Kolegji Riinvest

Zyra për planifikim akademik

Siguria e të Dhënave
KOMP503

Data e aprovimit:	Data
Verzioni:	Verzion
ECTS:	6
Bartësi i lëndës:	Driart Elshani
Email:	driart.elshani@riinvest.net
Telefoni:	038 224 322

Qëllimet

Lënda ka për qëllim kryesor njohjen dhe zbatimin e teknikave për sigurimin e të dhënave.

Rezultatet e pritura të lëndës

- Studentët do të jenë në gjendje të japin zgjidhje praktike të problemeve lidhur me lëminë e sigurisë së të dhënave. Ata do të mund të analizojnë karakteristikat kryesore të problemit dhe të ofrojnë zgjidhje të tij.
- Pas përfundimit të këtij kursi studentët do të jenë në gjendje të kuptojnë dhe shtjellojnë zgjidhjet e problemeve të sigurisë së të dhënave të ofruara nga kolegët, si dhe të definojnë dhe implementojnë zgjidhje të tjera të mundshme. Gjithashtu do të jenë në gjendje të shpjegojnë dobitë dhe kufizimet fundamentale të algoritmeve që përdoren si në enkriptimet simetrike ashtu edhe asimetrike.
- Implementimi i metodave të shifrimit, deshifrimit dhe protokoleve të sigurisë do të jenë sfida të njohura dhe të realizueshme me përfundimin e suksesshëm të këtij kursi.
- Përveç shkathtësive kompjuterike, në ketë kurs studenti do të zhvillojë edhe shkathtësitë për zgjedhjen e problemeve kriptografike.
- Do të avancohen shkathtësitë e komunikimit dhe prezantimit. Studentët do të jenë pjesëmarrës interaktiv gjatë ligjëratave. Gjithashtu, do të shkruajnë një raport sikurse edhe do të bëjnë një prezentim mbi temën e detyrës që kanë zgjedhur të punojnë.

Programi

Java	Tema	Aktivitetet
1	Hyrje	Rëndësia e sigurisë së të dhënave në një shoqëri të ndikuar nga teknologjia informative dhe zhvillimi i saj eksponencial
2	Metodat e shifrimit klasik	Shifrimi me rivendosje; shifrimi me ripozicionim

3	Enkriptimi simterik	Block ciphers and Stream ciphers (Data Encryption Standard DES, 3DES)
4	Enkriptimi asimetrik	RSA (Rivest, Shamir & Adleman)
5	Hash funksionet	MAC, MD5, SHA, Funksionet njëkahore
6	Nënshkrimet digjitale	Autorësia, autenticiteti, menaxhimi i çelësave, çertifikatat digjitale
7	Menaxhimi i çelësave publik	Shpërndarja e çelësave publikë (me enkriptim simetrik dhe asimetrik), Kerberos, X.509 çertifikatat
8	DoS dhe DDoS	DoS sulmet, DDoS arkitektura, konstruktimi i rrejtit sulmues, masat mbrojtëse
9	Autentikimi	Sistemi i autentikimit; fjalëkalimet; llojet e sulmit - sulmi i fjalorit
10	Biometrika	Teknikat e pëdorura për siguri: key strokes dynamics, iris, shenjat e gishtërinjve, zëri, fytyrat.
11	Access Control	Sistemi i sigurisë; Modelet e access control, Modelet e sigurisë (Bell LaPadulla, chinese wall)
12	Internet Security	Internet Security Protocol, Pretty Good Privacy, Transport Layer Security
13	Malicious Logic	Trojanët, virusët, krimbat dhe tipet e tjera
14	Siguria e e-mailit	Siguria e e-mailit
15	Perseritja e materialit pregaditje për test final.	Perseritja e materialit pregaditje për test final.

Informata shtesë 1:

Lënda e ka komponentin teorike dhe praktike te cilat realizohen nëpërmjet te ligjëratave, diskutimeve ushtrimeve dhe detyrave projektuese me qasje praktike nga jeta e përditshme. Raporti teori praktik mund te vlerësohet 50/50.

Informata shtesë 2:

MS SPSS, MS Word, MS Excel, MS Power Point, MS Project, MS Access, MS Visio, MS Visual Studio, MS SQL Server, Eclipse, NetBeans, Enterprise Architect, HTML, CSS, AJAX, XML, JavaScript, C#, Java, Java Android

Vlerësimi:

Nr.	Lloji Vleresimit	Perqindja	Pershkrimi
1	Test	15	Test teorik që përfshinë metodat e enkriptimit
2	Test	15	Test teorik që përfshinë access control dhe malicious logic
3	Detyra	20	Aplikacion i zhvilluar për njërën nga temat e trajtuara dhe/ose raporti i shkruar mbi të njejtën temë
4	Provimi Final	50	Provim i përbërë nga tri pjesë të cilat mbulojnë materialin e lëndës. Pohime logjike, pyetje me përgjigje të shumëfishta sikurse edhe detyra/probleme në pjesën e tretë të ndara në dy pjesë. Vetëm njëra nga këto dy duhet të zgjidhet.

Kushtet e përsëritjes:

Nëse në tri afatet pas ligjëratave (janar, prill, shtator ose qershor, gusht shtator) studenti nuk arrin ti realizojë pikët e mjaftueshme nga kapitulli i detyrave në syllabus, studenti duhet ta përsëris lëndën.

Burimet:

1. "Network Security Essentials – Application and Stntndards" by William Stallings, ISBN-10: 0132280321

- 1. "Network Security Essentials – Application and Stathdards" by William Stallings, ISBN-10: 0132380331, 2. “Handbook of Applied Cryptography” by Alfred J.Menzes, Paul C. van Oorschot and Scott A. Vanstone, ISBN: 0-8493-8523-7, http://www.cacr.math.uwaterloo.ca/hac, 3. "Internet Security Cryptographic Principles Algorithms and Protocols" by Man Young Rhee, ISBN 0-470-85285-2

Ndërtimi i ECTS-ve

Aktiviteti	Nr i oreve per Aktivitetin	
Ligjerata:	30	
Ushtrime:	30	
L+U:	60	
Seminar/praktike.:	20	
Studim i vazhdushem:	44	
Pregaditja e Provimit:	20	
Pjesemarrja ne teste:	4	
Pjesemarrja ne provimin final:	2	
Me profesorin dhe asistentin:	10	
Total Ore:	160	
ECTS:	6	