# Klasične šifre

## Transpozicijska šifra

V transpozicijski šifri ostanejo črke originalnega sporočila nespremenjene, njihova mesta pa so pomešana na kakšen sistematičen način

(primer: permutacija stolpcev).

Te šifre zlahka prepoznamo, če izračunamo gostoto samoglasnikov (v angleščini je ta 40%, in skoraj nikoli ne pade zunaj intervala 35%–45%).

Težko jih rešimo, vendar pa se potrpljenje na koncu običajno izplača.





**Simetrična šifra** *je peterica* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za katero velja:*

1. $\mathcal{P}$ *je končna množica možnih čistopisov*
2. $\mathcal{C}$ *je končna množica možnih tajnopisov*
3. $\mathcal{K}$ *je končna množica možnih ključev.*
4. *Za vsak ključ* $K \in \mathcal{K}$, *imamo šifrirni postopek* $e_K \in \mathcal{E}$ *in ustrezen odšifrirni postopek* $d_K \in \mathcal{D}$.

$$e_K : \mathcal{P} \longrightarrow \mathcal{C} \quad \text{in} \quad d_K : \mathcal{C} \longrightarrow \mathcal{P}$$

*sta taki funkciji, da je* $d_K(e_K(x)) = x$ *za vsak* $x \in \mathcal{P}$.





**Pomična šifra** (angl. shift cipher) je poseben primer zamenjalne šifre.

`wewillmeetatmidnight`

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19
7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

`HPHTWWXPPELEXTOYTRSE`

Cezarjeva šifra zašifrira njegovo ime v Ehbčt.

Cezar ukazal napad

↓

Ehbčt žnčbčo rčščg





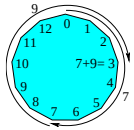
V kriptografiji si na splošno radi omislimo končne množice, kot pri številčnici na uri (npr. praštevilske obsege $\mathbb{Z}_p$).

**Kongruence:** naj bosta $a$ in $b$ celi števili in $m$ naravno število.

$$a \equiv b \pmod{m} \iff m | b - a.$$

**Primer:** za $p = 13$ velja
$7 +_{13} 9 = 7 + 9 \mod 13 = 3$ in
$5 *_{13} 4 = 5 * 4 \mod 13 = 7$

(saj ima pri deljenju s 13
vsota 16 ostanek 3,
produkt 20 pa ostanek 7),
možno pa je tudi deljenje.








Deljenje v primeru $p = 13$:

| $*_{13}$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | **1** | 3 | 5 | 7 | 9 | 11 |
| 3 | 3 | 6 | 9 | 12 | 2 | 5 | 8 | 11 | **1** | 4 | 7 | 10 |
| 4 | 4 | 8 | 12 | 3 | 7 | 11 | 2 | 6 | 10 | **1** | 5 | 9 |
| 5 | 5 | 10 | 2 | 7 | 12 | 4 | 9 | **1** | 6 | 11 | 3 | 8 |
| 6 | 6 | 12 | 5 | 11 | 4 | 10 | 3 | 9 | 2 | 8 | **1** | 7 |
| 7 | 7 | **1** | 8 | 2 | 9 | 3 | 10 | 4 | 11 | 5 | 12 | 6 |
| 8 | 8 | 3 | 11 | 6 | **1** | 9 | 4 | 12 | 7 | 2 | 10 | 5 |
| 9 | 9 | 5 | **1** | 10 | 6 | 2 | 11 | 7 | 3 | 12 | 8 | 4 |
| 10 | 10 | 7 | 4 | **1** | 11 | 8 | 5 | 2 | 12 | 9 | 6 | 3 |
| 11 | 11 | 9 | 7 | 5 | 3 | **1** | 12 | 10 | 8 | 6 | 4 | 2 |
| 12 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | **1** |





**Afina šifra:**

$$e(x) = ax + b \pmod{26} \qquad \text{za } a, b \in \mathbb{Z}_{26}$$

Za $a = 1$ dobimo pomično šifro.
Funkcija je injektivna, če in samo če je $D(a, 26) = 1$.

Imamo $|\mathcal{K}| = 12 \times 26 = 312$ možnih ključev.

Za pomično šifro in afino šifro pravimo, da sta **monoabecedni**, ker preslikamo vsako črko v natanko določeno črko.





**Vigenèrejeva šifra** (1586):

Naj bo $m \in \mathbb{N}$ in

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m.$$

Za ključ $K = (k_1, k_2, \ldots, k_m)$ definiramo

$$e(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) \text{ in}$$
$$d(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m),$$

kjer sta operaciji "+" in "−" opravljeni po modulu 26.





| | 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 | 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 | 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 | 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 | 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 | 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 |
| F | 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 |
| G | 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 |
| H | 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 |
| I | 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 |
| J | 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 |
| K | 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 |
| L | 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 |
| M | 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 |
| N | 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 |
| O | 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 |
| P | 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 |
| Q | 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 |
| R | 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 |
| S | 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 |
| T | 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 |
| U | 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 |
| V | 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 |
| W | 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 |
| X | 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 |
| Y | 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 |
| Z | 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 |

Sporočilo

```
TO BE OR NOT TO BE THAT IS THE QUESTION
```

zašifriramo s ključem `RELATIONS`:

```
ključ:       RELAT IONSR ELATI ONSRE LATIO NSREL
čistopis:    TOBEO RNOTT OBETH ATIST HEQUE STION
tajnopis:    KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
```

Npr. prvo črko tajnopisa dobimo tako, da pogledamo v tabelo na mesto (`R`, `T`).

Kako pa najdemo iz `T` in `K` nazaj `R`?





To ni monoabecedna šifra.

Pravimo ji **poliabecedna šifra**.

Vigenèrejeva šifra in $26^m$ možnih ključev.

Za $m = 5$ je število $1.1 \times 10^7$ že preveliko, da bi "peš" iskali pravi ključ.





**Hillova šifra** (1929)

Naj bo $m$ neko naravno število in naj bo

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m.$$

Za $K$ vzemimo obrnljivo $m \times m$ matriko in definirajmo

$$e_K(x) = xK \quad \text{in} \quad d_K(y) = yK^{-1},$$

pri čemer so vse operacije opravljene v $\mathbb{Z}_{26}$.





**Ponovimo:**

**Odšifriranje (razbijanje) klasičnih šifer**

Kriptografske sisteme kontroliramo s pomočjo ključev, ki določijo transformacijo podatkov.
Seveda imajo tudi ključi digitalno obliko (binarno zaporedje: 01001101010101...).

Držali se bomo **Kerckhoffovega principa**, ki pravi, da "nasprotnik"

*pozna kriptosistem oziroma algoritme, ki jih uporabljamo, ne pa tudi ključe, ki nam zagotavljajo varnost.*





Ločimo naslednje nivoje napadov na kriptosisteme:

1. **samo tajnopis**: *nasprotnik ima del tajnopisa,*
2. **poznani čistopis**: *nasprotnik ima del čistopisa ter ustrezen tajnopis,*
3. **izbrani čistopis**: *nasprotnik ima začasno na voljo šifrirno mašinerijo ter za izbrani $x \in \mathcal{P}$ konstruira $e(x)$,*
4. **izbrani tajnopis**: *nasprotnik ima začasno na voljo odšifrirno mašinerijo ter za izbrani $y \in \mathcal{C}$ konstruira $d(y)$.*