Y36BEZ – Bezpečnost přenosu a zpracování dat

Róbert Lórencz

2. přednáška

Úvod 2

http://service.felk.cvut.cz/courses/Y36BEZ
lorencz@fel.cvut.cz

Obsah přednášky

- Vlastnosti prvočísel
- Umocňování v modulární aritmetice
- Základní pojmy v kryptologii
- Substituční šifry

Vlastnosti prvočísel (1)

Věta 17

Existuje nekonečně mnoho prvočísel.

Důkaz: Důkaz provedeme nepřímo sporem. Předpokládejme, že existuje jen konečně mnoho prvočísel a označme je $p_1, p_2, \ldots, p_k$. Mějme číslo $P = p_1 \cdot p_2 \cdots p_k + 1$. Pak $P > 1$ a z toho plyne, že P je buď prvočíslo, nebo složené číslo. Pokud je prvočíslo $\Rightarrow$ spor s předpokladem, že $p_1, p_2, \ldots, p_k$ jsou všechna prvočísla. Pokud P je složené číslo, pak je dělitelné podle Věty 13 (1. přednáška) některým z prvočísel $p_1, p_2, \ldots, p_k$. Potom ze vztahu $P = p_1 \cdot p_2 \cdots p_k + 1$ dostáváme

$$1 = P - p_1 \cdot p_2 \cdot \cdots \cdot p_k$$

a z Věty 14 (1. přednáška) dále plyne, že pravá strana a pak také levá strana jsou dělitelné některým z prvočísel $p_1, p_2, \ldots, p_k$. To je ale spor, protože 1 není dělitelná žádným prvočíslem. Předpoklad o konečnosti množiny prvočísel vede ke sporu, proto je prvočísel nekonečně mnoho!

Vlastnosti prvočísel (2)

Definice funkce $\pi(x)$

Funkce $\pi(x)$, kde $x \in \mathbb{R}^+$, označuje počet prvočísel, která jsou menší než x.

Příklad: $\pi(10) = 4$, protože počet prvočísel menší než 10 je právě 4 a jsou to prvočísla: 2, 3, 5 a 7.

Věta 18 – Věta o prvočíslech

Poměr $\pi(x)$ k funkci $x/\log(x)$ se s rostoucím x přibližuje hodnotě 1, tj.

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1 \ .$$

Věta o prvočíslech byla formulována bez důkazu v roce 1791 matematikem Gaussem. Až v roce 1896 nezávisle na sobě je dokázali matematici Hadamard a Poussin.

Vlastnosti prvočísel (3)

V tabulce jsou uvedeny některé hodnoty x hodnoty $\pi(x)$, $x/\log(x)$ a poměr $\pi(x)/\frac{x}{\log(x)}$, které předpovídají platnost věty o prvočíslech.

x	$\pi(x)$	$x/\log(x)$	$\pi(x)/\frac{x}{\log(x)}$
10^3	168	144,8	1,160
10^4	1229	1085,7	1,132
10^5	9592	8685,9	1,104
10^6	78498	72382,4	1,085
10^7	664579	620420,7	1,071
10^8	5761455	5428681,0	1,061
10^9	50847534	48254942,4	1,054
10^{10}	455052512	434294481,9	1,048
10^{11}	4118054813	3948131663,7	1,043
10^{12}	37607912018	36191206825,3	1,039

Vlastnosti prvočísel (4)

Věta 19 - Malá Fermatova věta

Když p je prvočíslo a $a \in \mathbb{N}$ takové, že platí $p \nmid a$, potom

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

Věta 20 – pomocná

Když $a, b, c, m \in \mathbb{Z}$, $m > 0$, $d = \gcd(c, m)$ a $ac \equiv bc \pmod{m}$ potom platí:

$$a \equiv b \pmod{m/d}.$$

Důkaz pomocné věty: Když $ac \equiv bc \pmod{m}$, potom $m|(ac - bc)$ a existuje celé číslo k takové, že $c(a - b) = km$. Pokud vydělíme obě strany poslední rovnosti číslem d, pak

$$(c/d)(a - b) = k(m/d).$$

Protože $\gcd(m/d, c/d) = 1$ (Věta 8) a vzhledem k pomocné Větě 11 platí $(m/d)|(a - b)$, tj. $a \equiv b \pmod{m/d}$.

Vlastnosti prvočísel (5)

Důkaz Malé Fematovy věty: Uvažujme $(p-1)$ celých čísel $a, 2a, \ldots, (p-1)a$. Žádné z těchto čísel není dělitelné prvočíslem p. Pokud by $p|(ja) \Rightarrow$ z platnosti $p \nmid a$ a z pomocné Věty 11 plyne, že $p|j$ a to není možné, protože $1 \leq j \leq p-1$. Dále také žádná dvojice z těchto čísel není navzájem kongruentní modulo p. To je možné dokázat, pokud předpokládáme, že $ja \equiv ka \pmod{p}$, kde $1 \leq j < k \leq p-1$. Potom vzhledem k tomu, že $\gcd(a,p) = 1$ a z pomocné Věty 20 platí $j \equiv k \pmod{p}$ a to je nemožné, protože $1 \leq j < k \leq p-1$.
Čísla $a, 2a, \ldots, (p-1)a$ mají nenulové kongruence modulo p a žádná dvě nejsou vzájemně kongruentní modulo p. Pak nejmenší kladná rezidua těchto čísel modulo p tvoří množinu čísel $\{1, 2, \ldots, p-1\} \Rightarrow$

$$\begin{aligned} a \cdot 2a \cdots (p-1)a &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p}, \end{aligned}$$

s využitím pomocné věty 20 a platnosti $\gcd((p-1)!, p) = 1$.

Vlastnosti prvočísel (6)

Příklad: Mějme $p = 5$ a $a = 3$. Pak $1 \cdot 3 \equiv 3 \pmod 5$, $2 \cdot 3 \equiv 1 \pmod 5$, $3 \cdot 3 \equiv 4 \pmod 5$, $4 \cdot 3 \equiv 2 \pmod 5$, a tak

$$\begin{aligned} (1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) &\equiv 3 \cdot 1 \cdot 4 \cdot 2 \pmod 5 \\ 3^4 \cdot 1 \cdot 2 \cdot 3 \cdot 4 &\equiv 3 \cdot 1 \cdot 4 \cdot 2 \pmod 5 \\ 3^4 \cdot 4! &\equiv 4! \pmod 5 \\ 3^4 &\equiv 1 \pmod 5 . \end{aligned}$$

Věta 21

Když p je prvočíslo a $a \in \mathbb{N}$ potom

$$a^p \equiv a \pmod p .$$

Důkaz: Pro $p \nmid a$ z Malé Fermatovy věty plyne, že $a^{p-1} \equiv 1 \pmod p$. Vynásobením levé a pravé strany kongruence číslem a získáme kongruenci $a^p \equiv a \pmod p$. Pokud $p|a$, pak taky $p|a^p$, a platí $a^p \equiv a \equiv 0 \pmod p \Rightarrow a^p \equiv a \pmod p$ jak pro $p \nmid a$, tak pro $p|a$.

Vlastnosti prvočísel (7)

Malá Fermatova věta je užitečná při hledání nejmenšího kladného rezidua mocniny.

Příklad: Najděte nejmenší kladný zbytek mocniny 5^{203} modulo 101. Z malé Fermatovy věty víme, že platí $5^{100} \equiv 1 \pmod{101}$, a pak $5^{203} = (5^{100})^2 \cdot 5^3 \equiv 125 \equiv 24 \pmod{101}$.

Další možností použití malé Fermatovy věty je výpočet multiplikativní inverze čísla $a \in \mathbb{N}$ modulo p.

Věta 22

Pokud je p prvočíslo, $a \in \mathbb{N}$ a platí, že $p \nmid a$, pak a^{p-2} je multiplikativní inverzí čísla a modulo p.

Důkaz: Když $p \nmid a$, pak z malé Fermatovy věty plyne, že $a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$. Z Definice 4 je potom a^{p-2} multiplikativní inverzí čísla a modulo p.

Vlastnosti prvočísel (8)

Příklad: Z předcházející věty plyne, že $2^5 = 32 \equiv 4 \pmod 7$. Potom číslo 4 je multiplikativní inverzí čísla 2 modulo 7.

Když modul je složené číslo $\Rightarrow$ nelze využít vlastností plynoucích z Malé Fermatovy věty pro výpočty mocnin a multiplikativních inverzí. Pro tento účel je vhodné využít Eulerovu větu. Nejdřív si uvedeme definice Eulerovy funkce Φ a redukovaného zbytkového systému.

Definice Eulerovy funkce

Nechť $n \in \mathbb{N}$. Eulerova funkce $\Phi(n)$ je definována jako funkce proměnné n, která udává počet kladných celých čísel menších než n a nesoudělných s n.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Tabulka: Hodnoty pro Eulerovu funkci $\Phi(n)$

Vlastnosti prvočísel (9)

Definice Redukovaného zbytkového systému

Redukovaný zbytkový systém je množinou $\Phi(n)$ celých čísel, kde každé číslo z této množiny je nesoudělné s n a každá dvojice čísel z této množiny je vzájemně nekongruentní modulo n.

Příklad: Množina $\Phi(8) = 4$ celých čísel $\{1, 3, 5, 7\}$ tvoří redukovaný zbytkový systém modulo 8. Množina $\{-3, -1, 1, 3\}$ tvoří také redukovaný zbytkový systém modulo 8.

Věta 23

Když $r_1, r_2, \ldots, r_{\Phi(n)}$ je redukovaný zbytkový systém modulo n, $a \in \mathbb{N}$ a $\gcd(a, n) = 1$, potom množina $ar_1, ar_2, \ldots, ar_{\Phi(n)}$ je také redukovaný zbytkový systém modulo n.

Vlastnosti prvočísel (10)

Důkaz (2): Abychom dokázali, že každé celé číslo ar_j a číslo n jsou nesoudělná, budeme předpokládat, že $\gcd(ar_j, n) > 1$. Pak existuje prvočíselný dělitel p čísla $\gcd(ar_j, n)$. Proto buď $p|a$, nebo $p|r_j$. Tedy buď $p|a$ a $p|n$, nebo $p|r_j$ a $p|n$. Avšak nemůže platit, že $p|r_j$ a současně $p|n$ protože r_j je prvkem redukovaného zbytkového systému modulo n. Také neplatí, že $p|a$ a $p|n$, protože $\gcd(a, n) = 1$. Pak ar_j a n jsou nesoudělná pro $j = 1, 2, \ldots, \Phi(n)$.

Abychom dokázali tvrzení, že každá dvě čísla ar_j a ar_k nejsou kongruentní modulo n, budeme předpokládat, že $ar_j \equiv ar_k \pmod{n}$, kde j a k jsou rozdílná kladná celá čísla, pro která platí: $1 \leq j \leq \Phi(n)$ a $1 \leq k \leq \Phi(n)$. Protože $\gcd(a, n) = 1$ s pomocné Věty 20 dostáváme: $r_j \equiv r_k \pmod{n}$. Toto je ale spor, protože r_j a r_k jsou prvky redukovaného zbytkového systému modulo n. Pro prvky r_j a r_k takového systému platí $r_j \not\equiv r_k \pmod{n}$.

Vlastnosti prvočísel (11)

Příklad: Množina $\Phi(8) = 4$ celých čísel $\{1, 3, 5, 7\}$ tvoří redukovaný zbytkový systém modulo 8. Protože $\gcd(3, 8) = 1$, z Věty 24 plyne, že čísla $3, 9, 15$ a 21 tvoří také redukovaný zbytkový systém modulo 8.

Věta 24 – Eulerova věta

Nechť $m \in \mathbb{N}$ a $a \in \mathbb{Z}$. Když $\gcd(a, m) = 1 \Rightarrow \quad a^{\Phi(m)} \equiv 1 \pmod{m}$.

Důkaz: Nechť $r_1, r_2, \ldots, r_{\Phi(m)}$ označuje redukovaný zbytkový systém. Protože $\gcd(a, m) = 1$, a platí Věta 23, je množina $\{ar_1, ar_2, \ldots, ar_{\Phi(m)}\}$ také redukovaným zbytkovým systémem modulo m. Proto nejmenší kladné zbytky musí tvořit množinu celých čísel $\{r_1, r_2, \ldots, r_{\Phi(m)}\} \Rightarrow$

$$ar_1 \cdot ar_2 \cdots ar_{\Phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\Phi(m)} \pmod{m}$$

$$a^{\Phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\Phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\Phi(m)} \pmod{m}.$$

Protože $\gcd(r_i, m) = 1$ pro $i = 1, \ldots, \Phi(m)$ a tak s pomocnou Větou 20 dostáváme $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Vlastnosti prvočísel (12)

Pro nalezení multiplikativní inverze celého čísla a modulo m, kde $\gcd(a, m) = 1$, použijeme Větu 24 (Eulerovu)

$$a \cdot a^{\Phi(m)-1} = a^{\Phi(m)} \equiv 1 \pmod{m}.$$

Pak $a^{\Phi(m)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod{9} \Rightarrow |5 \cdot 2|_9 = 1$.

Věta 25

Když p je prvočíslo, potom $\Phi(p) = p - 1$. Obráceně, pokud $p \in \mathbb{N}$ a platí $\Phi(p) = p - 1$, pak p je prvočíslo.

Důkaz: Když p je prvočíslo $\Rightarrow$ každé kladné číslo $< p$ je nesoudělné s p. Existuje právě $p - 1$ takových kladných čísel, a platí $\Phi(p) = p - 1$. Obráceně, kdyby bylo p složené číslo, pak p má dělitele d, pro který platí $1 < d < p$. Odsud plyne, že nejméně jedno číslo z $p - 1$ celých kladných čísel $1, 2, \ldots, p - 1$, jmenovitě $d \mid p$, tj. $\Phi(p) \leq p - 2$. Proto, když $\Phi(p) = p - 1 \Rightarrow p$ musí být prvočíslo.

Vlastnosti prvočísel (13)

Věta 26

Nechť p je prvočíslo a $a \in \mathbb{N}$. Potom

$$\Phi(p^a) = p^a - p^{a-1}.$$

Důkaz: Kladná celá čísla menší než p^a, která jsou soudělná s prvočíslem p, jsou celá kladná čísla, která jsou dělitelná prvočíslem p. Potom je můžeme vyjádřit ve tvaru kp, kde $1 \leq k \leq p^{a-1}$. Z toho vyplývá, že existuje přesně p^{a-1} takových čísel, a tak je právě $p^a - p^{a-1}$ celých čísel menších než p^a, která nejsou soudělná s prvočíslem p, pak $\Phi(p^a) = p^a - p^{a-1}$.

Věta 27

Nechť $m, n \in \mathbb{N}$ a $\gcd(m, n) = 1$. Potom

$$\Phi(mn) = \Phi(m)\Phi(n).$$

Vlastnosti prvočísel (14)

Důkaz (1): Uveďme kladná celá čísla menší než mn ve tvaru matice $m \times n$:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & & \vdots \\ r & m+r & 2m+r & \cdots & (n-1)m+r \\ \vdots & \vdots & \vdots & & \vdots \\ m & 2m & 3m & \cdots & nm\,. \end{array}$$

Nyní předpokládejme, že r je kladné celé číslo, které není větší než m. Dále nechť platí $\gcd(m, r) = d > 1$. Pak každé číslo v r-tém řádku je soudělné s mn, protože každý prvek tohoto řádku můžeme vyjádřit jako číslo $km + r$, kde $k \in \mathbb{Z}$ a $1 \leq k \leq n - 1$, a tak $d|(km + r)$, protože $d|m$ a $d|r$.

Vlastnosti prvočísel (15)

Důkaz (2): Pro nalezení celých čísel, která jsou nesoudělná s mn, potřebujeme vyhledat takové řádky, pro které platí $\gcd(m, r) = 1$. Prvky takových řádků jsou $r, m + r, 2m + r, \ldots, (n - 1)m + r$. Protože platí $\gcd(r, m) = 1$, každý prvek tohoto řádku je nesoudělný s m. Množina prvků řádku r tvoří úplný zbytkový systém modulo n. V případě, že dané tvrzení neplatí, jsou minimálně dva prvky řádku r kongruentní modulo n, tj. $im + r \equiv jm + r \pmod{n}$. Protože $\gcd(m, n) = 1$, tak po úpravě dostáváme $i \equiv j \pmod{n}$. Pokud $i \neq j$ platí $i \not\equiv j \pmod{n}$. Protože řádek r je složený s n navzájem nekongruentních prvků, tvoří úplný zbytkový systém modulo n. Funkce $\Phi(n)$ tak udává počet těch prvků zbytkového systému, které jsou nesoudělné s číslem n. Protože tato čísla jsou také nesoudělná s číslem m, jsou také nesoudělná s číslem mn.
Protože existuje $\Phi(m)$ řádků, které obsahují $\Phi(n)$ nesoudělných prvků k mn, můžeme psát $\Phi(mn) = \Phi(m)\Phi(n)$.

Vlastnosti prvočísel (16)

Věta 28

Nechť číslo $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ je kanonický rozklad složeného čísla $n \in \mathbb{N}$. Potom

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

Důkaz (1): Vzhledem k tomu, že funkce Φ je multiplikativní, můžeme psát

$$\Phi(n) = \Phi(p_1^{\alpha_1})\Phi(p_2^{\alpha_2})\cdots\Phi(p_k^{\alpha_k}).$$

Z Věty 26 víme, že platí

$$\Phi(p_j^{\alpha_j}) = p_j^{\alpha_j} - p_j^{\alpha_j - 1} = p_j^{\alpha_j}\left(1 - \frac{1}{p_j}\right), \text{ pro } j = 1, 2, \ldots, k.$$

Odsud

$$\begin{aligned}\Phi(n) &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Vlastnosti prvočísel (17)

Důkaz (2):

$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Příklad: S použitím věty 28 pro hodnotu $\Phi(100)$ můžeme psát

$$\Phi(100) = \Phi(2^2 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

a

$$\Phi(360) = \Phi(2^3 3^2 5) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 96.$$

Umocňování v modulární aritmetice (1)

V kryptografii se setkáme s požadavkem velké mocniny celého čísla. Příklad $|2^{644}|_{645} = ?$. Výpočtem 2^{644} dostaneme číslo s 194 desítkovými číslicemi! Namísto toho si nejdříve vyjádříme exponent v binárním zápisu:

$$(644)_{10} = (1010000100)_2.$$

Dále si spočítáme nejmenší pozitivní rezidua mocnin $2, 2^2, 2^4, \ldots, 2^{512}$, jako postupné umocňování na druhou a redukce modulo 645 $\Rightarrow$

$$\begin{aligned}
|2|_{645} &= 2, \\
|2^2|_{645} &= 4, \\
|2^4|_{645} &= 16, \\
|2^8|_{645} &= 256, \\
|2^{16}|_{645} &= 391, \\
|2^{32}|_{645} &= 16, \\
|2^{64}|_{645} &= 256, \\
|2^{128}|_{645} &= 391, \\
|2^{256}|_{645} &= 16, \\
|2^{512}|_{645} &= 256.
\end{aligned}$$

Umocňování v modulární aritmetice (2)

Dále můžeme výpočet $|2^{644}|_{645}$ provést jako násobení nejmenších kladných zbytků odpovídajících mocnin dvou. Potom dostáváme

$$\begin{aligned} |2^{644}|_{645} &= |2^{512+128+4}|_{645} = \left||2^{512}|_{645}|2^{128}|_{645}|2^{4}|_{645}\right|_{645} \\ &= |256 \cdot 391 \cdot 16|_{645} = |1601536|_{645} = 1. \end{aligned}$$

V předchozím příkladě jsme právě ilustrovali všeobecnou proceduru *modulárního umocňování*, tj. výpočet $|b^N|_m$, kde b, m a N jsou nezáporná celá čísla. Exponent N si vyjádříme v binárním zápisu $N = (a_k, a_{k-1}, \ldots, a_1, a_0)_2$. Následně najdeme postupným umocňováním na druhou a následnou redukcí modulo m nejmenší kladná celá rezidua mocnin $b, b^2, b^4, b^8, \ldots, b^{2^k}$. Nakonec vynásobíme nejmenší kladná rezidua $|b^j|_m$ pro takové j, pro které platí $a_j = 1$, přičemž po každém násobení provádíme redukci modulo m vzniklého součinu.

Umocňování v modulární aritmetice (3)

Věta 29 – Odhad počtu bitových operací modulárního umocňování.

Nechť b, m a N jsou kladná celá čísla, kde platí $b < m$. Potom nejmenší kladné reziduum mocniny $|b^N|_m$ může být vypočteno s použitím $O((\log_2 m)^2 \log_2 N)$ bitových operací.

Důkaz: Pro nalezení nejmenšího kladného rezidua $|b^N|_m$ můžeme použít popsaný algoritmus. Nejdříve vypočítáme nejmenší kladná rezidua $b, b^2, b^4, b^8, \ldots, b^{2^k}$ modulo m, kde $2^k \leq N < 2^{k+1}$ postupným umocňováním na druhou s redukcí modulo m. To vyžaduje $O((\log_2 m)^2 \log_2 N)$ bitových operací. Dále vynásobíme nejmenší kladná rezidua $|b^j|_m$ pro takové j, pro které platí $a_j = 1$, přičemž po každém násobení redukujeme vzniklý součin modulo m. To také vyžaduje $O((\log_2 m)^2 \log_2 N)$ bitových operací, protože existuje nanejvýš $\log_2 N$ násobení a každé vyžaduje $O((\log_2 m)^2)$ bitových operací. Z toho plyne, že pro všechny operace potřebujeme $O((\log_2 m)^2 \log_2 N)$ bitových operací.

Základní pojmy v kryptologii (1)

- Kryptologie – tvorba a luštění šifer.
  - Kryptografie – věda o tvorbě šifer.
  - Kryptoanalýza – věda o luštění šifer.
- Otevřený Text (OT) – text, který je určen k utajení.
- Šifrování – proces převádející otevřený text do Šifrového Textu (ŠT).
- Šifra – metoda, která převádí text do utajené formy.
- Dešifrování – proces opačný k procesu šifrování, je založený na znalosti šifry.

Luštění:

- Identifikace – jaký šifrovací systém byl použit.
- Prolomení – způsob šifrování zprávy, určení neměnných částí systému.
- Nastavení – určení, jak se mění proměnlivé části kryptosystému.

Základní pojmy v kryptologii (2)

Šifra – utajení obsahu zprávy před nepovolanou osobou.

Kód – neutajuje se zpráva, ale upravuje tak, aby ji bylo možné přenést přes nějaký kanál!

- Například kódy pro detekci chyb – paritní, nebo
- samoopravné kódy – Hammingovy kódy.

Šifrovací systémy vytváří šifrovou zprávu z OT pomocí nějakého pravidla – šifrovacího algoritmu.

Do nástupu počítačů dominovaly 3 základní metody:

1. substituční,
2. transpoziční,
3. metoda kódové knihy.

Šifrovací systémy byly založeny na jedné z nich nebo na nějaké kombinaci 2 nebo 3 těchto metod.

Základní pojmy v kryptologii (3)

Šifry využívající substituci

- Jednoduchá substituce – jednu a tutéž záměnu (zamíchání) pro celý OT $\Rightarrow$, Caesarova šifra (A $\rightarrow$ D, B $\rightarrow$ E, ... W $\rightarrow$ Z, X $\rightarrow$ A, Y $\rightarrow$ B, Z $\rightarrow$ C). Pokud A = 0, B =1, ..., Z = 25, p označuje písmeno OT a c označuje písmeno ŠT pak $c = |p + 3|_{26}$, kde $0 \leq c \leq 25$.
- Polyalfabetická substituce – pro každé písmeno OT můžeme abecedu nově zamíchat. Například k písmenům OT pořadě přičítáme (modulo 26) nějaká jiná čísla – písmena nahrazena čísly – klíč. Periodicky opakující se heslo $\Rightarrow$ Vigenerův systém.

Šifry transpoziční – šifrování spočívá v zamíchaní písmen OT – nemění je za jiné. Nejjednodušší příklad jsou přesmyčky nebo lišťovky.

Substituční a transpoziční šifry jsou symetrické, protože používají stejný klíč pro šifrování a dešifrování.

Základní pojmy v kryptologii (4)

Šifrování pomoci kódové knihy

- Slovník s běžnými frázemi tvořenými jedným nebo více písmeny, čísly, nebo slovy, typicky nahrazované čtveřicemi nebo pěticemi písmen nebo čísel – kódové skupiny.
- K často používaným výrazům nebo písmenům může kódová kniha obsahovat několik kódových skupin. Umožní odeslílateli výběr a ztíží identifikaci často používaných frází ("pondělí" = 2476 nebo 7032 nebo 6845).
- Překlad zprávy do jiného jazyka lze považovat za šifrování pomocí kódové knihy – slovníku. Význam pojmu kódová kniha je v tomto případě rozšířen do krajnosti. Použití málo známeho jazyka k předávání zpráv krátkodobého významu (II. světová válka, americká armáda v pacifiku – jazyk Navajů).
- Osobní těsnopis (středověk) k psaní osobních deníků. Pravidelný výskyt symbolů (názvy dnů atd.) poskytují dostatečný klíč k rozluštění.

Základní pojmy v kryptologii (5)

Posuzování spolehlivosti šifrových systémů

Při posuzování navrhovaného šifrovacího systému je důležité posoudit jeho sílu – odolnost vůči všem známým útokům za předpokladu znalosti typu tohoto šifrovacího systému.

Odolnost šifrovacího systému může být posuzována ve 3 různých situacích. Kryptoanalytik má :

1. ŠT (systém rozluštěný v této situaci za rozumnou dobu je nepoužitelný)
2. ŠT a odpovídající OT (zpráva je šifrována jak pomocí "starého" tak "nového" systému, kde "starý" systém je rozluštěn),
3. ŠT a odpovídající OT, který si sám zvolil (situace typická při posuzování navrhovaného šifrovacího systému kryptoanalytiky).

2. a 3. situace může nastat, pokud jsou k dispozici pro kryptoanalýzu zprávy od špionů.

Základní pojmy v kryptologii (6)

Existují jiné metody skrývání smyslu nebo obsahu zprávy, které nejsou založené na šifrách. Za zmínku stojí steganografie, která je založená na principu vkládání zprávy do běžných a nepodezřelých objektů – textových zpráv, programů, obrázků atd.

V dalším textu budeme také používat následující pojmy:

- Monogram – jedno písmeno v jakékoliv abecedě.
- Bigram – jakákoliv dvojice sousedních písmen v textu.
- Trigram – trojice po sobě následujících písmen.
- Polygram – nespecifikovaný počet písmen po sobě jdoucích v textu.
- Symbol – jakékoliv písmeno, číslice, interpunkční znaménko atd., které se mohlo v textu vyskytnout.
- Řetězec – jakákoliv posloupnost po sobě jdoucích symbolů.

Substituční šifry (1)

Substituční šifry

Šifra použitá Juliem Caesarem je vyjádřena vztahem: $c = |p + 3|_{26}$, kde $0 \leq c \leq 25$. Dále budeme používat označení p pro písmeno OT a c pro písmeno ŠT. Za standard si vezmeme písmena anglické abecedy a přidělíme jim celá čísla od 0 do 25, viz Tabulka

Tabulka: Numerický ekvivalent písmenům anglické abecedy

písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
num. ekv.	0	1	2	3	4	5	6	7	8	9	10	11	12
písmeno	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
num.ekv.	13	14	15	16	17	18	19	20	21	22	23	24	25

Příklad: Otevřený text seskupíme do bloků po pěti písmenech. Toto seskupení písmen do bloků je jakousi jednoduchou prevencí proti provedení krytoanalýzy založené na rozpoznávání jednotlivých slov.

Substituční šifry (2)

Takže zprávu

THIS MESSAGE IS TOP SECRET

převedeme do bloků po pěti písmenech

THISM ESSAG EISTO PSECR ET.

Převodem písmen do jejich numerických ekvivalentů dostaneme

19 7 8 18 12 4 18 18 0 6 4 8 18 19 14 15 18 4 2 17 4 15.

S použitím Caesarovy transformace $c = |p + 3|_{26}$ dostáváme

22 10 11 21 15 7 21 21 3 9 7 11 21 22 17 18 21 7 5 20 7 18

a převodem zpět na písmena obdržíme šifrový text

WKLVP HVVDJ HLVWR SVHFU HW.

Substituční šifry (3)

Příjemce zašifrované zprávy ji dešifruje následujícím způsobem:

1. převede písmena na jejich číselné ekvivalenty.
2. na základě vztahu $p = |c - 3|_{26}$, $0 \leq p \leq 25$ převede ŠT v číselné podobě na číselnu podobu OT.
3. převede zprávu do písemné podoby.

Dešifrovací postup si můžeme ukázat na dešifrování následující zprávy, která je šifrována Caesarovou šifrou:

WKLVL VKRZZ HGHFL SKHU.

Takže nejdříve převedeme zprávu do číselné podoby a získáme

22 10 11 21 11 21 10 17 25 25 7 6 7 5 11 18 10 7 20.

Dále provedeme transformaci $p = |c - 3|_{26}$, $0 \leq p \leq 25$, a tím získáme otevřený text v číselné podobě

19 7 8 18 8 18 7 14 22 22 4 3 4 2 8 15 7 4 17.

Substituční šifry (4)

Převodem na písmena dostáváme otevřený text v blocích po pěti písmenech

THISI SHOWW EDECI PHER.

Kombinací příslušných písmen vytvoříme slova a naše zpráva je

THIS IS HOW WE DECIPHER.

Caesarova šifra patří do rodiny jednoduchých šifer popsaných *transformací posunem*

$$c = |p + k|_{26}, \qquad 0 \leq c \leq 25,$$

kde k je klíč reprezentující velikost posunutí písmen v abecedě. Existuje 26 různých transformací tohoto typu šifry, zahrnující také $|k|_{26} = 0$, kde nedochází k žádnému posunu.

Je zřejmé, že obecně existuje 26! možných způsobů generování substituční šifry s písmeny abecedy založené na posunu.

Substituční šifry (5)

O něco málo obecnější šifrou je šifra s transformací typu

$$c = |ap + b|_{26}, \qquad 0 \leq c \leq 25, \tag{1}$$

kde $a, b \in \mathbb{Z}$ a splňují podmínku $\gcd(a, 26) = 1$. Tato šifra je tzv. afinní transformace. Transformace posunem je afinní transformací pro $a = 1$. Když $\gcd(a, 26) = 1 \Rightarrow p$ a c je také z úplného systému reziduí modulo 26 a to nám umožňuje vybrat 12 konstant a ($\Phi(26) = 12$) a 26 b a tedy $12 \cdot 26 = 312$ transformací tohoto typu (zahrnující také $c = |p|_{26}$, pro $a = 1$ a $b = 0$). Pokud je vztah OT a ŠT popsaný vzájemným vztahem (1), potom je inverzní vztah daný

$$p = |(a^{-1}(26)) \cdot (c - b)|_{26}, \qquad 0 \leq p \leq 25. \tag{2}$$

Příklad: Pro $a = 7$ a $b = 10$ a tedy $c = |7p + 10|_{26} \Rightarrow$ pro dešifrování platí $p = |15(c - 10)|_{26} = |15c + 6|_{26}$, protože $15^{-1}(26) = |7|_{26}$.

Substituční šifry (6)

Pro ilustraci šifrujme OT: "PLEASE SEND MONEY",
který je převeden do ŠT: "LJMKG MGMFQ EXMW".

Obráceně ŠT: "FEXEN ZMBMK JNHMG MYZMN"
odpovídá OT: "DONOT REVEA LTHES ECRET"

a po seskupení slov máme "DO NOT REVEAL THE SECRET".

Tabulka: Vzájemý vztah písmen pro šifru: $c = |7p + 10|_{26}$

OT	A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
ŠT	K 10	R 17	Y 24	F 5	M 12	T 19	A 0	H 7	O 14	V 21	C 2	J 9	Q 16
OT	N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25
ŠT	X 23	E 4	L 11	S 18	Z 25	G 6	N 13	U 20	B 1	I 8	P 15	W 22	D 3

Substituční šifry (7)

Dále se budeme zabývat některými jednoduchými postupy kryptoanalýzy šifer založených na afinních transformacích.

Pokus prolomit nějakou znakovou šifru může začít porovnáním četnosti výskytu písmen v ŠT a OT. Takto získáme informaci o vztahu mezi písmeny ŠT a OT. Různá frekvence výskytu 26 písmen anglické abecedy v OT je uvedena v % v tabulce.

Tabulka: Četnost výskytu jednotlivých písmen v běžném anglickém textu.

písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
četnost[%]	7	1	3	4	13	3	2	3	8	<1	<1	4	3
písmeno	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
četnost[%]	8	7	3	<1	8	6	9	3	1	1	<1	2	<1

Vidíme, že typický anglický text má největší výskyt písmen E, T, N, R, I, O a A. E má 13% a T, N, R, I, O a A mají výskyt v rozmezí 7% až 9%. Tuto informaci můžeme dobře využít pro určení koeficientů afinní šifry.

Substituční šifry (8)

Mějme k šifrování šifru s posunem: $c = |p + k|_{26}$, $0 \leq c \leq 25$. Nechť ŠT určený ke kryptoanalýze na základě uvedených předpokladů je

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDLR PD.

V tabulce jsou uvedeny hodnoty četností výskytu písmen ŠT.

písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
četnost	1	0	4	5	1	3	0	0	0	1	0	1	1
písmeno	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
četnost	1	0	7	2	2	2	3	0	0	1	2	3	2

Relativně největší výskyt písmen v ŠT je P, C, D, F, T a Y. Odhad: P v ŠT reprezentuje E v OT. Potom $|4 + k|_{26} = 15$ a z toho $|11|_{26} = k$. Po dosazení máme pro $c = |p + 11|_{26}$ a obráceně $p = |c - 11|_{26}$. Použitím tohoto vztahu můžeme z uvedeného ŠT psát následující OT:

NUMBER THEORY IS USEFUL FOR ENCIPHERING MESSAGES.

Z toho je vidět, že naše předpoklady byly správné.

Substituční šifry (9)

Dále předpokládejme použití afinní transformace podle vztahu (1), kterou byla šifrována následující zpráva

USLEL JUTCC YRTPS URKLT YGGFV
ELYUS LRYXD JURTU ULVCU URJRK
QLLQL YXSRV LBRYZ CYREK LVEXB
RYZDG HRGUS LJLLM LYPDJ LJTJU
FALGU PTGVT JULYU SLDAL TJRWU
SLJFE OLPU

V tabulce jsou uvedeny četnosti výskytu jednotlivých písmen v ŠT.

písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
četnost	2	2	4	4	5	3	6	1	0	10	3	22	1
písmeno	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
četnost	0	1	4	2	12	7	8	16	5	1	3	10	2

Substituční šifry (10)

Znovu předpokládejme, že písmeno L, které se nejvíce vyskytuje v ŠT je písmenem E v OT a písmeno U v ŠT, které má druhou největší četnost, odpovídá písmenu T v OT. Potom podle vztahu (1) dostáváme soustavu dvou kongruencí.

$$\begin{aligned} |4a+b|_{26} &= 11 \\ |19a+b|_{26} &= 20 \end{aligned}$$

Řešení této soustavy je: $|a|_{26} = 11$ a $|b|_{26} = 19$. Pokud jsou to konstanty šifrovací transformace (1) $\Rightarrow$ dostáváme podle (2) (vzhledem k tomu, že $11^{-1}(26) = 19$) pro dešifrování transformaci:

$$p = |19(c-19)|_{26} = |19c - 361|_{26} = |19c+3|_{26}, \quad 0 \leq p \leq 25.$$

Pomocí tohoto předpisu se pokusíme šifrový text dešifrovat. Jak je vidět, po prvních slovech zjistíme, že náš předpoklad a následný výpočet byl správný

THEBE STAPP ROACH TOLEA RNNUM ...