Diskrétní matematika – cvičení 6. týden

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

jaro 2020

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Protokol probíhá tak, že si účastníci zvolí soukromé klíče – exponenty a a b a pošlou si navzájem příslušné mocniny $g^a \pmod p$ a $g^b \pmod p$, přičemž se (zatím?) neumí efektivně z těchto mocnin získat exponent $a \equiv \log_g g^a \pmod{\varphi(p)}$, tedy tzv. *diskrétní logaritmus*.

Společný souromý klíč se pak stanoví jako $g^{ab} \pmod p$. Druhý účastník jej spočítá jako $(g^a)^b$ z obdržené mocniny g^a a svého soukromého klíče b, první symetricky jako $(g^b)^a$.

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Při této příležitosti si ukážeme další způsob počítání mocnin (jde vpodstatě jen o jiný zápis), vhodný k algoritmizaci: mocninu g^a budeme v krocích výpočtu zapisovat ve tvaru $x \cdot y^z$ (začneme tedy s $1 \cdot g^a$) a postupně budeme zmenšovat exponent z – když dojdeme k $z = 0$, výpočet končí s výsledkem x. V každém kroku snížíme exponent na polovinu: pokud je $z = 2z'$, upravíme

$$x \cdot y^z \equiv x \cdot (y^2)^{z'} \equiv x \cdot (y')^{z'}$$

kde $y' \equiv y^2$ spočítáme explicitně. Pokud $z = 2z' + 1$, upravíme

$$x \cdot y^z \equiv x \cdot y \cdot (y^2)^{z'} \equiv x' \cdot (y')^{z'}$$

kde $x' \equiv x \cdot y$ a $y' \equiv y^2$ spočítáme explicitně.

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Budeme volit $a = 7$, $b = 11$ (lepší volit čísla nesoudělná s $\varphi(61)$, jinak bychom například mohli dospět k $a = 6$, $b = 10 \Rightarrow$ $7^{ab} \equiv 7^{60} \equiv 1 \pmod{61}$). Alice tedy spočítá a pošle

$$\begin{aligned} g^a &\equiv 7^7 \equiv 1 \cdot 7^7 \\ &\equiv 1 \cdot 7 \cdot (7^2)^3 \equiv 7 \cdot (-12)^3 \\ &\equiv 7 \cdot (-12) \cdot ((-12)^2)^1 \equiv (-23) \cdot 22^1 \\ &\equiv 43. \end{aligned}$$

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Bob pak spočítá a pošle

$$\begin{aligned} g^b &\equiv 7^{11} \equiv 1 \cdot 7^{11} \\ &\equiv 1 \cdot 7 \cdot (7^2)^5 \equiv 7 \cdot (-12)^5 \\ &\equiv 7 \cdot (-12) \cdot ((-12)^2)^2 \equiv (-23) \cdot 22^2 \\ &\equiv (-23) \cdot (22^2)^1 \equiv (-23) \cdot (-4)^1 \\ &\equiv 31. \end{aligned}$$

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Tedy

$$(7) \qquad \text{Alice} \underset{31}{\overset{43}{\rightleftarrows}} \text{Bob} \qquad (11)$$

Bob spočítá společný soukromý klíč jako

$$\begin{aligned} g^{ab} &\equiv (g^a)^b \equiv 43^{11} \equiv 1 \cdot (-18)^{11} \\ &\equiv 1 \cdot (-18) \cdot ((-18)^2)^5 \equiv (-18) \cdot 19^5 \\ &\equiv (-18) \cdot 19 \cdot (19^2)^2 \equiv 24 \cdot (-5)^2 \\ &\equiv 24 \cdot ((-5)^2)^1 \equiv 24 \cdot 25^1 \\ &\equiv 51. \end{aligned}$$

Příklad

Demonstrujte protokol výměny klíčů Diffie–Hellman pro zvolené prvočíslo $p = 61$ a primitivní kořen $g = 7$ s různými volbami a a b.

Řešení

Tedy

$$7 \qquad \text{Alice} \xrightarrow{43} \xleftarrow{31} \text{Bob} \qquad 11$$

Alice spočítá společný soukromý klíč jako

$$\begin{aligned} g^{ab} &\equiv (g^b)^a \equiv 31^7 \equiv 1 \cdot 31^7 \\ &\equiv 1 \cdot 31 \cdot (31^2)^3 \equiv 31 \cdot (-15)^3 \\ &\equiv 31 \cdot (-15) \cdot ((-15)^2)^1 \equiv 23 \cdot (-19)^1 \\ &\equiv 51. \end{aligned}$$

Příklad

Martin a Honza chtějí komunikovat šifrou ElGamal navrženou egyptským matematikem Taherem Elgamalem podle protokolu Diffieho a Hellmana na výměnu klíčů. Martin si zvolil prvočíslo $p = 41$ a jemu příslušný primitivní kořen $g = 11$ a dále si zvolil soukromý klíč – exponent $a = 10$. Zveřejnil tedy trojici čísel $p = 41$, $g = 11$, $g^a \equiv 9$. Honza mu poslal veřejným kanálem dvojici čísel $g^b \equiv 22$, $c \equiv 6$. Jakou zprávu Honza poslal?

Řešení

První poslané číslo g^b slouží pouze ke stanovení společného klíče podle protokolu Diffie–Hellman; Martin jej spočítal jako $g^{ab} \equiv (g^b)^a \equiv 22^{10}$ (jak jej spočítal Honza se nedozvíme, protože neznáme Honzův soukromý klíč – exponent b). Vlastní šifrování pak probíhá snadno jako násobení tímto společným klíčem, tedy:

$$c \equiv g^{ab} \cdot m \pmod{p}.$$

Řešení

Spočítáme prvně $g^{ab} \equiv (g^b)^a \equiv 22^{10}$:

$$\begin{aligned} g^{ab} &\equiv (g^b)^a \equiv 22^{10} \equiv 1 \cdot 22^{10} \\ &\equiv 1 \cdot (22^2)^5 \equiv 1 \cdot (-8)^5 \\ &\equiv 1 \cdot (-8) \cdot ((-8)^2)^2 \equiv (-8) \cdot (-18)^2 \\ &\equiv (-8) \cdot ((-18)^2)^1 \equiv (-8) \cdot (-4)^1 \\ &\equiv 32. \end{aligned}$$

Dostáváme tak kongruenci:

$$6 \equiv c \equiv g^{ab} \cdot m \equiv 32 \cdot m \pmod{41}.$$

Nyní tuto kongruenci vyřešíme a tím bude dešifrování hotové.

Řešení

$$
\begin{aligned}
41 \cdot m &\equiv 0 \\
32 \cdot m &\equiv 6 \\
9 \cdot m &\equiv -6 \\
5 \cdot m &\equiv 24 \equiv -17 \\
4 \cdot m &\equiv 11 \\
1 \cdot m &\equiv 13
\end{aligned}
$$

Poslaná zpráva tedy byla $m \equiv 13 \pmod{41}$.

Příklad

V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23$, $q = 31$, veřejným klíčem je pak $n = p \cdot q = 713$. Zašifrujte pro Alici zprávu $m \equiv 327 \pmod{713}$ a ukažte, jak bude Alice tuto zprávu dešifrovat.

Řešení

V Rabinově kryptosystému je šifrování dané umocňováním na druhou, tj. $c \equiv m^2 \pmod{713}$. Budeme počítat zvlášť modulo 23 a modulo 31,

$$c \equiv 327^2 \equiv 5^2 \equiv 2 \pmod{23}$$
$$c \equiv 327^2 \equiv (-14)^2 \equiv 10 \pmod{31}$$

nyní dáme výsledky dohromady:

Řešení

Nyní dáme částečné výsledky $c \equiv 2 \pmod{23}$, $c \equiv 10 \pmod{31}$ dohromady modulo 713:

$$\begin{aligned} 31 \cdot c &\equiv 2 \cdot 31 \\ 23 \cdot c &\equiv \qquad 10 \cdot 23 \\ 8 \cdot c &\equiv 2 \cdot 31 - 10 \cdot 23 \\ 7 \cdot c &\equiv -4 \cdot 31 - 1 \cdot 23 \\ c &\equiv 6 \cdot 31 - 9 \cdot 23 \equiv 692 \pmod{713} \end{aligned}$$

(samozřejmě to šlo spočítat přímo a to se opravdu děje při realizaci tohoto kryptosystému).

Řešení

Nyní se zabývejme dešifrováním. Potřebujeme vlastně spočítat odmocninu z 692 (mod 713). Opět počítáme zvlášť modulo 23 a 31, pak dáme výsledky dohromady (odmocnina už se přímo neumí). Modulo 23 platí:

$$1 \equiv m^{22} \;\Rightarrow\; m^2 \equiv \underbrace{m^{24}}_{c^{12}} \;\Rightarrow\; m^2 \equiv (c^6)^2 \;\Rightarrow\; m \equiv \pm c^6 \pmod{23}$$

(poslední implikace platí jen modulo prvočíslo!). Podobně

$$1 \equiv m^{30} \;\Rightarrow\; m^2 \equiv m^{32} = \Rightarrow\; m^2 \equiv (c^8)^2 \;\Rightarrow\; m \equiv \pm c^8 \pmod{31}$$

Obecně odmocninu z $c \pmod p$ lze spočítat jako $\pm c^{\frac{p+1}{4}} \pmod p$. Číselně:

$$m \equiv \pm 692^6 \equiv \pm 2^6 \equiv \pm 18 \pmod{23}$$
$$m \equiv \pm 692^8 \equiv \pm 10^8 \equiv \pm 14 \pmod{31}$$

Řešení

$$m \equiv \pm 692^6 \equiv \pm 2^6 \equiv \pm 18 \equiv \pm 5 \pmod{23}$$
$$m \equiv \pm 692^8 \equiv \pm 10^8 \equiv \pm 14 \pmod{31}$$

Vyšly 4 možnosti a opravdu všechny jsou odmocniny z c. V realizaci kryptosystému je potřeba zaručit, aby vždy pouze jediná odmocnina byla přípustná (např. ta kladná/menší), případně dodatečnou informací specifikovat, která z odmocnin je správně. Ke všem čtyřem možnostem dopočítejme výsledek, začneme s $m \equiv 5 \pmod{23}$, $m \equiv 14 \pmod{31}$.

Řešení

Začneme s $m \equiv 5 \pmod{23}$, $m \equiv 14 \pmod{31}$:

$$\begin{aligned} 31 \cdot m &\equiv 5 \cdot 31 \\ 23 \cdot m &\equiv \qquad 14 \cdot 23 \\ 8 \cdot m &\equiv 5 \cdot 31 - 14 \cdot 23 \\ 7 \cdot m &\equiv -10 \cdot 31 + 11 \cdot 23 \\ m &\equiv 15 \cdot 31 + 6 \cdot 23 \equiv 603 \pmod{713} \end{aligned}$$

Pro $m \equiv -5 \pmod{23}$, $m \equiv -14 \pmod{31}$ by bylo vše pouze s opačným znaménkem, dostaneme tedy dvě odmocniny $\pm 603 \equiv \pm 110 \pmod{713}$.

Řešení

Zbylé dvě dostaneme z $m \equiv 5 \pmod{23}$, $m \equiv -14 \pmod{31}$:

$$\begin{aligned} 31 \cdot m &\equiv 5 \cdot 31 \\ 23 \cdot m &\equiv \qquad -14 \cdot 23 \\ 8 \cdot m &\equiv 5 \cdot 31 + 14 \cdot 23 \\ 7 \cdot m &\equiv -10 \cdot 31 - 11 \cdot 23 \\ m &\equiv 15 \cdot 31 - 6 \cdot 23 \equiv 327 \pmod{713} \end{aligned}$$

a podobně pro opačná znaménka opačný výsledek, tedy $\pm 327 \pmod{713}$. Poznamenejme, že tímto postupem vlastně můžeme dospět rovnou ke všem čtyřem výsledkům naráz $\pm 15 \cdot 31 \pm 6 \cdot 23 \pmod{713}$ (ale bacha na znaménka, nejlepší když už tak vypočítat s jednou sadou znamének a pak předělat na $\pm$).

Poznámka

Kdy můžeme z kongruence $x^2 \equiv y^2 \pmod{m}$ odvodit $x \equiv \pm y$?
Přepišme první kongruenci jako

$$0 \equiv x^2 - y^2 \equiv (x-y)(x+y) \pmod{m}$$

tedy $m \mid (x-y)(x+y)$. Pokud je m prvočíslo, můžeme z toho usoudit, že $m \mid x-y$ (a tedy $x \equiv y$) nebo $m \mid x+y$ (a tedy $x \equiv -y$). Zkuste si rozmyslet, kdy obecně toto funguje.

Poznámka

Bezpečnost Rabinova kryptosystému: Předpokládejme, že existuje algoritmus počítající nějakou z odmocnin $c \pmod n$, budeme ji značit $\sqrt{c}$. Náhodně zvolíme m a pomocí algoritmu spočítáme $\sqrt{m^2}$. S pravděpodobností $1/2$ se nebude jednat o $\pm m$. V takovém případě je rozdíl $m - \sqrt{m^2}$ násobkem p, ale nikoliv q (jeden ze zbytků modulo p a q je stejný, druhý má opačné znaménko). Můžeme tedy jedno z prvočísel získat jako největší společný dělitel $(n, m - \sqrt{m^2})$.