

Plán prednášok z predmetu BEZPEČNOSŤ INFORMAČNÝCH A KOMUNIKAČNÝCH SYSTÉMOV

(zimný semester 2025)

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. Autentizácia užívateľa v operačných systémoch Windows, Unix
5. Bezpečnosť softvéru, kryptografické knižnice
6. Bezpečnosť v architektúre TCP/IP I-II
7. Bezpečnosť v architektúre TCP/IP III
8. Post-quantová kryptografia
9. Ľahká (lightweight) kryptografia, bezpečnosť bezdrôtových sietí a IoT zariadení
10. Útoky s využitím postranných kanálov
11. Zápočtová písomka (30 bodov)
12. E-hlasovanie, Block-chain a kryptomeny
13. Forézna a penetračná analýza, Trendy vývoja v oblasti informačnej bezpečnosti

Plán cvičení z predmetu BEZPEČNOST' INFORMAČNÝCH A KOMUNIKAČNÝCH SYSTÉMOV (zimný semester 2025)

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)

Využitie **aritmetiky v GF**, princíp **zdieľania tajomstva** (Shamir's Secret Sharing), testovanie GCC nástrojov (cmake, make, ninja)

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 rc4, jazyk C)

3. Asymetrické šifrovanie a integrita správ

šifrovanie s využitím ECC, „ručný výpočet“ + jazyk C
Numerické zadanie 1

4. Bezpečnosť operačného systému MS Windows

extrakcia databázy hašovaných hesiel z OS Windows 7, prelomenie hesla
príklady nových hašovacích funkcií na hašovanie hesiel (jazyk C)

5. Bezpečnosť softvéru, kryptografické knižnice

pretečenie vyrovnávacej pamäte (buffer overflow), kontrola s využitím GCC prekladača
demonštrácia vybraných kryptografických knižníc

6. Bezpečnosť v architektúre TCP/IP I

prieskum (skenovanie) siete, príprava na útok
realizácia útokov (vzdialená extrakcia databázy hesiel, útok „pass the hash“)

7. Bezpečnosť v architektúre TCP/IP II

vybrané útoky na TCP/IP spojenie

8. Bezpečnosť v architektúre TCP/IP III

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

9. Post-quantová kryptografia

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

Numerické zadanie 2 + Experimentálne zadanie (spolu 10 bodov)

konzultácie a práca na zadaní

10. Práca na zadaní, konzultácie

11. Práca na zadaní, konzultácie

12. Odovzdanie zadaní (do systému Moodle TUKE)

13. Kontrola a obhajoba zadaní, udelenie zápočtov

Podmienky zápočtu:

- max. 3 **OSPRAVEDLNENÉ** neúčasti na seminároch,
- priebežne **vypracované domáce úlohy (aj neklasifikované)** a ich odovzdanie do systému Moodle **v definovaných termínoch** (nedodržanie priebežných termínov **je dôvodom na neudelenie zápočtu**),
- min. 21 bodov, max. 40 bodov.

Hodnotenie predmetu:**Zápočet:**

- **max. 40 bodov, 30** (zápočtová písomka **11. týždeň**) + **10** záverečné zadanie).

Skúška:

- písomná, **max. 60 bodov**,
- pre získanie celkového hodnotenia **A, B (81 a viac bodov)** je potrebné počas semestra vypracovať **priebežne zadávané bonusové úlohy a obhájiť ich riešenie.**

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 nevyhovet	< 51 bodov

Doporučená literatúra:

Levický, D.: Aplikovaná kryptografia, od utajenia správ ku kybernetickej bezpečnosti. Elfa, Košice 2018.

(<https://ebooks.lib.tuke.sk/login>)

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.

(<https://ebooks.lib.tuke.sk/login>).

Ďalšie užitočné zdroje:

Paar, Ch., Pelzl, J.: Understanding Cryptography, A Textbook for Students and Practitioners. Springer 2010, doi: 10.1007/978-3-642-04101-3. (<http://www.crypto-textbook.com/>).

Paar, Ch., Pelzl, J., Güneysu, T.: Understanding Cryptography, From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms. Second Edition, Springer 2024, doi: 10.1007/978-3-662-69007-9. (<http://www.crypto-textbook.com/>).