Vállalati informatika biztonság, INMGM9922E

Oktató: Huszti Andrea
Kurzuskód: INMGM9922E
Félév:2
Típus: Előadás
Óraszám/hét: 2
Kredit: 3
Státusz: Speciális ismeretek, választható tárgy
Előfeltételek:INCV131E, INCK531E, NBK451E
Vizsgáztatási módszer:Írásbeli
Oktatási módszer: tantermi előadás
Kompetencia: Vállalati rendszerek által feldolgozott, tárolt, elküldött adatok bizalmasságának, sértetlenségének védelmét biztosító megoldások ismertetése. Elektronikus fizetési rendszerek.
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
1. hét	Alapfogalmak, támadások, titkosítási folyamat, szimmetrikus, aszimmetrikus titkosítások
2. hét	Szimmetrikus kulcsú titkosítások – DES, AES
3. hét	Nyilvános kulcsú titkosítások - RSA
4. hét	Diszkrét logaritmuson alapuló rendszerek, Diffie-Hellman kulcscsere, ElGamal titkosítás
5. hét	Elliptikus görbe fogalma, pontok összeadása
6. hét	Az elliptikus görbe csoport, ECDLP.
7. hét	Elliptikus görbe titkosítás.
8. hét	*Szakmai napok*
9. hét	Digitális aláírások, RSA, DSA, ECDSA aláírás
10. hét	Felhasználó hitelesítése

11. hét	Hozzáférés szabályozása
12. hét	Anonimitás eszközei (vak aláírás, mix hálózatok)
13 hét	A Bitcoin elektronikus pénzérme
14 hét	A SET elektronikus tranzakciós rendszer

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
- Andreas Enge: Elliptic curves and their applications to Cryptography, An introduction, 2001, Kluwer Academic Publishers