

# BSc Matematika Alapszak, 2020.

Matematikai Intézet,

Természettudományi Kar,

Eötvös Loránd Tudományegyetem.

## Adatvédelem

- **Óraszám (ea+gy):** 2 + 0
- **Specializáció:** elemző
- **Kredit (ea+gy):** 3 + 0
- **Számonkérés:** kollokvium
- **Tárgykód (ea, gy):** adatvd1e0\_m17ea
- **Ajánlott félév:** 4
- **Státusz:** köt. vál.

## Tantárgyfelelős

- Szabó István, Valószínűségelméleti és Statisztika Tanszék, Matematikai Intézet.

## Előfeltételek

### ***Az előadás előfeltételei:***

- **Erős:** Algebra2E (algebr2\*0\_m17ea)
- **Erős:** Számelmélet1E (szamel1\*0\_m17ea)
- **Erős:** Valószínűségszámítás1E-m (valsz\_1m0\_m17ea) *vagy* Valószínűségszámítás1E-a (valsz\_1a0\_m17ea)

## Megjegyzések

- **Követelmény:** Szabadon választhatóan benyújtható az órák anyagához kapcsolódó házi feladatok megoldása (mely igazolja az adott óra

anyagának megértését). A kollokvium kellő számú házi feladat benyújtására megajánlott jeggyel is teljesíthető.

### **A tematikát kidolgozta:**

- Szabó István, Valószínűségelméleti és Statisztika Tanszék, Matematikai Intézet.

## **Szükséges előismeretek**

- **Algebrai, számelméleti ismeretek:** Mátrixok, műveletek, rang, lineáris leképezés és mátrixa, karakterisztikus polinom, csoport, elemrendje, elemi kombinatorika, kongruenciák, Euler-Fermat-tétel, véges testek.
- **Valószínűségszámításból:** Valószínűségi mező, véges valószínűségi mezők, feltételes valószínűség, függetlenség, nevezetes diszkrét eloszlások.

## **A tantárgy célkitűzése**

A tárgy célja az adatvédelem alapvető fogalmainak és legfontosabb eredményeinek megismertetése.

## **Irodalom**

- **Nemetz T – Vajda I:** *Algoritmikus adatvédelem*. Akadémia, 1991;
- **Buttyán L – Vajda I:** *Kriptográfia és alkalmazásai*. Typotex, 2004;
- **B. Schneier:** *Applied Cryptography*. Wiley, 1996.
- **A. Menezes–P.Ororschot–S.Vanstone:** *Handbook of Applied Cryptography*. CRC Press, 1996;
- A kapcsolódó számelméleti, algebrai, információelméleti, bonyolultságelméleti tankönyvek.

## **Tematika**

### **Az informatikai adatvédelem alapjai:**

- jogi környezet, veszélyek csoportosítása

- **programozott fenyegetések:** terjedő fenyegetések (vírusok, wormok, nyulak, Hoax-ok); nem terjedő programozott fenyegetések (back door, trójai falvak, ...); egyéb, interaktív fenyegetések (SPAM, DOS, Sniffing, Spoofing, Phishing, Social Attack,...)
- programhibákon alapuló fenyegetések (Buffer Owerflow, SQL Injection, ...)
- helytelen használatból adódó fenyegetések (titkosítás elleni támadások, jelszótörő algoritmusok,...)
- különböző IT rendszerek elleni fenyegetések osztályozásai (Landwehr taxonómia, ...)
- Data Hiding módszerek osztályozásai (Covert Chanel, Anonymous Channel, Tamper Protection, Copyright Protection, Szteganográfiai rendszerek típusai, a szteganográfia és kriptográfia kapcsolata).
- **Kriptográfiai alapfogalmak**, kriptográfia-történeti tanulságok.

### **Adatvédelmi módszerek:**

- az algoritmikus biztonság garanciális /bizonyítási/ módszerei
- Információelméleti biztonsági modell (Shannon modell, egyértelműségi pont, OTP)
- Stream ciphers: Véletlenszám-generátorok követelményei, statisztikai ellenőrzési módszerei, gyakorlati folyam-titkosítók (pl. GSM, Bluetooth, WORD...titkosítás)
- Block ciphers (LUCIFER, DES, PES, IDEA, AES)
- **Aszimmetrikus (nyilvános) kulcsú (PKI) rendszerek:**
- PKI kódolók (RSA, ECC), faktorizációs módszerek és kriptográfiai hatásuk
- Kulcsegyeztető algoritmusok (a diszkrét logaritmus problémán alapuló Merkle-Hellmann módszer, ...)
- Elektronikus aláíró algoritmusok (RSA, ECDSA),
- elektronikus aláírási rendszerek (technológia, jogi-és szervezeti intézményi rendszer), egyéb protokollok (blind signature, secret sharing, ...).

- **Adatvédelmi rendszerek felépítése:** primitívek, sémák, protokollok, alkalmazások (gyenge pontok és követelmények)
- **Nemzetközi és hazai kriptográfiai szabványok:** (ISO/IEC, NIST, ANSI, FIPS, RFC; PKCS)
- **IT biztonsági módszertanok:** MSZ ISO/IEC 15408: /Common Criteria; CEM/; FIPS PUB 140-2, MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítása Séma), ISO/IEC 27001