

Jak funguje asymetrické šifrování?

Petr Vodstrčil

`petr.vodstrcil@vsb.cz`

Katedra aplikované matematiky, Fakulta elektrotechniky a informatiky,
Vysoká škola báňská–Technická univerzita Ostrava



23.3. 2018

(MODAM 2018)

Nejprve bude potřeba připomenout si některé pojmy.

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- dělitelnost, symbol $a|b$, zbytek po dělení, kongruence

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- dělitelnost, symbol $a|b$, zbytek po dělení, kongruence
- **prvočísla**

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- dělitelnost, symbol $a|b$, zbytek po dělení, kongruence
- prvočísla
- společný dělitel čísel a a b , největší společný dělitel ($\text{nsd}(a, b)$), nesoudělná čísla

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- dělitelnost, symbol $a|b$, zbytek po dělení, kongruence
- prvočísla
- společný dělitel čísel a a b , největší společný dělitel ($\text{nsd}(a, b)$), nesoudělná čísla
- Eukleidův algoritmus

Nejprve bude potřeba připomenout si některé pojmy.

- přirozená čísla ($\mathbb{N} = \{1, 2, 3, \dots\}$), celá čísla ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- dělitelnost, symbol $a|b$, zbytek po dělení, kongruence
- prvočísla
- společný dělitel čísel a a b , největší společný dělitel ($\text{nsd}(a, b)$), nesoudělná čísla
- Eukleidův algoritmus

Věta. (Bézoutova rovnost)

Nechť $a, b \in \mathbb{N}$. Pak existují čísla $\alpha, \beta \in \mathbb{Z}$ (Bézoutovy koeficienty) taková, že

$$\alpha a + \beta b = \text{nsd}(a, b).$$

Věta. (Bézoutova rovnost)

Nechť $a, b \in \mathbb{N}$. Pak existují čísla $\alpha, \beta \in \mathbb{Z}$ (Bézoutovy koeficienty) taková, že

$$\alpha a + \beta b = \text{nsd}(a, b).$$

Poznámka.

Čísla α a β se hledají Eukleidovým algoritmem.

Věta. (Bézoutova rovnost)

Nechť $a, b \in \mathbb{N}$. Pak existují čísla $\alpha, \beta \in \mathbb{Z}$ (Bézoutovy koeficienty) taková, že

$$\alpha a + \beta b = \text{nsd}(a, b).$$

Poznámka.

Čísla α a β se hledají Eukleidovým algoritmem.

Příklad.

Najděte Bézoutovy koeficienty α a β v případě, že $a = 19$ a $b = 27$.

Věta. (Bézoutova rovnost)

Nechť $a, b \in \mathbb{N}$. Pak existují čísla $\alpha, \beta \in \mathbb{Z}$ (Bézoutovy koeficienty) taková, že

$$\alpha a + \beta b = \text{nsd}(a, b).$$

Poznámka.

Čísla α a β se hledají Eukleidovým algoritmem.

Příklad.

Najděte Bézoutovy koeficienty α a β v případě, že $a = 19$ a $b = 27$.

Příklad.

Pro přirozená čísla a, b, c dokažte následující implikaci:

$$a|bc \wedge \text{nsd}(a, b) = 1 \implies a|c.$$

Věta.

Každé přirozené číslo n , $n \geq 2$, lze jednoznačně (až na pořadí činitelů) psát ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde p_1, p_2, \dots, p_k jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$.

Věta.

Každé přirozené číslo n , $n \geq 2$, lze jednoznačně (až na pořadí činitelů) psát ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde p_1, p_2, \dots, p_k jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$.

Definice. (Eulerova funkce)

Nechť $n \in \mathbb{N}$ je libovolné. Označme M_n množinu takových čísel $z \in \{1, 2, \dots, n\}$, která jsou nesoudělná s n , tzn.

$$M_n = \{i \in \{1, 2, \dots, n\} : \text{nsd}(i, n) = 1\}.$$

Eulerovu funkci φ pak definujeme

$$\varphi(n) = |M_n|. \quad (\text{počet prvků množiny } M_n)$$

Věta.

Každé přirozené číslo n , $n \geq 2$, lze jednoznačně (až na pořadí činitelů) psát ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde p_1, p_2, \dots, p_k jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$.

Definice. (Eulerova funkce)

Nechť $n \in \mathbb{N}$ je libovolné. Označme M_n množinu takových čísel $z \in \{1, 2, \dots, n\}$, která jsou nesoudělná s n , tzn.

$$M_n = \{i \in \{1, 2, \dots, n\} : \text{nsd}(i, n) = 1\}.$$

Eulerovu funkci φ pak definujeme

$$\varphi(n) = |M_n|. \quad (\text{počet prvků množiny } M_n)$$

Příklad.

$$\varphi(1) = 1, \quad \varphi(19) = 18, \quad \varphi(20) = 8, \quad \varphi(2018) = ?, \quad \varphi(1000000) = ?$$

Věta.

Nechť $n \in \mathbb{N}$, $n \geq 2$, má prvočíselný rozklad $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Věta.

Nechť $n \in \mathbb{N}$, $n \geq 2$, má prvočíselný rozklad $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Důsledek.

Je-li n součinem dvou různých prvočísel p, q , pak

$$\varphi(n) = (p - 1)(q - 1).$$

Věta.

Nechť $n \in \mathbb{N}$, $n \geq 2$, má prvočíselný rozklad $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Důsledek.

Je-li n součinem dvou různých prvočísel p, q , pak

$$\varphi(n) = (p-1)(q-1).$$

Důkaz.

Víme, že $\varphi(n) = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) = pq \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} = (p-1)(q-1).$ □

Věta.

Nechť $n \in \mathbb{N}$, $n \geq 2$, má prvočíselný rozklad $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Důsledek.

Je-li n součinem dvou různých prvočísel p, q , pak

$$\varphi(n) = (p - 1)(q - 1).$$

Důkaz.

Víme, že $\varphi(n) = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) = pq \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} = (p-1)(q-1)$. □

Příklad.

Protože $1000000 = 10^6 = 2^6 \cdot 5^6$, je

$$\varphi(1000000) = 1000000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 1000000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400000.$$

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- **Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.**

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- **Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.**

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.
- K číslu v najdeme číslo $t \in \mathbb{N}$ tak, aby součin vt dával po dělení číslem $\varphi(n)$ zbytek 1. To lze díky Bézoutově rovnosti.

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.
- K číslu v najdeme číslo $t \in \mathbb{N}$ tak, aby součin vt dával po dělení číslem $\varphi(n)$ zbytek 1. To lze díky Bézoutově rovnosti.

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.
- K číslu v najdeme číslo $t \in \mathbb{N}$ tak, aby součin vt dával po dělení číslem $\varphi(n)$ zbytek 1. To lze díky Bézoutově rovnosti.

Dvojice (v, n) bude veřejný klíč – můžeme jej šířit.

Vygenerování veřejného a tajného klíče

- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.
- K číslu v najdeme číslo $t \in \mathbb{N}$ tak, aby součin vt dával po dělení číslem $\varphi(n)$ zbytek 1. To lze díky Bézoutově rovnosti.

Dvojice (v, n) bude veřejný klíč – můžeme jej šířit.

Dvojice (t, n) bude tajný klíč, který vlastníme pouze my.

Vygenerování veřejného a tajného klíče

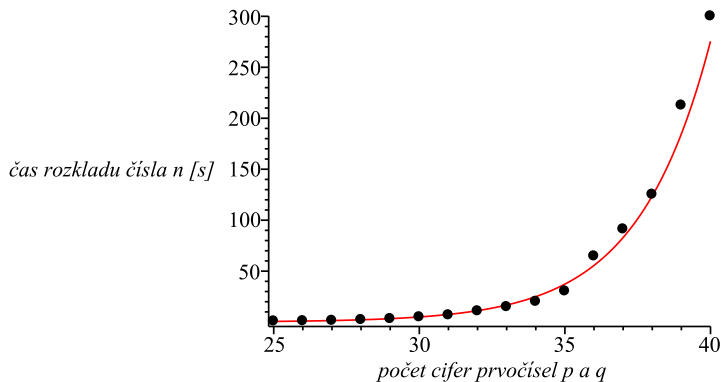
- Zvolíme dvě dostatečně velká a vzájemně různá prvočísla p, q a položíme $n = pq$.
- Dopočítáme $\varphi(n) = (p - 1)(q - 1)$.
- Náhodně vybereme číslo $v \in \mathbb{N}$, které je nesoudělné s $\varphi(n)$.
- K číslu v najdeme číslo $t \in \mathbb{N}$ tak, aby součin vt dával po dělení číslem $\varphi(n)$ zbytek 1. To lze díky Bézoutově rovnosti.

Dvojice (v, n) bude veřejný klíč – můžeme jej šířit.

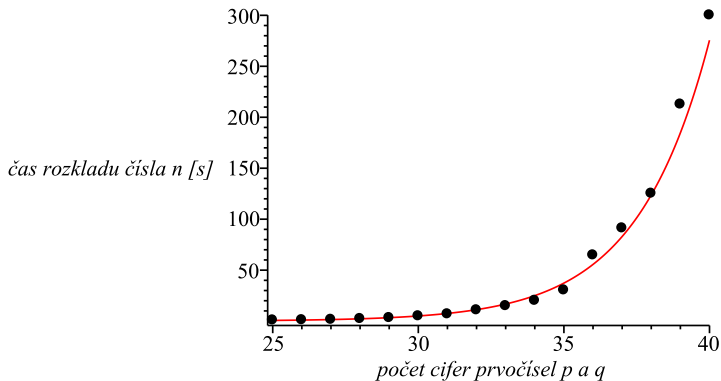
Dvojice (t, n) bude tajný klíč, který vlastníme pouze my.

Tajný klíč lze z veřejného dopočítat pouze v případě, že známe rozklad čísla n na prvočísla ($n = pq$). Zjištění tohoto rozkladu je však velmi časově náročné.

Časy potřebné k prolomení klíče



Časy potřebné k prolomení klíče



Pokud by prvočísla p a q byla 50-ti místná, trval by zpětný rozklad čísla n cca. 4 hodiny, pro 60-ti místná by to bylo 9,5 dne, pro 70-ti místná 1,5 roku a pro 80-ti místná 78 let....

Časy potřebné k prolomení klíče

Systém

Procesor:	Intel(R) Core(TM) i7-4702MQ CPU @ 2.20GHz 2.20 GHz
Nainstalovaná paměť (RAM):	8,00 GB (použitelné: 7,76 GB)
Typ systému:	64bitový operační systém, procesor pro platformu x64
Pero a dotykové ovládaní:	Pro tento displej není k dispozici zadávání perem ani dotykové zadávání.

lenovo.

[Informace o podpoře](#)

Pokud by prvočísla p a q byla 50-ti místná, trval by zpětný rozklad čísla n cca. 4 hodiny, pro 60-ti místná by to bylo 9,5 dne, pro 70-ti místná 1,5 roku a pro 80-ti místná 78 let....

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu.
Stáhneme si nejprve jeho veřejný klíč (v, n) .

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu.
Stáhneme si nejprve jeho veřejný klíč (v, n) .

Předpokládejme, že posíláme zprávu z , kde $z \in \mathbb{N}$, $z < n$.

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu. Stáhneme si nejprve jeho veřejný klíč (v, n) .

Předpokládejme, že posíláme zprávu z , kde $z \in \mathbb{N}$, $z < n$.

Vypočítáme zbytek čísla z^v po dělení číslem n . Tento zbytek (označme jej s) je hledaná šifra.

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu. Stáhneme si nejprve jeho veřejný klíč (v, n) .

Předpokládejme, že posíláme zprávu z , kde $z \in \mathbb{N}$, $z < n$.

Vypočítáme zbytek čísla z^v po dělení číslem n . Tento zbytek (označme jej s) je hledaná šifra.

Příjemce obdrží zašifrovanou zprávu s a chce ji rozšifrovat. K tomu potřebuje svůj tajný klíč (t, n) .

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu. Stáhneme si nejprve jeho veřejný klíč (v, n) .

Předpokládejme, že posíláme zprávu z , kde $z \in \mathbb{N}$, $z < n$.

Vypočítáme zbytek čísla z^v po dělení číslem n . Tento zbytek (označme jej s) je hledaná šifra.

Příjemce obdrží zašifrovanou zprávu s a chce ji rozšifrovat. K tomu potřebuje svůj tajný klíč (t, n) .

Příjemce vypočítá zbytek čísla s^t po dělení číslem n . Lze ukázat, že tento zbytek je roven původní zprávě z .

Princip (de)šifrování

Představme si situaci, že někomu chceme poslat důvěrnou zprávu. Stáhneme si nejprve jeho veřejný klíč (v, n) .

Předpokládejme, že posíláme zprávu z , kde $z \in \mathbb{N}$, $z < n$.

Vypočítáme zbytek čísla z^v po dělení číslem n . Tento zbytek (označme jej s) je hledaná šifra.

Příjemce obdrží zašifrovanou zprávu s a chce ji rozšifrovat. K tomu potřebuje svůj tajný klíč (t, n) .

Příjemce vypočítá zbytek čísla s^t po dělení číslem n . Lze ukázat, že tento zbytek je roven původní zprávě z .

Za vším je tzv. malá Fermatova věta, která říká, že pro každé přirozené číslo a a každé prvočíslo p je číslo $a^p - a$ dělitelné číslem p .

Příklad

Položme $n = 7 \cdot 11 = 77$. Pak jistě $\varphi(n) = 6 \cdot 10 = 60$. Zvolme např. $v = 17$.
Jistě $\text{nsd}(17, 60) = 1$.

Pak $t = 53$, neboť $vt = 17 \cdot 53 = 901$ dává po dělení číslem $\varphi(n) = 60$ zbytek 1.
Číslo t jsme schopni spočítat pomocí Eukleidova algoritmu.

Příklad

Položme $n = 7 \cdot 11 = 77$. Pak jistě $\varphi(n) = 6 \cdot 10 = 60$. Zvolme např. $v = 17$.
Jistě $\text{nsd}(17, 60) = 1$.

Pak $t = 53$, neboť $vt = 17 \cdot 53 = 901$ dává po dělení číslem $\varphi(n) = 60$ zbytek 1.
Číslo t jsme schopni spočítat pomocí Eukleidova algoritmu.

Dvojice $(17, 77)$ bude veřejný klíč a dvojice $(53, 77)$ bude tajný klíč.

Příklad

Položme $n = 7 \cdot 11 = 77$. Pak jistě $\varphi(n) = 6 \cdot 10 = 60$. Zvolme např. $v = 17$.
Jistě $\text{nsd}(17, 60) = 1$.

Pak $t = 53$, neboť $vt = 17 \cdot 53 = 901$ dává po dělení číslem $\varphi(n) = 60$ zbytek 1.
Číslo t jsme schopni spočítat pomocí Eukleidova algoritmu.

Dvojice $(17, 77)$ bude veřejný klíč a dvojice $(53, 77)$ bude tajný klíč.

Nyní např. budeme chtít zašifrovat zprávu $z = 19$.

Příklad

Položme $n = 7 \cdot 11 = 77$. Pak jistě $\varphi(n) = 6 \cdot 10 = 60$. Zvolme např. $v = 17$.
Jistě $\text{nsd}(17, 60) = 1$.

Pak $t = 53$, neboť $vt = 17 \cdot 53 = 901$ dává po dělení číslem $\varphi(n) = 60$ zbytek 1.
Číslo t jsme schopni spočítat pomocí Eukleidova algoritmu.

Dvojice $(17, 77)$ bude veřejný klíč a dvojice $(53, 77)$ bude tajný klíč.

Nyní např. budeme chtít zašifrovat zprávu $z = 19$.

$z^v = 19^{17} = 5480386857784802185939$. Zbytek tohoto čísla po dělení číslem 77 je 24. Zašifrovaná zpráva má tedy hodnotu $s = 24$.

Příklad

Položme $n = 7 \cdot 11 = 77$. Pak jistě $\varphi(n) = 6 \cdot 10 = 60$. Zvolme např. $v = 17$.
Jistě $\text{nsd}(17, 60) = 1$.

Pak $t = 53$, neboť $vt = 17 \cdot 53 = 901$ dává po dělení číslem $\varphi(n) = 60$ zbytek 1.
Číslo t jsme schopni spočítat pomocí Eukleidova algoritmu.

Dvojice $(17, 77)$ bude veřejný klíč a dvojice $(53, 77)$ bude tajný klíč.

Nyní např. budeme chtít zašifrovat zprávu $z = 19$.

$z^v = 19^{17} = 5480386857784802185939$. Zbytek tohoto čísla po dělení číslem 77 je 24. Zašifrovaná zpráva má tedy hodnotu $s = 24$.

Dešifrování:

$s^t = 24^{53} = 14164322640050739813527615873101833956776014430996525822459444296966733824$.
Zbytek po dělení číslem 77 je 19, což je hodnota původní zprávy.

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$24^2 = 576 \equiv 37$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$24^2 = 576 \equiv 37 \implies 24^4 \equiv 37^2 = 1369 \equiv 60$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$24^2 = 576 \equiv 37 \implies 24^4 \equiv 37^2 = 1369 \equiv 60 \implies 24^8 \equiv 60^2 = 3600 \equiv 58$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$\begin{aligned}24^2 = 576 \equiv 37 &\implies 24^4 \equiv 37^2 = 1369 \equiv 60 \implies 24^8 \equiv 60^2 = 3600 \equiv 58 \\ &\implies 24^{16} \equiv 58^2 = 3364 \equiv 53\end{aligned}$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$\begin{aligned}24^2 = 576 \equiv 37 &\implies 24^4 \equiv 37^2 = 1369 \equiv 60 \implies 24^8 \equiv 60^2 = 3600 \equiv 58 \\ &\implies 24^{16} \equiv 58^2 = 3364 \equiv 53 \implies 24^{32} \equiv 53^2 = 2809 \equiv 37.\end{aligned}$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$\begin{aligned}24^2 = 576 \equiv 37 &\implies 24^4 \equiv 37^2 = 1369 \equiv 60 \implies 24^8 \equiv 60^2 = 3600 \equiv 58 \\ &\implies 24^{16} \equiv 58^2 = 3364 \equiv 53 \implies 24^{32} \equiv 53^2 = 2809 \equiv 37.\end{aligned}$$

Odtud snadno spočítáme, že

$$24^{53} = 24^{32} \cdot 24^{16} \cdot 24^4 \cdot 24^1 \equiv 37 \cdot 53 \cdot 60 \cdot 24 = 2823840 \equiv 19.$$

Výpočet zbytků

Problém je, jak efektivně vypočítat např. zbytek čísla 24^{53} po dělení číslem 77.

Platí (všechny výpočty provádíme „modulo 77“)

$$\begin{aligned}24^2 = 576 \equiv 37 &\implies 24^4 \equiv 37^2 = 1369 \equiv 60 \implies 24^8 \equiv 60^2 = 3600 \equiv 58 \\ &\implies 24^{16} \equiv 58^2 = 3364 \equiv 53 \implies 24^{32} \equiv 53^2 = 2809 \equiv 37.\end{aligned}$$

Odtud snadno spočítáme, že

$$24^{53} = 24^{32} \cdot 24^{16} \cdot 24^4 \cdot 24^1 \equiv 37 \cdot 53 \cdot 60 \cdot 24 = 2823840 \equiv 19.$$

Tímto postupem se vyhneme práci s příliš velkými čísly.

Úkol.

Předpokládejme, že dvojice $(457, 667)$ je veřejný klíč osoby X . Tento klíč je samozřejmě všem dostupný. Podaří se nám odchytit zašifrovaný mail (určený osobě X), ve kterém nalezneme (zašifrovanou) zprávu $s = 109$.

Naším úkolem je prolomit klíč, tzn. najít příslušný tajný klíč a na základě tohoto klíče rozšifrovat zprávu.

Úkol.

Předpokládejme, že dvojice $(457, 667)$ je veřejný klíč osoby X . Tento klíč je samozřejmě všem dostupný. Podaří se nám odchytit zašifrovaný mail (určený osobě X), ve kterém nalezneme (zašifrovanou) zprávu $s = 109$.

Naším úkolem je prolomit klíč, tzn. najít příslušný tajný klíč a na základě tohoto klíče rozšifrovat zprávu.

Úkol.

Dokažte, že pro každé přirozené číslo n je výraz $n^5 - n$ dělitelný číslem 30.

Úkol.

Předpokládejme, že dvojice $(457, 667)$ je veřejný klíč osoby X . Tento klíč je samozřejmě všem dostupný. Podaří se nám odchytit zašifrovaný mail (určený osobě X), ve kterém nalezneme (zašifrovanou) zprávu $s = 109$.

Naším úkolem je prolomit klíč, tzn. najít příslušný tajný klíč a na základě tohoto klíče rozšifrovat zprávu.

Úkol.

Dokažte, že pro každé přirozené číslo n je výraz $n^5 - n$ dělitelný číslem 30.

Úkol.

Najděte **všechna** přirozená čísla n , pro která platí

$$\varphi(n) = \frac{n}{3}.$$



O asymetrickém šifrování na Wikipedii:

https://cs.wikipedia.org/wiki/Asymetrická_kryptografie



Další čtení o asymetrickém šifrování:

https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7027



Odkaz na stažení softwaru:

<https://www.gpg4usb.org>

Děkuji za pozornost.