

TANTÁRGYI KÖVETELMÉNYEK

Tantárgy kódja és neve: „PMB2516L” Informatikai Biztonság II.

Oktató neve: Halász Attila

Meghirdetés féléve: 2017/18 II. félév

Kredit: 2

Heti óraszám: 2

Értékelés módja: aláírás, kollokvium

Óra időpontja és helye: „NEPTUN SZERINT”

Oktató elérhetősége: halasz.attila@nye.hu, 42 599 400 /2828

Az előadások látogatása nem kötelező.

Az aláírás megszerzésének feltételei:

- Feladat beadása/bemutatása megadott határidőre.
- Zárthelyi dolgozat 60 %-os teljesítése.

A zárthelyi dolgozatokat a megadott időpontban lehet megírni ill. a következő órán lehet javítani. Esetleges pótlására csak a hiányzást követő első órán az orvosi igazolás bemutatása után van lehetőség. Aki a zárthelyin puskázik 0 pontot kap a dolgozatára.

Írásbeli vizsga a vizsgaidőszakra meghirdetett időpontokban.

Értékelés:

1. 0–59 %
2. 60-69%
3. 70-79%
4. 80-89%
5. 90-100%

Az írásbeli vizsga (zárthelyi dolgozat) kiváltható a kiadott gyakorlati feladatok bemutatásával.

A félév tervezett témakörei: a kiosztott tanmenet szerint.

A tantárgy célkitűzései: A tárgy célja a hallgatók megértésük a titkosítási technológiákat és megismerkedjenek azok gyakorlati alkalmazási lehetőségeivel.

Témakörök

Titkosítások

- Alapfogalmak
- A legfontosabb titkosítási alapelvek
- A titkosítási algoritmusok családfája
- A szimmetrikus (egykulcsos) titkosítási algoritmusok működése:DES, 3DES, AES.
- Az aszimmetrikus (két kulcsos, nyílt kulcsú) algoritmusok működése, DH, RSA
- A Diffie-Hellman kulcselosztási protokoll megértése
- Az RSA-algoritmus
- Digitális aláírás és nyílt kulcsú titkosítás RSA-val
- Titkosítások gyakorlati alkalmazásai : VPN,SSL/Tls, SSH, IpSec megoldások működésének áttekintése.
- Blokklánc technológiák.

A számítógépes hálózatok biztonsági kérdései II.

- Mobil biztonság
- E-mail és web biztonság.
- Vírusok és egyéb számítógépes visszaélések, fenyegetések és támadások.
- Hálózati támadások és védelem eszközei, (IDS/IPS)
- Tűzfalak típusai, tulajdonságaik, (Iptables)
- Az infrastruktúra felépítése hálózati a határvédelem tervezése

Kötelező ill. ajánlott irodalom:

Oktatói jegyzet: <http://moodle.nyf.hu> # IT Hálózati Biztonság

1. Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai: 2004, Budapest, ISBN: 978-0-7645-4188-9
2. SZENES K. (szerk.): Az informatikai biztonság kézikönyve, Dashöfer, Budapest, 2010. ISBN:9639313122
3. GYÖRFI L. - GYÖRI S. - VAJDA I.: Információ- és kódelmélet. Typotex Kiadó, Budapest, 2010. ISBN: 9789632791159
4. J. DYKSTRA: Essential Cybersecurity Science. O'Reilly Media, 2015. ISBN: 9781491920947
5. Cryptography for Dummies, ISBN: 978-0-7645-4188-9