Plán prednášok z predmetu BEZPEČNOSŤ V POČÍTAČOVÝCH SYSTÉMOCH (*letný semester 2021*)

1. **Počítačova 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 2021*)

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

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

   nástroje: 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
   písomka (10-minútovka, **10 bodov**)

6. **Digitálne podpisovanie dát, certifikáty**
   overenie princípu (CrypTool)
   generovanie certifikátov pomocou OpenSSL
   transformácia formátov

7. **Zabezpečená komunikácia klient-server, bezpečná výmena kľúčov, protokol TLS a využite certifikátov**
   zabezpečený prenos dát (jazyk C)
   autentizácia servera
   autentizácia klienta
   rozdelenie zadaní

8. **Šifrovanie elektronickej pošty, program PGP**
   súkromný a verejný kľúč užívateľa, generovanie kľúčov
   uloženie kľúčov vo verejných databázach
   prenos dát s využitím hybridného šifrovania
   digitálne podpísanie dát a verifikácia podpisu

9. **Písomná previerka (20 bodov)**

   odovzdanie zadaní (do systému Moodle TUKE)

10. **Šifrovanie vzdialeného úložiska**
    program **rclone**, bezpečné uloženie dát na vzdialenom úložisku
    príklad využitia prúdovej šifry **chacha20** (šifrovanie) a **poly1305** (autentizačný kód správy)

    Udelenie zápočtov

Poznámky:

Semináre:	utorok	9:10-10:40	L9_B221
	utorok (**písomky**)	16:50-18:20 (**týždeň 5,9**)	P25 (**len ak bude prezenčná výučba!**)
Prednášky:	utorok	10:50-12:20	L9_B221

Hodnotenie skúšky:
Zápočet (**max. 40 bodov, 10** (písomka 5. týždeň) + **20** (písomka 9. týždeň) + **10** (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. Pearson, 2012 (2e), 2018 (4e).