Plán prednášok z predmetu BEZPEČNOSŤ INFORMAČNÝCH A KOMUNIKAČNÝCH SYSTÉMOV

(zimný semester 2020)

1. **Informačná bezpečnosť, úvod do problematiky, základné pojmy, princípy a súvislosti**
2. **Symetrické šifrovanie, utajenie správ, autentizované šifrovanie**
3. **Asymetrické šifrovanie, integrita a autentizácia správ**
4. **Bezpečnosť operačných systémov, MS Windows, Unix**
5. **Bezpečnosť softvéru, kryptografické knižnice**
6. **Bezpečnosť v architektúre TCP/IP I**
7. **Bezpečnosť v architektúre TCP/IP II**
8. **Bezpečnosť bezdrôtových sietí a IoT zariadení**
9. **Post-kvantová kryptografia**
10. **Útoky s využitím postranných kanálov**
11. **E-hlasovanie, Block-chain a kryptomeny**
12. **Forézna a penetračná analýza**
13. **Trendy vývoja v oblasti informačnej bezpečnosti**

Plán cvičení z predmetu BEZPEČNOSŤ INFORMAČNÝCH A KOMUNIKAČNÝCH SYSTÉMOV (zimný semester 2020)

1. **Plán cvičení, použité vývojové nástroje**

   náplň cvičení, podmienky udelenia zápočtu (účasť na cvičeniach, vypracovanie domácich úloh, písomky a zadania). Domáce úlohy a zadania **odovzdávané v TERMÍNE cez systém Moodle TUKE.** Odovzdanie riešení domácich úloh a zadaní **v požadovaných termínoch je podmienkou udelenia zápočtu.**

   nástroje: obrazy OS Windows a OS Linux pre VirtualBox (testovanie inštalácie a nastavenie TCP/IP konektivity)

2. **Symetrické šifry, špecializované módy**
   základné operácie v GF(p) a GF(2^m) - opakovanie
   AES-GCM mód (jazyk C), testovacie vektory
   využitie prúdovej šifry (program rclone, jayzk C)

3. **Asymetrické šifrovanie a integrita správ**
   šifrovanie s využitím ECC, „ručný výpočet“ + jazyk C
   vybrané hašovacie funkcie
   Numerické zadanie 1 (5 bodov)

4. **Bezpečnosť operačného systému MS Windows**
   extrakcia databázy z Windows 7 OS, prelomenie hesla
   príklady novších hašovacích funkcií na hašovanie hesiel (jazyk C)
   Písomka („5-minútovka“, **10 bodov**)

5. **Bezpečnosť softvéru, kryptografické knižnice**
   pretečenie bufra (buffer overflow), kontrola s využitím GNU prekladača (jazyk C)
   demonštrácia vybraných kryptografických knižníc

6. **Bezpečnosť v architektúre TCP/IP I**
   prieskum (skenovanie) siete, príprava na útok

7. **Bezpečnosť v architektúre TCP/IP II**
   realizácia útokov (vzdialená extrakcia databázy hesiel, útok „pass the hash”)

8. **Bezpečnosť v architektúre TCP/IP III**
   vybrané útoky na TCP/IP spojenie

9. **Post-kvantová kryptografia**

   Overenie NTT algoritmu a jeho programová realizácia (ručný výpočet, jazyk C)

   Numerické zadanie 2 (10 bodov) + **Experimentálne zadanie** (15 bodov)

10. **Bezpečnosť v architektúre TCP/IP IV**

    útok a mazanie stôp, vytvorenie „zadných vrátok” pre vzdialený útok

    konzultácie a práca na zadaní

11. **Práca na zadaní, konzultácie**

12. **Práca na zadaní, konzultácie**

13. **Odovzdanie zadaní (do systému Moodle TUKE)**
    kontrola a obhajoba zadaní, udelenie zápočtov

Poznámky:

Cvičenia:	štvrtok	9:10-12:20	(2 skupiny)	PK13_L4
Prednášky:	pondelok	9:10-10:40		L9_A204

Hodnotenie skúšky:
Zápočet (**max. 40 bodov, 5** (5. týždeň) + **10** (5. týždeň) + **25** (10. týždeň)).
Písomka (max. 60 bodov).

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.: Aplikovaná kryptografia, od utajenia správ ku kybernetickej bezpečnosti. Elfa, Košice 2018.
Stallings, W.: Cryptography and network Security, Pearson 2018.
Stallings, W. - Brown, L.: Computer Security Principles and Practices, Pearson 2018.
Du, W.: Computer & Internet Security A Hands-on Approach, 2019.
Drutarovský, M.: Kryptografia pre vstavané procesorové systémy. Technická univerzita v Košiciach, 2017. (http://aplikovanakryptografia.fei.tuke.sk/).

Ďalšie užitočné zdroje:
Paar, Ch., Pelzl, J.: Understanding Cryptography. Springer 2010, (http://www.crypto-textbook.com/).