UNIVERSITETI - UNIVERSITY - UNIVERZITET
"HAXHI ZEKA"

SYLLABUSI I LËNDËS
KRIPTOGRAFIA DHE SIGURIA KIBERNETIKE

SYLLABUS							
Niveli i studimeve		Bachelor i shkencave	***Programi***	Teknologji Informacioni në biznes dhe ekonomi	***Viti akademik***	2023/2024	
LËNDA		**Kriptografia dhe siguria kibernetike**					
Viti	III	***Statusi i lëndës***	OBLIGATIVE	***Kodi***		***ECTS kredi***	6
Semestri	V						
Javët mësimore		15		***Orët mësimore***	Ligjerata	Ushtrime	
					2	2	
Metodologjia e mësimit		Ligjerata, ushtrime, punime seminarike, konsultime, teste, raste studimi, detyra					
Konsultime		Një orë para dhe një orë pas ligjëratave					
Mësimdhënësi		**Prof.dr. Artan Luma**		e-mail	**a.luma@seeu.edu.mk**		
				tel.	**+383 (0)70-527-124**		
Ushtrimet				e-mail			
				tel.			

Qëllimi studimor dhe përmbajtja e lëndës	Përfitimet e studentit
Kursi paraqet një hyrje të integruar në kriptografi me një gamë të gjerë. Janë shtjelluar këto tema: Konceptet e sigurisë së kompjuterit dhe rrjetit, Hyrje në teorinë e numrave, teknikat klasike të enkriptimit, shifrat e bllokut dhe standardi i enkriptimit të të dhënave, Fushat e fundme, Standardi i avancuar i enkriptimit, funksionimi i kodit të bllokut, gjenerimi i biteve të rastësishëm dhe shifrat e rrjedhës, çelësi publik Kriptografia dhe RSA, Kriptosistemet e Tjera me Çelës Publik, Funksionet e Hashit Kriptografik, Kodet e Autentifikimit të Mesazheve, Nënshkrimet Dixhitale	Pas përfundimit të kursit, studentët do të jenë në gjendje të: 1. Të kuptojnë bazat e kriptografisë. 2. Të demonstrojnë njohuri për zhvillimin historik të kriptografisë kompjuterike. 3. Të përcaktojnë termat që lidhen me kriptografinë kompjuterike. 4. Të demonstrojnë një kuptim themelor të kriptografisë kompjuterike. 5. Të kuptojnë marrëdhëniet ndërmjet algoritmeve të kriptografisë kompjuterike. 6. Të njihen me algoritmet e kriptografisë kompjuterike të përdorur gjerësisht RSA

Metodologjia për realizimin e temave mësimore:
• Prezantimi i temës mësimore në Power Point (studentët mund ta shkarkojnë atë pas çdo ligjërate nga Web faqja e fakultetit) • Rast studimi apo detyrë (për orën e ushtrimeve) lidhur me temën e ligjëruar • Përsëritja e temës paraprake nga grupi i caktuar i studentëve, analiza dhe diskutime
Kushtet për realizimin e temës mësimore:
• Salla e pajisur me kompjuterë dhe projektor

Mënyra e vlerësimit të studentit (në %) :

- Punimi seminarik 0-10%
- Testi I 0-15 %
- Testi II 0-15%
- Provimi përfundimtar 0- 50%
- Pjesëmarrja në ushtrime 0 - 5%
- Puna grupore në detyra dhe raste studimi 0- 5%

Vlerësimi në %	Nota përfundimtare
91-100	10 (dhjetë)
81-90	9 (nëntë)
71-80	8 (tetë)
61-70	7 (shtatë)
51-60	6 (gjashtë)
0-50	5 (pesë)

Obligimet e studentit:

Ligjërata	Ushtrime
• Vijimi i ligjëratave • Pjesëmarrja aktive në diskutime gjatë ligjëratave • Punimi seminarik • Pjesëmarrja në teste • Provimi përfundimtar	• Pjesëmarrja në ushtrime • Puna grupore në raste studimi dhe detyra • Pjesëmarrja në diskutime lidhur me rastet e studimit

Ngarkesa e studentit për lëndën

Aktiviteti	Orë	Ditë/Javë	Gjithsej
Ligjerata	**2**	**15**	**30**
Ushtrime	**2**	**15**	**30**
Punë praktike	**0**	**15**	**0**
Kontakte me mësimdhënësit/konsultimet	**0.5-1**	**10**	**10**
Ushtrime në terren	**-**	**-**	**0**
Kolokviume, seminare	**2**	**2**	**4**
Detyra të shtëpisë	**-**	**-**	**10**
Koha e studimit vetanak	**1.5**	**30**	**45**
Përgatitja përfundimtare për provim	**3**	**8**	**25**
Koha e kaluar në vlerësim (teste, kuiz, provim final, etj.)	**2**	**8**	**16**
Projektet, prezentimet, etj.	**1**	**10**	**10**
Vërejtje: 1 ECTS kredi = 30 orë angazhim, p.sh. nëse lënda i ka 6 ECTS kredi studenti duhet të ketë angazhim gjatë semestrit 180 orë		**Ngarkesa totale:**	**180**

Java	Ligjerata		Ushtrime	
	Tema	Orët	Tema	Orët
1.	Tema: Hyrje. Njoftimi me syllabusin e lëndës Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: Hyrje. Njoftimi me syllabusin e lëndës Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
2.	Tema: *Konceptet e sigurisë së kompjuterit dhe rrjetit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Konceptet e sigurisë së kompjuterit dhe rrjetit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
3.	Tema: *Hyrje në teorinë e numrave* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Hyrje në teorinë e numrave* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
4.	Tema: *Shifrat e bllokut dhe standardi i enkriptimit të të dhënave* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Shifrat e bllokut dhe standardi i enkriptimit të të dhënave* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
5.	Tema: *Fushat e fundme*	2	Tema: *Fushat e fundme*	2

	Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,		Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	
6.	Tema: *Standardi i avancuar i enkriptimit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Standardi i avancuar i enkriptimit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
7.	Tema: *Testi i parë* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Testi i parë* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
8.	Tema: *Funksionimi i kodit të bllokut* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Funksionimi i kodit të bllokut* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
9.	Tema: *Gjenerimi i rastësishëm i biteve dhe shifrat transmetimit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Gjenerimi i rastësishëm i biteve dhe shifrat transmetimit* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
10.	Tema: *Kriptografia me çelës publik dhe RSA* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Kriptografia me çelës publik dhe RSA* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
11.	Tema: *Kriptosisteme të tjera me çelës publik* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Kriptosisteme të tjera me çelës publik* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
12.	Tema: *Funksionet e hashit kriptografik* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Funksionet e hashit kriptografik* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
13.	Tema: *Kodet e vërtetimit të mesazheve* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Kodet e vërtetimit të mesazheve* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
14.	Tema: *Nënshkrimet dixhitale* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: *Nënshkrimet dixhitale* Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2
15.	Tema: Testi i dytë Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2	Tema: Testi i dytë Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017. Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,	2

LITERATURA:

Literatura bazë:

- Kriptografia dhe Siguria e Rrjetit: Parimet dhe Praktika (Edicioni i Shtatë), William Stallings, 2017.
- Një hyrje në kriptografi, Botimi i dytë, nga Richard A. Mollin, Botues: Chapman & Hall/CRC, 2007.

Literatura shtesë:

- An Introduction to Mathematical Cryptography, nga Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, Botues: Springer, 2008.
- Hyrje në kriptografinë moderne, Botimi i dytë, nga Jonathan Katz & Yehuda Lindell, CRC Press, 2015,

SHËNIM:

- *Për çdo temë mësimore, studentët do të pajisen me materiale të nevojshme.*
- *Në fund të çdo ore mësimore, grupet e caktuara të studentëve do të angazhohen me detyrë apo rast studimi lidhur me temën e ligjëruar. Rezultatet e arritura nga ajo detyrë, grupet e studentëve duhet ti prezantojë dhe t'i diskutojnë ato në orën e ushtrimeve.*

Vërejtje për studentin:

- Para së gjithash, studenti duhet të jetë i ndërgjegjshëm dhe të respektojë institucionin dhe rregullat shkollore
- Duhet të respektojë orarin e ligjëratave , ushtrimeve dhe të jetë i vëmendshëm në orën mësimore
- Është i obliguar posedimi dhe paraqitja e indeksit në teste dhe provim
- Gjatë hartimit të punimeve seminarike, studenti duhet ti përmbahet udhëzimeve të dhëna nga mësimdhënësi për realizimin hulumtues dhe teknik të punimit.