



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Šifrování dat

Obsah

- 1 / Šifrování dat**
- 2 / Využití šifrování**
- 3 / Symetrická šifra**
- 4 / Asymetrická šifra**
- 5 / Caesarova šifra**

1 / Šifrování dat

Šifrování dat je proces, kterým se nezabezpečená elektronický data převádí za pomoci kryptografie na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče.

Slouží k ochraně proti nežádoucímu zjištění cizí osobou.

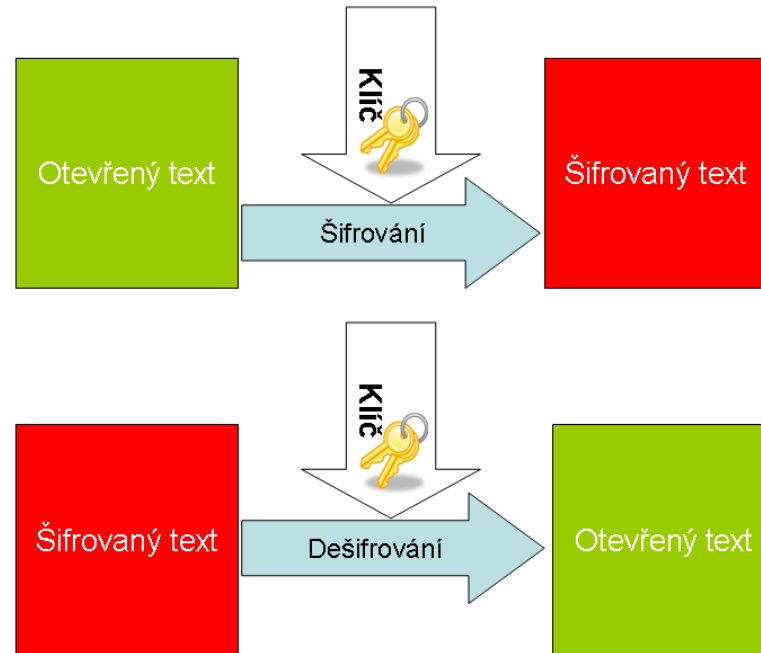


2 / Využití šifrování

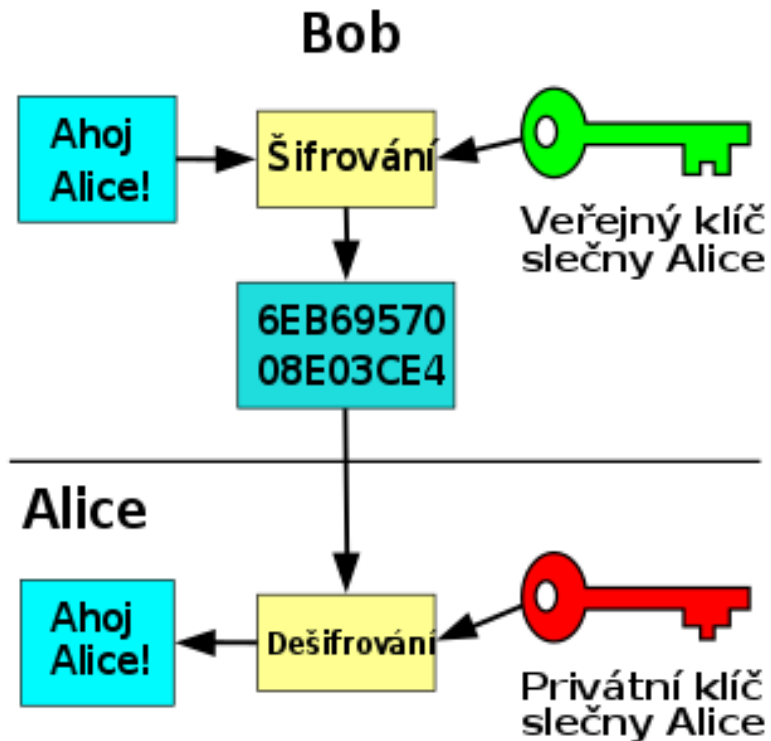
- Přeměna dat do speciálního formátu, který je pro ostatní nečitelný.
- Pokud neznají klíč nemohou si data přečíst.

2 / Symetrická šifra

- Rychlé
- Méně náročné na výpočty
- Méně bezpečné
- Jeden klíč na šifrování i dešifrování



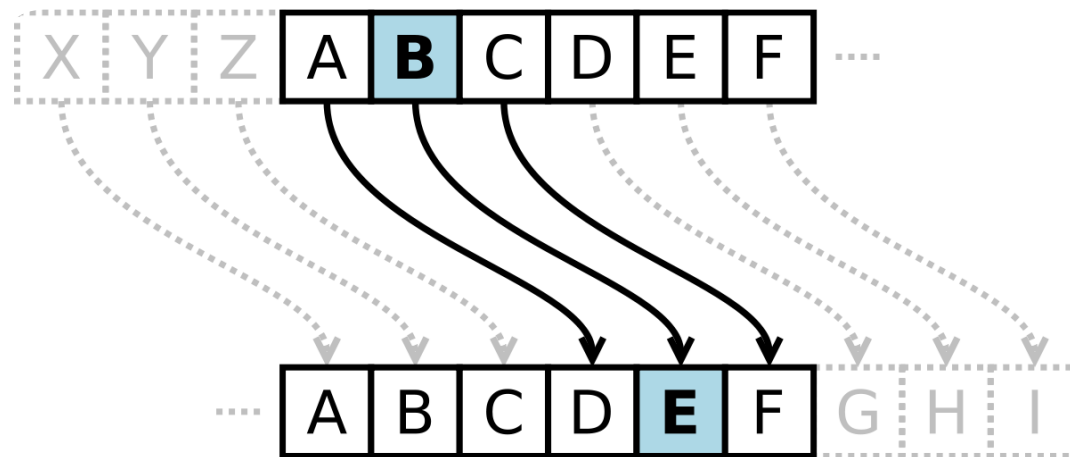
4 / Asymetrická šifra



- Pomalejší
- Náročnější na výkon
- Více bezpečné
- Dva klíče
 - Veřejný – šifrování
 - Soukromý (privátní) – dešifrování

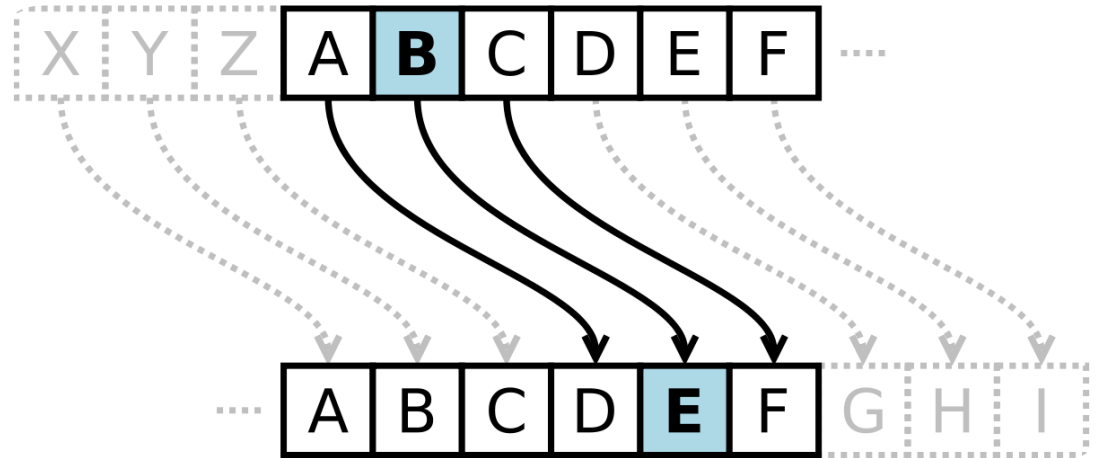
5 / Caesarova šifra

- Caesarova šifra spočívá v posunu znaků v zadaném textu vždy o stejnou zadanou číselnou hodnotu v abecedě.



5 / Caesarova šifra

- Příklad šifrování:
 - škola
 - tlpmb
- Příklad dešifrování:
 - epnpw
 - domov



Pracovní list 6