Plán cvičení z predmetu
APLIKOVANÁ KRYPTOGRAFIA
(letný semester 2008)

1. **Úvodné cvičenie**
   náplň cvičení,
   podmienky udelenia zápočtu
2. **Klasické kryptografické systémy**
   substitučné a transpozičné šifry, prehľad algoritmov a ich princíp,
   kryptoanalýza na báze frekvencie výskytu znakov,
   oboznámenie sa so softvérom CRYPTOOL
3. **Aplikovaná kryptografia v praxi**
   príklady a využitie AK, demonštrácia vybraných technických prostriedkov pre AK
4. **Algebraické systémy v kryptografii - modulárna aritmetika**
   modulárny operátor, vlastnosti modulárnej aritmetiky,
   grupy, okruhy, telesá a polia
5. **Algebraické systémy v kryptografii - Euklidov algoritmus, Galoisove polia**
   využitie rozšíreného Euklidovho algoritmu na hľadanie multiplikatívnej inverzie,
   konečné polia GF(p), konečné polia GF(2n),
   polynómy a polynomiálna aritmetika
6. **Šifrovací štandard AES**
   štruktúra šifry, vlastnosti,
   precvičenie základných operácií na príkladoch
7. **Teória čísel v kryptografii - prvočísla, diskrétne logaritmy**
   prvočísla a ich význam, kanonický tvar čísel,
   Fermatova veta, Eulerova veta, čínska veta o zvyškoch,
   výpočet diskrétnych logaritmov
8. **Kryptografia s verejným kľúčom – algoritmus RSA**
   popis a vlastnosti algoritmu RSA,
   precvičenie generovania kľúčov, šifrovania, dešifrovania
9. **PÍSOMKA**
   odovzdanie vypracovaných úloh zadávaných priebežne po každom cvičení,
   overenie zvládnutia učiva z cvičení 4 až 8
10. **Generátory náhodných čísel**
    základné princípy generovania náhodných čísel, hľadanie veľkých prvočísel,
    kryptograficky bezpečné generátory,
    testovanie náhodnosti
11. **Hašovacie (jednocestné) funkcie**
    význam, SHA1 – Secure Hash Standard FIPS PUB 180-1,
    kryptograficky generátor náhodných čísel na báze SHA1
12. **Eliptické krivky (ECC)**
    kryptografia na báze eliptických kriviek, digitálny podpis na báze ECC (ECDS)

Podmienky udelenia zápočtu:
- účasť na cvičeniach
- vypracovanie úloh