Lineární modely MB141, 3. část

David Kruml

3. 4. 2024

Připomenutí počítání ve zbytkových třídách, kongruence

Píšeme

$$a \equiv b \pmod{n},$$

pokud a, b dávají stejný zbytek po dělení n, rozdíl $a - b$ je dělitelný n, atd.

S kongruencemi pracujeme podobně jako s rovnicemi.

Násobení číslem soudělným s modulem není ekvivalentní operace (ztrácíme část informace).

Pro aplikace (šifrování) je velmi důležité naučit se efektivně umocňovat ve zbytkových třídách.

Přirozené číslo p nazýváme *prvočíslem*, pokud je různé od 1 a jeho jedinými děliteli jsou 1 a p.

Malá Fermatova věta

Nechť p je prvočíslo a a celé číslo, které není dělitelné p ($p \nmid a$). Pak platí:

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

(Důkaz se vede matematickou indukcí vzhledem k a a využívá binomickou větu aplikovanou na $(a+1)^p$.)

Příklad: Určete zbytek po dělení čísla 3^{2024} číslem 17.

Řešení: Protože $17 \nmid 3$, podle malé Fermatovy věty platí $3^{16} \equiv 1 \pmod{17}$.

Potřebujeme tedy zjistit, čemu je kongruentní exponent 2024 v modulu 16: Nejbližším menším násobkem šesnácti je číslo 2016, tj. $2024 \equiv 8 \pmod{16}$.

Celkem dostáváme $3^{2024} = 3^{16k+8} = (3^{16})^k \cdot 3^8 \equiv 1 \cdot 3^8 \equiv (3^2)^4 = 9^4 \equiv (-8)^4 = 64^2 \equiv 13^2 \equiv (-4)^2 = 16 \pmod{17}$.

Odpověď: Zbytek je 16.

Eulerova funkce

Eulerova funkce vyjadřuje počet celých čísel v množině $\{1, 2, \ldots, n-1\}$ nesoudělných s n.

Značíme $\phi(n)$.

Nepraktický vzorec:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right),$$

kde $p_1, p_2, \ldots, p_k$ jsou všechna prvočísla dělící n.

Praktický algoritmus:

- Pro prvočíslo p a přirozené k platí $\phi(p^k) = (p-1)p^{k-1}$.
- Pro nesoudělná m, n platí $\phi(mn) = \phi(m)\phi(n)$.

Příklad na Eulerovu funkci

Spočtěte $\phi(240)$.

Řešení: $\phi(240) = \phi(2^4 \cdot 3 \cdot 5) = \phi(2^4)\phi(3)\phi(5) =$
$(2-1) \cdot 2^3 \cdot (3-1) \cdot (5-1) = 8 \cdot 2 \cdot 4 = 64.$

Řešení nepraktickým vzorcem: $2, 3, 5 \mid 240$, tj.

$$\phi(240) = 240 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right)$$
$$= 240 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 64.$$

Eulerova věta

Pro nesoudělná a, n platí:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Eulerova věta zobecňuje malou Fermatovu větu, protože $\phi(p) = p - 1$ pro prvočíselné p.

Příklad: Spočtěte zbytek po dělení čísla 2^{2024} číslem 15.

Řešení: 2 a 15 jsou nesoudělná, můžeme tedy využít Eulerovu větu: $\phi(15) = \phi(3)\phi(5) = (3-1)\cdot(5-1) = 8$, $2^8 \equiv 1 \pmod{15}$.

Protože $8 \mid 2024$, dostáváme $2^{2024} = (2^8)^k \equiv 1 \pmod{15}$, tj. hledaný zbytek je 1.

Co když jsou a, n soudělná?

Je-li základ soudělný s modulem, obvykle dojde při umocňování k určité „degeneraci“.

Můžeme si pomoci rozkladem modulu na složku nesoudělnou s a a složku tvořenou prvočísly společnými s a.

Na první složku použijeme Eulerovu větu (nebo malou Fermatovu), ve druhé složce můžeme očekávat „rychlý konec“ — nulový zbytek (násobek modulu) se objeví už na menší mocnině.

Příklad: Určete poslední číslici čísla 2^{2024}.

Řešení: Základ 2 a modul 10 jsou soudělné, nemůžeme tedy využít Eulerovu větu přímo. Nicméně zjistíme zbytek po dělení 5: malá Fermatova věta říká $2^4 \equiv 1 \pmod 5$, tedy i $2^{2024} = (2^4)^k \equiv 1 \pmod 5$. Poslední číslicí tak může být 1 nebo 6.

Protože 2^{2024} je zřejmě sudé, poslední číslicí musí být 6.

Duševní příprava na řád čísla

Příklad: Najděte nějaké číslo $x \neq 1$ a exponent k, pro něž $x^k \equiv 1 \pmod{36}$ a nějaké číslo x, pro nějž žádný takový exponent k neexistuje.

Řešení: Zkusme třeba $x = 2$. Číslo x^k je vždy sudé, stejně jako modul 36, kongruence tedy platit nemůže. Našli jsme odpověď na druhou otázku. Podobně bychom zjistili, že ani $x = 3$ kongruenci nevyhoví kvůli soudělnosti s modulem, a stejně tak $x = 4$.

Pro $x = 5$ máme (v modulu 36):

$$
\begin{aligned}
5^2 &= 25, \\
5^3 &= 5 \cdot 25 = 125 = 3 \cdot 36 + 17 \equiv 17, \\
5^4 &= (5^2)^2 = 25^2 \equiv (-11)^2 = 121^2 \equiv 13, \\
5^5 &= 5^4 \cdot 5 \equiv 13 \cdot 5 = 65 \equiv -7, \\
5^6 &= 5^5 \cdot 5 \equiv -7 \cdot 5 = -35 \equiv 1,
\end{aligned}
$$

hurá!

Řád čísla

Úloha „pro dané x najít k, aby $x^k \equiv 1 \pmod{n}$“ je řešitelná právě tehdy, když x, n jsou nesoudělná.

Existenci takového k zaručuje Eulerova věta, ale často se zadaří najít k menší než $\phi(n)$.

Nejmenší k splňující $x^k \equiv 1 \pmod{n}$ nazýváme *řád čísla* x v modulu n.

Mocniny x se v modulu n chovají poměrně chaoticky, proto je zjišťování řádu těžké.

Platí ovšem důležitá věta: Řád dělí $\phi(n)$.

Vysvětlení: Jestliže $x^k \equiv 1$, pak i $x^{kl} = (x^k)^l \equiv 1$. Obráceně, pokud $x^k \equiv 1, x^l \equiv 1$, pak i $x^{\mathrm{nsd}(k,l)} \equiv 1$. Proto řád musí dělit jakékoli k řešící kongruenci, tedy i $\phi(n)$.

Příklad na řád

Určete řád čísla 7 v modulu 18.

Řešení: Čísla 7, 18 jsou nesoudělná, zadání tedy má smysl. Podle předchozího poznatku má cenu zkoušet pouze exponenty dělící $\phi(18) = (2-1)\cdot(3-1)\cdot 3 = 6$, tj. $k = 2, 3, 6$:

$$7^2 = 49 \equiv 13 \equiv -5,$$
$$7^3 = 7^2 \cdot 7 \equiv -5 \cdot 7 = -35 \equiv 1.$$

Odpověď: Řád čísla 7 modulo 18 je 3.

Poznámka: Množina dělitelů $\phi(n)$ (kandidátů na řád) je docela důkladně provázána relací dělitelnosti. To se nám hodí, protože můžeme při výpočtu zužitkovat dílčí výsledky pro předchozí (menší) kandidáty.

Při zkoušení kandidátů postupujeme samozřejmě od menších exponentů k větším, protože je to jednodušší a nechceme řád „propást“.

Primitivní kořen

Číslo se nazývá *primitivní kořen* modulo n, pokud (je nesoudělné s n a) jeho řád je roven $\phi(n)$. (Tzn. řád primitivního kořene je „nejzazší možný“.)

Mocniny $x, x^2, \ldots, x^{\phi(n)}$ primitivního kořene x se neopakují, jinak by některé menší musely být 1 a x by nebyl primitivní. V důsledku toho mocniny „navštíví“ všechny nesoudělné prvky s n.

Pohyb mocnin po $\mathbb{Z}_n$ je „neuspořádaný“, proto je velmi těžké řešit obrácené úlohy, tzn. pro n, y nesoudělná počítat

- *odmocninu*: pro dané k a najít x,
- *diskrétní logaritmus*: pro dané x a najít k,

aby platilo

$$x^k \equiv y \pmod{n}.$$

Tohoto faktu využívají některé šifrovací metody, jak si brzy ukážeme.

Příkad na primitivní kořeny

Najděte všechny primitivní kořeny modulo 14.

Řešení: Bavíme se jen o prvcích v $\mathbb{Z}_{14}$ nesoudělných se 14, tj. $1, 3, 5, 9, 11, 13$.

Jedničku ihned vyřadíme, protože ji řeší exponent $k = 1$. Podobně vyřadíme 13, protože $13 \equiv -1$ a $(-1)^2 = 1$.

Ostatní prvky zkusíme umocnit na 2 a 3, což jsou dělitelé $\phi(14) = 6$. Předtím si ještě všimněme, že jsou v $\mathbb{Z}_{14}$ rozmístěny „středově symetricky“, čehož využijeme přepisem $11 = -3, 9 = -5$:

$$3^2 = 9 \not\equiv 1, \qquad 3^3 = 9 \cdot 3 = 27 \not\equiv 1,$$
$$5^2 = 25 \equiv -3 \not\equiv 1, \qquad 5^3 = -3 \cdot 5 = -15 \equiv -1 \not\equiv 1,$$
$$(-3)^2 = 9 \not\equiv 1, \qquad (-3)^3 = 9 \cdot (-3) = -27 \equiv 1,$$
$$(-5)^2 = 25 \equiv -3 \not\equiv 1, \qquad (-5)^3 = -3 \cdot (-5) = 15 \equiv 1,$$

Řád čísel 9 a 11 je jen 3, nejde tedy o primitivní kořeny.

Odpověď: Primitivní kořeny modulo 14 jsou 3 a 5.

Komentáře k mocninám ve zbytkových třídách

- Při „ručním“ výpočtu mocnin využíváme přednostně umocňování na druhou než prosté opakované násobení, např. $3^6 = (3^2)^2 \cdot 3^2$.
- Víc než kdekoli jinde se vyplácí přepis „horní poloviny“ zbytků do záporných reprezentantů.
- V mocninách vyšších než $\phi(n)$ se výsledky zacyklí.
- To se děje i u prvků nesoudělných s n, které nejsou primitivními kořeny, ale cyklus je kratší.
- Prvky nesoudělné s n jsou invertibilní. Inverzí primitivního kořene je primitivní kořen.
- **Požadavky:** Znát malou Fermatovu větu, Eulerovu větu, pojmy řád čísla, primitivní kořen, vědět, že řád dělí $\phi(n)$. Umět počítat $\phi(n)$, poradit si s jakoukoli vysokou mocninou v $\mathbb{Z}_n$, určit řád čísla, prověřit primitivnost kořene.

Lineární kongruence

Z dřívějšího umíme řešit (jednodušší) kongruence tvaru

$$ax \equiv b \pmod{n},$$

tj. určit x pro daná n, a, b.

Obvykle si pomáháme vhodným násobením.

Systematický přístup: najdeme inverzi a^{-1} k a a spočítáme $x \equiv a^{-1}b$.

Příklad: Řešte kongruenci $5x \equiv 3 \pmod{7}$.

Řešení: 1) Řešení $x \equiv 2$ uhodneme, neboť $5 \cdot 2 = 10 \equiv 3 \pmod{7}$.

2) Koeficienty $5, 3$ nahradíme podle kongruencí $5 \equiv -2, 3 \equiv -4$. Odtud $-2x \equiv -4$, a tedy $x \equiv 2$. (Poslední krok využívá faktu, že 2,7 jsou nesoudělná, a tedy -2 má inverzi.)

3) $5 \cdot 3 = 15 \equiv 1$, tj. $5^{-1} \equiv 3$, proto $x = 5^{-1} \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2$.

Rozklad modulu

Inverze ne vždy existuje (a, n soudělná) a výpočet může být komplikovaný.

Někdy pomáhá rozbití složeného modulu na menší činitele, což vede na řešení soustavy kongruencí:

$$\begin{aligned} ax &\equiv b \pmod{n_1} \\ ax &\equiv b \pmod{n_2} \\ &\vdots \\ ax &\equiv b \pmod{n_k} \end{aligned}$$

Dílčí kongruence můžeme samostatně řešit a dosadit do následující (obdoba řešení soustav lineárních rovnic). Např. řešení 1. kongruence $x \equiv c \pmod{n_1}$ dosadíme do 2. kongruence jako $x = dn_1 + c$, spočítáme d, vyjádříme x v modulu $n_1 n_2$ atd.

Příklad na složený modul I

Řešte kongruenci

$$21x \equiv 18 \pmod{60}.$$

Řešení: $60 = 2^2 \cdot 3 \cdot 5$, kongruenci tedy rozložíme na soustavu:

$$\begin{aligned} 21x &\equiv 18 \pmod{4} \\ 21x &\equiv 18 \pmod{3} \\ 21x &\equiv 18 \pmod{5} \end{aligned}$$

Po úpravě v dílčích modulech dostáváme:

$$\begin{aligned} x &\equiv 2 \pmod{4} \\ 0x &\equiv 0 \pmod{3} \\ x &\equiv -2 \pmod{5} \end{aligned}$$

Druhá kongruence platí vždy, nic se z ní nedozvíme.

Příklad na složený modul II

V soustavě

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv -2 \pmod 5 \end{aligned}$$

můžeme první kongruenci přepsat také jako $x \equiv -2 \pmod 4$, a odtud bychom měli hned $x \equiv -2 \pmod{20}$.

Tvařme se, že nás to nenapadlo. Vyjádříme $x = 2 + 4a$ a dosadíme do $x \equiv -2 \pmod 5$:

$$\begin{aligned} 2 + 4a &\equiv -2 \pmod 5 \\ 4a &\equiv -4 \\ a &\equiv -1 \end{aligned}$$

Příklad na složený modul III

Celkem tedy $x \equiv 2 - 4 = -2 \pmod{20}$ (či $x \equiv 18$).

V modulu 60 máme 3 řešení:

$$\begin{aligned} x_1 &\equiv 18 \pmod{60}, \\ x_2 &\equiv 38, \\ x_3 &\equiv 58. \end{aligned}$$

Příklad na soustavu kongruencí I

Řešte soustavu kongruencí

$$\begin{aligned} 3x &\equiv 4 \pmod 7 \\ 5x &\equiv 2 \pmod 8 \\ 4x &\equiv 6 \pmod 9 \end{aligned}$$

Řešení: První kongruenci vynásobíme 5: $15x \equiv 20, x \equiv -1 \pmod 7$, tj. $x = 7a - 1$.

Dosazení do druhé kongruence:
$5 \cdot (7a - 1) \equiv -3 \cdot (-a - 1) = 3a + 3 \equiv 2, 3a \equiv -1 \pmod 8$.

Vynásobíme 3: $9a \equiv -3, a \equiv -3 \equiv 5 \pmod 8$.

Odtud $x \equiv 7 \cdot 5 - 1 = 34 \pmod{56}$.

Příklad na soustavu kongruencí II

Víme $x = 56b + 34$. Dosadíme do třetí kongruence:
$4 \cdot (56b + 34) \equiv 4 \cdot (2b - 2) = 8b - 8 \equiv -b + 1 \equiv 6, b \equiv -5 \equiv 4 \pmod 9$.

Dostáváme $x \equiv 56 \cdot 4 + 34 = 258 \pmod{504}$.

Zkouška:

$$\begin{aligned} 258 &\equiv -1 \pmod 7, & 3 \cdot (-1) &= -3 \equiv 4 \pmod 7, \\ 258 &\equiv 2 \pmod 8, & 5 \cdot 2 &= 10 \equiv 2 \pmod 8, \\ 258 &\equiv -3 \pmod 9, & 4 \cdot (-3) &= -12 \equiv 6 \pmod 9. \end{aligned}$$

Čínská zbytková věta

Zaručuje existenci řešení soustavy kongruencí (již upravených se separovaným x).

Jsou-li $n_1, n_2, \ldots n_k$ po dvou nesoudělné moduly, pak má soustava kongruencí

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

jediné řešení v modulu $n_1 n_2 \ldots n_k$.

Příklad na složenou mocninu

Určete zbytek po dělení čísla $12^{12^{12}}$ číslem 25.

Řešení: $\phi(25) = (5-1)\cdot 5 = 20$. Z Eulerovy věty víme, že $12^{\phi(25)} \equiv 1 \pmod{25}$, potřebujeme tedy zjistit zbytek po dělení 12^{12} dvaceti.

Čísla 12, 20 jsou soudělná, budeme tedy samostatně řešit zbytek pro moduly 4 a 5. Zřejmě $12^{12} \equiv 0 \pmod{4}$, v druhém případě využijeme malou Fermatovu větu: $12^4 \equiv 1 \pmod{5}$, proto i $12^{12} \equiv 1 \pmod{5}$. Tedy $12^{12} = 4a$ a $4a \equiv 1 \pmod{5}$. Odtud $a \equiv 4 \pmod{5}$ a $12^{12} \equiv 16 \pmod{20}$.

Můžeme se vrátit na začátek a dopočítat zbytek pro $12^{12^{12}}$:

$$12^{12^{12}} \equiv 12^{16} = (12^2)^8 = 144^8 \equiv (-6)^8 = (6^2)^4 = 36^4 \equiv 11^4 =$$

$$= (11^2)^2 = 121^2 \equiv (-4)^2 = 16 \pmod{25}.$$

Odpověď: Hledaný zbytek je 16.

Komentáře k soustavám kongruencí

- Inverzní prvky můžeme i pro složený modul počítat z Bezoutovy rovnosti (a mnohdy je to rychlejší).
- Pro dosazování výsledků dílčích kongruencí nepotřebujeme mít kongruence „učesané“ jako v čínské zbytkové větě. Úpravy provedeme až po dosazení — analogie s řešením soustav lineárních rovnic a zpětným dosazováním.
- **Požadavky:** Umět počítat soustavy lineárních kongruencí. Využívat tuto schopnost při rozkladu složeného modulu a při výpočtu složených mocnin.
- Doporučení: zopakovat si druhé mocniny čísel do 20 a třetí mocniny do 10.

Historie kryptografie

Využití: diplomacie, vojenství, bankovnictví, přístupová práva, elektronický podpis, atd.

Základní způsoby šifrování:

- transpoziční — písmena jsou prohozena (skytála, mřížka),
- steganografie — zpráva je skryta balastní informací (šifra ve Švejkovi, tj. výběr písmen z knihy),
- substituční — písmena/shluky písmen jsou nahrazovány jinými (Caesar, Vigenèr, Enigma),
- kombinace — DES, AES, speciální čipy.

Většina „tradičních“ systémů je *symetrická*: šifrování a dešifrování jsou stejně náročné a vzájemně inverzní procesy.

Vigenèrova šifra — šifrování

$$\mathrm{A} = 1, \qquad \mathrm{B} = 2, \qquad \mathrm{C} = 3, \qquad \ldots$$

Zpráva: TOTOJEVELMITAJNAZPRAVA

Klíč: PRUDUCH

Šifrování — rozkopírujeme klíč podle délky zprávy: PRUDUCHPRUDUCHPRUDUCHP a sčítáme se zprávou modulo 26:

$$\begin{aligned} T + P &= 20 + 16 = 36 \equiv 10 = J \pmod{26} \\ O + R &= 15 + 18 = 33 \equiv 7 = G \\ T + U &= 20 + 21 = 41 \equiv 15 = O \\ &\vdots \end{aligned}$$

Zašifrovaná zpráva: JGO...

Vigenèrova šifra — dešifrování

$$
\begin{aligned}
J - P = 10 - 16 = -6 \equiv 20 = T \pmod{26} \\
G - R = 7 - 18 = -11 \equiv 15 = O \\
O - U = 15 - 21 = -6 \equiv 20 = T \\
\vdots
\end{aligned}
$$

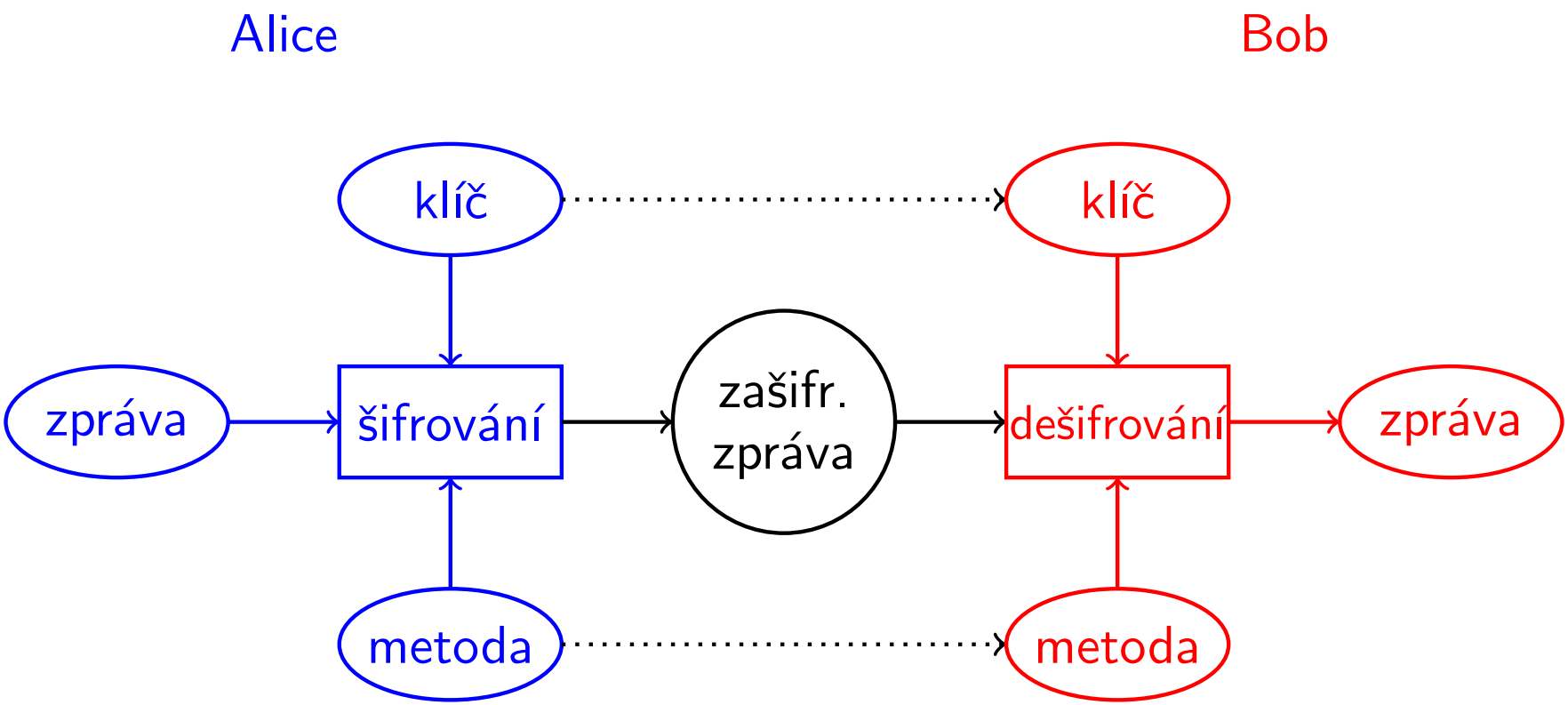
nebo si nejdřív připravíme dešifrovací klíč

$$
\begin{aligned}
26 - P = 26 - 16 = 10 = J \\
26 - R = 26 - 18 = 8 = H \\
26 - U = 26 - 21 = 5 = E \\
\vdots
\end{aligned}
$$

a ten přičítáme k zašifrované zprávě:

$$
\begin{aligned}
J + J = 10 + 10 = 20 = T \pmod{26} \\
G + H = 7 + 8 = 15 = O \\
O + E = 15 + 5 = 20 = T \\
\vdots
\end{aligned}
$$

Obecný princip šifrování



Zranitelnost šifry

Tři informační kanály:

- dohoda o metodě (nebo předání šifrovacího stroje, atp.),
- předání šifrovacího/dešifrovacího klíče,
- předání zašifrované zprávy.

Mnohé staší šifrovací způsoby podceňují možnosti útoku na první dva kanály.

Samotný přenos zašifrované zprávy pokládáme za bezpečný (věříme šifře), v zásadě je tedy veřejný.

Ovšem i zpráva může být podrobena zejména frekvenční analýze. Východiskem může být dostatečně rozsáhlý klíč, ale pak se opět dostáváme k problémům s přenosem klíče.

Optimální situace: přenos informací všemi třemi kanály bude veřejný, přesto se útočník ke zprávě nedostane.

Tzv. *asymetrické šifrování*: využívá se „mezer v matematice“ — jedním směrem to jde snadno, obráceně velmi ztuha.

RSA (Rivest, Shamir, Adleman 1977, Cocks 1973)

n ... dostatečně velké číslo takové, že $n = pq$, p, q prvočísla, rozklad n je soukromý,

$\phi(n)$ ... kvůli velikosti n a neznámému rozkladu $n = pq$ není možné efektivně spočítat,

e ... *veřejný klíč* (šifrovací), nesoudělný s $\phi(n)$,

d ... *soukromý klíč* (dešifrovací), splňuje $de \equiv 1 \pmod{\phi(n)}$,

M ... *zpráva*,

C ... *zašifrovaná zpráva*.

Šifrování: $C \equiv M^e \pmod{n}$.

Dešifrování: $M \equiv C^d$, protože $(M^e)^d = M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod{n}$.

Shrnutí RSA

n, e ... veřejné,

p, q, d ... soukromé.

Důkaz korektnosti dešifrování provádíme pomocí čínské zbytkové věty pro moduly p a q. (Pokud by M byla soudělná s p nebo q, je v tomoto modulu kongruentní s 0, a tedy i její mocniny. Tj. malá Fermatova věta ve formě $a^p \equiv a \pmod{p}$ platí i bez předpokladu nesoudělnosti.)

Faktory $p-1, q-1$ čísla $\phi(n)$ by měly být „málo soudělné“, jinak hrozí snazší prolomení.

Využití pro digitální podpis: majiteli soukromého klíče d pošleme zprávu M, on nám vrátí M^d. Pomocí veřejného klíče e zkontrolujeme, že $(M^d)^e = M$.

Příklad na RSA I

a) Zašifrujte zprávu $M = 123$ užitím veřejného klíče $n = 209, e = 7$.

b) Šifru prolomte a dešifrujte zprávu.

Řešení: a) $C = M^e = 123^7 \pmod{n}$ se nám počítat nechce bez znalosti rozkladu n. Začněme tedy částečným prolomením $209 = 11 \cdot 19$, spočítáme C pro faktory 11 a 19 a výsledky poskládáme přes čínskou zbytkovou větu:

$$123^7 \equiv 2^7 = (2^3)^2 \cdot 2 \equiv (-3)^2 \cdot 2 \equiv -2 \cdot 2 = -4 \pmod{11}$$
$$123^7 \equiv 9^7 = (9^2)^3 \cdot 9 \equiv 5^3 \cdot 9 \equiv 11 \cdot 9 \equiv 4 \pmod{19}$$

Tedy $123^7 = 11k - 4$ a $11k - 4 \equiv 4 \pmod{19}$. Po úpravě $-8k \equiv 8$, tj. $k \equiv -1 \pmod{19}$. Celkem $C = 123^7 \equiv -15 \equiv 194 \pmod{209}$.

Příklad na RSA II

b) $\phi(209) = (11-1)\cdot(19-1) = 180$.

Prolomení dešifrovacího klíče: inverzi d k $e = 7$ najdeme např. pomocí Eukleidova algoritmu pro hledání koeficientů do Bezoutovy rovnosti

$$180a + 7b = 1.$$

z	a	b
180	1	0
7	0	1
5	1	-25
2	-1	26
1	3	-77

Tj. $d \equiv -77 \equiv 103 \pmod{180}$.

Příklad na RSA III

Dešifrování: $M = C^d = 194^{103} \equiv (-15)^{103} \pmod{209}$. Obdobně jako u šifrování počítáme M odděleně přes faktory 11 a 19:

$$(-15)^{103} \equiv -4^{10\cdot 10+3} \equiv -4^3 \equiv -64 \equiv 2 \pmod{11}$$

$$(-15)^{103} \equiv 4^{5\cdot 18+13} = (4^3)^4 \cdot 4 \equiv 7^4 \cdot 4 \equiv 49^2 \cdot 4 \equiv \pmod{19}$$

$$\equiv (-8)^2 \cdot 4 \equiv 7 \cdot 4 \equiv 9$$

Tedy $(-15)^{103} = 11k + 2, 11k + 2 \equiv 9, 11k \equiv 7 \pmod{19}$.

Odtud $-8k \equiv 12, 2k \equiv 3 \equiv 22, k \equiv 11$.

Celkem $M = 194^{103} \equiv 11 \cdot 11 + 2 = 123 \pmod{209}$.

Vyšlo.

Výměna klíčů (Diffie, Hellman 1976, Williamson 1974)

p . . . prvočíslo (modul),

g . . . primitivní kořen v modulu p. (Tzn. nejmenší n splňující $g^n \equiv 1 \pmod{n}$ je $n = p - 1$.)

a . . . Alicin soukromý klíč (libovolný),

b . . . Bobův soukromý klíč (libovolný),

Alice pošle veřejně Bobovi g^a, podobně Bob pošle Alici g^b.

Přidáním svého klíče do mocniny si obě strany umí spočítat g^{ab}, což bude jejich *společný klíč*.

p, g, g^a, g^b jsou tedy veřejné,

Alice navíc vidí a, g^{ab}

a Bob navíc vidí b, g^{ab}.

Šifrování na základě Diffie–Hellman, šifra ElGamal

Po výpočtu společného soukromého klíče $e = g^{ab}$ mohou své soukromé klíče a, b obě strany zapomenout.

Dešifrovacím klíčem je inverze d k e (v modulu p), kterou si obě strany umí spočítat.

Alice zašifruje zprávu $C = Me$.

Bob dešifruje zprávu $M = Cd$.

Pro jednostranně posílánou zprávu stačí provést tyto kroky:

- Kdokoli zveřejní p, g,
- Bob zveřejní g^b,
- Alice si spočítá $e = g^{ab}$ a zveřejní g^a, $C = Me$,
- Bob spočítá $d = e^{-1}$ a $M = Cd$.

K prolomení šifry by bylo třeba z p, g, g^a umět určit a, o čemž jsme si říkali, že je obtížné (diskrétní logaritmus).

Příklad na šifru ElGamal

Nechť $p = 13, g = 7$ a Alice má veřejný klíč $g^a = 6$.

a) Ověřte, že g je primitivní kořen v modulu p.

b) Prolomte šifru nalezením Alicina soukromého klíče a.

Řešení: a) Musí platit $g^{12} \equiv 1 \pmod{13}$, ale my potřebujeme ověřit, že neplatí podobná kongruence pro menší exponent. Stačí ověřit $g^4 \not\equiv 1, g^6 \not\equiv 1$:

$$7^4 = (7^2)^2 \equiv (-3)^2 \equiv -4 \pmod{13},$$
$$7^6 = (7^2)^3 \equiv (-3)^3 \equiv -4 \cdot (-3) \equiv -1.$$

b) V a) jsme si rozumnou úvahou o kandidátních mocninách ušetřili práci, ale teď ty ostatní stejně musíme „otrocky“ vyzkoušet:

$$7^2 \equiv -3, \qquad 7^3 = 7^2 \cdot 7 \equiv -3 \cdot 7 \equiv 5,$$
$$7^5 = 7^2 \cdot 7^3 \equiv -3 \cdot 5 \equiv -2, \qquad 7^7 = 7^2 \cdot 7^5 \equiv -3 \cdot (-2) \equiv 6.$$

Odpověď: $a = 7$.

Komentáře k šifrování

- I protokol Diffie–Hellman / ElGamal lze využít k digitálnímu podpisu: ověřovatel vytvoří zprávu m a Alici (majitelce klíče a) pošle g^m. Ona odpoví $(g^m)^a = g^{am}$. Ověřovatel si výsledek zkontroluje jako $(g^a)^m$.
- Moderní šifrovací protokoly neutajují metodu. I bezpečná výměna klíčů může probíhat veřejně.
- U digitálního podpisu se nadělá spousta řečí kolem *hashování* zprávy, což jsme pro jednoduchost ignorovali. Zpráva by měla podepisovaného dostatečně prověřit a současně nevystavit nebezpečí prolomení soukromého klíče.
- **Požadavky:** Porozumět základní podstatě šifrování, dešifrování, digitálního podpisu. Znát princip protokolů RSA a Diffie–Hellman / ElGamal. Umět v nich šifrovat, dešifrovat a prolomit šifru pro malý modul.