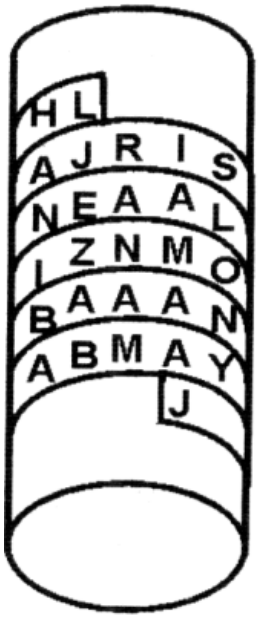
História a princípy šifrovania - Scytale (skytalé), Cézarova šifra, šifrovací disk, Vigenerova šifra, Cardanova šifra, Vernamova šifra, kľúč, substitučné a transpozičné šifry :)

UPOZORNENIE

Šifry sa používajú od nepamäti – prvá zmienka o nich pochádza z Egypta asi spred 4000 rokov. Cieľom šifrovania vždy bolo nájdenie takej šifry, ktorú by nezasvätený nemohol rozlúštiť. Medzi najstaršie patrí Scytale a Cézarova šifra.

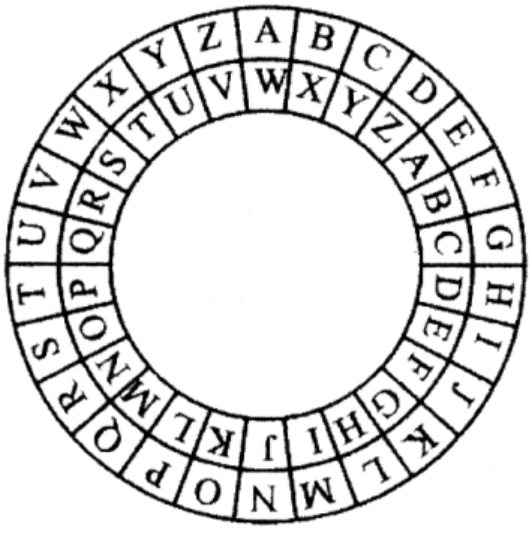
Scytale používali Sparťania v starovekom Grécku. Princíp je postavený na šifrovacom valci, ktorý sa omotá tenkým prúžkom pergamenu. Na tento sa napíše správa (zvyčajne zľava doprava). Keď sa prúžok odmoce, výsledkom je sled nesúvisiacich znakov. Na to, aby príjemca dokázal správu rozlúštiť potrebuje rovnako hrubý valec (inak sa písmena nezobrazia v správnych riadkoch).



Skytale so správou

Cézarova šifru vymyslel v období dobývania sveta Gaius Julius Caesar (100-44 p.n.l.) a spočíva v posúvaní znakov o zadanú hodnotu. Napr. pre text „Ahoj“ a hodnotu 3 sa všetky znaky posunú o 3 miesta a výsledkom bude „Dkrm“. V prípade, že sa pri presúvaní prejde za koniec abecedy, začína sa zasa od jej začiatku (napr. Z by sa zakódovalo ako C). Dešifrovanie spočíva v opačnom posúvaní.

Aplikáciu Cézarovej šifry predstavuje **šifrovací disk**, ktorý pozostáva z dvoch kotúčov s abecedou. Po otočení o zadaný počet miest jeden kotúč (napr. vnútorný) predstavuje znaky abecedy, druhý ich zašifrovanú podobu.



Šifrovací disk

Prostredníctvom šifrovacieho kotúča mono realizovať i kódovanie založené na **Vigenerovej šifre**. Vigenerova šifra tiež posúva znaky, posun je však daný zložitejším kľúčom (pozostávajúcim zo znakov abecedy). Kľúč sa opakovanie podpíše pod text, ktorý sa má zašifrovať a pre každý znak sa hľadá jeho ekvivalent v riadku s abecedou posunutou tak, aby začínala písmenom kľúča.

Kvôli zjednodušeniu (aby sme nemuseli vykresľovať všetky posunutia abecedy) si vyberieme kľúč *beda*, ktorým zašifrujeme správu: *„utekajte maju aj dela“*.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

U	T	E	K	A	J	T	E	M	A	J	U	A	J	D	E	L	A
B	E	D	A	B	E	D	A	B	E	D	A	B	E	D	A	B	E

Správa *„utekajte maju dela"* zašifrovaná kľúčom *beda*

Písmeno *U* zašifrujeme tak, že nájdeme jeho ekvivalent v riadku začínajúcom písmenom *B* – teda v druhom: **V**. Písmenu *T* hľadáme ekvivalent v riadku začínajúcom *E* – výsledkom je **X**. Pre písmeno *E* pozrieme do riadku začínajúceho *D* – *H* atď. Výsledkom šifrovania bude *VXHKBNWE NEMU BN GEME*.

Pre dešifrovanie použijeme podobnú mriežku, len abeceda sa bude v jednotlivých riadkoch posúvať opačným smerom. Celý proces je veľmi jednoduché transformovať do posúvania o zadaný počet znakov a naprogramovať.

Uvedené šifrovacie algoritmy patria medzi **substitučné šifry**. Pre túto kategóriu je typické nahrádzanie znakov či skupín znakov inými znakmi alebo skupinami (napr. postupnosť *AHA* bude nahrádzaná skupinou *FTG*, prípade *B* bude náhodne nahradené *FT* alebo *PO* atď.). Vigenerova šifra pozostáva z kombinácie viacerých substitučných šifier (podľa dĺžky kľúča).

Druhú kategóriu klasických šifier tvoria **transpozičné šifry**. Základná myšlienka týchto šifier spočíva v napísaní textu do tabuľky tak, aby text tiekol odhora nadol a potom v jeho prepísaní po riadkoch:

TURCI SU ZA HRADBAMI, UTEKAJTE

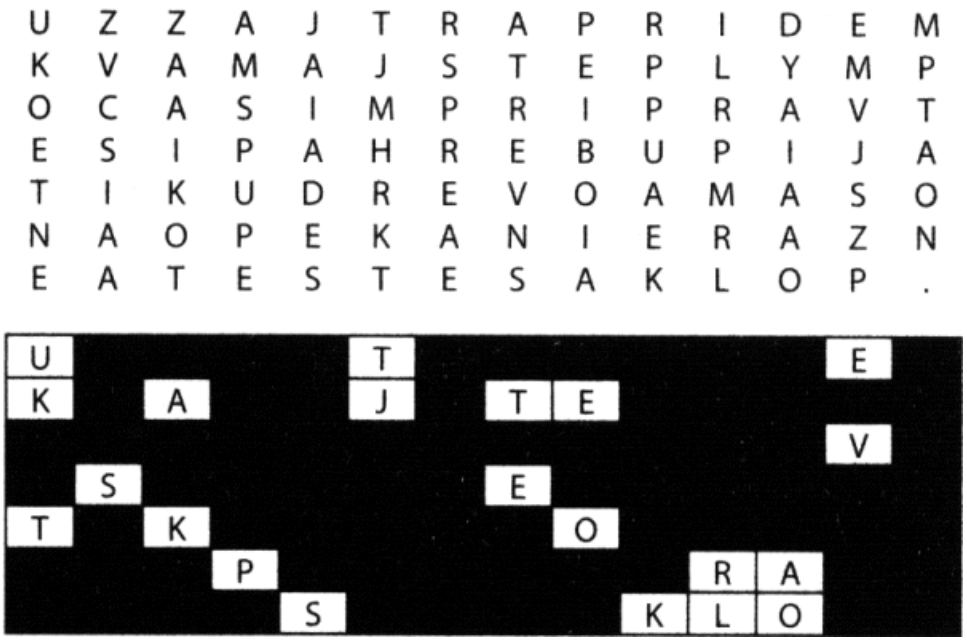
T	S	R	M	K
U	U	A	I	A
R	Z	D	U	J
C	A	B	T	T
I	H	A	E	E

TSRMKUUAIARZDUJCABTTIHAEE

Jednoduchá transpozičná šifra

Dešifrovanie spočíva v opätovnom prepísaní do mriežky so zadanými rozmermi (prípadne otočení zápisu) a prečítaní – znaky sa ničím nenahrádzajú, mení sa len ich postupnosť.

Cardanova šifra je založená na použití mriežky, v ktorej sú vystrihnuté otvory. Do týchto sa napíše správa, mriežka sa odloží a prázdne miesta sa vyplnia náhodnými znakmi. Existuje i niekoľko pokročilejších variantov, z ktorých stojí za zmienku napr. umiestnenie otvorov v mriežke tak, aby pri otáčaní o 90° pokrývali vždy iné políčka – týmto spôsobom síce nezmetieme nepriateľa náhodnými znakmi, ale dokážeme naplno využiť všetky políčka tabuľky a nielen ¼ ako v prípade základnej verzie.



Text pred a po použití Cardanovej mriežky

Rozšifrovať správu bez **kľúča** hociktorým z týchto postupov je náročné, ale pokiaľ poznáte šifrovací algoritmus a viete trošku kombinovať, nie nemožné.

Po zapojení elektroniky do lúštenie sa postup neuveriteľne zrýchlil, pretože ide vlastne len o nájdenie všetkých možných kombinácií a vyhľadávanie správnej. Zvyčajne existujú i mnohé urýchlenia využívajúce napr. vlastnosti jazyka, v ktorom bol pôvodný text napísaný.

Významný rozvoj kryptografie nastal začiatkom 20. storočia, keď sa začal používať telegraf. V roku 1917 bol navrhnutý jediný **dokázateľne nerozlúštiteľný** šifrovací algoritmus – **Vernamova šifra**. Základná myšlienka a nerozlúštiteľnosť spočíva v tom, že šifrovací kľúč je minimálne tak dlhý ako posielaná správa a použije sa len raz.

Kľúč je vygenerovaný úplne náhodne, medzi jeho časťami neexistuje žiadna závislosť, bol vytvorený len v dvoch kópiách, a tak jeho zistenie iným človekom alebo počítačom nie je možné. V prípade opakovaného použitia toho istého kľúča sa však šance na jeho odhalenie podstatne zvyšujú.

Ak by sme chceli ísť do detailov, postup je nasledovný:
1. vyhotoví sa kľúč (postupnosť náhodných číslic, znakov alebo bitov) v dvoch kópiách, jednu dostane odosielateľ, druhú príjemca,
2. odosielateľ napíše správu, ktorú šifruje pomocou kľúča. Po zašifrovaní použitú časť kľúča zničí,
3. príjemca na správu aplikuje potrebnú dĺžku kľúča, prečíta si správu a použitú časť kľúča zničí,
4. pri ďalšej správe sa pokračuje v kľúči ďalej.
Obdobie Prvej a Druhej svetovej vojny je charakterizované hlavne používaním zložitých mechanických a elektromechanických šifrovacích strojov. Zo šifrovania sa stala dôležitá zbraň zabezpečujúca bezpečnú výmenu informácií. Medzi najvýznamnejšie šifrovacie prístroje tej doby patrila **Enigma**, ktorá bola používaná Nemcami počas Druhej svetovej vojny a dlho predstavovala pre Spojencov nerozlúštiteľný systém. Napokon však bola rozlomená vďaka kombinácií úsilia britského matematika Alana Turinga a zajatia nemeckej ponorky s funkčným prístrojom na palube.

Šifrovanie, kryptológia, kryptografia, kryptoanalýza, šifrovací/dešifrovací algoritmus, kľúč ↑

Súčasnosť šifrovania - symetrické a asymetrické šifry, DES, IDEA, RSA, PGP ↓

Zdroje
Prevzaté a upravené z:
Ján Skalka, Cyril Klimeš, Gabriela Lovászová, Peter Švec, *Informatika na maturity a prijímacie skúšky*, Enigma, Nitra 2007, ISBN 978-80-89132-50-8.
Dobré, použiteľné stránky:
· ***Prečo správy šifrujeme?*,**
· ***Dôležité medzníky v histórii kryptológie*.**

