3 body ♣

1. Uveďte aspoň dve pravidlá voľby šifrovacieho exponentu, resp. dešifrovacieho exponentu, pre algoritmus RSA.

Riešenie: Pravidlá voľby šifrovacieho a dešifrovacieho exponentu pre RSA algoritmus sú:

1. Nevhodná voľba je $e = d$! Toto nastáva vtedy, keď $e^2 \equiv 1 \pmod{\varphi(pq)}$

2. Aby e_k bola permutácia na $\mathbb{Z}_n^*$, musí platiť

$$\gcd(e, \varphi(pq)) = 1 \quad \Rightarrow \quad \gcd(e, \varphi(p-1)) = \gcd(e, \varphi(q-1)) = 1$$

3. Prvočísla p a q sa vyberajú tak, aby čísla $p \pm 1$ a $q \pm 1$ mali veľké faktory. Platí totiž

$$\text{Označme} \quad e_k^h(x) = \underbrace{e_k(e_k \dots e_k(x)) \dots)}_{h\text{-krát}},$$

$$\text{potom ak} \quad e_k^{h+1}(x) = e_k(x), \quad \text{tak } e_k^h(x) = x$$

   Dá sa ukázať, že exponent h závisí od faktorizácie $\varphi(n)$. Preto sa vyberajú *silné prvočísla*. Sú nimi napr. *Sophie Germain prvočísla*. To sú prvočísla p v tvare

$$p = 2p_1 + 1, \quad \text{kde } p_1 \text{ je tiež prvočíslo.}$$

4. Často sa vyberá $e = 3$ alebo $e = 2^{16} + 1$. Vo všeobecnosti sa číslam $e = 2^k + 1$ hovorí *krátke exponenty*. Tie môžu urýchliť šifrovanie, ale systém používajúci krátke exponenty nie je bezpečný.

3 body ♢

2. (a) **(2b)** Formálne zadefinujte asymetrický kryptosystém.
   (b) **(1b)** V čom spočíva hlavný rozdiel medzi symetrickou a asymetrickou kryptografiou?

Riešenie:

(a) Nech $\mathcal{A} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je kryptosystém. Nech pre každé $k \in \mathcal{K}$ existujú funkcie

$$e_k : \mathcal{P} \to \mathcal{C} \qquad \text{a} \qquad d_k : \mathcal{C} \to \mathcal{P}$$

také, že platí

(i) Pre $\forall x \in \mathcal{P}$ platí $d_k(e_k(x)) = x$.
(ii) Pre $\forall k \in \mathcal{K}$ je výpočtovo jednoduché určiť pár e_k a d_k.
(iii) Pre $\forall k \in \mathcal{K}$ sú funkcie e_k a d_k výpočtovo jednoduché.
(iv) Pre skoro všetky $k \in \mathcal{K}$ je výpočtovo náročné určiť d_k zo znalosti e_k.

Potom sa $\mathcal{A}$ nazýva **asymetrický kryptosystém**. Zobrazenie e_k je verejné a d_k je tajné.

(b) Pri symetrickej kryptografii sa správa šifruje aj dešifruje tým istým kľúčom. Pri asymetrickej kryptografii sa správa šifruje verejným kľúčom a dešifruje sa privátnym (tajným) kľúčom, pričom tieto kľúče sú rôzne.

5 bodov

3. Pre ktorú triedu prvočísel p vieme ľahko vypočítať odmocninu z $a \pmod p$ a ako sa táto odmocnina počíta?

Riešenie: Pre prvočísla p, pre ktoré platí kongruencia

$$p \equiv 3 \pmod 4 .$$

Pre takéto prvočísla p má rovnica $x^2 \equiv a \pmod p$ riešenie

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p ,$$

pretože podľa Eulerovho kritéria dostávame

$$x^2 \equiv a^{\frac{p+1}{2}} \pmod p \equiv a^{\frac{p-1}{2}} \pmod p = a$$

12 bodov ★

4. (a) **(2b)** Čo znamená, že šifra je absolútne bezpečná, v zmysle Shannonovej teórie?
   (b) **(4b)** Uveďte tvrdenie Shannonovej pesimistickej vety.
   (c) **(4b)** Popíšte Vernamovu šifru.
   (d) **(2b)** Koľkokrát možno pri Vernamovej šifre použiť ten istý kľúč pri nezmenenej miere bezpečnosti?

Riešenie:

(a) Šifra (šifrovací algoritmus) sa nazýva **absolútne bezpečná** v zmysle Shannonovej teórie, ak zašifrovaný text neposkytuje žiadnu informáciu o otvorenom texte. V zmysle Shannonovej teórie informácie teda platí $I(M, C) = 0$, kde M označuje otvorený text (Message) a C označuje zašifrovaný text (Cipher text). Hovoríme aj, že náhodné premenné M a C sú stochasticky nezávislé.

(b) **Shannonova pesimistická veta** hovorí, že pre akúkoľvek absolútne bezpečnú symetrickú šifru s jednoznačným dešifrovaním, musí platiť nerovnosť $H(K) \geq H(M)$, čiže entropia kľúča musí byť aspoň taká veľká ako je entropia otvoreného textu.

(c) **Vernamova šifra**

- ▷ **Otvorený text:** $M \in \mathbb{Z}_2^n$.
- ▷ **Kľúč:** $K \in \mathbb{Z}_2^n$ tak, aby platilo $P(K = (k_1, \ldots, k_n)) = 2^{-n}$.
- ▷ **Zašifrovaný text:** $C \in \mathbb{Z}_2^n$, kde $c_i = m_i \oplus k_i$, pre $i \in \{1, \ldots, n\}$.

(d) Len raz!

17 bodov ♠

5. (a) **(5b)** Uveďte definíciu primitívneho prvku (generátora) v grupe $\mathbb{Z}_p^*$ pre prvočíslo p.
   (b) **(3b)** Definujte problém diskrétneho logaritmu.
   (c) **(6b)** Popíšte Diffie-Hellmanov protokol výmeny kľúča. Čo je verejné a čo tajné?
   (d) **(3b)** Predpokladajme, že útočník odpočúva komunikáciu medzi obidvoma stranami počas výmeny kľúča podľa Diffie-Hellmanovho protokolu. Dokáže útočník z obsahu komunikácie určiť tajný kľúč? Vaše tvrdenie zdôvodnite.

Riešenie:

(a) Vo všeobecnosti, $a \in \mathbb{Z}_n^*$ je **primitívny prvok** grupy $(\mathbb{Z}_n^*, \odot)$ práve vtedy ak platí

$$\mathbb{Z}_n^* = \left\{ a^i : \ 1 \leq i \leq \varphi(n) - 1 \right\} ,$$

pričom zápis a^i označuje i-krát opakovanú grupovú operáciu, t. j. $a^i = \underbrace{a \odot a \odot \ldots \odot a}_{i\text{-krát}}$.

Konkrétne ak $n = p$, kde p je prvočíslo, tak $a \in \mathbb{Z}_p^*$ je **primitívny prvok** grupy $(\mathbb{Z}_p^*, \odot)$ práve vtedy ak platí $\mathbb{Z}_p^* = \{a^i : \ 1 \leq i \leq p - 2\}$.

(b) Majme cyklickú grupu $(G, \odot)$ a nech $a \in G$ je jej primitívny prvok. **Problém diskrétneho logaritmu** je potom úloha pre dané $b \in G$ nájsť $1 \leq e \leq |G| - 1$, pre ktoré platí

$$a^e = b\,, \quad \text{kde} \quad a^e = \underbrace{a \odot a \odot \ldots \odot a}_{e\text{-krát}}$$

(c) **Diffie-Helmanov protokol výmeny kľúča**

(i) Alica a Bob sa dohodnú na veľkom prvočísle p a čísle a, ktoré je primitívnym prvkom grupy $\mathbb{Z}_p^*$. Čísla p a a nemusia byť tajné, sú verejné.

(ii) Alica si zvolí tajné číslo $x \in \mathbb{Z}_p^*$ a Bobovi pošle číslo $X = a^x \pmod p$.

(iii) Bob si zvolí tajné číslo $y \in \mathbb{Z}_p^*$ a Alici pošle číslo $Y = a^y \pmod p$.

(iv) Alica si vypočíta $k_1 = Y^x = a^{yx}| ! \pmod p$, Bob si vypočíta $k_2 = X^y = a^{xy} \pmod p$. Samozrejme platí $k_1 = k_2$.

(v) Číslo $k = k_1 = k_2$ bude **spoločným tajným kľúčom** Alice a Boba.

(d) Ak útočník odpočúva kompletne celú komunikáciu Alice a Boba, viď predošlý bod, tak pozná čísla p, a, $X = a^x \pmod p$ a $Y = a^y \pmod p$. Na to, aby vedel určiť tajný kľúč, by musel vedieť vyriešiť problém diskrétneho logaritmu, viď bod (b), čo je časovo veľmi náročná úloha. Pri správnej voľbe parametrov zo strany Alice a Boba, je určenie tajného kľúča pre útočníka v praxi nerealizovateľné.

4 body ♣

1. Vypočítajte hodnoty $J\left(\frac{86}{29}\right)$, $J\left(\frac{3k-1}{k}\right)$, kde $k \pmod 4 = 1$.

Riešenie: Nech $m \geq 3$, $n \geq 3$ sú nepárne celé čísla a $a, b \in \mathbb{Z}$. Pri riešení tejto úlohy budeme využívať nasledujúce vzťahy pre Jacobiho symbol

$$J\left(\frac{1}{n}\right) = 1 \tag{1}$$

$$J\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \tag{2}$$

$$J\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \tag{3}$$

$$J\left(\frac{ab}{n}\right) = J\left(\frac{a}{n}\right) \cdot J\left(\frac{b}{n}\right) \tag{4}$$

$$J\left(\frac{a}{n}\right) = J\left(\frac{b}{n}\right), \quad \text{ak} \quad a \equiv b \pmod n \tag{5}$$

$$J\left(\frac{m}{n}\right) = J\left(\frac{n}{m}\right) \cdot (-1)^{\frac{(m-1)(n-1)}{4}} \tag{6}$$

▷ $J\left(\frac{86}{29}\right) \overset{(5)}{=} J\left(\frac{28}{29}\right) \overset{(4)}{=} J\left(\frac{4}{29}\right) \cdot J\left(\frac{7}{29}\right) \overset{(4,3,6,5)}{=} J\left(\frac{1}{7}\right) \overset{(1)}{=} 1$

▷ $J\left(\frac{3k-1}{k}\right) \overset{(5)}{=} J\left(\frac{-1}{k}\right) \overset{(2)}{=} (-1)^{\frac{k-1}{2}}$

Podľa zadania je $k \pmod 4 = 1$. To znamená, že $k = 4m + 1$ pre nejaké $m \in \mathbb{N}$. Potom ale

$$\frac{k-1}{2} = \frac{4m+1-1}{2} = 2m\,, \quad \text{čo je párne číslo.}$$

Preto

$$J\left(\frac{3k-1}{k}\right) = (-1)^{\frac{k-1}{2}} = (-1)^{2m} = 1\,.$$

8 bodov ♢

2. Pomocou Gordonovho / Hellman-Bachovho algoritmu nájdite silné, aspoň 12 bitové, prvočíslo. Na testovanie prvočíselnosti čísel môžete použiť ľubovoľnú metódu. Pre čísla väčšie než 9 999 doporučujeme použiť Rabin-Millerov test.
Pomôcka: ako východzie prvočísla si zvoľte $s = 61$ a $t = 83$.

Riešenie: Gordonov, resp. Hellman-Bachov algoritmus na generovanie silných prvočísel sa dá zapísať nasledovným pseudokódom

---

Gordonov algoritmus generovania silného prvočísla

VSTUP: Požadovaný počet bitov b silného prvočísla p.
VÝSTUP: Silné prvočíslo p.

---

vygenerujme dve prvočísla s a t približne rovnakej bitovej dĺžky. ;
`%` postačujúca bitová dĺžka je viac než $\frac{b}{3}$ a najviac $\frac{b}{2}$.
`%` Prvočíselnosť s a t testujeme Rabin-Millerovým testom.
$i = 1$;
repeat
  $q = 2it + 1$;
  `%` To, či je q prvočíslo, testujeme Rabin-Millerovým testom. $i = i + 1$;
until q *nie je prvočíslo*;
$p_0 = 2\big(s^{q-2} \pmod q\big)s - 1$;
$i = 0$;
repeat
  $p = p_0 + 2iqs$;
  `%` To, či je p prvočíslo, testujeme Rabin-Millerovým testom.
  $i = i + 1$;
until p *nie je prvočíslo*;
vráť „p je silné prvočíslo s aspoň b bitmi.“;

V našom príklade je $b = 12$, $s = 61$ a $t = 83$. Tieto hodnoty sú dané v zadaní, a preto nie je potrebné overovať, že s a t sú prvočísla.
V prvom **repeat** cykle hľadáme najmenšie také číslo q, ktoré je prvočíslom. Nájdeme ho veľmi rýchlo, pretože uz pre $i = 1$ dostaneme $q = 167$, čo je prvočíslo. Keďže $\sqrt{167} \approx 12.9$, môžeme vykonať skúšku prvočíselnosti delením. Stačí overiť, že 167 nie je deliteľné žiadnym z prvočísel $\{2, 3, 5, 7, 11\}$.
Potom vypočítame hodnotu p_0

$$p_0 = 2\left(61^{165} \pmod{167}\right) 61 - 1 = 2.115.61 - 1 = 14029$$

Na výpočet $61^{165} \pmod{167}$ použijeme squaring algoritmus. Platí $165_{10} = 10100101_2$ a výpočet squaring algoritmom je uvedený v nasledujúcej tabuľke.

(mod 167)								
i	7	6	5	4	3	2	1	0
b_i	1	0	1	0	0	1	0	1
s	61	47	147	66	14	99	115	115

Pre číslo $p_0 = 14029$ platí $\sqrt{14029} \approx 118.4$. Jeho prvočíselnosť je preto ešte reálne overovať aj skúšaním. Stačilo by overiť, že nie je deliteľné žiadnym z prvých 30 prvočísel

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113\}$.

Alebo môžeme použiť na testovanie jeho prvočíselnosti Rabin-Millerov test, ktorého algoritmus má pseudokód

Rabin-Millerov test

VSTUP: nepárne číslo p, pre ktoré $p - 1 = 2^k m$, kde m je nepárne
VÝSTUP: číslo p „JE“ / „NIE JE“ prvočíslo

zvoľme $a \in \mathbb{Z}_p^* : \ 2 \leq a \leq p - 2$;
$b = a^m \pmod p$;
if $b \neq 1 \pmod p \ \wedge \ b \neq -1 \pmod p$ **then**
  $i = 1$;
  while $i \leq (k - 1) \ \wedge \ b \neq -1 \pmod p$ **do**
    $b = b^2 \pmod p$;
    if $b = 1 \pmod p$ **then**
      vráť „p NIE JE prvočíslo.“;
    end
    $i = i + 1$;
  end
  if $b \neq -1 \pmod p$ **then**
    vráť „p NIE JE prvočíslo.“;
  end
end
vráť „p JE prvočíslo.“;

Pre $p = 14029$ platí

$$14029 - 1 = 14028 = 2^2.3507 \quad \Rightarrow \quad k = 2 \ \text{a} \ m = 3507\,.$$

Potom ak si zvolíme $a = 3$, tak

$$b = 3^{3507} \pmod{14029} = 14028 \equiv -1 \pmod{14029}$$

uvedenú hodnotu vypočítame pomocou squaring algoritmu $\left(3507_{10} = 110110110011_2\right)$ a Rabin-Millerov test nám hneď v prvom kroku vráti odpoveď „p JE prvočíslo“. Rovnako aj pre $a \in \{5, 7, 11, 17, 19\}$ nám Rabin-Millerov test vráti odpoveď „p JE prvočíslo“ hneď v prvom kroku.
Rabin-Millerov test je pravdepodobnostný, s pravdepodobnosťou chyby približne 25 %. Takže kladná odpoveď ešte nemusí znamenať, že testované p je skutočne prvočíslo. Avšak na úspešné vyriešenie úlohy stačí spraviť Rabin-Millerov test pre jedno a. V našom prípade $\log_2 14029 \approx 13.8$ a číslo $p = 14029$ skutočne **je** prvočíslo. Takže je to viac než 12-bitové **silné prvočíslo**.

10 bodov ♢

3. Majme grupu eliptickej krivky nad $\mathbb{Z}_{13}$ danú rovnicou $y^2 = x^3 + x + 7$.
   (a) **(4b)** Nájdite, okrem neutrálneho prvku, dva rôzne body P a $Q \neq -P$ tejto krivky.
   (b) **(4b)** S bodmi P a Q vykonajte na danej krivke operácie $P + P$ a $P - Q$.
   (c) **(2b)** Ako spoznáte, že výsledok sčitovania je neutrálny prvok?

Riešenie:

(a) V rovnici $y^2 \equiv x^3 + ax + b \pmod p$ máme koeficienty $a = 1$, $b = 7$ a $p = 13$. Keďže pre tieto koeficienty platí $4a^3 + 27b^2 \not\equiv 0 \pmod p$, jedná sa skutočne o eliptickú krivku.

V našom prípade $13 \not\equiv 3 \pmod 4$, a preto nemôžeme použiť jednoduchý algoritmus generovania bodov danej eliptickej krivky. Body na krivke musíme hľadať skúšaním. Množina $\mathbb{Z}_{13} \times \mathbb{Z}_{13}$ má 169 bodov a ich dosadením do rovnice eliptickej krivky, nájdeme tie, ktoré na krivke ležia. Je to nasledovných 12 bodov

$$\mathcal{E} = \{(1,3),(1,10),(2,2),(2,11),(4,6),(4,7),(9,2),(9,11),(10,4),(10,9),(11,6),(11,7)\}$$

Spomedzi týchto bodov si vyberieme dva, vyhovujúce zadaniu. Môžu to byť napríklad body $P = (1,3)$ a $Q = (2,2)$.

(b) Súčet bodov na eliptickej krivke $\mathcal{E}$ je definovaný takto

- ▷ všetky výpočty sa robia v $\mathbb{Z}_p^*$, t. j. $\pmod p$,
- ▷ body $P = (x_1, y_1)$ a $Q = (x_2, y_2)$ ležia na eliptickej krivke $\mathcal{E}$,
- ▷ pre $\forall P \in \mathcal{E}$ platí $P + \mathcal{O} = \mathcal{O} + P = P$,
- ▷ ak $x_2 = x_1$ a $y_2 = -y_1$, tak $P + Q = \mathcal{O}$,
- ▷ inak $P + Q = (x_3, y_3)$, kde

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \text{a} \qquad y_3 = \lambda(x_1 - x_3) - y_1\,,$$

pričom

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}\,, & \text{ak } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}\,, & \text{ak } P = Q\,. \end{cases}$$

Na eliptickej krivke zo zadania si teda zvolíme nejaký bod rôzny od bodu v nekonečne. Napr. $P = (1,3)$, ako v časti (a). Teraz podľa pravidiel pre súčet bodov na eliptickej krivke, vypočítame bod $P + P$. Kompletná (okrem bodu $\mathcal{O}$) súčtová tabuľka bodov eliptickej krivky zo zadania úlohy, je tabuľka 1 na strane 10. Pre bod $P = (1,3)$ platí

$$P + P = (10,4) \quad \text{a označme si tento bod} \quad Q = (10,4)\,.$$

Vidíme teda, že druhý bod eliptickej krivky, rôzny od bodu v nekonečne a bodu P, nemusíme zvlášť hľadať, ale pokiaľ $P + P \neq \mathcal{O}$, môžeme vziať $Q = P + P$. Teraz ešte vypočítame súčet $P - Q$. Odčítanie na eliptickej krivke sa realizuje ako *pričítanie inverzného prvku*. V našom prípade $-Q = (10,9)$, takže

$$P - Q = (1,3) + (10,9) = (1,10)\,.$$

- Podľa pravidla na sčítanie dvoch bodov eliptickej krivky z časti (b) to spoznáme tak, že súradnice sčítavaných bodov sú $P = (x,y)$ a $Q = (x,-y)$. Samozrejme hodnotu $-y$ treba chápať na $\mathbb{Z}_p^*$.

$+$	$(1,3)$	$(1,10)$	$(2,2)$	$(2,11)$	$(4,6)$	$(4,7)$	$(9,2)$	$(9,11)$	$(10,4)$	$(10,9)$	$(11,6)$	$(11,7)$
$(1,3)$	$(10,4)$	$\mathcal{O}$	$(11,7)$	$(9,11)$	$(9,2)$	$(4,6)$	$(2,2)$	$(4,7)$	$(11,6)$	$(1,10)$	$(2,11)$	$(10,9)$
$(1,10)$	$\mathcal{O}$	$(10,9)$	$(9,2)$	$(11,6)$	$(4,7)$	$(9,11)$	$(4,6)$	$(2,11)$	$(1,3)$	$(11,7)$	$(10,4)$	$(2,2)$
$(2,2)$	$(11,7)$	$(9,2)$	$(9,11)$	$\mathcal{O}$	$(11,6)$	$(10,4)$	$(2,11)$	$(1,3)$	$(10,9)$	$(4,6)$	$(1,10)$	$(4,7)$
$(2,11)$	$(9,11)$	$(11,6)$	$\mathcal{O}$	$(9,2)$	$(10,9)$	$(11,7)$	$(1,10)$	$(2,2)$	$(4,7)$	$(10,4)$	$(4,6)$	$(1,3)$
$(4,6)$	$(9,2)$	$(4,7)$	$(11,6)$	$(10,9)$	$(1,3)$	$\mathcal{O}$	$(10,4)$	$(1,10)$	$(2,2)$	$(9,11)$	$(11,7)$	$(2,11)$
$(4,7)$	$(4,6)$	$(9,11)$	$(10,4)$	$(11,7)$	$\mathcal{O}$	$(1,10)$	$(1,3)$	$(10,9)$	$(9,2)$	$(2,11)$	$(2,2)$	$(11,6)$
$(9,2)$	$(2,2)$	$(4,6)$	$(2,11)$	$(1,10)$	$(10,4)$	$(1,3)$	$(11,6)$	$\mathcal{O}$	$(11,7)$	$(4,7)$	$(10,9)$	$(9,11)$
$(9,11)$	$(4,7)$	$(2,11)$	$(1,3)$	$(2,2)$	$(1,10)$	$(10,9)$	$\mathcal{O}$	$(11,7)$	$(4,6)$	$(11,6)$	$(9,2)$	$(10,4)$
$(10,4)$	$(11,6)$	$(1,3)$	$(10,9)$	$(4,7)$	$(2,2)$	$(9,2)$	$(11,7)$	$(4,6)$	$(2,11)$	$\mathcal{O}$	$(9,11)$	$(1,10)$
$(10,9)$	$(1,10)$	$(11,7)$	$(4,6)$	$(10,4)$	$(9,11)$	$(2,11)$	$(4,7)$	$(11,6)$	$\mathcal{O}$	$(2,2)$	$(1,3)$	$(9,2)$
$(11,6)$	$(2,11)$	$(10,4)$	$(1,10)$	$(4,6)$	$(11,7)$	$(2,2)$	$(10,9)$	$(9,2)$	$(9,11)$	$(1,3)$	$(4,7)$	$\mathcal{O}$
$(11,7)$	$(10,9)$	$(2,2)$	$(4,7)$	$(1,3)$	$(2,11)$	$(11,6)$	$(9,11)$	$(10,4)$	$(1,10)$	$(9,2)$	$\mathcal{O}$	$(4,6)$

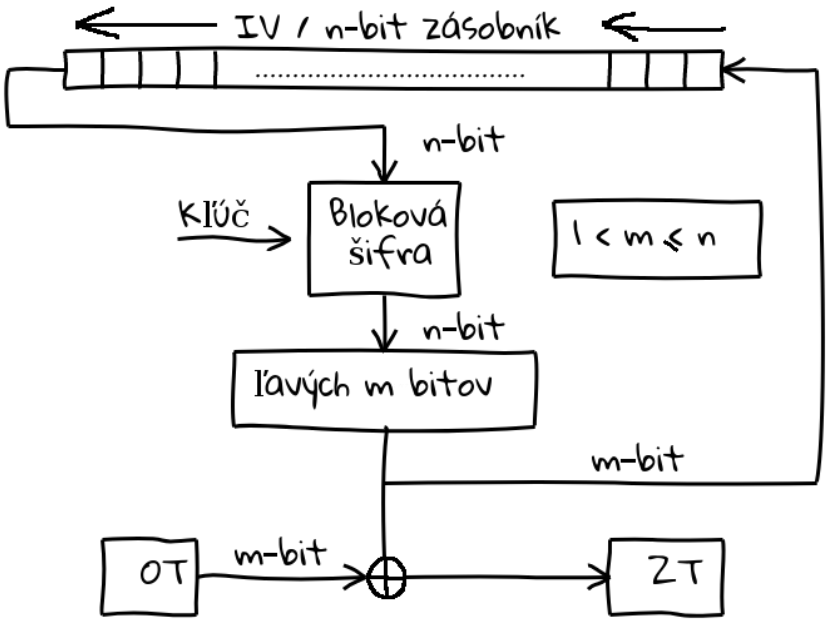
Tabuľka 1: Súčtová tabuľka eliptickej krivky $y^2 = x^3 + x + 7$ na $\mathbb{Z}_{13}$

12 bodov ♡

4. Uvažujme dvojkolovú feistalovskú šifru s veľkosťou bloku 6 bitov. V šifre sa používa funkcia $f : \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to \mathbb{Z}_2^3,\ f(\mathbf{x}, \mathbf{K}) = \mathbf{x} \oplus \mathbf{K}$.
   (a) **(8b)** Pomocou takto definovanej šifry zašifrujte správu 101 101 101 101 v móde OFB. Použite podkľúče $\mathbf{K_1} = 001$, $\mathbf{K_2} = 010$ a inicializačný vektor 111 111.
   (b) **(4b)** Zašifrovanú správu z predošlej časti následne dešifrujte.

Riešenie:

(a) Šifrovanie v OFB móde je schématicky znázornené na obrázku 1.



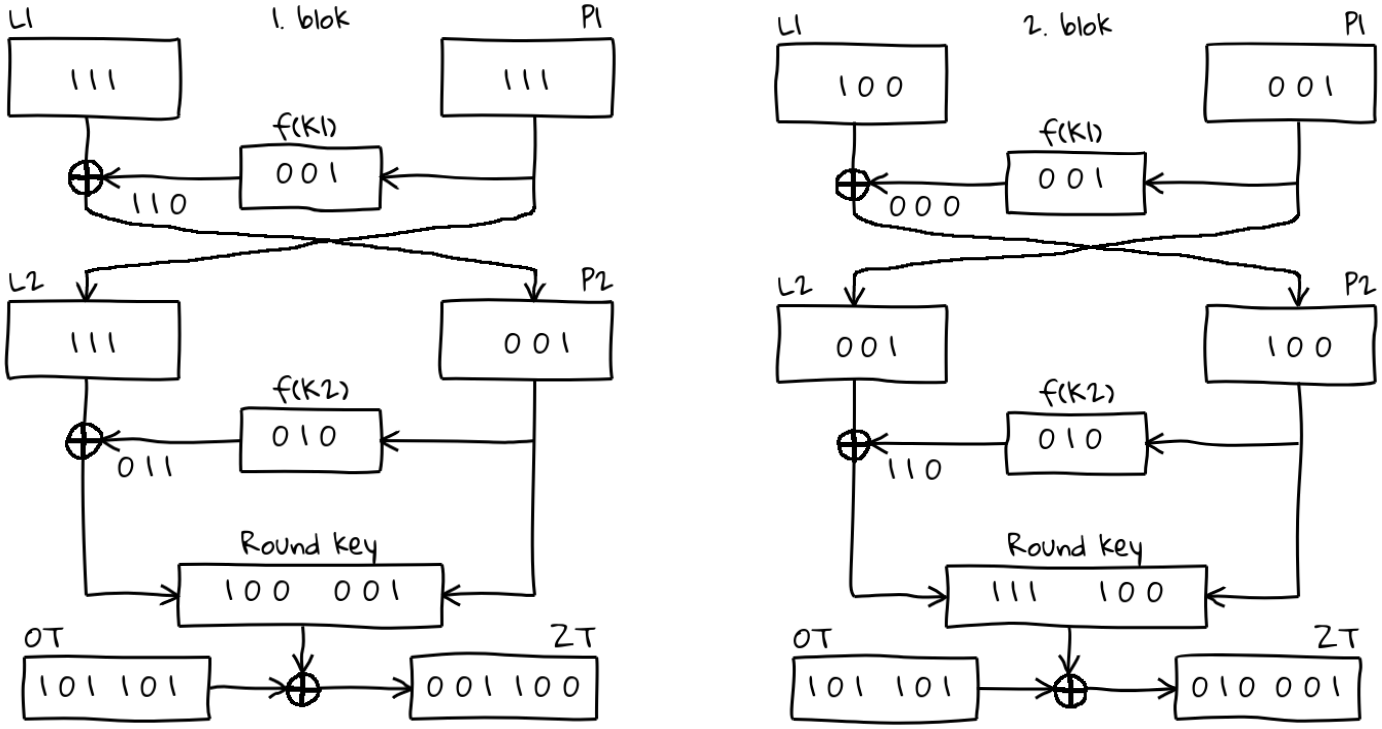
Obr. 1: Šifrovanie v OFB móde

Bloková šifra v predošlej schéme je realizovaná pomocou dvojkolovej feistalovej šifry. Šifrovanie správy zo zadania je znázornené na obrázku 2. Správa má dva 6-bitové bloky a

$$\mathrm{OT}_1 = (1\,0\,1\ 1\,0\,1) \qquad \text{sa zašifruje na} \qquad \mathrm{ZT}_1 = (0\,0\,1\ 1\,0\,0)$$

$$\mathrm{OT}_2 = (1\,0\,1\ 1\,0\,1) \qquad \text{sa zašifruje na} \qquad \mathrm{ZT}_2 = (0\,1\,0\ 0\,0\,1)\,.$$

(b) Pri OFB móde sa pri šifrovaní aj dešifrovaní používa ten istý algoritmus a kolový kľúč (na obrázku 2 označený ako *„Round key“*) nezávisí ani od OT, ani od ZT. Takže pri dešifrovaní správy stačí na obrázku 2 „prehodiť“ okienka pre OT a ZT v poslednom riadku obrázku.



Obr. 2: Šifrovanie 1. a 2. bloku správy zo zadania úlohy

12 bodov ♡

5. Uvažujme funkciu $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ danú predpisom $f(x_0, x_1, x_2) = x_0 \oplus x_0x_2 \oplus x_1x_2$
   (a) **(2b)** Určte, či je funkcia f balansovaná.
   (b) **(5b)** Vypočítajte nelinearitu, t. j. stupeň nelinearity, funkcie f.
   (c) **(5b)** Zistite, či je funkcia f úplná a či spĺňa SAC kritérium.

Riešenie:

(a) Tabuľka 2 zobrazuje pravdivostné hodnoty danej funkcie a aj všetky pomocné výpočty k nej.

	x_0	x_1	x_2	$f(\vec{x}_i)$	$s_0(\vec{x}_i)$	$s_1(\vec{x}_i)$	$s_2(\vec{x}_i)$	$\hat{f}(\vec{x}_i)$
$\vec{x}_0 =$	(0	0	0)	0	1	0	0	0
$\vec{x}_1 =$	(1	0	0)	1	1	0	1	4
$\vec{x}_2 =$	(0	1	0)	0	1	0	1	4
$\vec{x}_3 =$	(1	1	0)	1	1	0	0	0
$\vec{x}_4 =$	(0	0	1)	0	0	1	0	0
$\vec{x}_5 =$	(1	0	1)	0	0	1	1	4
$\vec{x}_6 =$	(0	1	1)	1	0	1	1	−4
$\vec{x}_7 =$	(1	1	1)	1	0	1	0	0

Tabuľka 2: Tabuľka k 5. príkladu

Z tabuľky 2 ihneď vidno, že funkcia f je balansovaná, pretože 0 a 1 nadobúda s rovnakou pravdepodobnosťou (má 4 nuly a 4 jednotky).

(b) Nelinearitu (stupeň nelinearity) boolovskej funkcie zistíme pomocou Walsh-Hadamardovej transformácie $\hat{f}(\vec{x}_i)$. Jej hodnoty, pre danú funkciu, máme v poslednom stĺpci tabuľky 2. Nelinearita boolovskej funkcie je potom:

$$N_f = \min_{\forall \vec{x}_i \in Z_2^3} \left\{ 2^{n-1} \pm \frac{\hat{f}(\vec{x}_i)}{2} \right\},$$

čiže v našom prípade $N_f = 2$.

(c) Označme si $\vec{c}_i$ vektory zo $\mathbb{Z}_2^3$, ktoré majú hammingovú váhu 1. Čiže $\vec{c}_0 = (1, 0, 0)$, $\vec{c}_1 = (0, 1, 0)$ a $\vec{c}_2 = (0, 0, 1)$. Ďalej si označme $s_j(\vec{x}_i) = f(\vec{x}_i) \oplus f(\vec{x}_i \oplus \vec{c}_j)$. Podľa definície daná boolovská funkcia spĺňa SAC kritérium, keď platí

$$\text{Pre } \forall c_j : \quad \sum_{\forall \vec{x}_i \in Z_2^3} s_j(\vec{x}_i) = 4$$

Ako vidno z tabuľky 2, v stĺpcoch pre $s_0(\vec{x}_i)$ až $s_2(\vec{x}_i)$ je uvedená podmienka splnená. To znamená, že funkcia f spĺňa SAC kritérium a z toho vyplýva, že musí byť aj úplná. Úplnosť je totiž slabšia podmienka než SAC kritérium. Úplnosť znamená, že funkcia závisí od každej svojej premennej.

14 bodov ♠

6. Zachytili ste správu „19“, o ktorej viete, že bola zašifrovaná RSA algoritmom s verejným kľúčom ($n = 187,\ e = 3$).

(a) **(4b)** Pomocou Fermatovej metódy faktorizujte modul $n = 187$.

(b) **(4b)** Vypočítajte najmenší možný dešifrovací exponent.

(c) **(6b)** Dešifrujte správu „19“ pomocou algoritmu rýchleho dešifrovania.

Dôkladne popíšte svoj postup.

Riešenie:

(a) Fermatova faktorizačná metóda funguje pomerne rýchlo len vtedy, ak číslo n má faktor blízky ku $\sqrt{n}$.

Fermatova faktorizačná metóda

VSTUP: n – nepárne číslo

$x \leftarrow \lceil \sqrt{n} \rceil$;

$y \leftarrow \sqrt{x^2 - n}$;

while *(y nie je celé číslo)* **do**
  if $(x + y < n)$ **then**
    $x \leftarrow x + 1$;
    $y \leftarrow \sqrt{x^2 - n}$;
  else
    Stop;
  end
end

if *(y je celé číslo)* **then**
  $p = x - y$;
end

VÝSTUP: p je faktor n

Pre $n = 187$ dostaneme faktorizáciu $p = 11$ a $q = 17$ už po prvom kroku algoritmu.

(b) V RSA algoritme je dešifrovací exponent d číslo, pre ktoré platí $e.d \equiv 1 \pmod{\varphi(n)}$ alebo, ak chceme dosiahnuť najmenší možný dešifrovací exponent, použijeme namiesto Eulerovej Carmichaelovu funkciu $e.d \equiv 1 \pmod{\lambda(n)}$. Pre $n = 187$ máme $\lambda(187) = \mathrm{LCM}\,(10, 16) = 80$ a $e = 3$. Takže $3.d \equiv 1 (\mathrm{mod}\ 80) \ \Rightarrow\ d = 27$.
Pri použití Eulerovej funkcie by sme dostali $\varphi(187) = 160$ a $d = 107$.

(c) Pri dešifrovaní v RSA sa pôvodná zpráva vypočíta ako $x = y^d \pmod{n}$. Pre hodnoty zo zadania je to $x = 19^{27} \pmod{187}$. Pomocou algoritmu rýchleho dešifrovania, pre $p = 11$, $q = 17$, $y = 19$, $n = 187$ a $d = 27$, vyzerá výpočet nasledovne

- $\diamond$ $d_1 = 27 \pmod{10} = 7$
- $\diamond$ $d_2 = 27 \pmod{16} = 11$
- $\diamond$ $y_1 = 19 \pmod{11} = 8$
- $\diamond$ $y_2 = 19 \pmod{17} = 2$
- $\diamond$ $x_1 = 8^7 \pmod{11} = 2$
- $\diamond$ $x_2 = 2^{11} \pmod{17} = 8$
- $\diamond$ $u = 17^{-1}$ v $\mathbb{Z}_{11} = 2$
- $\diamond$ $v = 11^{-1}$ v $\mathbb{Z}_{17} = 14$

Napokon

$$x = (x_1.u.q + x_2.v.p) \pmod{n} \quad \text{čiže} \quad x = (2.2.17 + 8.14.11) \pmod{187} = 178\,.$$

Pôvodná zpráva bola $y =$ `178`.