Vnitrosemestrální písemka – MIN401 – jaro 2022 – 6. 4. 2022

Veškeré odpovědi musí být zdůvodněny a výpočty musí být doprovozeny komentářem. (Řešení sestávající pouze z odpovědí budou považována za opsaná a hodnocena 0 body.)

1. (3 body) Najděte všechna celá čísla, která vyhovují soustavě kongruencí

$$\begin{aligned} 5x &\equiv 1 \pmod{14}, \\ 17x &\equiv 2 \pmod{35}, \\ 5x &\equiv 15 \pmod{18}. \end{aligned}$$

2. (3.5 bodu) V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 7$, $q = 23$. Veřejným klíčem je $n = 161$. Dešifrujte obdrženou zprávu $C = 116$ (tj. najděte všechny možnosti pro poslanou zprávu).

3. (3.5 bodu) Julie a Romeo komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 19$ a na primitivním kořenu $g = 10$. Julie si za svůj tajný klíč zvolila číslo $a = 11$, Romeo má svůj tajný klíč b.

(a) Ověřte, že 10 je skutečně primitivní kořen modulo 19. [5 bodů]

(b) Jaký údaj poskytla Julie Romeovi? [5 bodů]

(c) Romeo posléze poslal Julii jako zprávu dvojici čísel ($g^b \equiv 7,\ 4$). Pomozte Julii s dešifrováním zprávy. [15 bodů]

Řešení a bodování:

1. [**3 body**] Třetí rovnici lze podělit pěti. Dostáváme jednodušší

$$x \equiv 3 \pmod{18}.$$

Vezmeme jednu rovnici, vyřešíme, dosadíme do druhé, vyřešíme, dosadíme do třetí a dostaneme celkový výsledek. Prvně počítejme modulo 35:

$$\begin{aligned} 17x &\equiv 2 \pmod{35}, \\ 34x &\equiv 4 \pmod{35}, \\ x &\equiv 31 \pmod{35}. \end{aligned}$$

Proto $x = 35a + 31$ dosadíme do prvé rovnice a počítáme modulo 14:

$$\begin{aligned} 5(35a+31)x &\equiv 1 \pmod{14}, \\ 5(7a+3) &\equiv 1 \pmod{14}, \\ 7a+1 &\equiv 1 \pmod{14}, \\ 7a &\equiv 0 \pmod{14}, \text{ dělení } 7, \\ a &\equiv 0 \pmod{2}. \end{aligned}$$

Tedy $a = 2b$ a $x = 35(2b) + 31$. Dosadíme do třetí kongruence a počítáme modulo 18:

$$\begin{aligned} 35(2b)+31 &\equiv 3 \pmod{18}, \\ 70b+31 &\equiv 3 \pmod{18}, \\ -2b &\equiv 8 \pmod{18}, \\ -b &\equiv 4 \pmod{9}, \text{ dělení } 2, \\ b &\equiv 5 \pmod{9}. \end{aligned}$$

Odtud $b = 9c + 5$ a dosazením do x dostaneme

$$x = 35(2(9c+5)) + 31 = 630c + 350 + 31 = 630c + 381.$$

Bodování: Počítání modulo 35 za [0.8], počítání modulo 14 za [0.8], počítání modulo 18 za [0.8] a správný výsledek [0.6b]. Za každé chybné dělení strhnout [0.5b].

2. [**3.5 bodu**] Dešifrovaná zpráva M splňuje $Z^2 \equiv C \mod n$. Takové jsou 4 a jsou ve tvaru

$$M \equiv \pm apQ \pm bqP \mod n,$$

kde a, b, P, Q jsou celá čísla splňující

1. $ap + bq = 1$,
2. $P \equiv C^{\frac{p+1}{4}} \mod p$,
3. $Q \equiv C^{\frac{q+1}{4}} \mod q$.

Pomocí algoritmu spočítáme $a = 10$, $b = -3$. Dále počítáme modulo 7

$$116^2 \equiv 4^2 \equiv 16 \equiv 2 \mod 7.$$

Tedy $P = 2$.

Počítáním modulo 23

$$116^6 \equiv 1^6 \equiv 1 \mod 23.$$

Tedy $Q = 1$. Proto

$$M \equiv \pm 10 \cdot 7 \cdot 1 \pm 3 \cdot 23 \cdot 2 = \pm 70 \pm 138.$$

Dešifrovaná zpráva je jedna z následujících: 47, 68, 93, 114.

O správnosti výpočtu se můžeme přesvědčit tím, že ověříme platnost kongruencí

$$M^2 \equiv 116 \equiv 4 \mod 7,$$
$$M^2 \equiv 116 \equiv 1 \mod 23.$$

Bodování: Správný vzorec pro M [1b], výpočet čísel a, b [0.4b], výpočet $P \equiv M^{\frac{p+1}{4}} \mod p$ [0.2], výpočet $Q \equiv M^{\frac{q+1}{4}} \mod q$ [1b], správné hodnoty M [0.5b]. Ověření správnosti není třeba provádět.

3. [**3.5 bodu**] **(a)** $\varphi(19) = 18 = 2 \cdot 3^2$. Proto $10^{18} \equiv 1 \mod 19$. Počítáme modulo 19

$$10^6 \equiv 100^3 \equiv 5^3 \equiv 6 \cdot 5 \equiv 11,$$
$$10^9 \equiv 10^6 \cdot 100 \cdot 10 \equiv 11 \cdot 5 \cdot 10 \equiv 11 \cdot 12 \equiv 8 \cdot 7 \equiv 18.$$

Tedy 10 je primitivní kořen.

(b) Julie poskytla údaj

$$g^a \equiv 10^{11} \equiv 10^9 \cdot 100 \equiv (-1) \cdot 5 \equiv 14, \quad \mod 19.$$

(c) Romeo zašifroval zprávu M jako dvojici $(g^b, M(g^a)^b) = (7, 4)$. Proto dešifrujeme takto

$$M \equiv M(g^a)^b \cdot \left((g^b)^a\right)^{-1} \equiv 4 \cdot \left(7^{11}\right)^{-1} \equiv 4 \cdot (11)^{-1} \equiv 4 \cdot 7 \equiv 9 \mod 19.$$

Výpočet

$$7^{11} \equiv 49^5 \cdot 7 \equiv 11^5 \cdot 7 \equiv (-8)^5 \cdot 7 \equiv -64^2 \cdot 56 \equiv -7^2(-1) \equiv 11 \mod 19.$$

Inverze k $11 \mod 19$ se najde jako číslo a takové, že $11a + 19b = 1$ pro nějaké b. Jednoduše $(a, b) = (7, -4)$. Inverze je tedy 7.

Bodování: **(a)** Za $\varphi(19)$ a jeho rozklad [0.2], za každou mocninu [0.2b], celkem [0.4b]. **(b)** Postup [0.4b], mocnina [0.2]. **(c)** Správný vzorec [1b], mocnina [0.4b], inverze [0.4b], správný výsledek [0.5b].