Kolegji Riinvest

Zyra për planifikim akademik

Siguria e të Dhënave
KOMP503

Bartësi i lëndës:	Fatbardh Veseli
Email:	fatbardh.veseli@riinvest.net
Telefoni:	
Mësimdhënësit e Lëndës:	Malesore Gashi

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 nga historia deri sot dhe pjesa organizative e lendes
2	Hyrje ne Kriptografi	Sistemet kriptografike, Kriptografia simetrike, Shifrimi me zevendesim, i Cezarit, Aritmetika Modulare
3	DES / AES	Pershkrimi i algoritmit simetrik DES
	AES dhe modet e	Pershkrimi i algoritmit AES; ECB Mode, CBC Mode, CF Mode, OF

4	AES dhe modet e enkriptimit ne bllok	Pershkrimi Algoritmit AES, ECB Mode, CBC Mode, CF Mode, OF Mode, C Mode
5	Kriptografia Asimetrike	Kriptografia me celes publik, nenshkrimet digjitale
6	Hash funksionet, MAC	Hash Funksionet, MAC
7	Malware and Computer System Security	Viruset, Worms, Ransomware, etc.
8	Cyber Defense Operations	Guest Lecture: A real life experience from a blue teamer
9	Autentikimi	Sistemet e autentikimit, biometria, rreziet, mbrojtjet
10	Privacy and Data Protection	Regulation, Technologies, Frameworks
11	Mobile Security	Guest lecture: Architecture, Technologies and Market for Mobile
12	Access Control	Sistemi i sigurisë; Modelet e access control, Modelet e sigurisë (Bell LaPadulla, chinese wall)

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	Përqindja	Oblig.	Përshkrimi
1	Ese	30		Ese mbi nje teme nga fusha e sigurise kibernetike, qe deshmon edhe shkathtesite e fituara ne kete fushe si dhe shkrimin akademik
2	Provimi Final	40	Po	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.
3	Pjesëmarrja	10		Vijueshmeria ne ligjerata
4	Detyra	20	Po	Detyra nga ushtrimet

Kushtet e përsëritjes:

Shikoni rregulloren e Kolegjit

Burimet:

- 1. “Network Security Essentials – Application and Statndards” 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	