Bezpečnost

3. Blokové, transpoziční a exponenciální šifry

doc. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

Obsah přednášky

- Blokové – polygrafické substituční šifry
- Polyalfabetické šifry
- Transpoziční šifry
- Exponenciální šifry
- Zřízení společného klíče

Blokové – polygrafické substituční šifry (1)

Shrnutí – afinní substituční šifry

- Zranitelné při použití kryptoanalýzy založené na frekvenční analýze zašifrovaného textu.
- K eliminaci těchto nevýhod byl vyvinut systém, který nahrazuje bloky určité délky otevřeného textu $\Rightarrow$ šifry blokové – polygrafické.
- Dále: blokové – polygrafické šifry založené na modulární aritmetice, které byly vyvinuté Hillem v roce 1930.

Blokové – polygrafické substituční šifry

Uvažujeme šifru s blokem o délce jednoho bigramu OT, který je převáděn do ŠT s dvoupísmenovými bloky. Na konec zprávy přidáváme písmeno X v případě, že zpráva končí blokem s jedním písmenem. Zpráva

THE GOLD IS BURIED IN ORONO

je seskupená jako

TH EG OL DI SB UR IE DI NO RO NO.

Blokové – polygrafické substituční šifry (2)

V dalším jsou tato písmena přeložena do jejich číselných ekvivalentů

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14.

Každý blok dvou čísel p_1, p_2 otevřeného textu je převeden do bloku dvou čísel c_1, c_2 šifrového textu pomocí definice c_1 jako nejmenšího nezáporného zbytku modulo 26 lineární kombinace p_1 a p_2 a definice c_2 jako nejmenšího nezáporného zbytku modulo 26 lineární kombinace p_1 a p_2. Například:

$$\begin{aligned} c_1 &= |5p_1 + 17p_2|_{26}, \qquad 0 \leq c_1 < 26 \\ c_2 &= |4p_1 + 15p_2|_{26}, \qquad 0 \leq c_2 < 26. \end{aligned} \tag{1}$$

První blok 19 7 je převeden do bloku 6 25 protože

$$\begin{aligned} c_1 &= |5 \cdot 19 + 17 \cdot 7|_{26} = 6, \\ c_2 &= |4 \cdot 19 + 15 \cdot 7|_{26} = 25. \end{aligned}$$

Blokové – polygrafické substituční šifry (3)

Po aplikaci této transformace na všechny bloky zprávy otevřeného textu je šifrový text

$$6\ 25\ 18\ 2\ 23\ 13\ 21\ 2\ 3\ 9\ 25\ 23\ 4\ 14\ 21\ 2\ 17\ 2\ 11\ 18\ 17\ 2.$$

Pokud tyto bloky převedeme na písmena, máme šifrový text

$$\text{GZ SC XN VC DJ ZX EO VC RC LS RC.}$$

Dešifrovací předpis pro tento šifrovací systém získáme řešením soustavy kongruencí (1), tj. řešením soustavy dvou lineárních rovnic v modulární aritmetice s modulem 26 pro neznámé p_1 a p_2

$$\begin{aligned} p_1 &= |17c_1 + 5c_2|_{26}, \qquad 0 \leq p_1 < 26 \\ p_2 &= |18c_1 + 23c_2|_{26}, \qquad 0 \leq p_2 < 26, \end{aligned} \tag{2}$$

kde pro determinant $\triangle$ soustavy (1) platí $\gcd(\triangle, 26) = 1$.

Blokové – polygrafické substituční šifry (4)

V maticovém zápisu můžeme rovnici (1) vyjádřit následovně

$$\left|\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}\right|_{26} = \left|\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}\right|_{26} \tag{3}$$

a pro rovnici (2) je maticový zápis

$$\left|\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}\right|_{26} = \left|\begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}\right|_{26} \tag{4}$$

Obecně, v Hillově šifrovacím systému, tj. blokové – polygrafické šifře, je ŠT získaný seskupením písmen OT do bloků o velikosti n, převodem písmen do číselných ekvivalentů a generováním ŠT podle vztahu

$$|\mathbf{c}|_{26} = |\mathbf{Ap}|_{26}, \tag{5}$$

kde $\mathbf{A}$ je matice dimenze $n \times n$ a platí $\gcd(\det \mathbf{A}, 26) = 1$, elementy $c_1, c_2, \ldots, c_n$ vektoru $\mathbf{c}$ představují blok ŠT odpovídající bloku OT, který je reprezentován elementy $p_1, p_2, \ldots, p_n$ vektoru $\mathbf{p}$ a nakonec je ŠT vyjádřen v číselných ekvivalentech převeden do písmen.

Blokové – polygrafické substituční šifry (5)

Pro dešifrování je použita inverzní matice $\mathbf{A}^{-1}$ k matici $\mathbf{A}$ modulo 26, kterou lze získat například GJ eliminačním procesem aplikovaným na matici $\mathbf{A}$ a současně matici jednotkovou $\mathbf{E}$ v modulární aritmetice s modulem 26. Můžeme psát za použití platnosti $|\mathbf{A}\mathbf{A}^{-1}|_{26} = |\mathbf{E}|_{26}$

$$|\mathbf{A}^{-1}\mathbf{c}|_{26} = |\mathbf{A}^{-1}(\mathbf{A}\mathbf{p})|_{26} = |(\mathbf{A}^{-1}\mathbf{A})\mathbf{p}|_{26} = |\mathbf{p}|_{26}.$$

Takže, pro získání otevřeného textu ze šifrového textu použijeme následující vztah

$$|\mathbf{p}|_{26} = |\mathbf{A}^{-1}\mathbf{c}|_{26}. \tag{6}$$

Ilustrujme si popsanou proceduru na příkladě pro $n = 3$ se šifrovací maticí

$$\mathbf{A} = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}.$$

Blokové – polygrafické substituční šifry (6)

Vzhledem k tomu, že determinant matice $\det \mathbf{A} = 5$ a platí $\gcd(5, 26) = 1$ existuje inverzní matice k matici $\mathbf{A}$ a můžeme pro šifrování s bloky o velikosti třech písmen psát

$$\left| \begin{pmatrix} c_1 \\ c_2 \\ c_2 \end{pmatrix} \right|_{26} = \left| \mathbf{A} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \right|_{26} .$$

K zašifrování zprávy STOP PAYMENT nejdříve seskupíme zprávu do bloků po třech písmenech s přidáním fiktivního písmena X na konec posledního bloku (výplň — padding). Takto dostáváme OT v blocích

STO PPA YME NTX.

Převodem těchto písmen do jejich číselných ekvivalentů dostáváme:

18 19 14 15 15 0 24 12 4 13 19 23.

Blokové – polygrafické substituční šifry (7)

První blok šifrového textu vypočítáme následovně:

$$\left|\begin{pmatrix} c_1 \\ c_2 \\ c_2 \end{pmatrix}\right|_{26} = \left|\begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}\begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix}\right|_{26} = \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix}$$

Zašifrováním celé zprávy otevřeného textu dostáváme

8 19 13 13 4 15 0 2 22 20 11 0

a konečně šifrový text v písmenné podobě je

ITN NEP ACW ULA.

Pro dešifrovací proces použijeme transformaci

$$\left|\begin{pmatrix} p_1 \\ p_2 \\ p_2 \end{pmatrix}\right|_{26} = \left|\mathbf{A}^{-1}\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}\right|_{26},$$

Blokové – polygrafické substituční šifry (8)

kde

$$\left|\mathbf{A}^{-1}\right|_{26} = \left| \begin{pmatrix} 6 & 21 & 11 \\ 21 & 25 & 16 \\ 19 & 3 & 7 \end{pmatrix} \right|_{26} .$$

- S blokovými šiframi je možné provádět kryptoanalýzu založenou na frekvenční analýze bloků *n* písmen (jednopísmenná frekvenční analýza je neučinná).
- Pro blokovou šifru se dvěma písmeny v jednom bloku existuje 26^2 kombinací dvou písmen v bloku.
- Existují studie výskytu dvou písmen v textech různých jazyků. Bylo zjištěno, že nejčastěji se vyskytující dvojice písmen v anglickém textu je TH, a potom dvojice HE.

Pokud Hillův blokový šifrovací systém o délce bloků dvou písmen byl použit pro zašifrování zprávy, ve které se nejčastěji vyskytuje dvojice písmen KX a následně dvojice VZ, můžeme se domnívat, že dvojicím písmen KX a VZ v ŠT odpovídají dvojice písmen TH a HE v OT.

Blokové – polygrafické substituční šifry (9)

Bloky 19 7 a 7 4 mohou být v ŠT bloky 10 23 a 21 25. Pokud **A** je šifrovací matice, potom na základě těchto zjištění můžeme psát

$$\left|\mathbf{A}\begin{pmatrix}19 & 7\\ 7 & 4\end{pmatrix}\right|_{26} = \left|\begin{pmatrix}10 & 21\\ 23 & 25\end{pmatrix}\right|_{26}.$$

Pokud platí

$$\left|\begin{pmatrix}4 & 19\\ 19 & 19\end{pmatrix}\right|_{26} = \left|\begin{pmatrix}19 & 7\\ 7 & 4\end{pmatrix}^{-1}\right|_{26},$$

pak

$$\mathbf{A} = \left|\begin{pmatrix}10 & 21\\ 23 & 25\end{pmatrix}\begin{pmatrix}4 & 19\\ 19 & 19\end{pmatrix}\right|_{26} = \begin{pmatrix}23 & 17\\ 21 & 2\end{pmatrix},$$

a

$$\left|\mathbf{A}^{-1}\right|_{26} = \left|\begin{pmatrix}2 & 9\\ 5 & 23\end{pmatrix}\right|_{26}.$$

ve vztahu (6) dešifrujeme ŠT, a po této operaci vidíme, jestli náš předpoklad byl správný, tj. jestli je takto získaný OT smysluplný.

Blokové – polygrafické substituční šifry (10)

Zobecnění: Pokud víme, že bloky o velikosti n znaků ŠT
$c_{1j}, c_{2j}, \ldots, c_{nj},\ j = 1, 2, \ldots, n$, a bloky o velikosti n znaků OT
$p_{1j}, p_{2j}, \ldots, p_{nj},\ j = 1, 2, \ldots, n$ si vzhledem k četnosti výskytu v ŠT a OT vzájemně odpovídají $\Rightarrow$ obdržíme soustavu n lineárních kongruencí

$$\left| \mathbf{A} \begin{pmatrix} p_{11} & \ldots & p_{1j} & \ldots & p_{1n} \\ p_{21} & \ldots & p_{2j} & \ldots & p_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{n1} & \ldots & p_{nj} & \ldots & p_{nn} \end{pmatrix} \right|_{26} = \left| \begin{pmatrix} c_{11} & \ldots & c_{1j} & \ldots & c_{1n} \\ c_{21} & \ldots & c_{2j} & \ldots & c_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nj} & \ldots & c_{nn} \end{pmatrix} \right|_{26}$$

a maticově

$$|\mathbf{AP}|_{26} = |\mathbf{C}|_{26},$$

kde $\mathbf{P}$ a $\mathbf{C}$ jsou matice dimenze $n \times n$ s elementy p_{ij} a c_{ij}. Pokud platí $\gcd(\det \mathbf{P}, 26) = 1$, $\Rightarrow$ pro $\mathbf{A}$ platí

$$|\mathbf{A}|_{26} = |\mathbf{C}\mathbf{P}^{-1}|_{26},$$

kde $\mathbf{P}^{-1}$ je inverzní matice k matici $\mathbf{P}$ modulo 26.

Blokové – polygrafické substituční šifry (11)

Shrnutí:

- Kryptoanalýza blokových šifer s použitím výskytu četnosti jednotlivých kombinací písmen v bloku o velikosti n má smysl jen tehdy, když n je malé číslo.
- Například, pokud $n = 10$, existuje $26^{10} = 1,4 \times 10^{14}$ kombinací písmen s touto délkou bloků.
- Pro tak velký počet různých kombinací deseti písmen v bloku je extrémně obtížné použít analýzu založenou na srovnání relativních četností těchto kombinací v šifrovém textu s výsledky relativní četnosti získanými z obyčejného textu.

Polyalfabetické šifry (1)

- Monoalfabetické šifry jsou málo bezpečné protože distribuce frekvence výskytu elementů ŠT je odrazem distribuce frekvence výskytu elementů OT.
- Polyalfabetické šifry řeší tento nedostatek.

Systém polyalfabetických šifer nad abecedou $\mathbb{Z}_N$ tvoří konečná případně nekonečná posloupnost monoalfabetických transformací $(T_1, T_2, \ldots, T_n, \ldots)$ nad abecedou $\mathbb{Z}_N$. Tyto posloupnosti tvoří prostor klíčů tohto systému

$$K = \{T_1, T_2, \ldots, T_n, \ldots\}$$

Specielním případem polyalfabetických šifer je systém Vigenerovských šifer. Tyto šifry tvoří konečnou posloupnost Caesarovských transformací. Naříklad při základní abecede mohout být posloupnosti klíčů:

$$K = \{k_1, k_2, \ldots, k_n\}$$

kde $k_i \in \mathbb{Z}_N$, pro $i \in \langle 1, 2, \ldots, n \rangle$.

Polyalfabetické šifry (2)

Kryptografická transformace OT $(p_1, p_2, \dots)$ odvozená od klíče K je

$$c_j = |p_j + k_{|j|_n}|_N$$

Číslo n se nazýva periodou Vigenerovské šifry, nebo také délkou klíče.

Příklad: Nechť $K = (' B', ' R', ' I', ' D', ' G', ' E') = (1, 17, 8, 3, 6, 4)$. OT je

THE LITERATURE OF CRYPTOGRAPHY HAS A CURIOUS HISTORY

ŠT tohoto OT v 5 písmenových blocích Vigenerovy šifry s klíčem K je:

THELI	TERAT	UREOF	CRYPT	OGRAP	HYHAS	ACURI	...
BRIDG	EBRID	GEBRI	DGEBR	IDGEB	RIDGE	BRIDG	...
UYMOO	XFIIW	...					

Tento algoritmus snižuje použitím klíče K se 6 písmeny dostatečným způsobem vliv četnosti každého písmene OT na nerovnoměrnost distribuce proto, že má k dispozici 6 různých transformací. Vyhovující vyhlazení distribuce jsou schopná i klíče o 3 znacích.

Transpoziční šifry (1)

Transpozice – permutace

- Cílem substituce je konfúze, tj. ztížení určení způsobu transformace zprávy a klíče na ŠT.
- Transpozice je šifrování, kde dochází ke změně uspořádání písmen zprávy.
- Cílem transpozice je difúze, tj. rozptyl informace zprávy nebo klíče po celé šíří ŠT.
- Transpozice odstraňuje vzniklé systematické struktury.
- Transpozice je častokrát označována za permutaci, protože mění uspořádání symbolů zprávy.

Sloupcová transpozice

Sloupcová transpozice přerozděluje znaky OT do sloupců.

Transpoziční šifry (2)

Příklad: Mějme pětisloupcovou transpozici $\Rightarrow$ znaky OT se rozdělí do samostatních bloků po pěticích a zapíší se po sobě:

$$\begin{array}{ccccc} p_1 & p_2 & p_3 & p_4 & p_5 \\ p_6 & p_7 & p_8 & p_9 & p_{10} \\ p_{11} & p_{12} & p_{13} & \dots & \\ \dots & & & & \end{array}$$

Výsledný ŠT je potom

$$p_1 p_6 p_{11} \dots p_2 p_7 p_{12} \dots p_3 p_8 p_{13} \dots$$

Mějme dále OT:

THIS IS THE MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS

Tento OT text můžeme zapsat pomocí sloupcové transpozice například do 5 sloupců takto:

Transpoziční šifry (3)

T	*H*	*I*	*S*	*I*
S	*T*	*H*	*E*	*M*
E	*S*	*S*	*A*	*G*
E	*T*	*O*	*S*	*H*
O	*W*	*H*	*O*	*W*
A	*C*	*O*	*L*	*U*
M	*N*	*A*	*R*	*T*
R	*A*	*N*	*S*	*P*
O	*S*	*I*	*T*	*I*
O	*N*	*W*	*O*	*R*
K	*S*	*X*	*X*	*X* . . .

Výsledný ŠT je potom

TSEEO AMROO KHTST WCNAS NSIHS OHOAN

IWXSE ASOLR STOXI MGHWU TPIRX

Exponenciální šifry (1)

Exponenciální šifry

- Založené na modulárním umocňování.
- Byly uvedeny v roce 1978 Pohlingem a Hellmanem.
- značně odolné vůči kryptoanalýze

Postup šifrování pomoci exponenciální šifry:

- Nechť m je prvočíslo,
- e je celé kladné číslo a je klíč a
- platí $\gcd(e, m-1) = 1$.
- Pro zašifrování zprávy je nejdříve OT převeden do dvojciferného číselného ekvivalentu pomocí tabulky:

písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
num. ekv.	00	01	02	03	04	05	06	07	08	09	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

Exponenciální šifry (2)

- Seskupíme získaná čísla do $2s$ dekadických číslic tvořících číslo, kde s je počet písmen v jednom bloku.
- Tyto bloky tvoří čísla menší než m.
- Když $2525 < m < 252525$, potom $s = 2$.

Každý blok p s s písmeny OT, který reprezentuje celé číslo s $2s$ dekadickými číslicemi, převedeme na blok c ŠT vztahem

$$c = |p^e|_m, \quad 0 \leq c < m\,. \tag{7}$$

ŠT se skládá z takových bloků, že celá čísla, která je reprezentují, jsou menší než m. Hodnoty e určují rozdílné šifry, a proto e můžeme pojmenovat šifrovacím klíčem.

Příklad: Nechť $m = 2633$ (m je prvočíslo) a nechť šifrovací klíč $e = 29$, kde $\gcd(e, m-1) = \gcd(29, 2632) = 1$.

Exponenciální šifry (3)

K zašifrování OT zprávy

THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER,

kde její numerický ekvivalent se 4 číslicovými bloky (2 písmena) je

1907 0818 0818 0013 0423 0012 1511 0414 0500 1304
2315 1413 0413 1908 0019 0814 1302 0815 0704 1723.

Na konec zprávy bylo kvuli zarovnání do bloku přidáno písmeno X (hodnota 23). Každý blok p OT je převeden do bloků ŠT s použitím vztahu

$$c = |p^{29}|_{2633}, \quad 0 < c < 2633.$$

Například k zašifrování prvního bloku otevřeného textu počítáme

$$c = |1907^{29}|_{2633} = 2199.$$

Exponenciální šifry (4)

Pro efektivní modulární umocňování použijeme algoritmus uvedený ve druhé přednášce. Zašifrováním všech bloků OT dostáváme ŠT:

2199 1745 1745 1209 2437 2425 1729 1619 0935 0960
1072 1541 1701 1553 0735 2064 1351 1704 1741 1459.

K dešifrování bloku c ŠT potřebujeme znát dešifrovací klíč, tj. celé číslo d, pro které platí $de \equiv 1 \pmod{m-1} \Rightarrow d$ je multiplikativní inverze e modulo $(m-1)$, která existuje, pokud $\gcd(e, m-1) = 1 \Rightarrow$ dešifrovací vztah pro náš blok p OT získame:

$$|c^d|_m = |(p^e)^d|_m = |p^{ed}|_m = |p^{k(m-1)+1}|_m = |(p^{m-1})^k p|_m = |p|_m,$$

kde $de = k(m-1)+1$, pro nějaké celé číslo k, protože $de \equiv 1 \pmod{m-1}$. Při odvození vztahu pro dešifrování bloku ŠT jsme použili malou Fermatovu větu: $p^{m-1} \equiv 1 \pmod{m}$.

Exponenciální šifry (5)

Příklad: K dešifrování bloku šifrového textu, který byl vygenerován s použitím modula $m = 2633$ a šifrovacího klíče $e = 29$, potřebujeme vypočítat inverzi e modulo $m - 1 = 2632$.
Podle EA vypočítáme inverzi $e^{-1}(2632) \Rightarrow$
$|d|_{m-1} = e^{-1}(m-1) = 29^{-1}(2632) = 2269$. Potom dešifrování bloku ŠT c je vyjádřeno výpočtem p podle vztahu

$$p = |c^{2269}|_{2633}.$$

Pro dešifrování bloku 2199 šifrového textu potom platí

$$p = |2199^{2269}|_{2633} = 1907.$$

Modulární umocňování může být opět prováděno podle algoritmu uvedeném ve druhé přednášce.

Exponenciální šifry (6)

Časová složitost

- Pro každý blok p OT zašifrovaný pomocí $|p^e|_m$ potřebujeme $O((\log_2 m)^3)$ bitových operací – Věta 29.
- Před dešifrováním potřebujeme nalézt inverzi d čísla e modulo $m-1$. Výpočet proveden EA potřebuje $((\log_2 m)^3)$ bitových operací. Tento výpočet je potřebné ho provést jen jednou.
- K převodu bloku ŠT na blok OT potřebujeme vypočítat $|c^d|_m$ a to je možné vykonat s použitím $O((\log_2 m)^3)$ bitových operací.

S použitím modulárního umocňování může být celý proces šifrování a dešifrování proveden značně rychle.

Na druhé straně kryptoanalýza zprávy šifrované s použitím exponenciální šifry obecně nemůže být vykonána v přijatelně rozumné době se standardními výpočetními prostředky.

Exponenciální šifry (7)

Předpokládejme, že je použit pro exponenciální šifru modul m a navíc víme, jak vypadá blok OT p a blok ŠT c a platí

$$c = |p^e|_m. \tag{8}$$

Pro úspěšné provedení kryptoanalýzy potřebujeme najít šifrovací klíč e. Když vztah (8) platí, říkáme, že e je logaritmus c o bázi p modulo m.

- Algoritmy pro nalezení logaritmu o dané bázi modulo nějaké prvočíslo jsou známé jako problémy diskrétního logaritmu.
- Nejrychlejší algoritmy potřebují přibližně $\exp(\sqrt{\log m \log\log m})$ bitových operací.
- K nalezení logaritmu modulo nějaké prvočíslo s n dekadickými číslicemi a s použitím nejrychlejších známých algoritmů pro výpočet diskrétního logaritmu potřebujeme přibližně stejný počet bitových operací jako faktorizaci celého čísla o stejném počtu dekadických číslic s použitím nejrychlejších algoritmů.

Exponenciální šifry (8)

Příklad: Pro m se 100 dekadickými číslicemi, nalezení logaritmu modulo m vyžaduje přibližně desítky let a pro m s 200 dekadickými číslicemi to je přibližně 10^8 let.

- Délka klíče je jedním z parametrů, které určují bezpečnost šifry $\Rightarrow$
- jeden z útoků na prolomení šifry, je zjistit hodnotu klíče.
- Útok prováděný hrubou silou (brute-force attack) je vyzkoušení všech 2^n možných kombinací hodnot klíče (n je # bitů klíče).

V orientační tabulce jsou uvedeny hodnoty bitů n klíče, tak aby jeho prolomení mimo dosah možností různých kategorií luštitelů.

	hacker	firma	taj. služba	lidé	???
# μPC	1	10^3	10^5	10^8	10^{51}
# testů/s	10^4	10^6	10^9	10^{12}	10^{19}
čas [s]	1 W [10^6]	1 M [10^7]	1 Y [10^8]	100 Y [10^{10}]	1000 Y [10^{11}]
# operací	10^{10}	10^{16}	10^{22}	10^{30}	10^{81}
n	34	54	73	100	269

Zřízení společného klíče (1)

- Délka klíče je přímo úměrná kvalitě šifry.
- Když m je prvočíslo a $m-1$ je součinem malých prvočísel $\Rightarrow$ je možné použít specielních metod pro nalezení logaritmu modulo m s menším počtem binárních operací než $O(\log_2^2 m) \Rightarrow$
- je vhodné jako modula pro exponenciální šifrovací systémy používat čísla $m = 2q + 1$, kde q je prvočíslo.

Zřízení společného klíče

Exponenciální šifra je vhodná pro zřízení společného klíče pro dva nebo více subjektů. Společný klíč může být například použit jako šifrovací klíč pro šifrovací systém nějaké datové komunikace a je sestrojen tak, že neautorizovaný subjekt ho nemůže rozluštit v nějakém rozumném počítačovém čase.

Nechť m je velké prvočíslo a nechť a je nějaké celé číslo a platí $\gcd(m, a) = 1$. Každý subjekt v síti si vybere celé číslo k_i jako klíč tak, že $gcd(k_i, m-1) = 1$.

Zřízení společného klíče (2)

Když dva subjekty s klíči k_1 a k_2 si chtějí vygenerovat klíč, tak nejdříve první subjekt pošle druhému subjektu celé číslo y_1 takové, že platí

$$y_1 = |a^{k_1}|_m, \quad 0 < y_1 < m$$

a druhý subjekt vypočítá společný klíč K na základě vztahu

$$K = |y_1^{k_2}|_m = |a^{k_1 k_2}|_m, \quad 0 < K < m.$$

Podobně, druhý subjekt vyšle prvnímu subjektu celé číslo y_2, kde

$$y_2 = |a^{k_2}|_m, \quad 0 < y_2 < m$$

a první subjekt si vypočítá společný klíč K za pomocí vztahu

$$K = |y_2^{k_1}|_m = |a^{k_1 k_2}|_m, \quad 0 < K < m.$$

Neautorizované subjekty nacházející se v komunikační síti nemohou najít společný klíč K v rozumném počítačovém čase, protože jsou nuceni hledat logaritmus modulo m pro nalezení K.

Zřízení společného klíče (3)

Příklad: Mějme subjekt A, B a $m = 7, a = 4, k_1 = 5, k_2 = 4 \quad \Rightarrow$

1. A pošle B $y_1 = |a^{k_1}|_m = |4^5|_7 = 2$
2. B pošle A $y_2 = |a^{k_2}|_m = |4^4|_7 = 4$
3. A vypočítá společný klíč $K = |y_2^{k_1}|_m = |y_2^{k_1}|_m = |4^5|_7 = 2$
4. B vypočítá společný klíč $K = |y_1^{k_2}|_m = |y_1^{k_2}|_m = |2^4|_7 = 2$

Podobným způsobem je možné společný klíč K sdílet i s více než dvěma subjekty. V případě n subjektů má každý z těchto subjektů vlastní klíč $k_1, k_2, \ldots, k_n$. Potom pro společný klíč K platí

$$K = |a^{k_1 k_2 \cdots k_n}|_m, \quad 0 < K < m.$$

Úloha: Navrhněte schéma pro zřízení společného klíče K pro 3 subjekty A, B a C.

Zřízení společného klíče (4)

Předchozí schéma zřízení společného klíče je v podstatě

Diffie-Hellmanův kryptorafický algoritmus veřejného klíče

1. Volba veřejných prvků účastníkem A: m prvočísla a celého čísla $0 < a < m$.
2. Generování parametrů klíče účastníkem A: volba čísla $k_1 < m$ a výpočet $y_1 = |a^{k_1}|_m$,
   A odešle prostřednictvím komunikačního kanálu B čísla a, m a y_1.
3. Generování parametrů klíče účastníkem B: volba čísla $k_2 < m$ a výpočet $y_2 = |a^{k_2}|_m$,
   B odešle prostřednictvím komunikačního kanálu A číslo y_2.
4. Generování tajného klíče účastníkem A: $K = |y_2^{k_1}|_m$.
5. Generování tajného klíče účastníkem B: $K = |y_1^{k_2}|_m$.

Veřejné prvky jsou v tomto případě čísla m a a.