Kódovanie a šifrovanie informácií

Šifrovanie (kryptovanie) má za úlohu **utajiť posielané údaje, aby si ich nemohla prečítať tretia strana.** Zašifrovaná správa sa dá odšifrovať ak poznáme **kľúč** (heslo, spôsob šifrovania).

Ak by sa napríklad odosielateľ dohodol s príjemcom na zmene poradia o jeden symbol v Morseovej abecede, v tom prípade by už išlo o šifru a kľúčom by bolo samotné posunutie

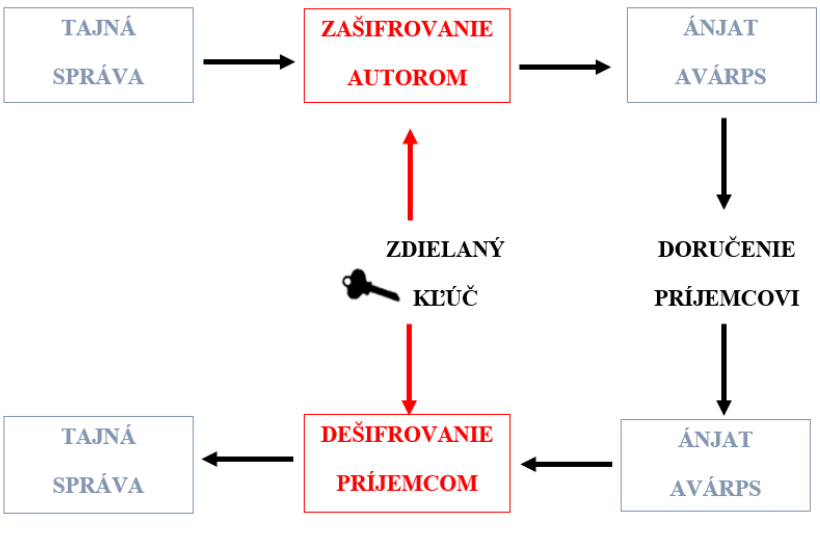
Ako prebieha šifrovanie a jeho účastníci: Osoba, nazývaná **odosielateľ**, posiela tajnú správu druhej osobe, ktorú voláme **prijímateľ**. Tajná správa má podobu textu, budeme ju označovať ako **otvorený text**. Otvorený text je napísaný v prirodzenom jazyku a je teda pre každého dobre čitateľný. Správu doručuje nie celkom stopercentne spoľahlivý posol, alebo sa posiela nechráneným verejným komunikačným kanálom. Aby sme zabránili niekomu nepovolanému, kto by sa akokoľvek k správe dostal, prečítal jej tajný obsah, pošleme správu v **šifrovanej forme**. **Spôsob šifrovania** a **dešifrovania** je spoločným tajomstvom odosielateľa a prijímateľa a šifrovanie sa vykonáva pomocou takzvaného **kľúča**. Zašifrovaný text voláme **krytpotext**. Po prijatí správy prijímateľ kryptotext **dešifruje**. Dešifrovaním sa z kryptotextu vytvorí opäť pôvodný otvorený text, ktorý prijímateľ môže bez problémov čítať.

Kryptológia (z gréckeho *kryptos* = ukrytý + *logos* = slovo, náuka) je veda o utajení obsahov správ. Rozdeľuje sa na kryptografiu, kryptoanalýzu a steganografiu.

- Cieľom **kryptografie** je **skúmanie a navrhovanie šifrovacích systémov**, ktoré budú spĺňať určité podmienky ako autenticitu, dôvernosť, dostupnosť, integritu... Ich úlohou je urobiť obsah správy nečitateľným v prípade jeho zachytenia treťou osobou.
- Cieľom **kryptoanalýzy** je skúmanie metód lúštenia šifrovacích systémov. Je to rozbor (analýza) zašifrovaných správ a ich metód šifrovania, ktorými sa **hľadá spôsob preniknutia do šifrovacieho systému.**
- Cieľom **steganografie** je zatajiť existenciu správy. Steganografické metódy obsahujú napríklad používanie neviditeľných atramentov a pod.

Šifry možno rozdeliť do dvoch základných kategórií:

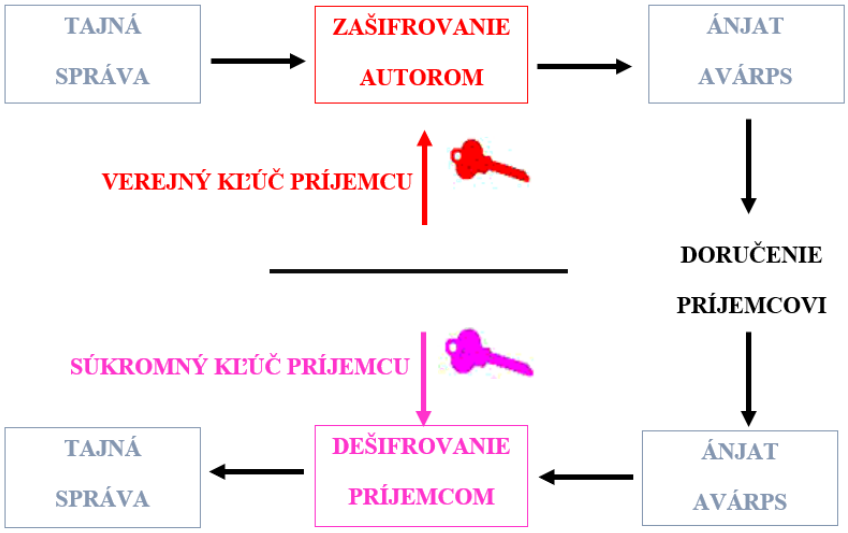
Symetrické šifry (symetrické šifrovanie) je charakteristické tým, že poznáme **jediný kľúč**, ktorým sa dá zašifrovaný dokument zašifrovať aj rozšifrovať. Všetky zúčastnené strany poznajú **vopred dohodnutý tajný kľúč**. Ak sa ten istý kľúč používa dlhšiu dobu, vzniká nebezpečenstvo jeho prezradenia alebo v prípade mnohonásobného používania i jeho dešifrovania, preto sa kľúče často obmieňajú.



Asymetrické šifrovanie používa **dva kľúče**. Jeden kľúč je **verejný** a **voľne dostupný**, druhý kľúč je **súkromný** a pozná ho len daný majiteľ, ktorý je zároveň aj majiteľom verejného kľúča. Tieto dva kľúče sú akosi matematicky zviazané, teda patria k sebe a boli spolu vygenerované.

Prostredníctvom verejného kľúča sa správa zašifruje, prostredníctvom súkromného kľúča dešifruje. Príjemca správy nemusí poznať kľúč, prostredníctvom ktorého boli údaje zašifrované a odosielateľ nesmie poznať kľúč, ktorý správu dešifruje.

Majiteľ svoj verejný kľúč poskytne všetkým partnerom, s ktorými chce komunikovať a oni správy prostredníctvom neho zašifrujú. Rozšifrovať takto zašifrovanú správu možno už len prostredníctvom súkromného kľúča, ktorého jediným vlastníkom je prijímateľ správy, tento kľúč musí byť uchovávaný na bezpečnom mieste. Sila tohto typu šifrovania spočíva v tom, že komunikujúci svoje kľúče nemusia poznať a z toho dôvodu ich nemôžu ani poskytnúť nikomu ďalšiemu. Znalosť jedného z dvojice kľúčov nepostačuje na získanie toho druhého.

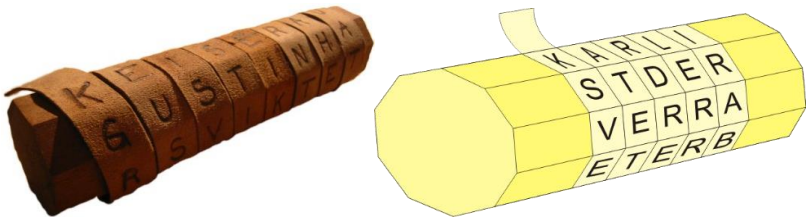


Druhy (typy) šifier:

- **transpozičné šifry** ktoré spočívajú v zamiešaní poradia písmen otvoreného textu (napr. slovo "pomôž mi" sa zmodifikovalo na "opômž im").
- **substitučné šifry**, ktoré spočívajú v systematickom nahradzovaní jednotlivých symbolov obsahu textu za určené ďalšie symboly alebo skupinu symbolov (napr. slovo "aha" sa zmodifikovalo na "ftg").

Príklady šifier

- **Skytalé** - tento spôsob utajovania informácií sa používal v starovekom Grécku a Sparte. Princíp šifrovania údajov spočíva v tom, že sa na drevený valec vopred dohodnutého priemeru namotal pásik pergamenu alebo kože a v smere hlavnej osi valca sa naň napísal text od jedného konca k druhému. Po jeho odmotaní na ňom zostali písmená, ktoré nedávali spolu zmysel. Jediným spôsobom, ako dešifrovať zašifrovaný text, bolo namotanie pásika na valec rovnakého priemeru.



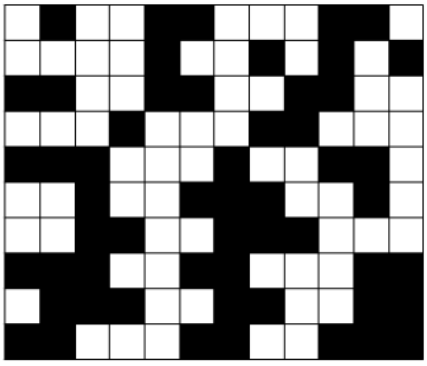
- **Cézarova šifra** (posuvná) - každé písmeno správy je posunuté o *n* pozícií ďalej v abecede, pričom *n* môže byť *1* až *m − 1*, kde *m* je počet znakov príslušnej abecedy. V prípade písmena vyskytujúceho sa na konci abecedy sa toto písmeno posunie opäť na začiatok abecedy. Spočíva v posúvaní znakov o zadanú hodnotu.
  Pre *n* = 3

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
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

  slovo “Ahoj“ sa zašifrujeme na “Dkrm“

- **Cardanova šifra** je založená na použití mriežky (jej rozmer – počet riadkov a stĺpčekov – si odosielateľ a prijímateľ dohodnú vopred), v ktorej sú vystrihnuté otvory. Do týchto sa napíše správa, mriežka sa odloží a prázdne miesta sa vyplnia náhodnými znakmi.
  Pokročilejší variant: 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.

W	I	H	A	E	R	T	I	S	Y	O	A
C	Y	N	I	E	C	?	W	A	G	M	A
S	E	A	N	I	S	W	H	I	N	O	K
N	O	W	H	S	T	H	T	H	E	P	R
I	E	T	I	C	E	E	O	F	T	N	E
V	E	I	R	Y	S	O	M	T	H	T	I
N	G	N	Y	A	N	T	H	I	D	T	H
R	U	O	E	V	G	N	A	L	U	O	L
E	E	Y	T	O	F	M	E	N	O	T	E
S	E	T	H	I	S	O	N	G	E	M	L



- **Vigenerova šifra** posúva znaky abecedy pomocou série Cézarových šifier, posun je daný kľúčom (pozostávajúcim zo znakov abecedy). Kľúč sa opakovane podpíše pod text, ktorý sa má zašifrovať, napr. informatika, kľúč: IKT, opakovaný kľúč: IKTIKTIKTIK. Pre každý znak kľúča sa pripíše posunutá abeceda a pre každý znak otvoreného textu sa hľadá jeho ekvivalent v riadku s abecedou posunutou tak, aby začínala písmenom kľúča. T.j. zoberieme prvé písmeno otvoreného textu a zašifrujeme ho pomocou tej šifrovej abecedy, ktorá zodpovedá prvému znaku z kľúča. Potom zoberieme druhé písmeno z otvoreného textu a zašifrujeme ho pomocou šifrovej abecedy, ktorá zodpovedá druhému znaku z kľúča.
  slovo “Ahoj“ sa zašifrujeme pomocou kľúča “pes“ na “plgy“

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
P																									
E																									
S																									
P																									

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
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
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
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
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

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
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
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
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
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

- **Transpozičná Route šifra** - pôvodný text sa najskôr zapíše do mriežky daných rozmerov – vždy z ľavého horného rohu smerom dolu, voľné bunky sa doplnia náhodnými písmenami a potom sa číta podľa vzoru uvedeného v kľúči.

B	I	E	H	E	H	D	E	E
O	S	O	A	N	N	U	C	J
L	T	D	L	Y	E	T	T	X

Za kľúč zvolíme „pravotočivú špirálu dovnútra, začínajúcu z pravého horného rohu“. Dostaneme: EJXTTEILDTLOBIEHEHDECUNNAOS