SYLLABUSI I LËNDËS "TEMA TË ZGJEDHURA NGA SIGURIA KOMPJUTERIKE"

Të dhëna bazike të lëndës	
Njësia akademike:	Fakulteti i Shkencave Kompjuterike
Titulli i lëndës:	Tema të zgjedhura nga siguria kompjuterike
Programi:	Shkenca Kompjuterike dhe Teknologji Komunikimi
Niveli:	Master
Statusi lëndës:	Obligative
Viti i studimeve:	2
Numri i orëve në javë:	2+2 (ligjërata dhe ushtrime)
Vlera në kredi – ECTS:	6 ECTS
Koha / lokacioni:	Të publikuara në web site të universitetit!
Mësimdhënësi i lëndës:	Prof. Asoc. Dr. Naim Baftiu
Të dhënat kontaktuese:	naim.baftiu@uni-prizren.com
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.
Qëllimi i 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 të nxënit:	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.

Ngarkesa e studentit (duhet të korrespondoj me rezultatet e të nxënit të studentit)			
Aktiviteti	**Orë**	**Ditë/javë**	**Gjithsej**
Ligjërata	2	15	30
Ushtrime teorike/laboratorike	2	15	30
Punë praktike	1	2	2

Kontaktet me mësimdhënësin/konsultimet	1	5	5
Ushtrime në terren	1	1	1
Kollokfiume, seminare	2	2	4
Detyra të shtëpisë	2	2	4
Koha e studimit vetanak të studentit (në bibliotekë ose në shtëpi)	3	10	30
Përgatitja përfundimtare për provim	5	6	30
Koha e kaluar në vlerësim (teste, kuiz, provim final)	2	3	6
Projektet, prezantimet, etj	4	2	8
Totali			**150 orë (6 ECTS)**
Metodologjia e mësimdhënies:	Lënda është kombinim i ligjëratave, diskutimeve, ushtrimeve numerike dhe laboratorike, ndërsa detyrat prezantohen nga asistenti në laborator.		
Metodologjia e vlerësimit:	• Vijueshmëria e rregullt dhe aktive: 10%. • Provimi i ndërmjemë (kollokviumi): 20%. • Projekti i kursit: 10%. • Provimi final: 60%.		
Literatura			
Literatura primare:	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:	4. 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."Using Client-Certificate based authentication with NGINX on Ubuntu - SSLTrust" 5. SSLTrust. Retrieved 13 June 2019.		

Plani i dizajnuar i mësimit:		
Java	**Ligjërata**	**Ushtrime**
Java e parë:	Hyrje në sigurinë e informacionit.	Lab 1: Statistikat Themelore te sigurise
Java e dytë:	Krijimi i një baze mbi sigurinë ete dhënave	Lab 2: Ndërfaqja aplikacioneve sofuerike në një kompjuter
Java e tretë:	Planifikimi i sigurisë ne arkitekturën e kompjuterëve	Lab 3: Kodi dhe algoritmat e nje algoritmi
Java e katërt:	Ndërtimi i sigurisë DES	Lab 4: Llogaritja e algiritmave AES,DES
Java e pestë:	True crypt	Lab 5:HASH funksioni
Java e gjashtë:	çelësat kriptografik	Lab 6: vleresimit I algoritmave sipas sigurise teknike.

Java e shtatë:	kriptografia moderne	Lab 7: analiza e tabelave me HASH funksionin
Java e tetë:	vlerësimi i ndërmjetëm (testi)	Lab 8: variablat me algoritmin MD5
Java e nëntë:	renditja e celesave simetrik	Lab 9: Diskutimi i Projekteve Semestrale
Java e dhjetë:	hash funksioni dhe kodet për autentifikacion te porosive	Lab 10: Laborator I llogaritjeve per kriptim dhe dekriptim
Java e njëmbëdhjetë:	algoritmet për kriptim dhe dekriptim algoritmi des (data encryption standard)	Lab 11: Zbatimet e algoritmeve ne softuera
Java e dymbëdhjetë:	algoritmi blowfish	Lab 12: Aplikimet I krptografise ne softuera
Java e trembëdhjetë:	sulmet teknike sulmet teknike dyn dhe mirari	Puna në projekte semestrale
Java e katërmbëdhjetë:	analizimi i algoritmeve sha-1 md-5 e tjera	Prezantimet e projekteve semestrale.
Java e pesëmbëdhjetë:	Vlerësimi përfundimtar	Prezantimi i projekteve të kursit.

Politikat akademike dhe kodi i sjelljes

- 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, buletinet nacionale, si dhe zbulimet dhe hulumtimet e fundit).
- Në mungesë të mundësisë që puna praktike të organizohet çdo javë, në bashkëpunim me menaxhmentin e universitetit, ky aktivitet do të organizohet në ditë të caktuara në: organizata, kompani, njësitë prodhuese-përpunuese, etj.
- Gjatë çdo seancë 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!