4 Reziduální aritmetika a RSA-šifrování

1. Řeště v $\mathbb{Z}$ zbytkovou soustavu:

$$x \equiv 3 \,(\mathrm{mod}\, 5)\ ,\ x \equiv 2 \,(\mathrm{mod}\, 8)\ ,\ x \equiv 5 \,(\mathrm{mod}\, 11).$$

2. Spočtěte reziduálně AB a A^B v $\mathbb{Z}_{440}$ pro $A = 21754$ a $B = 1213$.

3. Pro RSA šifrování je dáno $N = 247$ a veřejný klíč $t = 11$. Spočtěte soukromý klíč a dešifrujte zprávu $b = 147$. Pro dešifrování použijte Čínskou větu o zbytcích.

4. Zachytili jste zprávy $b = 31$ a $c = 47$, o kterých víte, že vznikly zašifrováním stejné zprávy a veřejnými klíči $(N = 91, t = 5)$ a $(N = 91, r = 7)$. Nalezněte zprávu a metodou útoku outsidera.

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(4.1.) Řešte v $\mathbb{Z}$ kbytkovou soustavu:

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

Nejprve spočtu sadu: $M = 5.8.11 = 440$

$\nu\ Z_{440}$ $\quad q_5 = 8.11.k$

$$\left[\nu\ Z_5 \quad \begin{aligned} 8.11.k &= 1 \\ 3.1.k &= 1 \\ 3k &= 1 \\ \underline{\underline{k}} &= \underline{\underline{2}} \end{aligned}\right]$$

$\nu\ Z_{440}$ $\quad q_8 = 5.11.k$

$$\left[\nu\ Z_8 \quad \begin{aligned} 5.11.k &= 1 \\ 5.3.k &= 1 \\ 15k &= 1 \\ 7k &= 1 \\ \underline{\underline{k}} &= \underline{\underline{7}} \end{aligned}\right]$$

$\nu\ Z_{440}$ $\quad q_{11} = 5.8.k$

$$\left[\nu\ Z_{11} \quad \begin{aligned} 5.8.k &= 1 \\ 40k &= 1 \\ \underline{\underline{k}} &= \underline{\underline{8}} \end{aligned}\right]$$

Nyní dosadím do rovnice

$$x = 3q_5 + 2q_8 + 5q_{11}$$
$$x = 3.8.11.2 + 2.5.11.7 + 5.8.8 = 698$$

$\nu\ Z_{440}$ $\quad x = (698 - 440) = \underline{\underline{258}} \rightarrow$ jediné řešení

$\nu\ \mathbb{Z}$ $\quad x = 258 + k.5.8.11 = \underline{258 + k.440}, \quad k \in \mathbb{Z}$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(2)

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

Pro výpočet použiji výpočty z příkladu 4.1. tím: $440 = 8.5.11 = 2^3.5.11$

$q_5 = 88$
$q_8 = 330$
$q_{11} = 280$

AB a A^B budu počítat v $\mathbb{Z}_5$, $\mathbb{Z}_8$ a $\mathbb{Z}_{11}$.

(A.B)

v $\mathbb{Z}_5$ $A.B = 21754.1213 = 4.3 = 12 \bmod 5 = \underline{2}$
v $\mathbb{Z}_8$ $A.B =$ —"— $= 2.5 = 10 \bmod 8 = \underline{2}$
v $\mathbb{Z}_{11}$ $A.B =$ —"— $= 7.-3 = -21 \bmod 11 = \underline{1}$

v $\mathbb{Z}_{440}$ $A.B = 2.q_5 + 2.q_8 + 1.q_{11} =$
$= 2.88 + 2.330 + 280 =$
$= 1166 \bmod 440 = \underline{\underline{236}}$

(A^B)

v $\mathbb{Z}_5$ $A^B = 4^B = 4^{1213} \overset{E.F.V.}{=} 4^{4.303+1} = (4^4)^{303}.4^1 =$
$= 1^{303}.4 = \underline{4}$

$GCD(5,4)$ $5 = 4.1 + \boxed{1} \rightarrow GCD = 1$
$4 = 1.4 + 0$

$\Rightarrow$ lze použít E.F.V $\rightarrow 4^4 \equiv 1$ v $\mathbb{Z}_5$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora11**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(3)

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

GCD (8, 2) → čísla jsou soudělná, použij binární rozklad
1213 binárně = 1 0 0 1 0 1 1 1 1 0 1
X S S S X S S X S X S X S X S S X
$a = 2$

1
$x = 1 . 2 = 2$
$S = 2^2 = 4$
$S = 4^2 = 16 \mod 8 = 0$
$S = 0^2 = 0$
⋮ ⋱ ⋮ další výpočty nejsou nutné
$x = 0$
⟶ $2^{1213} = 0$ v $\mathbb{Z}_8$

v $\mathbb{Z}_{11}$ $A^B = 4^B = 4^{1213} \overset{\text{E.F.V}}{=} 4^{10 . 121 + 3} = (4^{10})^{121} . 4^3$
$= 1^{211} . 343 = 343 \mod 11 = 2$

GCD (11, 7) $11 = 4 . 1 + 4$
$4 = 4 . 1 + 3$
$4 = 3 . 1 + 1$
$3 = 1 . 2 + 1$ → GCD = 1
$1 = 1 . 1 + 0$

→ $4^{10} \equiv 1$ v $\mathbb{Z}_{11}$

v $\mathbb{Z}_{440}$ $A^B = 4q_5 + 0q_8 + 2q_{11} = 4 . 88 + 0 + 2 . 280$
$= 912 \mod 440 = 32$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(4)

(4. 3.) Pro RSA šifrování je dáno $N = 247$ a veřejný klíč $l = 11$.
Spočtěte soukromý klíč a dešifrujte zprávu $b = 147$.
Pro dešifrování použijte činnost v. o zbytcích.

Nejprve nalezneme faktorizaci N.

$N = 247 = p \cdot q \rightarrow p, q = \sqrt{247} \doteq 15,7$

$p, q < 16$

Hrubou silou nalezneme prvočísla p, q

$247 = 13 \cdot 19$.

Nyní musím najít dešifrovací exponent.
K tomu potřebuji spočítat

$\varphi(N) = \varphi(247) = (p-1)(q-1)$

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

a dále v $\mathbb{Z}_{216}$ najít inverzi 11 pomocí rozšířeného Eukl. algoritmu (nebudu ho zde rozepisovat - viz ?.)

$11^{-1} = 59$

Soukromý klíč $(N, s) = (247, 59)$

$GCD(\overset{n}{216}, \overset{a}{11})$

$216 = 11.19 + 7$ $\quad 7 = 216 - 11.19$

$= n - 19a$

$11 = 7.1 + 4$ $\quad 4 = 11 - 7.1$

$= a - (n - 19a) = 20a - n$

$7 = 4.1 + 3$ $\quad 3 = 7 - 4.1$

$= n - 19a - (20a - n) = 2n - 39a$

$4 = 3.1 + \boxed{1} \rightarrow GCD$ $\quad 1 = 4 - 3.1$

$= 20a - n - (2n - 39a) = 59a - 3n$

$3 = 1.3 + 0$

$59a - 3n = 59.11 - 3.216 = 649 - 648 = 1$

$S = 59 \quad \rightarrow \quad 11^{-1} = 59$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(5)

Dešifrování: $c = b^s \pmod{N}$
$c = 147^{59} \pmod{247}$

Nejprve provedu binární rozvoj exponentu 59

$59_2 = 1\ 1\ 1\ 0\ 1\ 1$
$X\ S\ X\ S\ X\ S\ \ S\ X\ S\ X$

Podle zadání použiju Č.Z. o zbytcích.
Mám $M = (13, 19) \leftarrow 247 = 13 \cdot 19$
↳ budu počítat $\pmod{Z_{13}}$ a $\pmod{Z_{19}}$

$\pmod{Z_{13}}$		$\pmod{Z_{19}}$
$147^{59} = 4^{59} \rightarrow a = 4$		$147^{59} = 14^{59} \rightarrow a = 14$
$1 \cdot 4 = 4$	X	$1 \cdot 14 = 14$
$4^2 = 16 \mod 13 = 3$	S	$14^2 = 196 \mod 19 = 6$
$3 \cdot 4 = 12$	X	$6 \cdot 14 = 84 \mod 19 = 8$
$12^2 = 144 \mod 13 = 1$	S	$8^2 = 64 \mod 19 = 7$
$1 \cdot 4 = 4$	X	$7 \cdot 14 = 98 \mod 19 = 3$
$4^2 = 16 \mod 13 = 3$	S	$3^2 = 9$
$3^2 = 9$	S	$9^2 = 81 \mod 19 = 5$
$9 \cdot 4 = 36 \mod 13 = 10$	X	$5 \cdot 14 = 70 \mod 19 = 13$
$10^2 = 100 \mod 13 = 9$	S	$13^2 = 169 \mod 19 = 17$
$9 \cdot 4 = 36 \mod 13 = 10$	X	$17 \cdot 14 = 238 \mod 19 = 10$

Dále si vypočítám inverzní prvky
$13^{-1} \pmod{Z_{19}}$ a $19^{-1} \pmod{Z_{13}}$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(6)

$13^{-1} \text{ v } \mathbb{Z}_{19} \rightarrow GCD(\overset{n}{19}, \overset{a}{13})$

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

$13 = 6 \cdot 2 + \boxed{1} \rightarrow GCD \qquad 1 = 13 - 6 \cdot 2$
$= a - 2(n - a) = 3a - 2n$

$6 = 1 \cdot 6 + 0$

$13^{-1} \text{ v } \mathbb{Z}_{19} = 3a - 2n = 3 \cdot 13 - 2 \cdot 19 = 3$

$19^{-1} \text{ v } \mathbb{Z}_{13} \rightarrow GCD(13, 19)$
$\hookrightarrow 6^{-1} \text{ v } \mathbb{Z}_{13} \rightarrow GCD(\overset{n}{13}, \overset{a}{6})$

$13 = 6 \cdot 2 + \boxed{1} \rightarrow GCD \qquad 1 = 13 - 6 \cdot 2$
$= n - 2a$

$6 = 1 \cdot 6 + 0$

$6^{-1} \text{ v } \mathbb{Z}_{13} = -2 = 11$

Jednáním si rovnici k dešifrování zprávy
$c = 144^{59} \text{ v } \mathbb{Z}_{247}$

$c = 144^{59} = 10 \cdot 13 \cdot 3 + 10 \cdot 19 \cdot 11$
$\quad \rightarrow \cancel{x} \quad \rightarrow 13^{-1} \qquad \rightarrow x \quad \rightarrow 19^{-1}$
$\quad \text{v } \mathbb{Z}_{19} \qquad \text{v } \mathbb{Z}_{13}$

$= 390 + 2090 = 10 \text{ v } \mathbb{Z}_{247}$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(4)

4.4. Zachytili jsme zprávy $b = 31$ a $c = 47$, o kterých víme, že vznikly zašifrováním stejné zprávy a s veřejnými klíči $(N = 91, t = 5)$ a $(N = 91, r = 7)$.
Nalezněte zprávu a metodou útoku opakovaná.

U obou VK má N stejnou hodnotu → jde o tzv. „útok při sdíleném modulu".

O zprávách víme, že splňují v Z_{19} tyto rovnosti
$31 = a^5$
$47 = a^7$

Vzhledem k tomu, že evidentně platí $GCD(7,5) = 1$, spočítám rozšířeným Eukl. alg. Bezoutovu rovnost.
Pro výpočet si zavedu proměnné
$5 = e_1$
$7 = e_2$

$GCD(7,5)$
$7 = 5 \cdot 1 + 2$ $\quad 2 = e_2 - e_1$
$5 = 2 \cdot 2 + \boxed{1}$ → GCD $\quad 1 = 5 - 2 \cdot 2$
$= e_1 - 2(e_2 - e_1) = 3e_1 - 2e_2$

$1 = 3e_1 - 2e_2 \rightarrow 1 = 3 \cdot 5 - 2 \cdot 7$ v $\mathbb{Z}$
$3 \cdot 5 = 1 + (2 \cdot 7)$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(8)

Nyní řešením rovnici v $\mathbb{Z}_{91}$

$$a^{5.3} = a^{(7.2)+1}$$
$$(a^5)^3 = (a^7)^2 \cdot a^1$$
$$31^3 = 47^2 \cdot a \quad v \ \mathbb{Z}_{91}$$

Dále řeším jako lineární rovnici

$31^3 = 29\,791 \mod 91 = 34$
$47^2 = 2\,209 \mod 91 = 25$

dosazením do rovnice $\rightarrow$ $34 = a \cdot 25$

Předpoklad: pokud $GCD(91, 25) = 1$, pak má rovnice pouze jedno řešení

$$GCD(\underset{n}{91}, \underset{a}{25})$$

$91 = 3 \cdot 25 + 16$	$16 = 91 - 3 \cdot 25 = n - 3a$
$25 = 1 \cdot 16 + 9$	$9 = 25 - 16 = 4a - n$
$9 = 1 \cdot 7 + 2$	$7 = 16 - 9 = 2n - 7a$
$7 = 3 \cdot 2 + \boxed{1} \rightarrow GCD$	$2 = 9 - 7 = 11a - 3n$
$2 = 1 \cdot 2 + 0$	$1 = 7 - (3 \cdot 2) = 11n - 40a$

inverzní prvek $= -40$

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

$GCD(91, 25) = 1 \rightarrow$ v $\mathbb{Z}_{91}$ má rovnice pouze jedno řešení ~~$(1 = 11 \cdot 91 - 40 \cdot 25)$~~

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

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(9)

$34 = a \cdot 25$

$34 \cdot 25^{-1} = a \cdot \underbrace{25 \cdot 25^{-1}}_{=1}$

$34 \cdot 25^{-1} = a \cdot 1$

$34 \cdot 51 = a$

$a = 5 \nmid \mathbb{Z}_{91}$

Kontrola: $31 = 5^{-5} \nmid \mathbb{Z}_{91}$
$44 = 5^{7} \nmid \mathbb{Z}_{91}$ } OK