8 bodov ♣

1. Pomocou Gordonovho / Hellman-Bachovho algoritmu nájdite silné, aspoň 16 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 $s = 103$ a $t = 179$.

Riešenie: Gordonov, resp. Hellman-achov 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*;
$p_0 = 2\left(s^{q-2} \pmod q\right)s - 1$;
$i = 0$;
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 $b = 16$, $s = 103$ a $t = 179$. 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 $q = 359$, čo je prvočíslo. Keďže $\sqrt{359} \approx 18.9$, môžeme vykonať skúšku prvočíselnosti delením. Stačí overiť, že 359 nie je deliteľné žiadnym z prvočísel $\{2, 3, 5, 7, 11, 13, 17\}$.
Potom vypočítame hodnotu p_0

$$p_0 = 2\left(103^{357} \pmod{359}\right)103 - 1 = 2.122.103 - 1 = 25131$$

Na výpočet $103^{357} \pmod{359}$ použijeme squaring algoritmus. Platí $357_{10} = 101100101_2$ a výpočet squaring algoritmom je uvedený v nasledujúcej tabuľke.

$(\bmod 359)$									
i	8	7	6	5	4	3	2	1	0
b_i	1	0	1	1	0	0	1	0	1
s	103	198	339	274	45	230	157	237	122

Číslo $p_0 = 25131$ nie je prvočíslom, pretože jeho cifený súčet je 12, a teda je deliteľné číslom 3. V druhom **repeat** cykle budeme hľadať najmenšie číslo p, ktoré je prvočíslom. Pre $i = 1$ máme $p = 99085$, čo nie je prvočíslo, pretože je deliteľné číslom 5. Pre $i = 2$ dostávame $p = 173039$. Je to číslo príliš veľké na overovanie prvočíselnosti delením, pretože $\sqrt{173039} \approx 415.9$. Na testovanie prvočíselnosti preto použijeme 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 $a \in \mathbb{Z}_p^* : \ 2 \le a \le p - 2$;

$b = a^m \pmod{p}$;

if $b \neq 1 \pmod{p} \ \wedge \ b \neq -1 \pmod{p}$ **then**

  $i = 1$;

  while $i \le (k - 1) \ \wedge \ b \neq -1 \pmod{p}$ **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 $p = 173039$ platí

$$173039 - 1 = 173038 = 2^1.86519 \quad \Rightarrow \quad k = 1 \ \text{a} \ m = 86519\,.$$

Potom ak si zvolíme $a = 3$, tak

$$b = 3^{86519} \pmod{173039} = 1$$

uvedenú hodnotu vypočítame pomocou squaring algoritmu $\left(86519_{10} = 10101000111110111_2\right)$ a Rabin-Millerov test nám hneď v prvom kroku vráti odpoveď „p JE prvočíslo“. Rovnako aj pre $a \in \{5, 7, 11, 13, 17\}$ nám Rabin-Millerov test vráti odpoveď „p JE prvočíslo“ hneď v prvom kroku. Pre $a = 11$ bude $b = 173038$ $(= -1)$ a vo zvyšných prípadoch bude $b = 1$.

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-Milleor test pre jedno a. V našom prípade $\log_2 173019 \approx 17.4$ a číslo $p = 173039$ skutočne **je** prvočíslo a okrem toho je to aj 18-bitové **silné prvočílo**.

Bodovanie ★

- Za znalosť a správne použitie Gordonovho algoritmu na hľadanie silného prvočísla sú **3 body**.
- Za správny numerický výpočet kandidáta na prvočíslo p je **1 bod**.
- Za znalosť a správne použitie Rabin-Millerovho testu prvočíselnosti sú **3 body**.
- Za numerickú realizáciu Rabin-Millerovho testu pri ľubovoľnej báze a je **1 bod**.

10 bodov ♢

2. Zachytili sme správu „2229“, o ktorej vieme, že je zašifrovaná RSA algoritmom s verejným kľúčom ($n = 8633,\ e = 7$).

(a) **(2b)** Faktorizujte modul $n = 8633$.

(b) **(2b)** Vypočítajte dešifrovací exponent (použite Carmichaelovu funkciu λ).

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

Riešenie:

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

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 $n = 8633$ dostaneme faktorizáciu $p = 89$ a $q = 97$ už po prvom kroku algoritmu.

(b) V RSA algoritme je dešifrovací exponent d číslo, pre ktoré platí $e.d \equiv 1 \pmod{\varphi(n)}$. Namiesto Eulerovej funkcie môžeme použiť Carmichaelovu funkciu a dostaneme často výrazne menší dešifrovací exponent. Budeme preto hľadať také d, pre ktoré platí $e.d \equiv 1 \pmod{\lambda(n)}$. Pre $n = 8633$ máme $\lambda(8633) = \operatorname{lcm}\big((89-1)(97-1)\big) = 1056$ a $e = 7$. Takže

$$7.d \equiv 1 \pmod{1056} \ \Rightarrow\ d = 151\,.$$

Ak by sme použili Eulerovu funkciu, tak by sme dostali $d' = 1207$.

(c) Pri dešifrovaní v RSA sa pôvodná zpráva vypočíta ako $x = y^d \pmod{n}$. Pre hodnoty zo zadania je to $x = 2229^{151} \pmod{8633}$. Pomocou algoritmu rýchleho dešifrovania, pre $p = 89$, $q = 97$, $y = 2229$, $n = 8633$ a $d = 151$, vyzerá výpočet nasledovne

- $d_1 = 151 \,(\text{mod } 88) = 63$
- $d_2 = 151 \,(\text{mod } 96) = 55$
- $y_1 = 2229 \,(\text{mod } 89) = 4$
- $y_2 = 2229 \,(\text{mod } 97) = 95$
- $x_1 = 4^{63} \,(\text{mod } 89) = 32$
- $x_2 = 95^{55} \,(\text{mod } 97) = 66$
- $u = 97^{-1}$ v $\mathbb{Z}_{89} = 78$
- $v = 89^{-1}$ v $\mathbb{Z}_{97} = 12$

Napokon

$$x = (x_1.u.q + x_2.v.p) \pmod{n} \quad \text{čiže} \quad x = (32.78.97 + 66.12.89) \pmod{8633} = 1812\,.$$

Pôvodná zpráva bola $x = 1812$.

Bodovanie

- Pri faktorizácii je **1 bod** za algoritmus a **1 bod** za správny výpočet.
- Za správny postup pri výpočte dešifrovacieho exponentu (jedno či pomocou Eulerovej alebo Carmichaelovej funkcie) je **1 bod**. Ak bola pri výpočte dešifrovacieho exponentu použita Carmichaelova funkcia a výsledok je správny, tak je za to ďalší **1 bod**.
- Za správny predpis pre výpočet hodnôt $d_1, d_2, y_1, y_2, x_1, x_2, u, v, x$ je **5 bodov**. Za správny numerický výpočet je **1 bod**.

12 bodov

3. Zachytili sme správu zašifrovanú El-Gamalovou šifrou s verejným kľúčom $(23, 5, 22)$ (prvočíslo $p = 23$, generátor $\mathbb{Z}_p^*$ je $a = 5$ a číslo $c = a^b \pmod p = 22$). Zachytená správa je `((T,A),(Y,P),(U,R),(X,C))`. Znaky správy sú kódované podľa nasledovnej tabuľky

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	U	V	X	Y	Z

Rozlúštite zachytenú správu.

Riešenie: Lúštenie správy zašifrovanej El-Gamalovým kryptosystémom pozostáva z nájdenia súkromného kľúča, ktorým je číslo b. Ak získame súkromný kľúč, tak správu už len dešifrujeme podľa predpisu

$$x = y_2 \left(y_1^b\right)^{-1} \pmod p,$$

kde (y_1, y_2) je ZT zodpovedajúce znaku x OT. V danom prípade máme $5^b = 22 \pmod{23}$. Nájdenie čísla b teda zodpovedá vyriešeniu problému diskrétneho logaritmu $b = \log_5 22 \pmod{23}$. vzhľadom na malé hodnoty (číslo 23) vieme tento logaritmus nájsť pomocou tabuľky. Alebo ak poznáme tvrdenie

Nech p je nepárne prvočíslo, $\mathbb{Z}_p^*$ multiplikatívna grupa a $a \in \mathbb{Z}_p$ jej generátor. Potom

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

tak hneď vieme, že $b = 11$. Teraz, keď už poznáme b, stačí previesť znaky na čísla podľa kódovej tabuľky a dešifrovať text. Postup je uvedený v nasledujúcej tabuľke. Všetky výpočty v tabuľke sú robené $\pmod{23}$.

ZT $= (y_1, y_2)$	y_1^b	$\left(y_1^b\right)^{-1}$	$y_2 \left(y_1^b\right)^{-1}$	OT
`(T,A)`$=(17, 1)$	22	22	22	`Z`
`(Y,P)`$=(21, 14)$	22	22	9	`K`
`(U,R)`$=(18, 15)$	1	1	15	`R`
`(X,C)`$=(20, 2)$	22	22	21	`Y`

Bodovanie

- Za popis El-Gamalovho kryptosystému, najmä predpis na dešifrovania správy v ňom, je **6 bodov**.
- Za správny výpočet diskrétneho logaritmu (hodnota b), akýmkoľvek spôsobom, sú **2 body**.
- Za každý správne dešifrovaný znak OT je **1 bod**.

12 bodov ♠

4. Majme grupu eliptickej krivky nad $\mathbb{Z}_{11}$ danú rovnicou $y^2 = x^3 + 2x + 5$.
   (a) **(4b)** Nájdite, okrem neutrálneho prvku, dva rôzne body P a $Q \neq -P$ tejto krivky.
   (b) **(4b)** S bodmi P, Q vykonajte nasledujúce operácie na krivke $P+P$, $P+Q$ a $P-Q$.
   (c) **(4b)** Ako spoznáte, že výsledok sčitovania je neutrálny prvok?

Riešenie:

(a) V rovnici $y^2 = x^3 + ax + b \pmod p$ máme koeficienty $a = 2$, $b = 5$ a $p = 11$. Keďže pre tieto koeficienty platí $4a^3 + 27b^2 \neq 0 \pmod p$, jedná sa skutočne o eliptickú krivku.

Množina $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$ má 121 bodov a ich dosadením do rovnice eliptickej krivky, nájdeme tie, ktoré na krivke ležia. Je to nasledovných 9 bodov

$$\mathcal{E} = \{(0,4), (0,7), (3,4), (3,7), (4,0), (8,4), (8,7), (9,2), (9,9)\}$$

Keďže v tejto úlohe $p = 11$ a platí $p = 3 \pmod 4$, môžeme na generovanie bodov ležiacich na eliptickej krivke použiť algoritmus z prednášok.

Algoritmus hľadania bodov eliptickej krivky

VSTUP: prvočíslo p, pre ktoré platí $p \equiv 3 \pmod 4$ a čísla $a, b \in \mathbb{Z}_p^*$
VÝSTUP: $\mathcal{E}$ – množina bodov eliptickej krivky

$\mathcal{E} = \{\mathcal{O}\}$;
for $x = 0, \ldots, p-1$ **do**
  $z = x^3 + ax + b \pmod p$;
  if $\left(z^{\frac{p+1}{4}}\right)^2 \equiv z \pmod p$ **then**
    $\mathcal{E} = \mathcal{E} \cup \left\{\left(x, z^{\frac{p+1}{4}}\right), \left(x, -z^{\frac{p+1}{4}}\right)\right\}$;
  end
end

Spomedzi týchto bodov si vyberieme dva, vyhovujúce zadaniu. Môžu to byť napríklad body $P = (3,4)$ a $Q = (8,4)$.

(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 $\mathcal{E}$,

$+$	$(0,4)$	$(0,7)$	$(3,4)$	$(3,7)$	$(4,0)$	$(8,4)$	$(8,7)$	$(9,2)$	$(9,9)$
$(0,4)$	$(9,2)$	$\mathcal{O}$	$(8,7)$	$(9,9)$	$(8,4)$	$(3,7)$	$(4,0)$	$(3,4)$	$(0,7)$
$(0,7)$	$\mathcal{O}$	$(9,9)$	$(9,2)$	$(8,4)$	$(8,7)$	$(4,0)$	$(3,4)$	$(0,4)$	$(3,7)$
$(3,4)$	$(8,7)$	$(9,2)$	$(8,4)$	$\mathcal{O}$	$(9,9)$	$(0,7)$	$(3,7)$	$(4,0)$	$(0,4)$
$(3,7)$	$(9,9)$	$(8,4)$	$\mathcal{O}$	$(8,7)$	$(9,2)$	$(3,4)$	$(0,4)$	$(0,7)$	$(4,0)$
$(4,0)$	$(8,4)$	$(8,7)$	$(9,9)$	$(9,2)$	$\mathcal{O}$	$(0,4)$	$(0,7)$	$(3,7)$	$(3,4)$
$(8,4)$	$(3,7)$	$(4,0)$	$(0,7)$	$(3,4)$	$(0,4)$	$(9,2)$	$\mathcal{O}$	$(9,9)$	$(8,7)$
$(8,7)$	$(4,0)$	$(3,4)$	$(3,7)$	$(0,4)$	$(0,7)$	$\mathcal{O}$	$(9,9)$	$(8,4)$	$(9,2)$
$(9,2)$	$(3,4)$	$(0,4)$	$(4,0)$	$(0,7)$	$(3,7)$	$(9,9)$	$(8,4)$	$(8,7)$	$\mathcal{O}$
$(9,9)$	$(0,7)$	$(3,7)$	$(0,4)$	$(4,0)$	$(3,4)$	$(8,7)$	$(9,2)$	$\mathcal{O}$	$(8,4)$

Tabuľka 1: Súčtová tabuľka eliptickej krivky $y^2 = x^3 + 2x + 5$ na $\mathbb{Z}_{11}$

- ▷ 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. $P = (3,4)$, 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 **??**. Pre bod $P = (3,4)$ platí

$$P + P = (8,4) \quad \text{a označme si tento bod} \quad Q = (8,4)\,.$$

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 $Q = P + P$. Bod $-Q$ bude taký bod, pre ktorý platí $Q - Q = \mathcal{O}$. To je podľa tabuľky **??** bod $-Q = (8,7)$. Teraz ešte vypočítame súčty $P + Q$ a $P - Q$

$$\begin{aligned} P + Q &= (3,4) + (8,4) = (0,7) \\ P - Q &= (3,4) + (8,7) = (3,7) \end{aligned}$$

(c) 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 $\mathbb{Z}_p$.

Bodovanie

- Za nájdenie bodu P ležiaceho na danej eliptickej krivke sú **2 body**. Za nájdenie bodu $Q \neq -P$, ktorý leží na danej eliptickej krivke sú **2 body**.
- Za správny popis sčítavania dvoch bodov eliptickej krivky a vhodný výber dvoch bodov P a $Q \neq -P$ je **2.5 bodu**. Za správny výpočet každého zo súčtov $P + P$, $P + Q$ a $P - Q$ je **0.5 bodu**.
- Za správne uvedenie toho ako vyzerá inverzný prvok bodu P na eliptickej krivke sú **2 body**. Za správne zdôvodnenie prečo tomu tak je sú **2 body**.

8 bodov

5.

(a) **(2b)** Majme čísla $a = 11$ a kandidáta na prvočíslo $P = 15$. Aký bude výsledok Fermatovho testu čísla P pri báze a? Aký bude výsledok Solovayovho testu čísla P pri báze a?

(b) **(2b)** Majme čísla a a P také, že $\gcd(a, P) = 1$. Vieme, že číslo P prešlo Solovayovým testom prvočíselnosti pri báze a. Prejde aj Fermatovým testom pri báze a?

(c) **(2b)** Definujte problém diskrétneho logaritmu a uveďte príklad.

(d) **(2b)** Uveďte popis zovšeobecného Diffie-Hellmanovho protokolu výmeny kľúčov pre 3 komunikujúce strany. Koľko najmenej krokov (výmen čiastkových kľúčov) bude mať tento proces? Výmeny kľúčov sa uskutočňujú broadcastom, t. j. ak Alica posiela svoj čiastkový kľúč ostatným dvom účastníkom komunikácie, tak to považujeme za 1 krok.

Riešenie:

(a) Najskôr si pripomeňme ako vyzerjú Frematov a Solovayov test prvočíselnosti.

Fermatov test

Ak n je prvočíslo a $a \in \mathbb{Z}_n$ je také číslo, že $\gcd(a, n) = 1$, tak potom $a^{n-1} = 1 \pmod{n}$.

Solovayov test

Ak n je nepárne prvočíslo, tak pre všetky čísla $a \in \mathbb{Z}_n$ platí $J\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$.

V prípade Fermatovho testu máme $11^{14} = 1 \pmod{15}$, takže číslo $P = 15$ prejde Fermatovým testom pri báze $a = 11$. Ale v prípade Solovayovho testu máme

$$J\left(\frac{11}{15}\right) = J\left(\frac{11}{3}\right) J\left(\frac{11}{5}\right) = J\left(\frac{2}{3}\right) J\left(\frac{1}{5}\right) = -1$$

a $11^7 = 11 \pmod{15}$. Takže číslo $P = 15$ neprejde Solovayovým testom pri báze $a = 11$.

(b) Ak máme čísla a a P, pričom $\gcd(a, P) = 1$ a P prešlo Solovayovým testom, tak to znamená, že platí $J\left(\frac{a}{P}\right) = a^{\frac{P-1}{2}} = \pm 1 \pmod{P}$. Ak $\gcd(a, P) = 1$, tak $J\left(\frac{a}{P}\right) \neq 0$. Ale potom platí $\left(J\left(\frac{a}{P}\right)\right)^2 = a^{P-1} = 1 \pmod{P}$, čo znamená, že číslo P prejde aj Fermatovým testom.

(c) 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 také číslo $1 \leq e \leq |G| - 1$, pre ktoré platí

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

(d) Predpokladajme, že tri komunikujúce strany majú mená Alica, Bob a Cyril. Zovšeobecnený Diffie-Hellmanov protokol výmeny kľúča potom bude nasledovný

1) Alica, Bob a Cyril sa dohodnú na veľkom prvočísle p a čísle a, ktoré je primitívnym prvkom grupy $\left(\mathbb{Z}_p^*, \cdot\right)$. Čísla p a a nemusia byť tajné.
2) Alica si zvolí tajné číslo $x \in \mathbb{Z}_p^*$ a broadcastom pošle všetkým číslo $X = a^x \pmod p$.
3) Bob si zvolí tajné číslo $y \in \mathbb{Z}_p^*$ a broadcastom pošle všetkým číslo $Y = a^y \pmod p$.
4) Cyril si zvolí tajné číslo $z \in \mathbb{Z}_p^*$.
5) Alica vypočíta a broadcastom pošle všetkým číslo $XY = a^{xy} \pmod p$.
6) Cyril vypočíta a broadcastom pošle všetkým číslo $YZ = a^{yz} \pmod p$.
7) Cyril vypočíta a broadcastom pošle všetkým číslo $XZ = a^{xz} \pmod p$.
8) Alica, Bob aj Cyril si už v tomto momente vedia vypočítať číslo $k = a^{yxz} \pmod p$. Toto číslo bude *spoločným tajným kľúčom* Alice, Boba a Cyrila.

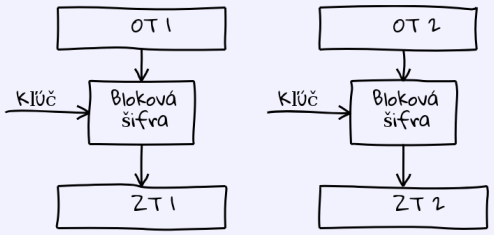
Uvedený protokol má 5 krokov (výmen čiastkových kľúčov) a tento počet je minimálny. Na konci potrebujeme mať čísla XY, YZ, XZ, aby si každý účastník komunikácie vedel vypočítať tajný kľúč. K tomu musíme poznať minimálne dve mocniny s jedným exponentom (Alica a Bob) a následne potrebujeme 3 mocniny s dvoma exponentami (Alica 1 a Cyril 2).

Bodovanie ★

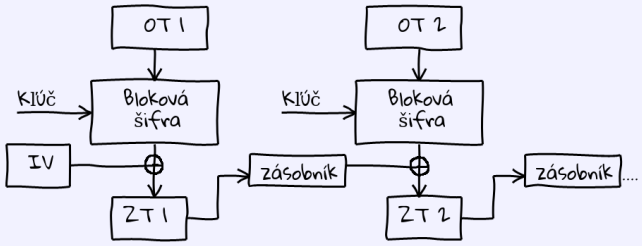
- Za správnu realizáciu Fermatovho testu pre číslo P pri báze a je **1 bod**. Rovnako aj za správnu realizáciu Solovayovho testu pre číslo P pri báze a je **1 bod**.
- Za správne zdôvodnenie toho, že úspešný Solovayov test implikuje úspešný Fermatov test sú **2 body**.
- Za správnu definíciu problému diskrétneho logaritmu sú **2 body**.
- Za zovšeobecnenie Diffie-Hellmanovho protokolu je **1 bod**. Pokiaľ nebude mať toto zovšeobecnenie viac než 5 krokov, tak je za to ďalší **1 bod**.

bonus 5 bodov ♠

6. Na nasledujúcich dvoch obrázkoch sú schématicky zobrazené dva šifrovacie módy blokových šifier. Porovnajte tieto dva módy z hľadiska ich bezpečnosti. Predpokladáme, že útočník pozná IV aj všetky ZT_i pri oboch módoch.



1. mód



2. mód

Riešenie: označme si funkciu šifrovania danou blokovou šifrou s kľúčom K ako $E(x, K)$. Šifrovací mód na prvom obrázku je ECB, s ktorým sme sa stretli aj na prednáškach. Šifrovanie i. bloku OT sa v tomto móde dá popísať funkciou $ZT_i = E(OT_i, K_i)$. ECB mód šifruje rovnaké bloky OT na rovnaké bloky ZT a zachováva veľkú časť štatistických vlastností OT. Jeho bezpečnosť je veľmi slabá a hodí sa len na šifrovanie 1 bloku OT (napr. šifrovanie kľúča).

Šifrovanie i. bloku OT v 2. zobrazenom móde sa dá popísať funkciou $ZT_i = E(OT_i, K_i) \oplus ZT_{i-1}$. Útočník však ZT, ako aj IV, ktorý nie je tajným parameterom, pozná. Preto pre všetky $i \in \mathbb{N}$ platí $ZT_i \oplus ZT_{i-1} = E(OT_i, K_i)$, pričom $ZT_0 = IV$. Útočník teda pozná OT_i zašifrovaný len blokovou šifrou s kľúčom K_i, rovnako ako v prípade 1. módu. Mód 2 je len „zakamuflovaný“ ECB mód.

Uvedené dva šifrovacie módy blokových šifier sú identické a v oboch prípadoch sa jedná o ECB mód. Jeho bezpečnosť je nízka a klesá s počtom zašifrovaných blokov OT.

Bodovanie ★

- Napriek poznámkam v poslednej vete a na konci popisu šifrovania v 1. móde, nebolo úlohou hodnotiť (ne)bezpečnosť ECB módu, ale len porovnať navzájom dané dva módy z hľadiska bezpečnosti. Na úspešné vyriešenie úlohy preto stačí uviesť, že dané dva módy sú identické a toto tvrdenie zdôvodniť.
- Za uvedenie toho, že v prípade 2. módu sa jedná len o inak nakreslený 1. mód (ECB), a preto bezpečnosť oboch módov je rovnaká, je **5 bodov**.