Základy kryptografie

Mgr. Petr Zaoral

- *Proč?*
- *Co je to kryptografie?*
- Symetrická kryptografie
- Asymetrická kryptografie
  - Asymetrické šifrování
  - Digitální podpis
- Hybridní kryptografie

Co je to kryptografie

- z řečtiny:

  Κρυτός (kryptós) = tajné

  Γράφειν (gráfein) = psaní
- bezpečná výměna zpráv v přítomnosti třetích stran
- teď v počítačové formě
- Kryptoanalýza – luštění zašifrovaných zpráv

- algoritmus popisuje, jak

  ze zprávy (plain-text) a klíče (key) vyrobit šifru (cipher-text)

  ze šifry (cipher-text) a klíče (key) rekonstruovat zprávu (plain-text)

- vymyslet dobrý algoritmus je obtížné, proto není vhodné držet algoritmus v tajnosti
- používáme dobře známé algoritmy a v tajnosti držíme klíče

Rozdělení kryptografie

- **symetrická**

  šifrování

  jeden tajný klíč (Secret-Key Cryptography)

- **asymetrická**

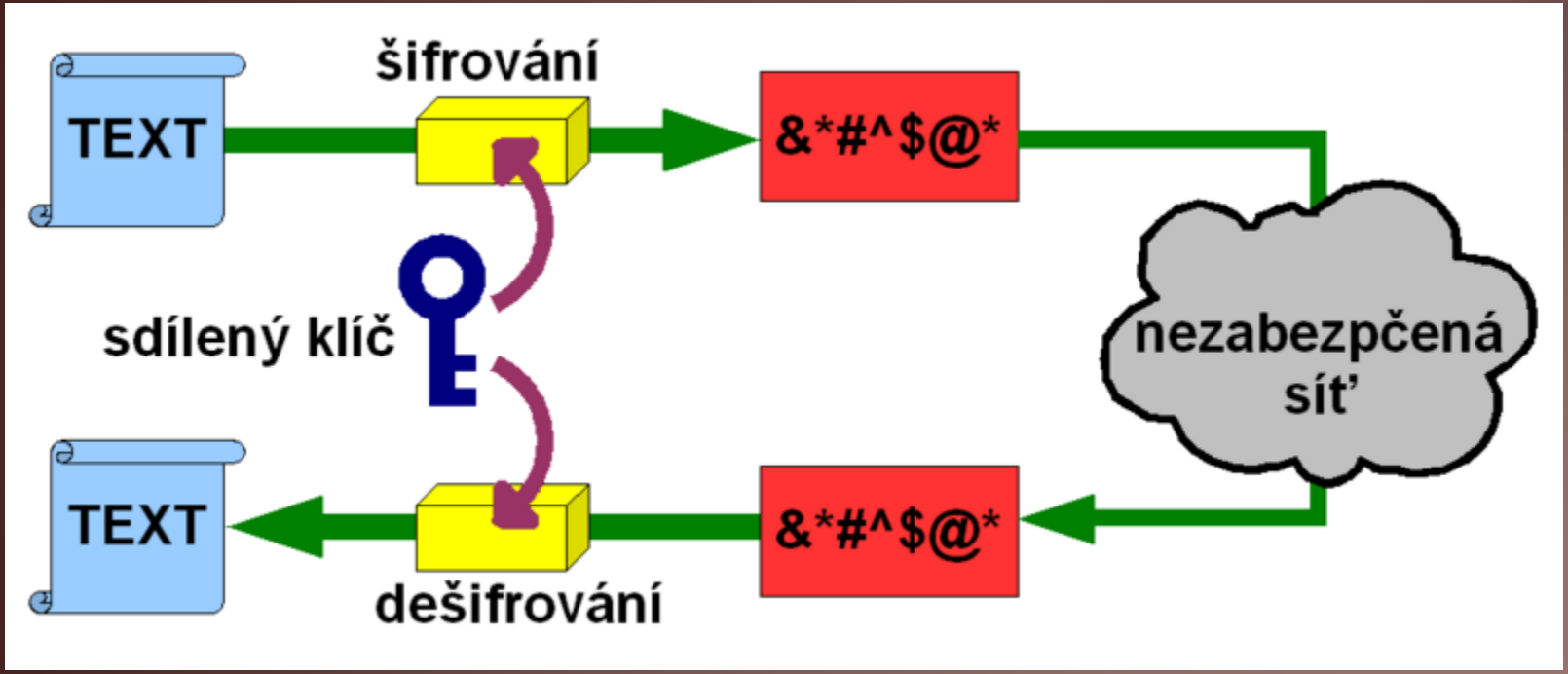
  šifrování a podepisování

  pár klíčů: soukromý a veřejný (Public-Key Cryptography)

- **hybridní**

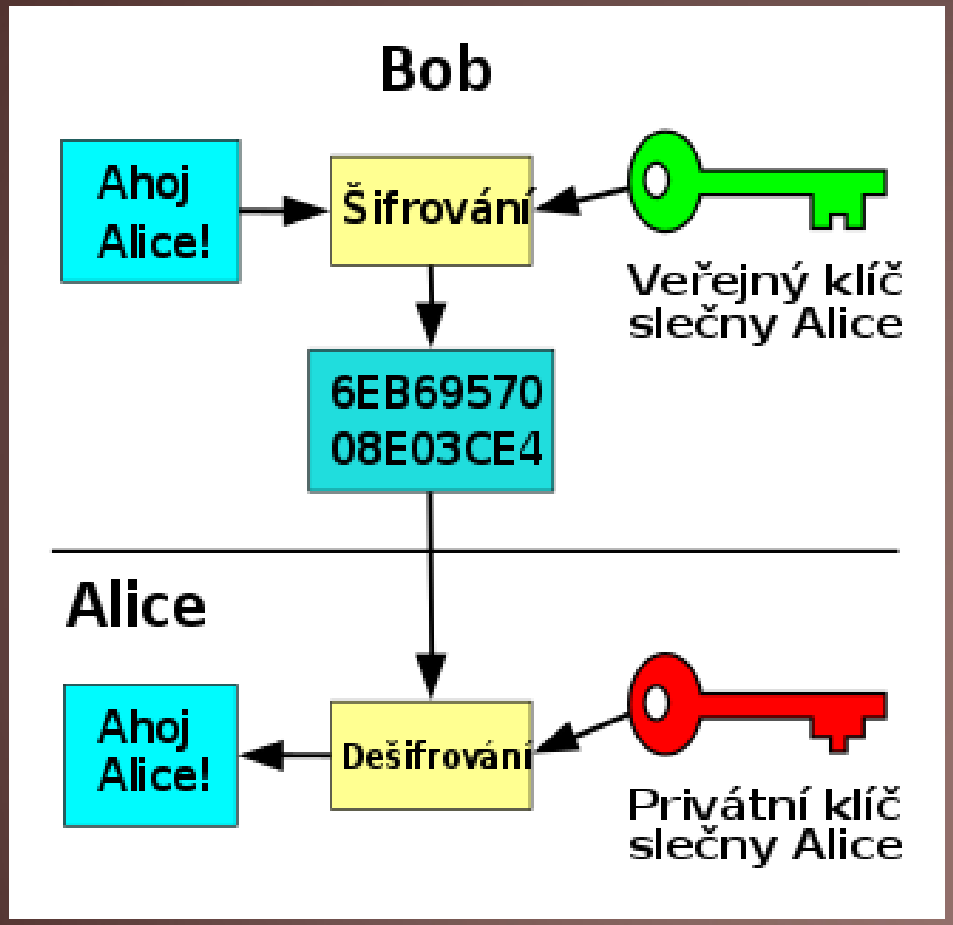
Symetrická kryptografie

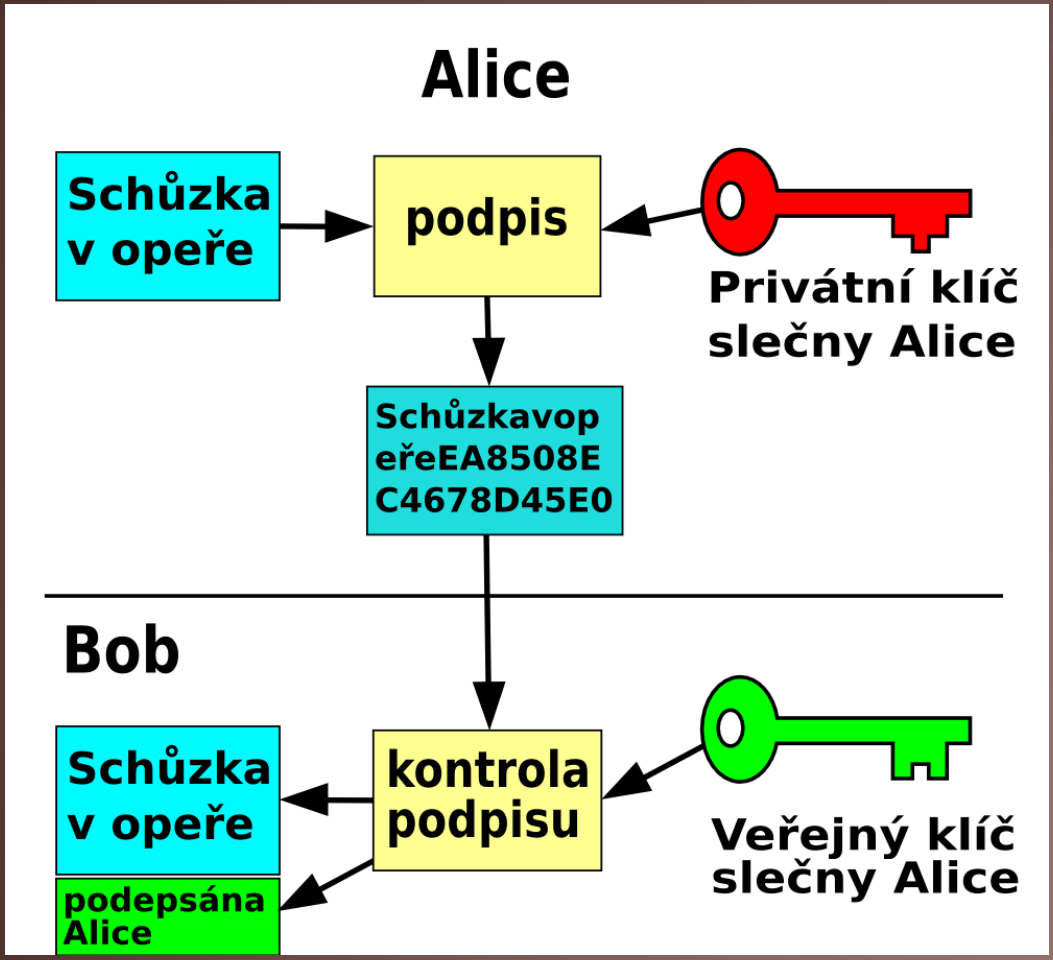
- rychlá
- za určitých podmínek neprolomitelná
- jednoduché použití
- problematická výměna klíče
  - nutný zabezpečený kanál
  - otázka důvěry
- kvalitní algoritmy: AES, CAST5, Blowfish, Twofish, ...
- nekvalitní algoritmy: DES (zastaralý), XOR (primitivní)


šifrování
TEXT
&*#^$@*
sdílený klíč
nezabezpčená síť
TEXT
&*#^$@*
dešifrování

Asymetrická kryptografie

- pomalá
- založena na matematickém problému
  - rozklad na prvočísla, inverzní transformace
  - teoreticky prolomitelná, prakticky je to příliš náročné
  - lze zlomit kvantovým počítačem
- veřejný klíč lze poslat komukoliv
  - řeší otázku důvěry, není nutný zabezpečený kanál
  - Man-in-the-Middle Attack: podvržení klíče
- soukromý klíč se nikomu neposílá


Bob
Ahoj Alice!
Šifrování
Veřejný klíč slečny Alice
6EB69570 08E03CE4
Alice
Ahoj Alice!
Dešifrování
Privátní klíč slečny Alice


Alice
Schůzka v opeře
podpis
Privátní klíč slečny Alice
Schůzkavop eřeEA8508E C4678D45E0
Bob
Schůzka v opeře
kontrola podpisu
Veřejný klíč slečny Alice
podepsána Alice

- kvalitní algoritmy
  - pro šifrování: RSA, ElGamal
  - pro podepisování: RSA, DSA
- prolomení: získání soukromého klíče z veřejného
  - lze řešit pouze obměnou klíčů
  - a volbou vhodné velikosti (alespoň 2048 bitů)

Hybridní kryptografie

- asymetrická kryptografie se nehodí pro velké zprávy (složité výpočty)
- řešení: hybridní kryptografie
  - vygeneruje se náhodný klíč na jedno použití (session key)
  - klíč se odešle pomocí asymetrické kryptografie
  - zpráva se zašifruje náhodným klíčem symetricky
- používá prakticky každý nástroj (PGP, GnuPG) a protokol (SSL, TLS) pro asymetrickou kryptografii

Závěr

- v kryptografii je zásadní správa klíčů
- symetrické šifrování se hodí pro osobní účely nebo pro dvojice osob
- asymetrické šifrování se hodí pro větší okruh osob
- digitální podepisování brání falšování zpráv a vydávání se za autora
- bez ověření klíče hrozí Man-in-the-Middle Attack

V práci odchází jeden z programátorů o hodinu dřív. Ostatní se diví, co se děje.

On na to:

"**Ale, žena slaví narozeniny**"

"**A kolik jí vlastně je?**"

"**32**"

"**Nekecej, kulatiny...!!!**"

Děkuji za pozornost.

https://www.youtube.com/watch?v=LTa7JOjAtQ4