

Základy šifrovania a dešifrovania

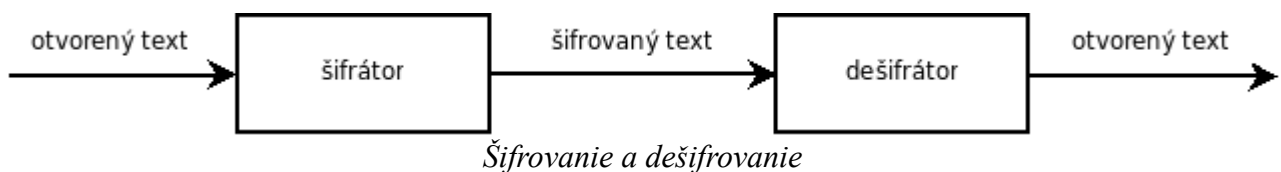
Úlohou šifrovania je uchovať v nebezpečnom prostredí dáta v bezpečí.

Proces šifrovania a následného dešifrovania údajov je možné vyjadriť pomocou dvoch funkcií.

Funkcia šifrovania $C = E(P)$

Funkcia dešifrovania $P = D(C)$

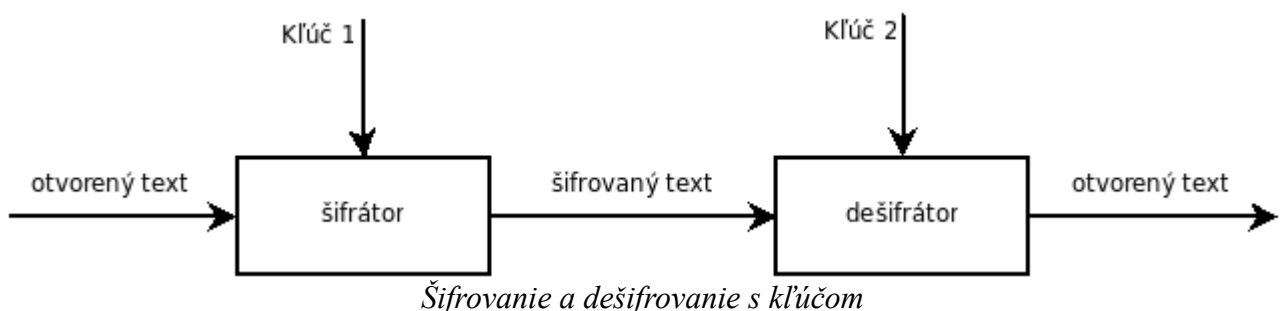
Kde C označuje šifrovaný text, P označuje otvorený (nešifrovaný) text.



Ak je šifrovací algoritmus známy iba oprávneným osobám, šifrovanie je možné považovať za bezpečné, keďže nik iný nedokáže šifrovaný text prečítať.

Šifrovací kľúč, symetrické a asymetrické šifrovanie

Rozšírené moderné šifrovacie metódy ale používajú verejne známe algoritmy. V takomto prípade je pre utajenie informácie nevyhnutné použiť tzv. *šifrovací kľúč*.



Poznáme dva druhy šifrovania údajov pomocou kľúča. Pri *symetrickom šifrovaní* je na šifrovanie aj dešifrovanie údajov použitý jeden a ten istý kľúč. Tento kľúč je nutné utajiť.

Asymetrické šifrovanie používa dva navzájom previazané kľúče - *verejný* a *privátny*. Oba tieto kľúče patria jednej osobe. Privátny kľúč môže poznať iba jeho vlastník. S k nemu prislúchajúcim verejným kľúčom je potrebné oboznámiť všetky osoby, s ktorými chce jeho vlastník komunikovať.

Pri posielaní údajov musia byť tieto zašifrované verejným kľúčom príjemcu. Takto šifrovaný

text je možné dešifrovať iba použitím privátneho kľúča príjemcu.

Mechanizmus asymetrického šifrovania sa používa aj pri overovaní identity, resp. *digitálnom podpise*.

Delenie šífier a šifrátorov

Podľa množstva bitov šifrovaných v jednom kroku môžeme šifrátory rozdeliť do týchto dvoch kategórií:

- *Blokový šifrátor* naraz šifruje viacero bitov.
- *Prúdový šifrátor* naraz šifruje len jeden bit

Klasické šifrovacie systémy sa rozdeľujú na dve skupiny.

- *Permutačné (transpozičné) systémy* menia poradie znakov v otvorenom texte a tak vytvárajú šifrovaný text.
- *Substitučné systémy* podľa predpisu (*šifrovacej abecedy*) nahrádzajú otvorený text šifrovaným textom. Podľa počtu predpisov sa ďalej delia na:
 - *monoalfabetické substitučné systémy*, ktoré využívajú jednu šifrovaciu abecedu
 - *polyalfabetické substitučné systémy* využívajúce viacero abecied

Cézarova šifra

Jedná sa o jednoduchú substitučnú monoalfabetickú šifru. Aplikácia Cézarovej šifry spočíva v „posunutí“ znakov abecedy o tri miesta, resp. výmene písmena za písmeno nachádzajúce sa v abecede o tri pozície ďalej. Napríklad písmeno „A“ z otvoreného textu je v šifrovanom texte nahradené písmenom „D“, písmeno „B“ písmenom „E“ atď.

Predpis Cézarovej šifry je možné vyjadriť nasledovne (pri použítí anglickej abecedy s 26 znakmi):

$$C_i = (P_i + 3) \bmod 26$$

Takúto šifru je možné prelomiť pomocou štatistickej analýzy výskytu písmen. Ak vieme, v akom jazyku bol napísaný otvorený text a vieme, že napr. písmeno „A“ sa v ňom vyskytuje najčastejšie, môžeme k znaku zo šifrovaného textu priradiť dané písmeno a takto pokračovať pre všetky písmená, resp. určiť posun použitý v šifrovacom predpise.

Polyalfabetické šifry

Polyalfabetické šifry sú navrhované so snahou dosiahnuť rovnakú frekvenciu výskytu pre všetky písmená v zašifrovanom texte. Eliminuje sa tak možnosť rozbiť šifru pomocou štatistickej analýzy ako v prípade monoalfabetických šífier.

Tieto šifry využívajú šifrovanie pomocou viacerých šifrovacích abecied, napríklad:

$$C_i = (3 \times P_i) \bmod 26$$
$$C_i = (5 \times P_i + b) \bmod 26$$

Šifrovacie tabuľky

Šifrovacie tabuľky (alebo *Vigenérova šifra*) je jednoduchá polyalfabetická substitučná šifra založená na viacnásobnom použití Cézarovej šifry. Predchádza sa tak rozbitiu šifry jednoduchou analýzou frekvencie výskytu písmen.

Šifrovacie tabuľky využívajú 26 rôznych šifrovacích abecied (pre každé písmeno abecedy jednu) a tajný kľúč určujúci, ktorá šifrovacia abeceda má byť pri konkrétnom písmene otvoreného textu použitá.

Šifrovacie abecedy môžu vyzerat' nasledovne:

	A	B	C	...	Z
A	a	b	c	...	z
B	b	c	d	...	a
C	c	d	e	...	b
D	d	e	f	...	c
...					
X	x	y	z	...	w
Y	y	z	a	...	x
Z	z	a	b	...	y

Prvý stĺpec obsahuje písmená otvoreného textu, prvý riadok „názvy“ jednotlivých šifrovacích abecied. Napríklad písmeno D zašifrované abecedou Z bude v šifrovanom texte zobrazené ako „c“.

Ako kľúč pri šifrovaní sa používa tajné slovo, ktoré sa zopakuje toľkokrát, aby malo dĺžku otvoreného textu. Tým sa ku každému písmenu otvoreného textu na základe kľúča priradí

špecifická abeceda.

Príklad šifrovania textu „It was the best of times“ s kľúčom „Dickens“.

Kľúč	D	I	C	K	E	N	S	D	I	C	K	E	N	S	D	I	C	K	E
Otvorený text	I	T	W	A	S	T	H	E	B	E	S	T	O	F	T	I	M	E	S
Šifrovaný text	l	b	y	k	w	g	z	h	j	g	c	x	b	x	w	q	o	o	v

Rozbitie metódou Kasiski

Táto metóda je založená na pravdepodobnosti výskytu skupín písmen (nazývaných *digramy*, *trigramy*, ...) v jazyku otvoreného textu. Pri jej aplikácii sa útočník snaží nájsť v zašifrovanom texte rovnaké skupiny písmen a tak stanoviť počet rôznych rotácií kľúča.

Postup pri použití metódy je nasledovný:

- 1) Nájsť v zašifrovanom texte opakovaný výskyt troch alebo viacerých písmen.
- 2) Pri každom výskyte skupiny určiť začiatočnú pozíciu výskytu.
- 3) Vypočítať rozdiel medzi pozíciami po sebe idúcich výskytov.
- 4) Faktorizuj všetky rozdiely.
- 5) Ak bola použitá polyalfabetická šifra, dĺžka kľúča bude jedným zo získaných faktorov.

Rozbitie na základe indexu koincidencie

Použitie tejto metódy vedie k stanoveniu počtu použitých šifrovacích abecied na základe odchýlky od normálnej frekvencie výskytu.

Pravdepodobnosť výskytu písmena i v otvorenom texte sa označuje P_i . Súčet pravdepodobností pre výskyt každého písmena je rovný 1.

$$\sum_{i=A}^Z P_i = 1$$

Pravdepodobnosť, že ľubovoľné dva znaky v zašifrovanom texte budú rovnaké je možné vyjadriť ako $P_i \cdot P_i$.

Ak počet písmen zašifrovaného textu označíme n a počet výskytov písmena i v zašifrovanom texte označíme F_i , index koincidencie (IC) vypočítame nasledovne:

$$IC = P_i^2 = \frac{\frac{F_i(F_i-1)}{2}}{\frac{n(n-1)}{2}} = \frac{F_i(F_i-1)}{n(n-1)}$$

Pre anglické texty nadobúda IC takéto hodnoty:

Počet abecied	1	2	3	4	5	10	veľký
IC	0,068	0,052	0,047	0,044	0,044	0,041	0,038

Vernamova šifra

Jedná sa o perfektnú substitučnú polyalfabetickú šifru. Používa toľko šifrovacích abecied, koľko je šifrovaných písmen. Žiadne dve písmená teda nie sú zašifrované rovnakou abecedou. Z toho vyplýva nutnosť použiť veľmi dlhý kľúč, dĺžka kľúča je rovnaká ako dĺžka textu. Každý kľúč je pritom jednorázový.

Jedná sa o dokázateľne teoreticky nerozbitnú šifru. Jej použitie v praxi je ale náročné z dôvodu zložitej distribúcie dlhých jednorázových kľúčov.

Permutačné šifry

Permutačné šifry (nazývané aj transpozičné) menia poradie znakov otvoreného textu. Môže byť využitá napríklad **stĺpcová transpozícia**.

Pri tejto metóde je potrebné otvorený text zapísať v takom tvare, aby tvoril niekoľko dlhých stĺpcov a následne tieto stĺpce prepísať ako šifrovaný text.

Príklad pre zašifrovanie otvoreného textu „THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS“:

THIS I
SAMES
SAGET
OSHOW
HOWAC
OLUMN
ARTRA
NSPOS
ITION
WORKS

Výsledný šifrovaný text: „tssoh oaniw haaso lrsto imghw utpir seeoa mrook istwc nasns“.

Rozbitie takýchto šifier je založené na pravdepodobnosti výskytu digramov a trigramov v jazyku.

Prúdové a blokové šifrátory

Pri prúdových šifrátoroch je entitou na zašifrovanie jeden znak, pri blokových šifrátoroch je ňou celý blok textu.

Prúdové šifrátory charakterizuje *konfúzia*, teda vlastnosť, ktorá určuje, ako dobre vie šifrátor skryť znak otvoreného textu pred útočníkom.

Blokové šifrátory využívajú rozšírenie jedného znaku otvoreného textu do všetkých znakov šifrovaného textu. Táto vlastnosť sa nazýva *difúzia*.

Prúdové šifrátory

Výhody

- rýchlosť
- nízka miera prenášaných kódovaných chýb

Nevýhody

- nízka miera difúzie
- zraniteľnosť na zlomyselné vkladanie znakov

Blokové šifrátory

Výhody

- vysoká miera difúzie
- odolnosť voči vkladaniu
- jeden znak otvoreného textu ovplyvní viacero znakov šifrovaného textu

Nevýhody

- pomalé šifrovanie
- treba čakať na prijatie celého bloku otvoreného textu
- šírenie chyby (chyba v jednom znaku ovplyvní všetky znaky bloku)

Prostriedky kryptoanalytikov

Útoky za účelom rozbitia šifry môžu byť realizované za rôznych podmienok a s rôznymi informáciami dostupnými v čase útoku.

Podľa dostupných prostriedkov sa útoky delia do týchto štyroch kategórií:

- *útok iba na šifrovaný text* – analytik má k dispozícii iba šifrovaný text a verejne známe informácie
- *útok so známym otvoreným textom* – analytik má k dispozícii celý šifrovaný text a časť alebo celý otvorený text
- *útok s ľubovoľným otvoreným textom* – analytik má prístup k šifrovaciemu zariadeniu
- *útok s vybraným šifrovaným textom* – analytik má k dispozícii algoritmus a šifrovaný text

Moderné šifrovacie systémy

Šifrovacie systémy sú v dnešnej dobe založené na problémoch veľkej zložitosti. Útok hrubou silou na takéto systémy by trval celé roky.

Zložitosť	Počet operácií pre $n = 10^6$	Doba riešenia pri 10^6 op/s (1 MIPS)
$O(1)$	1	10^{-6} s
$O(n)$	10^6	1 s
$O(n^2)$	10^{12}	1,6 dňa
$O(n^3)$	10^8	32 000 rokov
$O(2^n)$	10^{301030}	?

Trvanie útoku hrubou silou v závislosti od dĺžky kľúča:

Dĺžka kľúča (bit)	Počet pokusov	1 MIPS	10^6 MIPS
8	2^8	$256 \cdot 10^{-6}$ s	
56	2^{56}	1142 rokov	10 hodín
128	2^{128}	$5 \cdot 10^{24}$ rokov	$5 \cdot 10^8$ rokov
1024	2^{1024}	10^{295} rokov	
2048	2^{2048}	10^{597} rokov	

Problémy využité pri kryptografii môžu mať *polynomiálnu* (P) alebo *nepolynomiálnu* (NP) zložitosť.

Pri polynomiálnej zložitosti je doba riešenia obmedzená polynómom. Pri nepolynomiálnej zložitosti nie je možné v polynomiálnom čase nájsť výsledok, iba overiť jeho platnosť.

Pri triede problémov označovanej ako *NP-úplné problémy* je možné očíslovať všetky možnosti a nájsť riešenie ich postupným testovaním.

Vzťah medzi jednotlivými triedami problémov sa dá vyjadriť nasledovne:

$$P \subset NP \subseteq NP - \text{úplne}$$

V modernej kryptografii môže byť použitá **faktORIZÁCIA veľkých čísel** (rozklad čísla na prvočísla) alebo **hľadanie diskrétného logaritmu**.