Plán prednášok z predmetu BEZPEČNOSŤ V POČÍTAČOVÝCH SYSTÉMOCH
(letný semester 2024)

1. **Počítačová bezpečnosť, úvod do problematiky, základné pojmy, princípy a súvislosti**
2. **Symetrické šifry**
3. **Kryptografia s verejným kľúčom I**
4. **Kryptografia s verejným kľúčom II**
5. **Hašovacie funkcie**
6. **Generátory náhodných čísel**
7. **Digitálne podpisy, certifikáty**
8. **Autentizácia používateľov a autorizácia dát**
9. **Ochrana emailovej komunikácie, Škodlivý softvér**
10. **Trendy vývoja v oblasti počítačovej bezpečnosti**

Plán cvičení z predmetu BEZPEČNOSŤ V POČÍTAČOVÝCH SYSTÉMOCH
(letný semester 2024)

1. **Plán cvičení, použité vývojové nástroje, vybrané klasické šifry**

   náplň cvičení**, podmienky udelenia zápočtu** (vypracovanie domácich úloh a zadaní, absolvovanie písomky)**. Domáce úlohy (DU) a zadania odovzdávané v TERMÍNE** cez systém Moodle TUKE. Odovzdanie riešenia DU a zadaní **v požadovaných termínoch je podmienkou udelenia zápočtu.** Nástroje využívané na cvičeniach: **Magma, gcc, CrypTool** (testovanie inštalácií):

   Cézarova šifra **(CrypTool),** Symetrická šifra **(XTEA),** Modulárne umocnenie **(Magma)**

2. **Modulárna aritmetika, konečné polia v kryptografii**
   základné operácie v GF(p) a GF(2^m), „ručný výpočet“, jazyk C
   modulárne umocnenie, princíp, „ručný výpočet“, Magma
   S-box v šifre AES, princíp využitia tabuliek (jazyk C)

3. **Symetrická šifra AES, režimy blokových šifier**
   štruktúra výpočtu v AES (jazyk C)
   módy ECB, CBC, OFB, ..., CTR

4. **Kryptografia s verejným kľúčom, teória čísel v kryptografii, algoritmus RSA**
   Euklidov algoritmus a rozšírený Euklidov algoritmus
   RSA, princíp a overenie (Magma)
   RSA, práca s veľkými číslami (jazyk C)

5. **Hašovacie funkcie z rodiny SHA**
   implementácia SHA2 v jazyku C
   využitie „hash chain“ na bezpečnú autentizáciu

6. **Generovanie náhodných čísel a ich využitie v kryptografii, Digitálne podpisovanie dát, certifikáty**
   generovanie náhodných čísel pod OS Windows a OS Linux (jazyk C)
   testovanie kvality (štatistické testy FIPS)
   generovanie certifikátov pomocou OpenSSL, overenie princípu (CrypTool)

7. **Zabezpečená komunikácia klient-server, bezpečná výmena kľúčov, protokol TLS a využite certifikátov**
   zabezpečená komunikácia klient-server, prenos dát (jazyk C)
   autentizácia servera a autentizácia klienta s využitím OpenSSL

8. **Protokol TLS a využite certifikátov**
   príkazy OpenSSL na vizualizáciu obsahu certifikátov
   zreťazené certifikáty a ich overenie
   zadanie semestrálnych zadaní + informácie o nastavení sietového rozhrania vo Virtual Boxe

9. **Semestrálna písomka**

10. **Šifrovanie elektronickej pošty, program PGP, Šifrovanie vzdialeného úložiska**
    súkromný a verejný kľúč užívateľa, generovanie kľúčov
    uloženie kľúčov vo verejných databázach
    prenos dát s využitím hybridného šifrovania, digitálne podpísanie dát a verifikácia podpisu
    program rclone, bezpečné uloženie dát na vzdialenom úložisku
    príklad využitia prúdovej šifry chacha20 (šifrovanie) a poly1305 (autentizačný kód správy)
    Udelenie zápočtov

Poznámky:
Semináre: streda 15:10-16:40 **dištančne** + **ZP4** (písomka týždeň 9))
Prednášky: utorok 10:50-12:20 **P25 prezenčne**

Podmienky zápočtu:
- priebežne **vypracované domáce** úlohy (**aj neklasifikované**) a ich odovzdanie do systému Moodle **v definovaných termínoch** (nedodržanie priebežných termínov **je dôvodom na neudelenie zápočtu**),
- úspešné abdolvovanie semestrálnej písomky.

Hodnotenie predmetu:
Zápočet (**max. 40 bodov, 30** (semestrálna písomka 9. týždeň) + **10** záverečné zadanie).
Skúška (**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.
Drutarovský, M.: Kryptografia pre vstavané procesorové systémy. Technická univerzita v Košiciach, 2017. (http://aplikovanakryptografia.fei.tuke.sk/), dostupná online cez portál TUKE knižnice http://ebooks.lib.tuke.sk/login

Ďalšie užitočné zdroje:
Paar, Ch., Pelzl, J.: Understanding Cryptography. Springer 2010, (http://www.crypto-textbook.com/)
Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson 2014 (6e), 2017 (7e).
Stallings, W., Brown, L.: Computer Security: Principles and Practice