Úvod do kryptografie

Andrew Kozlík

KA MFF UK

Úvod

Webová stránka přednášky:
`http://www.karlin.mff.cuni.cz/~kozlik/udk`

Zápočet a zkouška:

- Na cvičení bude možné získat až 100 bodů za domácí úkoly. (Zadaných úkolů může být víc než za 100 bodů.)
- U zkoušky bude možné získat dalších 100 bodů.
- Na cvičení je třeba získat alespoň 75 bodů.
- U zkoušky je třeba získat alespoň 60 bodů.
- Známka se určí z celkového počtu bodů:
  - 185–200 bodů výborně,
  - 160–184 bodů velmi dobře,
  - 135–159 bodů dobře.

Čím se zabývá kryptografie?

- Utajení informací.
- Autentizace subjektu. (Ověření identity subjektu.)
  Neplést s autorizací! (Ověření, že subjekt má určité právo).
- Autentizace původce zprávy.
- Zajištění integrity dat (zajištění detekovatelnosti náhodných nebo záměrných změn v datech).
- Nepopiratelnost jednání (u elektronického podpisu).
- Dokazování s nulovou znalostí.
- Generování náhodných čísel.
- Anonymita (u e-voleb nebo e-mincí).
- Popiratelné šifrování.
- A další . . .

Program přednášky

- Shannonova teorie tajné komunikace:
  - Entropie.
  - Absolutně bezpečné šifry.
- Symetrická kryptografie:
  - Blokové šifry (DES, AES) a operační režimy.
  - Meet-in-the-middle útok na 2DES.
  - Proudové šifry (A5/1).
  - Hashovací funkce a narozeninový paradox.
  - Merkleovo-Damgårdovo schéma.
  - Autentizační kód zprávy (MAC).
- Asymetrická kryptografie:
  - Diffieho-Hellmanův protokol.
  - Elektronický podpis a RSA.
  - ElGamalův šifrovací systém a podpisové schéma.
  - Algoritmus DSA.

Ujasnění některých pojmů

- **Šifra**
  Sada algoritmů sloužící k utajení významového obsahu dat.

- **Kód**
  Systém symbolů sloužící k reprezentaci informací.
  - Morseova abeceda.
  - Samoopravný kód.
  - Zvukový nebo obrazový kodek.
  - Výjimka: *kódová kniha* je název šifry.

- **Steganografie**
  Obor, který se věnuje utajení přítomnosti dat.
  - Neviditelný inkoust.
  - Skrývání zpráv uvnitř obrázků.