $\mathbb{Z}_{13}$

v $\mathbb{Z}_{247}$

$147^{59} = 10 \cdot 13 \cdot 3 + 10 \cdot 19 \cdot 11 = 390 + 2090 = 2480 = \underline{\underline{10}}$

Kamil Dorda

(4.4) Zachytili jsme zprávy $b = 31$ a $c = 47$, o kterých víme, že vznikly zašifrováním stejné zprávy a veřejnými klíči $(N = 91, 1 = 5)$ a $(N = 91, n = 7)$. Nalezněte zprávu a nebudou účely odhalen.

víme, že zprávy splňují splňují tyto rovnosti

v $\mathbb{Z}_{91}$

$31 = R^5$ $\quad 47 = R^7$ $\quad R \in \mathbb{Z}_{91}$ je hledaná zpráva

rozšířeným Eukleidovým algoritmem najdeme Bezoutovu rovnost.

v $\mathbb{Z}$ počítáme

$\gcd(7,5)$ $\quad 7 = n \quad 5 = a$

$7 = 1 \cdot 5 + 2$ $\quad 2 = n - a$

$5 = 2 \cdot 2 + 1$ $\quad 1 = a - 2n + 2a = 3a - 2n$

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

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

v $\mathbb{Z}_{91}$ sestavíme následující rovnici

$$R^{3 \cdot 5} = R^{1 + 2 \cdot 7}$$

využijeme rovnosti definovaných na začátku příkladu

$$31^3 = R^{3 \cdot 5} = R \cdot R^{2 \cdot 7} = R \cdot 47^2$$

$$31^3 = R \cdot 47^2$$

dále řešíme lineární rovnici v $\mathbb{Z}_{91}$

$29\,791 = R \cdot 2209$

$34 = R \cdot 25$

(4.4) pokračování

$\gcd(91,25)$ $\quad n=91 \quad a=25$

$91 = 3\cdot 25 + 16$ $\quad 16 = n - 3a$

$25 = 1\cdot 16 + 9$ $\quad 9 = a - n + 3a = 4a - n$

$16 = 1\cdot 9 + 7$ $\quad 7 = n - 3a - 4a + n = 2n - 7a$

$9 = 1\cdot 7 + 2$ $\quad 2 = 4a - n - 2n + 7a = 11a - 3n$

$7 = 3\cdot 2 + 1$ $\quad 1 = 2n - 7a - 33a + 9n = 11n - 40a$

$1 = 11\cdot 91 - 40\cdot 25$

protože $\gcd(91,25) = 1$ máme právě jedno řešení

$25^{-1} = -40 = 51 \ v \ \mathbb{Z}_{91}$

$34 = 2\cdot 25$

$34\cdot 51 = 2$

$2 = 5 \ v \ \mathbb{Z}_{91}$