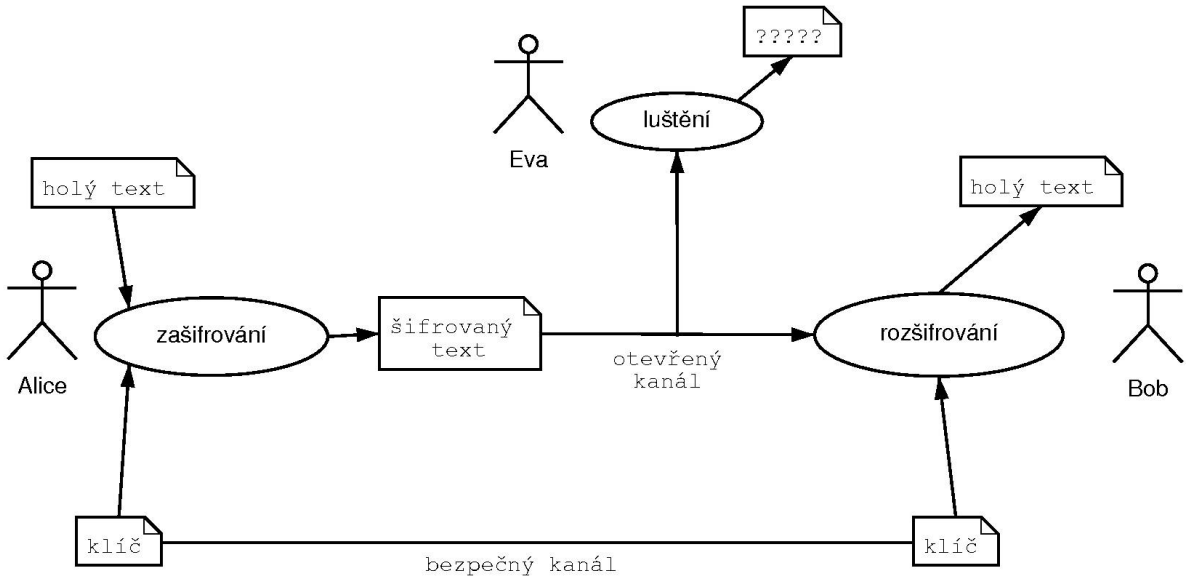
Rychlokurz kryptologie

Základní pojmy



- kryptografie – šifrování
- kryptoanalýza – luštění
- kryptologie – všechno dohromady

Transpoziční šifry

- změna pořadí znaků
- znaky zůstavají zachovány

PNZRCNIEA

Substituční šifry

- změna (náhrada, substituce) jednotlivých znaků
- Caesarova šifra = posun o tři pozice v abecedě

```
VLKODLAK
YONRGODN
```

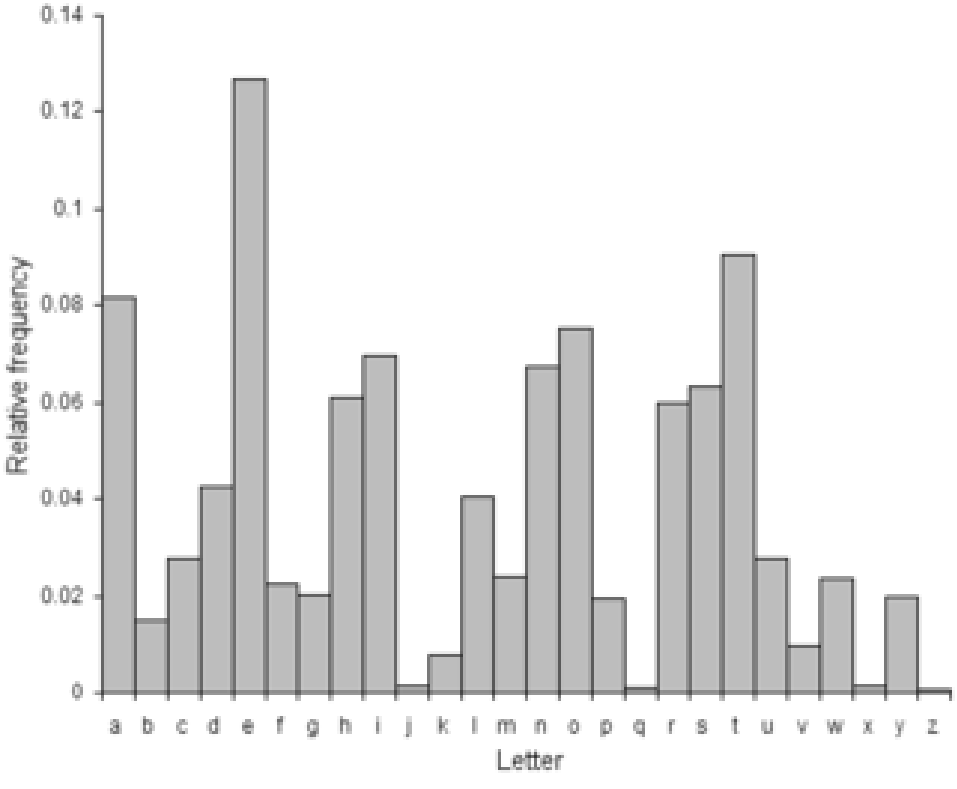
Steganografie

- skrývání existence zprávy
- např. tetování na hlavě otroka

Trójský kůň

Je něčím jiným, než se zdá!

Kryptoanalýza: frekvenční analýza



Příklad 1

DFSWFOB LBSLVMLB

Příklad 2

```
UKIL SAPRT MDE
SA A KRUH E NS
```

Příklad 3

WOEUIGNABOXBNPIASHBOATASBAAS

SLGWIOSODSHBIANESOWHOIASOIIO

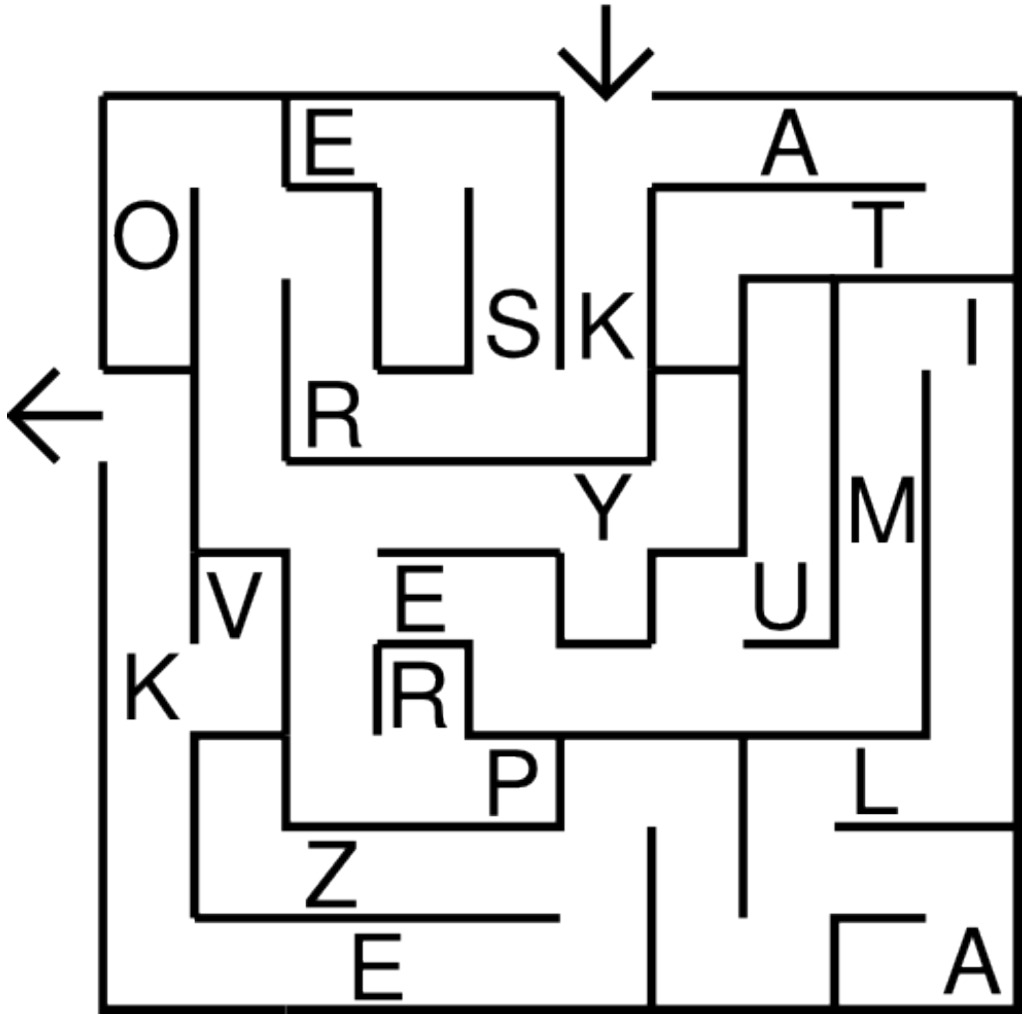
AODSHBOWINOBASWEONBAOEIHNABE

AWHONBDAOSNBIAJEDNOROZECCOHB

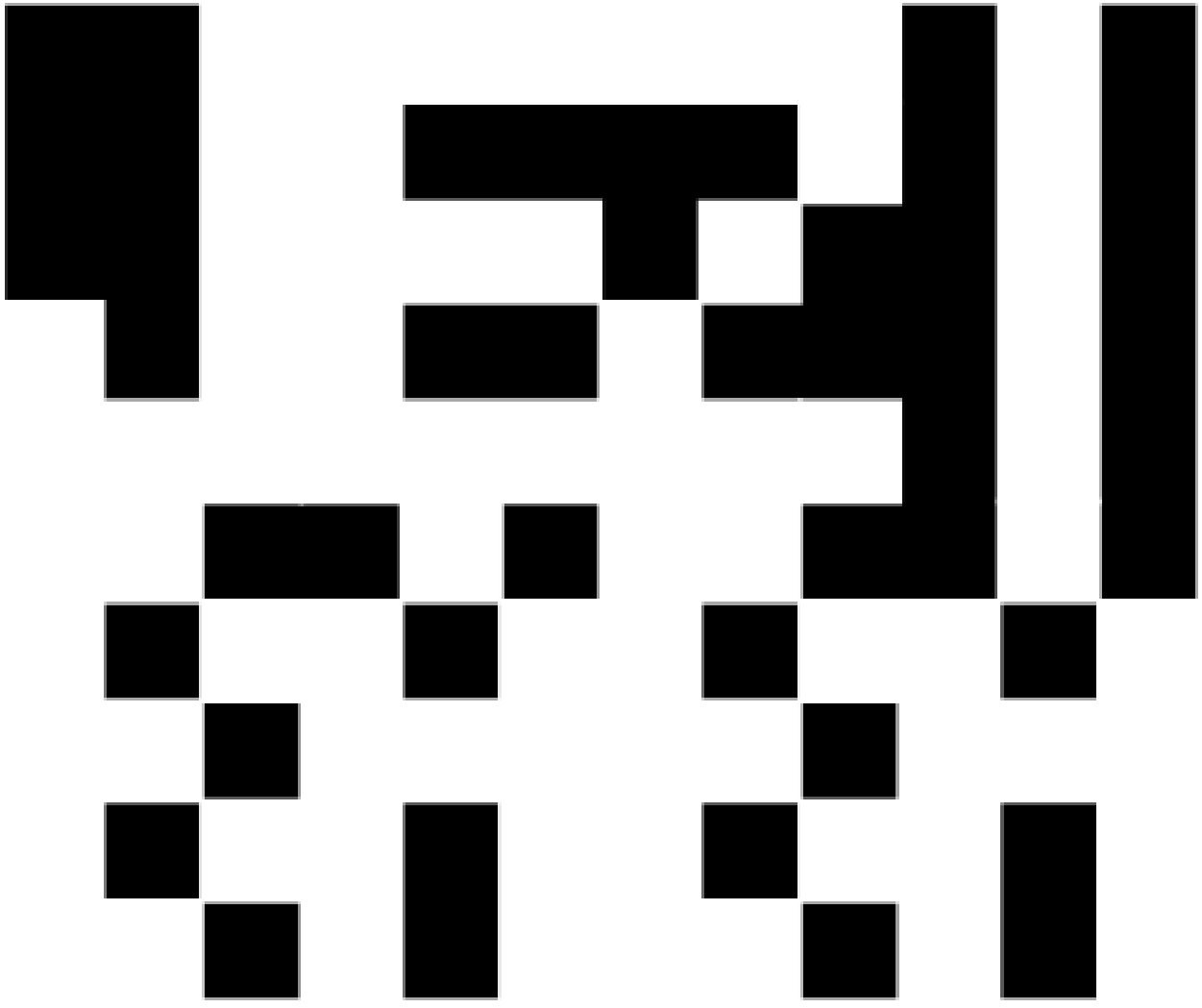
XBNOWOPWONBAPZOIWNBIAPLDFBOA

ASLGWOINBAOEHDSBASBNAOSBNAOS

Příklad 4



Příklad 5



Konec

Odevzdejte odpovědi!