Kriptográfia

Kurzuskód: INMPM0103E
Félév: 1
Típus: Előadás+labor
Óraszám/hét: 2+0+2
Kredit: 6
Előfeltételek: Diszkrét matematikai alapfogalmak ismerete. Alapvető programozási ismeretek. Alapvető hálózati ismeretek
Vizsgáztatási módszer: szóbeli vizsga és gyakorlati aláírás.

Hetekre bontott óraterv:

Hét	Óraterv
1. hét	A bizalmas üzenettovábbítás matematikai modellje, a kriptográfia szerepe a digitális adatok védelmében.
2. hét	Kriptográfiai alapfogalmak: üzenet, kódoló- és dekódoló függvény, kulcs. Álvéletlenszám generálás, folyamtitkosítás.
3. hét	A modern szimmetrikus titkosító algoritmusok tervezésének alapjai; Feinstel hálózatok és DES.
4. hét	A modern szimmetrikus titkosító algoritmusok tervezésének alapjai; a helyettesítő és permutáló blokkok módszere, AES.
5. hét	A blokktitkosítás alkalmazásának a módjai: ECB, CBC, CFB. Padding.
6. hét	Az aszimmetrikus titkosítás szükségessége és annak alapjai. Egyirányú és egyirányú csapóajtó, valamint hash függvények.
7. hét	Az RSA számelméleti alapjai, algoritmusa.
8. hét	Az RSA paraméterek megválasztása. Prímtesztek és faktorizáció.
9. hét	A diszkrét logaritmus problémán alapuló nyilvános kulcsú kriptográfiai rendszerek: Diffie-Hellmann kulcscsere és ELGamal titkosítás.
10. hét	A diszkrét elliptikus logaritmuson alapuló kriptográfiai rendszerek.
11. hét	Digitális aláírás szükségessége, és alkalmazásai.
12. hét	Digitális aláírás sémák. RSA, ELGamal és DSA digitális aláírás algoritmusok. Vak aláírási sémák, alkalmazások.
13. hét	Nyilvános kulcs infrastruktúra. Kvantumszámítógép-rezisztens kriptográfiai algoritmusok.

Vizsgatételek:

1. A bizalmas üzenettovábbítás matematikai modellje, a kriptográfia szerepe a digitális adatok védelmében.
2. Kriptográfiai alapfogalmak: üzenet, kódoló- és dekódoló függvény, kulcs. Álvéletlenszám generálás.
3. A modern szimmetrikus titkosító algoritmusok tervezésének alapjai; Feinstel hálózatok és DES.

4. A modern szimmetrikus titkosító algoritmusok tervezésének alapjai; a helyettesítő és permutáló blokkok módszere, AES.
5. A blokktitkosítás alkalmazásának a módjai: ECB, CBC, CFB. Padding.
6. Az aszimmetrikus titkosítás szükségessége és annak alapjai. Egyirányú és egyirányú csapóajtó, valamint hash függvények.
7. Az RSA számelméleti alapjai, algoritmusa.
8. Az RSA paraméterek megválasztása. Prímtesztek és faktorizáció.
9. A diszkrét logaritmus problémán alapuló nyilvános kulcsú kriptográfiai rendszerek: Diffie-Hellmann kulcscsere és ELGamal titkosítás.
10. A diszrét elliptikus logaritmuson alapuló kriptográfiai rendszerek.
11. Digitális aláírás szükségessége, és alkalmazásai.
12. Digitális aláírás sémák. RSA, ELGamal és DSA digitális aláírás algoritmusok. Vak aláírási sémák, alkalmazások.
13. Nyilvános kulcs infrastruktúra.

Ajánlott irodalom:

- Gyöfi László, Győri Sándor, Vajda István, Információ és kódelmélet, negyedik kiadás, Typotex, 2010.
- William Stallings, Cryptography and Network Security Principles and Practice (6. edition), 2014
- Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer 2014, ISBN: 978-1-4939-1711-2
- Folláth János, Huszti Andrea és Pethő Attila, Informatikai biztonság és kriptográfia, jegyzet, 2010.