# Adatbiztonság, INBC411

**Oktató: Huszti Andrea**
**Kurzuskód: INCV581, INBC411**
**Félév:**7
**Típus:**Előadás/Labor
**Óraszám/hét:**4+2
**Kredit:**6
**Státusz:** Differenciált szakmai tárgy
**Előfeltételek:**INCV131E, INCK531E, NBK451E
**Vizsgáztatási módszer:**Írásbeli
A gyakorlati aláírás megszerzésének a feltétele: sikeres zárthelyi dolgozat és a program beadása,sikeres megvédése.
**Oktatási módszer:** tantermi előadás és labor gyakorlat
**Kompetencia:** A kurzus sikeres teljesítése esetén ahallgatók megismerkednek az alapvető kriptográfiai rendszerekkel, valamint kriptográfiai protokollokkal.
**Fogadóóra:**Kedd 15-16,Szerda 13-14**Helye**: I113

**Etikai elvárások:**
A hallgatókkal kapcsolatos etikai normákra A DEBRECENI EGYETEM ETIKAI KÓDEXE az irányadó lsd.:http://www.unideb.hu/portal/hu/node/47:A Debreceni Egyetem Etikai Kódexe (Vizsgakódex).
**Az etikai normákat megsértők:**

a. Automatikusan elégtelent kapnak a tárgyból.
**b.** A hallgató neve az IK oktatói között nyilvánosságra kerül.

**Hetekre bontott óraterv:**

| Hét | Előadás | Gyakorlat |
|---|---|---|
| 1. hét | Algebrai struktúrák, Elemi számelméleti ismeretek I | Számelméleti alapismeretek, Kibővített euklideszi algoritmus |
| 2. hét | Elemi számelméleti ismeretek II, Alapfogalmak | Gyors hatványozás, Algoritmusok implementálása |
| 3. hét | Titkosítási rendszerek, támadások, klasszikus titkosító módszerek | Prímtesztek |
| 4. hét | Szimmetrikus kulcsú titkosítások – DES, AES | RSA algoritmus, Kínai maradéktétel alkalmazása |
| 5. hét | Blokktitkosítási módok, folyamtitkosítók | Algoritmusok implementálása |
| 6. hét | Nyilvános kulcsú titkosítások - RSA | Diszkrét logaritmuson alapuló rendszerek – Diffie-Hellman kulcscsere, ElGamal |
| 7. hét | Diszkrét logaritmuson alapuló rendszerek – Diffie-Hellman kulcscsere, ElGamal titkosítás, Kriptográfiai hash függvények, MAC | Digitális aláírások |

| | | |
|---|---|---|
| 8. hét | *Szakmai napok* | *Szakmai napok* |
| 9. hét | Digitális aláírások, RSA, DSA aláírás | Teszttanúsítvány igénylése és használata, GNUPG |
| 10. hét | *Zárthelyi dolgozat*,Felhasználó hitelesítése | Programok bemutatása |
| 11. hét | Kulcscsere protokollok, Internet biztonsági protokollok (SSL\TLS, PGP) | Programok bemutatása |
| 12. hét | Elektronikus fizetési rendszerek (SSL-alapú, SET) | *Javító dolgozat* |

**Irodalom**:


- William Stallings, Cryptography and Network SecurityPrinciples and Practice (6. edition), 2014
- Buttyán Levente és Vajda István, Kriptográfia és alkalmazásai, Tipotex, 2004. ISBN: 963 9326 13 8
- Ködmön József, Kriptográfia, ComputerBooks, 2000.
- Folláth János, Huszti Andrea, Pethő Attila, Informatikai biztonság és kriptográfia, jegyzet, 2011


**Szoftverek**:

- GNUPG