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.

4.1

1) vypočtu sadu $M = (5.8.11) = 440 \rightarrow \mathbb{Z}_{440}$
např. $x \equiv 3 \,(\mathrm{mod}\, 5)$ $x \equiv 2 \,(\mathrm{mod}\, 8)$ $x \equiv 5 \,(\mathrm{mod}\, 11)$

2) vypočtu q_5, q_8 a q_{11} v $\mathbb{Z}_{440}$
$q_5 = 8.11.k \rightarrow$ v $\mathbb{Z}_5 = 8.11.k = 1 \rightarrow k = 2$
$q_8 = 5.11.k \rightarrow$ v $\mathbb{Z}_8 = 5.11.k = 1 \rightarrow k = 7$
$q_{11} = 5.8.k \rightarrow$ v $\mathbb{Z}_{11} = 5.8.k = 1 \rightarrow k = 8$

3) dosadím do rovnice
$x = 3q_5 + 2q_8 + 5q_{11}$
$= 3(8.11.2) + 2(5.11.7) + 5(5.8.8) = 698$
v $\mathbb{Z}_{440}$ $x = (698 - 440) = 258 \rightarrow$ jediné řešení

4.2

1) ~~440 (=440)~~ n (= 440) rozložím na prvočísla – viz 4.1

2) určím, v jakých $\mathbb{Z}_n$ budu počítat (tedy v $\mathbb{Z}_5$, $\mathbb{Z}_8$ a $\mathbb{Z}_{11}$)

3) vypočtu $A.B$ v $\mathbb{Z}_5$, $\mathbb{Z}_8$ a $\mathbb{Z}_{11}$

4) v $\mathbb{Z}_{440}$ $A.B = (AB$ v $\mathbb{Z}_5)q_5 + (AB$ v $\mathbb{Z}_8)q_8 + (AB$ v $\mathbb{Z}_{11})q_{11}$
výsledek AB v $\mathbb{Z}_5$ → ~~výsledek~~ výp. viz 4.1

5) vypočtu A^3 v $\mathbb{Z}_5$, $\mathbb{Z}_8$ a $\mathbb{Z}_{11}$
– GCD = 1 → použít E-F.V (viz 3.3)
= soudělná č. → použít opak. čtverce (3.3)

6) v $\mathbb{Z}_{440}$ $A^B = (A^3$ v $\mathbb{Z}_5)q_5 + (A^3$ v $\mathbb{Z}_8)q_8 + (A^3$ v $\mathbb{Z}_{11})q_{11}$

(4.3) 1) najít faktorizaci $N \rightarrow N = p \cdot q$

$p, q \doteq \sqrt{N} : 2$

prvočísla p, q dohledat hrubou silou

2) najít dešifrovací exponent – k tomu potřebuji výpočet $\varphi(N) = (p-1)(q-1) \rightarrow n(\mathbb{Z}_n)$

3) vzdy $\mathbb{Z}_{216}$ a najít inverzi k veřejnému klíči $\underline{t}$ $(= 11)$, tzn. výpočet přes rozšířený Euklid $GCD(216, 11)$

4) inverze $= S$ pro soubor. klíč (N, S)

5) dešifrování $c = b^s \in \mathbb{Z}_N$

vzdy $c = 147^{59} \in \mathbb{Z}_{247}$

6) použít binární rozvoj exponentu

7) mám použít Č.V $\rightarrow$ určím počet $M = (p, q)$

8) ad 6) budu počítat v $\mathbb{Z}_p$ a $\mathbb{Z}_q$

- nejprve upravit základ 147^{59} mod p a mod q
- výsledkem bude $\underline{a}$ pro $\mathbb{Z}_p$ a pro $\mathbb{Z}_q$

9) najdu inverzní prvky $p^{-1} \in \mathbb{Z}_q$ a $q^{-1} \in \mathbb{Z}_p$

$p^{-1} \in \mathbb{Z}_q \rightarrow GCD(q, p)$

$q^{-1} \in \mathbb{Z}_p \rightarrow GCD(p, q)$

10) sestavím rovnici k dešifrování

$c = 147^{59} \in \mathbb{Z}_{247}$

$= \underbrace{\text{výsl. ČV} \cdot p \cdot p^{-1}}_{\in \mathbb{Z}_q} + \underbrace{\text{výsl. ČV} \cdot q \cdot q^{-1}}_{\in \mathbb{Z}_p}$

a vypočtu

(4.4) Idea: „útok sdíleného modulu", protože N má stejnou hodnotu u obou VK

- $N \Rightarrow$ hodnota $\mathbb{Z}_n$
- zprávy $b = 31$ a $c = 47$
- VK = $(N = 91, k = 5)$ a $(N = 91, r = 7)$
- zprávy a splňují v $\mathbb{Z}_{91}$ rovnosti:
  $31 = a^5$ a $47 = a^7$

(1) $GCD(7,5) = 1 \Rightarrow$ spočítat Bezoutovu rovnost rozšířeným Euklidem
vhodné zvolit si jiné proměnné než standardní r, a např. $3.5 = 1 + 2.7$

2) přetvořit rovnici v $\mathbb{Z}_{91}$

$a^{3.5} = a^{2.7+1} \Rightarrow (a^5)^3 = (a^7)^2 . a^1$ v $\mathbb{Z}_{91}$

$31^3 = 47^2 . a$

3) dále řešit jako lineární rovnici

$31^3 = \ldots \mod 91 = 34$
$47^2 = \ldots \mod 91 = 25$
$\Rightarrow 34 = a . 25$

4) předpoklad $GCD(91,25) = 1 \Rightarrow$ pak má rovnice jen jedno řešení
vypočítat a^{-1} v $\mathbb{Z}_{91}$ $\quad a^{-1} = 51$

5) dopočítat $34 = a . 25 \Rightarrow$ ~~$34 = a . 1$~~

$34 . 25^{-1} = a . 25 . 25^{-1} \Rightarrow = 1$

$34 . 25^{-1} = a . 1$

$35 . 51 = a$

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

6) kontrola $31 = a^5 = 5^5$
$47 = a^7 = 5^7$ v $\mathbb{Z}_{91}$