SYLLABUSI

Të dhëna bazike rreth lëndës	
Universiteti:	**Universiteti "Ukshin Hoti" - Prizren**
Njësia akademike:	**Fakulteti i Shkencave Kompjuterike**
Programi i studimit:	**Shkenca Kompjuterike dhe Teknologji Komunikimi**
Lënda:	**Tema të zgjedhura nga siguria kompjuterike**
Niveli i studimeve:	**Master**
Statusi i lëndës:	**Obligative**
Viti i studimeve:	**1**
Numri i orëve në javë:	**2+2**
Vlera në kredi - ECTS:	**6**
Koha / lokacioni:	**Do të publikohen në web site të universitetit!**
Mësimdhënësit:	**Prof. Asoc. Dr. Naim Baftiu**
Detajet kontaktuese:	**naim.baftiu@uni-prizren.com ; +383 44 234 018**
Përshkrimi i lëndës:	Kursi ofron njohuri mbi principet kryesore te sigurisë ne kompjuterë. Kursi do të mbulojë sistemet e sigurisë se te dhënave duke i shndërruar ato ne te dhëna për kriptim dhe dekriptim.
Qëllimet e lëndës:	Qëllimet e lëndës janë që ti mundësoj studentit të jetë në gjendje të identifikoj sigurinë e kompjuterëve si dhe sigurinë e aplikacioneve softuerikë. Përdorimi i hash funksioneve për autentifikim. Objektivi kryesor i kësaj lënde është që studentëve t'u ofrojë njohuri për sigurinë e kompjuterëve të identifikojnë dhe përdorin mjetet për siguri kompjuterike.
Rezultatet e pritura:	Pas përfundimin e këtij kursi, studentët do të jenë në gjendje që: - Me mbarimin e kësaj lënde, studentët do të kenë njohuri se si të organizojnë dhe planifikojnë sigurinë e te dhënave përmesë hash funksionit si dhe enkriptimin dhe dekriptimin e te dhënave ne fushën e sigurisë. - Të zhvillojë një kuptim të përdorimit të algoritmeve për siguri ne kompjuter.

	- Të zhvillojnë një algoritëm te AES,RSA,DES e tjera. - Të interpretojnë algoritmet e sigurisë për plantext dhe cipher tekst. - Për të zhvilluar një aplikacion ne kuptimin e sigurisë dhe ndërhyrjet ne algoritëm. - Analizaen e HASH funksionit dhe zbatimi i tij ne praktike. - Përdorimi i celsave per kriptim dhe dekritim gjithmonë duke përdor algoritmet aktual.

Kontributi/ ngarkesa e studentit (që duhet të korrespondoj me rezultatet e të nxënit të mësimeve nga studenti)			
Aktiviteti	**Orë**	**Ditë/javë**	**Gjithsej/orë**
Ligjërata	2	15	30
Ushtrime teorike/laboratorike	2	15	30
Punë praktike	1	3	3
Kontaktet me mësimdhënësin/konsultime	1	15	15
Ushtrime në terren	1	3	3
Kollokviume	2	2	4
Detyra laboratorike	1	13	13
Koha e studimit vetanak të studentit (në bibliotekë ose në shtëpi)	2	15	30
Përgatitja përfundimtare për provim	2	8	16
Koha e kaluar në vlerësim (teste, kuiz, provim final)	2	2	4
Projektet, prezantimet, etj.	2	1	2
Totali			**150**
Vërejtje: 1 ECTS (kredi) = 25 orë angazhim, p. sh., nëse lënda ka 6 ECTS (kredi) studenti duhet të angazhohet 150 orë gjatë semestrit.			
Metodologjia e mësimëdhënies:	Lënda është kombinim i ligjëratave, diskutimeve, ushtrimeve numerike dhe laboratorike, ndërsa detyrat prezantohen nga mësimdhënësi i lëndës në laborator!		
Metodat e vlerësimit:	- Vijueshmëria e rregullt dhe aktive: 10%. - Provimi i ndërmjemë (kollokviumi): 20%. - Projekti i kursit: 10%. - Provimi final: 60%.		
Vlerësimi/ Nota përfundimtare:	**Vlerësimi në %**	**Nota përfundimtare**	
	91% - 100%	10	

	81% - 90%	9
	71% - 80%	8
	61% - 70%	7
	51% - 60%	6
	0% - 50%	5

Literatura	
Literatura bazë:	1. William Stallings-Cryptography and Network Security_ Principles and Practice (6th Edition)-Pearson. 2. Joan Daemen, "Introduction to Permutation – based cryptography", Croatia Crypto Summer School, June 2017. 3. Understanding Cryptography by C. Paar and J. Pelzl, Copyright Springer-Verlag, 2010.
Literatura shtesë:	1. G. Ramesh, R.Umarani "A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms", International Journal of Computer Applications (0975 – 8887) Volume 46– No.13, May 2012. 2. *SSLTrust. Retrieved 13 June 2019.*

Plani mësimor	
Java	**Ligjëratat/njësia mësimore**
Java e parë:	• Hyrje në sigurinë e informacionit.
Java e dytë:	• Krijimi i një baze mbi sigurinë ete dhënave
***Java e tretë*:**	• Planifikimi i sigurisë ne arkitekturën e kompjuterëve
Java e katërt:	• Ndërtimi i sigurisë DES
Java e pestë:	• True crypt
***Java e gjashtë*:**	• çelësat kriptografik
Java e shtatë:	• kriptografia moderne
Java e tetë:	• vlerësimi i ndërmjetëm (testi)
Java e nëntë:	• **renditja e celesave simetrik**
Java e dhjetë:	• **hash funksioni dhe kodet për autentifikacion te porosive**
***Java e njëmbëdhjetë*:**	algoritmet për kriptim dhe dekriptim • algoritmi des (data encryption standard)
***Java e dymbëdhjetë*:**	• algoritmi blowfish
***Java e trembëdhjetë*:**	• sulmet teknike **sulmet teknike dyn dhe mirari**
***Java e katërmbëdhjetë*:**	• analizimi i algoritmeve sha-1 md-5 e tjera
***Java e pesëmbëdhjetë*:**	• Vlerësimi përfundimtar

Ushtrimet

Plani mësimor	
Java	**Ushtrimet**
Java e parë:	• Lab 1: Statistikat Themelore te sigurise
Java e dytë:	• Lab 2: Ndërfaqja aplikacioneve sofuerike në një kompjuter
***Java e tretë*:**	• Lab 3: Kodi dhe algoritmat e nje algoritmi
Java e katërt:	• Lab 4: Llogaritja e algiritmave AES,DES
Java e pestë:	• Lab 5:HASH funksioni
***Java e gjashtë*:**	• Lab 6: vleresimit I algoritmave sipas sigurise teknike.
Java e shtatë:	• Lab 7: analiza e tabelave me HASH funksionin
Java e tetë:	• Lab 8: variablat me algoritmin MD5
Java e nëntë:	• Lab 9: Diskutimi i Projekteve Semestrale
Java e dhjetë:	• Lab 10: Laborator I llogaritjeve per kriptim dhe dekriptim
***Java e njëmbëdhjetë*:**	• Lab 11: Zbatimet e algoritmeve ne softuera
***Java e dymbëdhjetë*:**	• Lab 12: Aplikimet I krptografise ne softuera
***Java e trembëdhjetë*:**	• Puna në projekte semestrale
***Java e katërmbëdhjetë*:**	• Prezantimet e projekteve semestrale.
Java e pesëmbëdhjetë:	• Prezantimi i projekteve të kursit.

Politikat akademike dhe rregullat e mirësjelljes
• Në përgjithësi prezantimet e ligjëratave do të bëhen përmes MS PowerPoint, tabelës, përdorimit të materialeve, programeve kompjuterike dhe ushtrimeve numerike. • Po ashtu, nga mësimdhënësit do të sigurohen edhe materiale tjera shtesë (punime shkencore, publikime, buletine nacionale, si dhe zbulimet dhe hulumtimet e fundit). • Gjatë çdo seance do të organizohet qasja e bashkëbisedimit dhe bashkëparticipimit me studentë! • Nga studentët kërkohet që të jenë të rregullt në ligjërata dhe ushtrime! • Do të vlerësohet kontributi i studentëve kur ata bashkëpunojnë dhe participojn në ligjëratat dhe ushtrimet e lëndës! • Ardhja e studentëve me kohë në ligjërata dhe ushtrime është e obligueshme!