SYLLABUSI

Të dhëna bazike rreth lëndës	
Universiteti:	**Universiteti "Ukshin Hoti" - Prizren**
Njësia akademike:	**Fakulteti i Shkencave Kompjuterike**
Programi i studimit:	**Teknologjitë e Informacionit dhe Telekomunikimi**
Lënda:	**Autentifikimi dhe kriptografia**
Niveli i studimeve:	**Baçelor**
Statusi i lëndës:	**Obligative**
Viti i studimeve:	**2**
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** **Ass. Arbër Beshiri, Ph. D. c.**
Detajet 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.
Qëllimet e 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 pritura:	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.

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	2	2
Kontaktet me mësimdhënësin/konsultime	1	5	5
Ushtrime në terren	1	1	1
Kollokviume	2	2	4
Detyra laboratorike	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**
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 në ligjërata dhe ushtrime: 5% - Projekti/detyrat laboratorike: 35%. - Kollokviumi 1: 30%.

	- Kollokviumi 2: 30%. - Ose provimi përfundimtar: 100%.	
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 Practices. Pearson. 7th / 8th Edition, 2016 / 2019. 2. N. Deepa. IT Security and Cryptography Lab, 2017.	
Literatura shtesë:	1. Christof Paar and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010. 2. Behrouz A. Forouzan. Cryptography and Network Security. McGraw-Hill, 2007.	

Plani mësimor	
Java	**Ligjëratat/njësia mësimore**
Java e parë:	• Prezantimi i syllabusit (rreth ligjëratave). • Koncepte rreth sigurisë së kompjuterit dhe të rrjetit.
Java e dytë:	• Hyrje në teorin e numrave - algoritmi i Euklidit.
***Java e tretë*:**	• Enkriptimi simetrik - metodat e enkriptimit klasik (1).
Java e katërt:	• Metodat e enkriptimit klasik (2).
Java e pestë:	• Bllok shifruesit dhe DES (DES i thjeshtë).
***Java e gjashtë*:**	• Koncepte nga teoria e numrave dhe fushat e fundme.
Java e shtatë:	• AES dhe AES i thjeshtë (1).
Java e tetë:	• Kollokviumi 1.
Java e nëntë:	• AES dhe AES i thjeshtë (2).
Java e dhjetë:	• Kriptografia me çelësa publik dhe algoritmi RSA.
***Java e njëmbëdhjetë*:**	• Shpërndarja e çelsave sipas Diffie-Hellman. • Sistemet kriptografike Elgamal. • Sistemet kriptografike eliptike.
***Java e dymbëdhjetë*:**	• Hash funksionet dhe algoritmi SHA. • SHA-3 dhe MD5. • Autentikimi i mesazheve me Hash funksione.
***Java e trembëdhjetë*:**	• Kodet për autentifikimin e mesazheve.

	• Siguria e MAC. • MAC i bazuar në Hash funksione - HMAC.
***Java e katërmbëdhjetë*:**	• Nënshkrimet digjitale. • Skema e nënshkrimeve digjitale Elgamal. • Algoritmet e nënshkrimeve digjitale të bazuara në sistemet kriptografike eliptike.
Java e pesëmbëdhjetë:	• Kollokviumi 2.

Ushtrimet

Plani mësimor	
Java	**Ushtrimet**
Java e parë:	• Prezantimi i syllabusit (rreth ushtrimeve). • Koncepte rreth sigurisë së kompjuterit dhe të rrjetit.
Java e dytë:	• Algoritmi i Euklidit. • Shifruesi i Cesarit - enkriptimi dhe dekriptimi.
***Java e tretë*:**	• Shifruesi me zëvendësim (monoalfabetik) - enkriptimi dhe dekriptimi. • Shifruesi me zhvendosje (Rail Fence) - enkriptimi dhe dekriptimi.
Java e katërt:	• Shifruesi Playfair - enkriptimi dhe dekriptimi. • Shifruesi i Hillit - enkriptimi dhe dekriptimi.
Java e pestë:	• Shifruesi i Vernamit - enkriptimi dhe dekriptimi. • Shifruesi i Vernamit (One-Time Pad) - enkriptimi dhe dekriptimi.
***Java e gjashtë*:**	• Shifruesi i Vigenere - enkriptimi dhe dekriptimi. • Steganografia.
Java e shtatë:	• DES i thjeshtë - enkriptimi dhe dekriptimi.
Java e tetë:	• Konsultime rreth kollokviumit 1.
Java e nëntë:	• Algoritmi i zgjeruar i Euklidit. • AES i thjeshtë - enkriptimi.
Java e dhjetë:	• AES i thjeshtë - dekriptimi. • RSA - enkriptimi dhe dekriptimi.
***Java e njëmbëdhjetë*:**	• Shpërndarja e çelësave sipas Diffie-Hellman.
***Java e dymbëdhjetë*:**	• Hash funksionet dhe algoritmi SHA. • SHA-1 dhe MD 5.
***Java e trembëdhjetë*:**	• Siguria e MAC. • Nënshkrimet digjitale.
***Java e katërmbëdhjetë*:**	• WEP dhe WPA. • Intrusion Detection System.
Java e pesëmbëdhjetë:	• Konsultime rreth kollokviumit 2.

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!