Tréningový modul: 7

INFORMAČNÁ BEZPEČNOSŤ V MULTIMÉDIÁCH

- **Informačná, počítačová a sieťová bezpečnosť**
  - Základné pojmy
  - Služby bezpečnosti, mechanizmy bezpečnosti a útoky na bezpečnosť
  - Architektúra bezpečnosti v modeli OSI
- **Klasické kryptografické systémy (prehľad)**
  - Základné pojmy
  - Princíp konvenčného šifrovania
  - Model konvenčného kryptografického systému
  - Klasifikácia kryptografických systémov a šifier
  - Bezpečnosť kryptografických algoritmov
- **Symetrické šifry (prehľad)**
  - Princípy symetrických blokových šifier
  - Šifrovací štandard DES
    - *Opis algoritmu DES*
    - *Bezpečnosť algoritmu DES*
  - Trojnásobný DES
  - AES
    - *Opis štandardu AES*
    - *Operácia Add Round Key*
    - *Operácia Key Expansion*
- **Kryptografia s verejným kľúčom (prehľad)**
  - Princíp kryptografie s verejným kľúčom
  - Kryptografické systémy s verejným kľúčom
  - Podmienky realizovateľnosti kryptografického systému s verejným kľúčom
  - Kategorizácia kryptografických systémov s verejným kľúčom
  - Algoritmy kryptografických systémov s verejným kľúčom
    - *Algoritmus na výmenu kľúčov Diffie – Hellman*
    - *Algoritmus RSA*
- **Autentizácia používateľov a autorizácia dát (prehľad)**
  - Šifrovanie správy
  - Autentizačný kód správy MAC
  - Hašovacie funkcie
  - Digitálne podpisy
    - *Štandardy pre digitálne podpisy*