Modeli i Planit mësimor të lëndës

Syllabusi

Universiteti i Prishtinës

Departmenti/Fakulteti/Njësia akademike: Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike

Titulli i kursit (lëndës mësimore) : Siguria e të dhënave

Niveli dhe lloji i kursit: Bachelor /obligative

Viti i studimeve dhe semestri: II, semestri 4

Kodi ose shifra e lëndës:

Vlera në kredi ECTS : 5

Koha/lokacioni (termini i mbajtjes së ligjëratës dhe salla): E marte 09.00 – 12:00, salla 621

Mësimdhënësi i kursit:

Emri: Prof. Dr. techn Blerim Rexha, email: blerim.rexha@uni-pr.edu
MSc. Mërgim Hoti, email: mergim.hoti@uni-pr.edu
MSc. Arbena Musa, email: arbena.musa@uni-pr.edu

Konsultimet: E hënë dhe e marte 10.00 -11.00, zyra 704.

Qëllimet e kursit(modulit):
Njohja me algoritmet për enkriptim, masat për rritjen e sigurisë së të dhënave, certifikata digjitale, smart kartela dhe aplikimi i tyre në praktikë

Rezultatet e pritura të nxënies
Pas përfundimit të këtij kursi (lënde) studenti duhet:

1. të zotërojë njohuri themelore mbi kriptografinë,
2. të ketë njohuri themelore mbi enkriptimin simetrik dhe josemtrik,
3. të jetë në gjendje t'i aplikoj algoritmet për enkriptim
4. të ketë njohuri themelore mbi smart kartelat dhe aplikimin e tyre në praktikë,
5. të jetë në gjendje të bëjë menaxhimin e çelësave publik,
6. t'i kuptoje protokollet tjera që bazohen në kriptografi

Metodologjia e mësimdhënies: ligjëratë, seminar, dhe ushtrime numerike

Literatura bazë :

Autoret	*Titulli*
Niels Ferguson Bruce Schneier Tadayoshi Kohno	Cryptography Engineering: Design Principles and Practical Applications, ISBN: 978-0-470-47424-2, 2010
Christof Paar Jan Pelzl	Understanding Cryptography, ISBN: 978-3642041006 2010 2ed. 2024
C# Data Security	Matthew MacDonald & Erik Johansson, ISBN=1-86100-801-5, 2003

Plani i detajizuar i mësimit për një semestër:

Java e parë: Bazat e kriptografisë: Hyrje në kriptografi, Terminologjia, Steganografia, Algoritmet

Java e dytë: DES-i (Enkriptimi simetrik): 12.1 Hyrje, 12.2 Pershkrimi i DES-it, 12.3 Siguria e DES-it, 12.6 Variantet e DES –it.

Java e tretë: RSA (Enkriptimi asimetrik, algoritmet me çelesa publik): 19.3 RSA

Java e katërt: Hash funksionet 2.3 Funsionet e njëkahëshe, 18 Hash funksionet njëkahëshe, 18.5 MD5, 18.7 SHA,

Java e pestë: Nënshkrimet digjitale: 2.6 Nënshkrimet digjitale, 2.7 Nënshkrimet digjitale dhe enkriptimi.

Java e gjashtë: Menaxhimi i çelësave sekret, privat dhe publik: 8.1 Gjenerimi i çelësave, 8.3 Shkëmbimi i çelësave,

Java e shtatë: X.509 certifikatat: Certifikatat digjitale, X.509 certifikatat, ISO Standardi

Java e tetë: Public Key Infrastructure (PKI) 8.4 Verifikimi i çelësave, 8.6 Freskimi i çelësave, 8.7 Ruajtja e çelësave, 8.8 Çelësat reservë, 8.12 Menaxhimi i çelësave publik.

Java e nëntë: Standardet për enkriptim (PKCS#1 – PKCS#15): 24.14 Përshkrimi dhe funksioni i secilit standard.

Java e dhjetë: Smart kartelat I: Hyrje, Llojet e smart kartelave, Vetitë fizike dhe elektrike, Sistemi operativ për smart kartela.

Java e dymbëdhjetë: Smart kartelat III:, PC/SC Arkitektura, Smart kartelat pa kontakt, Struktura e memories, Standardet, Aplikacionet me smart kartela pa kontakt etj.

Java trembëdhjetë: Perdorimi i funksioneve kriptografike : CAPICOM dhe CryotoAPI

Java e katërmbëdhjetë: Aplikimi i teknologjive për enkryptim në raste konkrete: Shkëmbimi i email-ave në form të enkriptuar,

Java e pesëmbëdhjetë: Aplikimi i teknologjive për enkryptim në raste konkrete Pagesat elektronike përmes Internetit, Paratë elektronike, Pagesat me anë të smart kartelatave. e-Commerece, e-Government.

Vërejtje: terminin e vlerësimeve intermediere e cakton mësimdhënësi sipas planifikimit të lëndës që e ligjëron.

Metodat e vlerësimit:

1. Vijimi i ligjëratave dhe ushtrimeve: 10 pikë = 5 nga ligjërata + 5 nga suhtrimet.
2. Pjesës praktike – detyrat e shtëpisë: 40 pikë.
3. Pjesës me shkrim – testi: 50 pikë

Totali (max): 100 pikë

Pjesa me shkrim – testi final: 50 pikë
Testi ka ~20 pyetje ne te cilat studenti duhet te përgjigjet:

- Përgjigja e saktë: 3 pikë,
- Përgjigja e pjesshme: 1 ose 2 pikë
- Pa përgjigje ose përgjigje e gabuar: 0 pikë

Për të kaluar provimin studenti duhet te grumbulloje se paku:

- Nga vijueshmëria min. 50%, pra 5 pikë
- Nga pjesa praktike min. 50%, pra 20 pikë
- Minimum nga testi min. 50%%, pra 25 pikë, dhe
- Shuma nga pika 1, 2 dhe 3 duhet te jetë më e madhe se 50 pikë

Politikat akademike dhe rregullat e mirësjelljes: (mësimdhënësi cakton kriteret për vijimin e rregullt në ligjërata dhe ushtrime dhe rregullat e mirësjelljes si:mbajtja e qetësisë në mësim, shkyqja e telefonave celular, hyrja në sallë me kohë,etj.)

Litaratura shtesë dhe bibliografia:
Nuk ka.