SYLLABUSI I LËNDËS "AUTENTIFIKIMI DHE KRIPTOGRAFIA"

Të dhëna bazike të lëndës	
Njësia akademike:	Fakulteti i Shkencave Kompjuterike
Titulli i lëndës:	Autentifikimi dhe kriptografia
Programi:	Teknologjitë e Informacionit dhe Telekomunikimi
Niveli:	Baçelor
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!
Mësimdhënësit e lëndës:	Prof. Asoc. Dr. Naim Baftiu Ass. Arbër Beshiri, Ph. D. c.
Të dhënat kontaktuese:	naim.baftiu@uni-prizren.com arber.beshiri@uni-prizren.com
Përshkrimi i lëndës:	Kjo lëndë lidhet me kriptografinë nga këndvështrimi teorik dhe praktikë. Ajo përfshin funksionalitetin e kriptografisë, si analizohet siguria teoritikisht dhe si e funksionalizojmë atë në praktikë. Në këtë lëndë do të shtjellohet ekriptimi simetrik, bllok shifuesit, kodet e autentifikimit të mesazheve, enkriptimi asimetrik (RSA dhe enrkiptimet me vlera diskrete), AES, DES dhe nënshkrimet digjitale. Përmes kësaj lëndë do të paraqiten koncepte themelore, përkufizime dhe rezultate që formalisht lidhen me kriptografinë dhe autentifikimin.
Qëllimi i lëndës:	Paisja e studentëve me njohuri mbi mënyrën si të krijojmë sisteme të sigurta ashtu që të garantohet integriteti, autenticiteti i informacionit dhe siguria në Internet. Gjithashtu, të kuptojmë se si të mbrohemi nga sulmet e mundshme dhe si të dizajnojmë dhe vlerësojmë zgjidhjet e sigurta në kohën moderne të teknologjisë.
Rezultatet e të nxënit:	Pas ndjekjes së kursit studentët do të jenë në gjendje: • të kuptojnë parimet bazë të kriptografisë dhe kriptoanalizës, • të njihen me konceptet e enkriptimeve simetrike dhe autentikimit, enkriptimin e mesazheve duke përdorur enkriptimet me çelësa publik, nënshkrimet digjitale dhe zgjedhjen e çelësit, • të njohin dhe kuptojnë përdorimin e skemave kriptografike, duke përfshirë AES, algoritmin RSA, nënshkrimit dixhitale, shpërndarjen e çelësave sipas Diffie-Hellman, vendosjen e protokolit dhe të kuptojnë se si dhe kur t'i zbatojnë ato, të krijojnë, ndërtojnë dhe analizojnë zgjidhje të thjeshta kriptografike.

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 mësimdhënësi në laborator.		
Metodologjia e vlerësimit:	• Vijueshmëria në ligjërata dhe ushtrime: 5% • Projekti/detyrat laboratorike: 35%. • Kollokviumi 1: 30%. • Kollokviumi 2: 30%. • Ose provimi përfundimtar: 100%.		
Literatura			
Literatura primare:	1. William Stallings. Cryptography and Network Security. Principles and Practices. Pearson. 7th / 8th Edition, 2016 / 2019. 2. N. Deepa. IT Security and Cryptography Lab, 2017.		
Literatura shtesë:	3. Christof Paar and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010. 4. Behrouz A. Forouzan. Cryptography and Network Security. McGraw-Hill, 2007.		

Plani i dizajnuar i mësimit:		
Java	**Ligjërata**	**Ushtrime**
Java e parë:	• Prezantimi i syllabusit (rreth ligjëratave). • Koncepte rreth sigurisë së kompjuterit dhe të rrjetit.	• Prezantimi i syllabusit (rreth ushtrimeve). • Koncepte rreth sigurisë së kompjuterit dhe të rrjetit.
Java e dytë:	• Hyrje në teorin e numrave - algoritmi i Euklidit.	• Algoritmi i Euklidit. • Shifruesi i Cesarit - enkriptimi dhe dekriptimi.
Java e tretë:	• Enkriptimi simetrik - metodat e enkriptimit klasik (1).	• Shifruesi me zëvendësim (monoalfabetik) - enkriptimi dhe dekriptimi. • Shifruesi me zhvendosje (Rail Fence) - enkriptimi dhe

		dekriptimi.
Java e katërt:	• Metodat e enkriptimit klasik (2).	• Shifruesi Playfair - enkriptimi dhe dekriptimi. • Shifruesi i Hillit - enkriptimi dhe dekriptimi.
Java e pestë:	• Bllok shifruesit dhe DES (DES i thjeshtë).	• Shifruesi i Vernamit - enkriptimi dhe dekriptimi. • Shifruesi i Vernamit (One-Time Pad) - enkriptimi dhe dekriptimi.
Java e gjashtë:	• Koncepte nga teoria e numrave dhe fushat e fundme.	• Shifruesi i Vigenere - enkriptimi dhe dekriptimi. • Steganografia.
Java e shtatë:	• AES dhe AES i thjeshtë (1).	• DES i thjeshtë - enkriptimi dhe dekriptimi.
Java e tetë:	• Kollokviumi 1.	• Konsultime rreth kollokviumit 1.
Java e nëntë:	• AES dhe AES i thjeshtë (2).	• Algoritmi i zgjeruar i Euklidit. • AES i thjeshtë - enkriptimi.
Java e dhjetë:	• Kriptografia me çelësa publik dhe algoritmi RSA.	• AES i thjeshtë - dekriptimi. • RSA - enkriptimi dhe dekriptimi.
Java e njëmbëdhjetë:	• Shpërndarja e çelsave sipas Diffie-Hellman. • Sistemet kriptografike Elgamal. • Sistemet kriptografike eliptike.	• Shpërndarja e çelësave sipas Diffie-Hellman.
Java e dymbëdhjetë:	• Hash funksionet dhe algoritmi SHA. • SHA-3 dhe MD5. • Autentikimi i mesazheve me Hash funksione.	• Hash funksionet dhe algoritmi SHA. • SHA-1 dhe MD 5.
Java e trembëdhjetë:	• Kodet për autentifikimin e mesazheve. • Siguria e MAC. • MAC i bazuar në Hash funksione - HMAC.	• Siguria e MAC. • Nënshkrimet digjitale.
Java e katërmbëdhjetë:	• Nënshkrimet digjitale. • Skema e nënshkrimeve digjitale Elgamal. • Algoritmet e nënshkrimeve digjitale të bazuara në sistemet kriptografike eliptike.	• WEP dhe WPA. • Intrusion Detection System.
Java e pesëmbëdhjetë:	• Kollokviumi 2.	• Konsultime rreth kollokviumit 2.
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!