Základy kryptografie

Beret

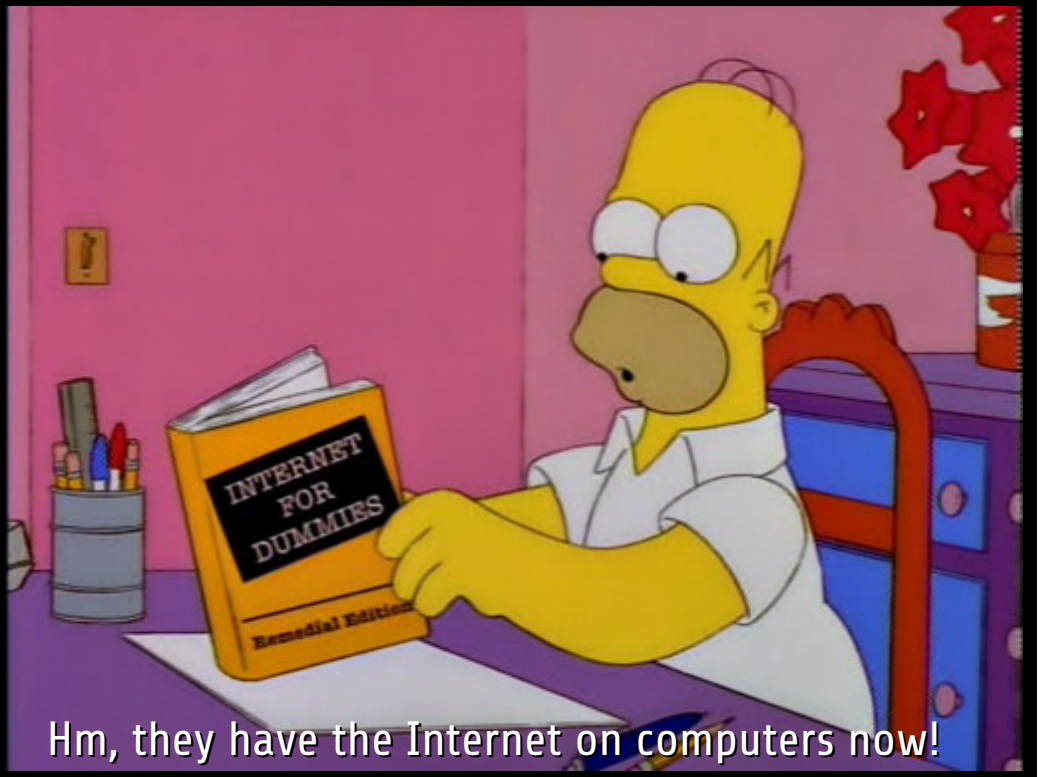
CryptoParty 11.02.2013

Obsah prezentace

1. Co je to kryptografie
2. Symetrická kryptografie
3. Asymetrická kryptografie
   - Asymetrické šifrování
   - Digitální podpis
4. Hybridní kryptografie

Co je to kryptografie

- z řečtiny:
  - κρυπτός (kryptós) = tajné
  - γράφειν (gráfein) = psaní
- bezpečná výměna zpráv v přítomnosti třetích stran
- teď je na počítačích



Kryptografické algoritmy

- 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

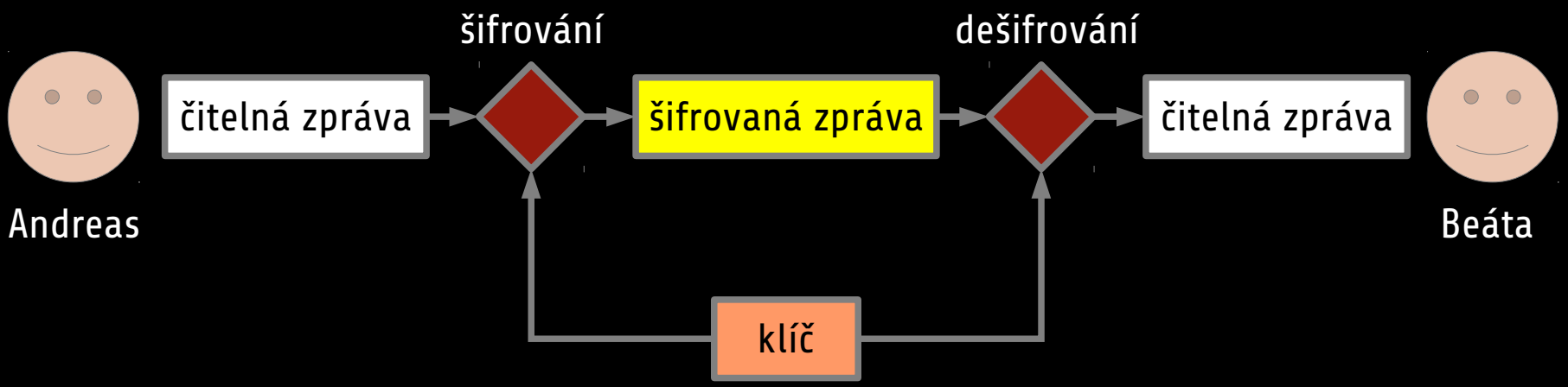
Rozdělení kryptografie

- 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
  - gpg --symmetric, rar, ...
- problematická výměna klíče
  - nutný zabezpečený kanál
  - otázka důvěry
- kvalitní algoritmy: AES, CAST5, Blowfish, Twofish, ...
- nekvalitní algoritmy: DES (zastaralý), XOR (primitivní)

Symetrická kryptografie

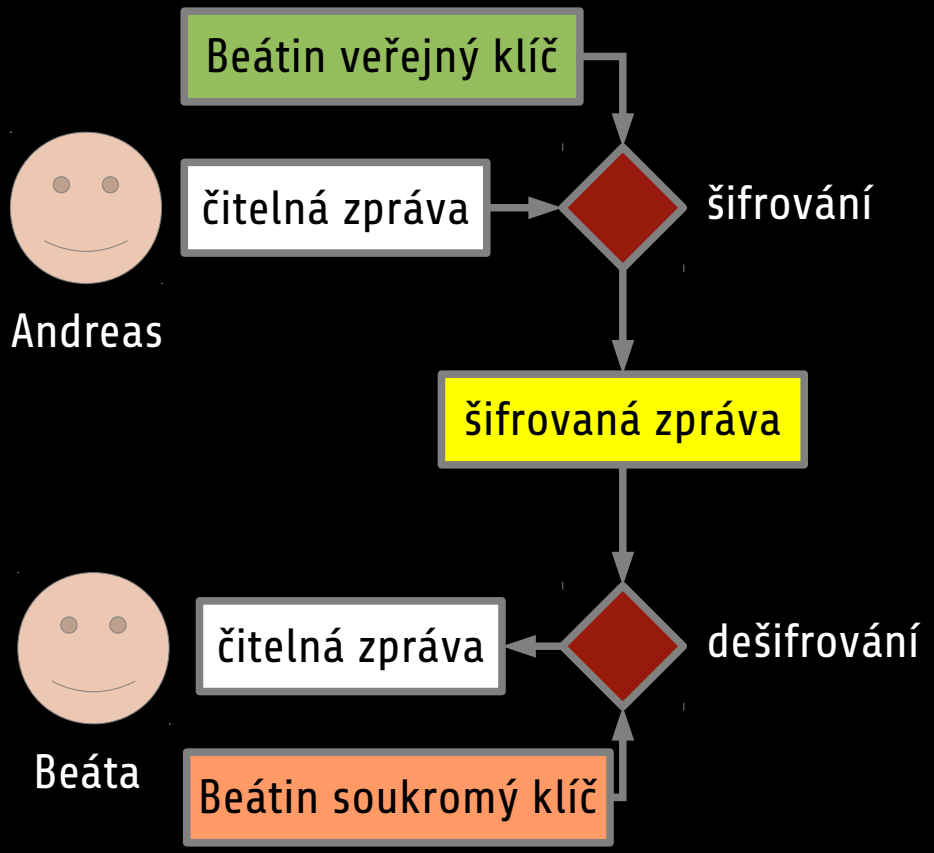


Asymetrická kryptografie

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

Asymetrické šifrování

- veřejný klíč k šifrování
  - šifrovat může kdokoliv
- soukromý klíč k dešifrování
  - dešifrovat může pouze příjemce
- brání proti čtení třetími stranami

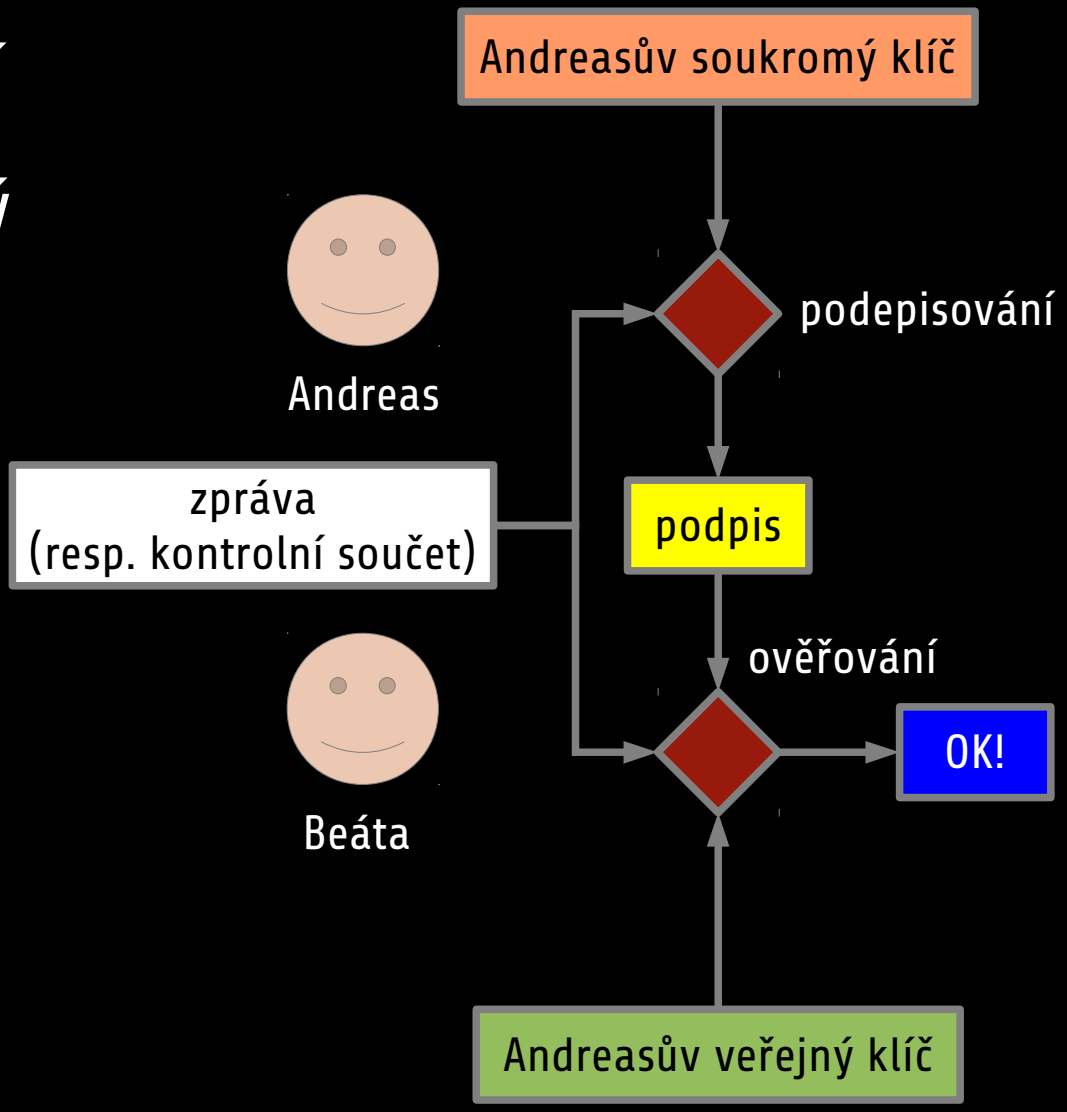


Asymetrické šifrování

- co když klíče použijeme obráceně?
  - šifrovat soukromým klíčem
  - dešifrovat veřejným klíčem
- získáme šifru, kterou umí vytvořit pouze jeden subjekt, ale dešifrovat kdokoliv
  - je to k něčemu užitečné?

Digitální podpis

- soukromý klíč k podepsání
  - podepsat může pouze pravý autor zprávy
- veřejný klíč k ověření
  - ověřit může kdokoliv
- zajišťuje pravost autora a integritu zprávy
- brání proti podvržení třetími stranami



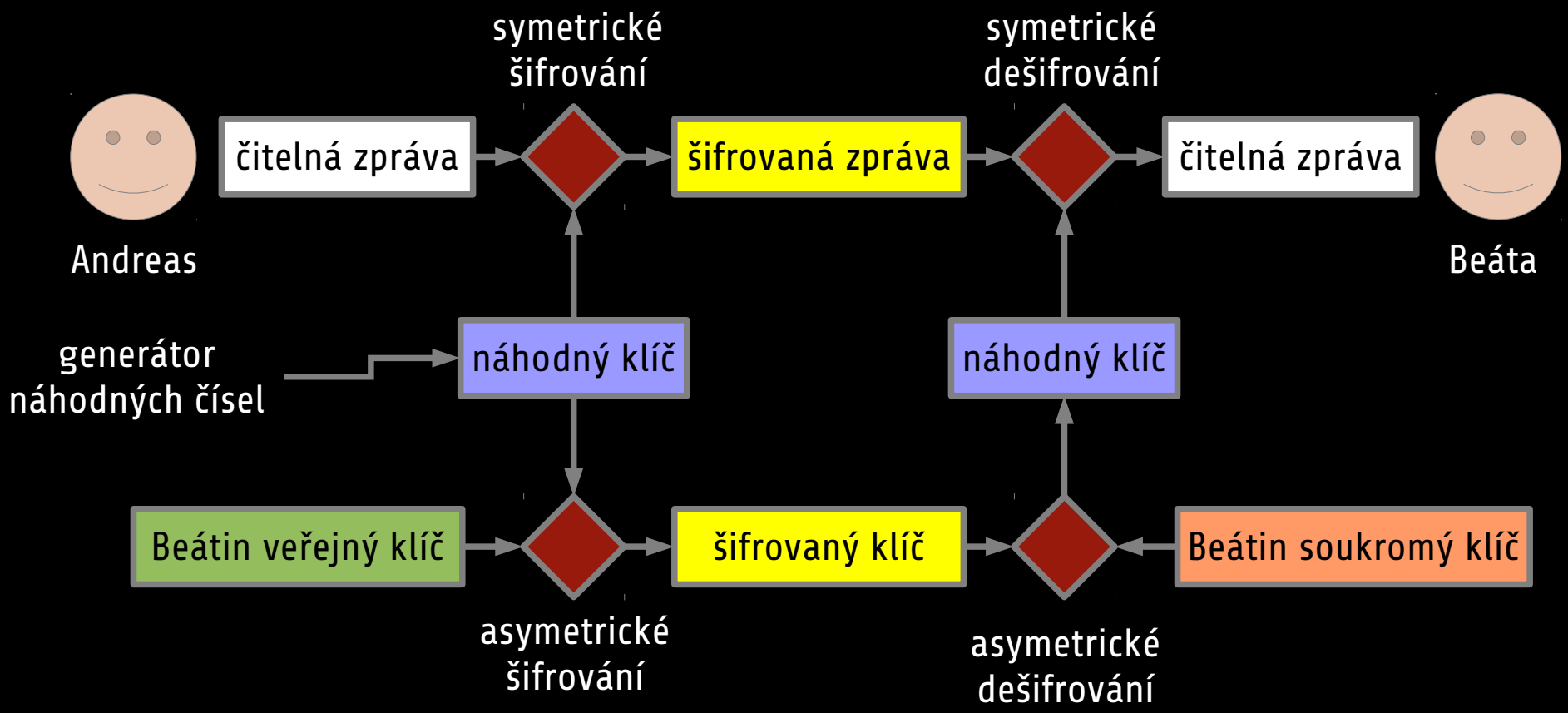
Asymetrická kryptografie

- 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

Hybridní kryptografie



Závěr

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

K zamyšlení

- kryptografie je (stále) legální, až na výjimky
  - USA – exportní zákony
  - UK a spol. – povinné vydávání hesel
  - rubber-hose attack
- bezpečí bývá často protipólem pohodlí
- nenechte se zmást falešným pocitem bezpečí