Plán prednášok z predmetu APLIKOVANÁ KRYPTOGRAFIA
(zimný semester 2018)

1. **Úvod do problematiky, základné pojmy, princípy a klasifikácia**
2. **Algebraické systémy v kryptografii - modulárna aritmetika**
3. **Symetrické šifry DES a 3DES**
4. **AES a vybrané typy symetrických šifier**
5. **Princípy kryptografie s verejným kľúčom, algoritmy Diffie- Hellman, RSA a Al Gamal**
6. **Kryptografia na báze ECC**
7. **Manažment kľúčov v kryptografii s verejným kľúčom**
8. **Autentizácia používateľov a autorizácia dát**
9. **Hašovacie funkcie, vybrané typy hašovacích funkcií**
10. **Elektronické a digitálne podpisy**
11. **Aplikácie kryptografie v informačnej a sieťovej bezpečnosti – časť I**
12. **Aplikácie kryptografie v informačnej a sieťovej bezpečnosti. – časť II**

Plán cvičení z predmetu APLIKOVANÁ KRYPTOGRAFIA (zimný semester 2018)

1. **Úvodné cvičenie**

   - náplň cvičení, podmienky udelenia zápočtu (účasť na cvičeniach, vypracovanie úloh a zadania, min. 21 bodov z písomky)

   Algebraické systémy v kryptografii - modulárna aritmetika, modulárny operátor, vlastnosti modulárnej aritmetiky, grupy, okruhy, telesá a polia

2. **Individuálne riešenie úloh z polynomiálnej aritmetiky**
3. **Modulárna aritmetika a jazyk C**

   operácie s veľkými číslami, softvérový balík Magma

4. **Algebraické systémy v kryptografii - Euklidov algoritmus, Galoisove polia**

   využitie rozšíreného Euklidovho algoritmu na hľadanie multiplikatívnej inverzie,

   konečné polia GF(p), konečné polia GF(2^n), polynómy a polynomiálna aritmetika

5. **Šifrovací štandard AES**

   štruktúra šifry, vlastnosti, precvičenie základných operácií na príkladoch

6. **Individuálne oboznámenie sa so systémom CRYPTOOL**

   Klasické kryptografické systémy

   - substitučné a transpozičné šifry, prehľad algoritmov a ich princíp

7. **Teória čísel v kryptografii – prvočísla**

   princípy jednocestnosti, prvočísla a ich význam, kanonický tvar čísel, Fermatova veta,

   Eulerova veta

8. **Teória čísel v kryptografii - diskrétne logaritmy**

   výpočet diskrétnych logaritmov, Čínska veta o zvyškoch

9. **Kryptografia s verejným kľúčom**

   popis a vlastnosti algoritmu RSA, generovanie kľúčov, šifrovanie, dešifrovanie,

   algoritmus na výmenu kľúčov Diffie-Hellman

10. **Kryptografia na báze eliptických kriviek**
11. **PÍSOMKA**

    odovzdávanie vypracovaných úloh zadávaných priebežne po každom cvičení, overenie zvládnutia učiva z cvičení 2 až 10

12. **Oboznámenie sa so systémom CALC**

    Riešenie zadaní

13. **Udelenie zápočtov**

Poznámky:

Cvičenia:	Štvrtok	7:30 – 9:00	BN32_L512
Prednášky:	Pondelok	10:50 – 13:05	PK13_L2

Hodnotenie skúšky:
Zápočet (**max. 40 bodov**).
Písomka + test (**max. 45 bodov**).
Obhajoba zadania a problematiky riešenej v zadaní (**max. 15 bodov**).
Počas obhajoby zadania bude možné použiť ľubovoľné materiály a vlastný počítač.

hodnotenie:	A výborne	91-100 bodov
	B veľmi dobre	81-90 bodov
	C dobre	71-80 bodov
	D uspokojivo	61-70 bodov
	E dostatočne	51-60 bodov
	FX nevyhovel	< 51 bodov

Doporučená literatúra
Levický, D.: Kryptografia a bezpečnosť komunikačných sietí, Elfa, Košice 2016
Drutarovský, M.: Kryptografia pre vstavané procesorové systémy, Technická univerzita v Košiciach, 2017

Ďalšie užitočné zdroje
Paar, Ch., Pelzl, J.: Understanding Cryptography, Springer 2010
Martin, K.: Everyday Cryptography, Fundamental Principles & Applications, Oxford University Press, 2010
Menezes, A.K., Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography, CRC Press, 2001
Hankerson, D. , Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography, Springer, 2010
web stránka predmetu so študijnými materiálmi