

UČNI NAČRT PREDMETA / COURSE SYLLABUS (leto / year 2016/17)						
<b>Predmet:</b>		Teorija kodiranja in kriptografija				
<b>Course title:</b>		Coding theory and cryptography				
<b>Študijski program in stopnja</b> Study programme and level		<b>Študijska smer</b> Study field		<b>Letnik</b> Academic year	<b>Semester</b> Semester	
Univerzitetni študijski program Finančna matematika		ni smeri		3	drugi	
First cycle academic study programme Financial Mathematics		none		3	second	
<b>Vrsta predmeta / Course type</b>				izbirni / elective		
<b>Univerzitetna koda predmeta / University course code:</b>				M0329		
<b>Predavanja</b> Lectures	<b>Seminar</b> Seminar	<b>Vaje</b> Tutorial	<b>Klinične vaje</b> work	<b>Druge oblike študija</b>	<b>Samost. delo</b> Individ. work	<b>ECTS</b>
30		30			90	5
<b>Nosilec predmeta / Lecturer:</b>		prof. dr. Marko Petkovšek, prof. dr. Primož Potočnik, doc. dr. Arjana Žitnik				
<b>Jeziki / Languages:</b>		<b>Predavanja / Lectures:</b>		slovenski / Slovene		
		<b>Vaje / Tutorial:</b>		slovenski / Slovene		
<b>Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:</b>				<b>Prerequisites:</b>		
Vpis v letnik študija.				Enrolment in the programme.		
Opravljeni predmeti Algebra 1, Uvod v programiranje in Verjetnost 1.				Completed courses Algebra 1, Introduction to programming and Probability 1.		
<b>Vsebina:</b>				<b>Content (Syllabus outline):</b>		

<p>Teorija kodiranja. Informacija in entropija. Shannonova teorija. Koda za popravljanje napak. Zgornje meje za število kodnih besed. Linearni, Hammingovi, ciklični in Reed-Mullerjevi kodi.</p> <p>Kriptografija. Klasična kriptografija. Sistemi z zasebnim ključem. RSA in sistemi z javnim ključem. Digitalni podpisi. Zgoščevalne funkcije. Distribucija in izmenjava ključev. Identificiranje, overjanje in delitev skrivnosti. Generiranje psevdo-naključnih števil. Dokazi z ničelno informacijo.</p>	<p>Coding theory. Information and entropy. Shannon's theory. Error-correcting codes. Bounds on the size of codes. Linear, Hamming, cyclic and Reed-Muller codes. Cryptography. Classical cryptography. Symmetric-key cryptosystems. RSA cryptosystem and public-key cryptography. Digital signatures. Hash functions. Key distribution and key agreement schemes. Identification, authentication, secret sharing schemes. Zero-knowledge proofs.</p>
--	--

**Temeljni literatura in viri / Readings:**

D. R. Stinson: Cryptography : Theory and Practice, 3rd edition, Chapman & Hall/CRC, Boca Raton, 2005.

J. Talbot, D. Welsh: Complexity and Cryptography, Cambridge Univ. Press, Cambridge, 2006.

D. Welsh: Codes and Cryptography, Oxford Univ. Press, Oxford, 1988.

**Cilji in kompetence:**

Študent spozna osnove teorije kodiranja in kriptografije.

**Objectives and competences:**

Students learn the basics of coding theory and cryptography.

**Predvideni študijski rezultati:**

Znanje in razumevanje: Matematični postopki, s katerimi zagotavljamo zanesljivo in varno komunikacijo.

Uporaba: Kodiranje in kriptografija se uporabljata pri digitalnih komunikacijah in za zagotavljanje informacijske varnosti.

Refleksija: Osnovne tehnike sodobne kriptografije temeljijo na matematičnih pojmi in postopkih, ki zagotavljajo največjo znano

**Intended learning outcomes:**

Knowledge and understanding: Mathematical procedures that enable reliable and secure communication.

Application: Coding theory and cryptography are used in digital communications and for providing information security.

Reflection: Basic techniques of modern cryptography are based on mathematical concepts and

mero varnosti.

Prenosljive spretnosti – niso vezane le na en predmet: Študent pridobi sposobnost kritičnega razmišljanja in analize komunikacijskih kanalov in računalniških sistemov s stališča informacijske varnosti.

procedures that provide the maximum level of security known.

Transferable skills:  
The students will acquire skills of critical thinking and analysis of the communication channels and computer systems with respect to information security.

**Metode poučevanja in učenja:**

Predavanja, vaje, domače naloge, konzultacije

**Learning and teaching methods:**

Lectures, exercises, homework, consultations

**Načini ocenjevanja:**

Delež (v %) /

Weight (in %)

**Assessment:**

Način (pisni izpit, ustno izpraševanje, naloge, projekt):

2 kolokvija namesto izpita iz vaj, izpit iz vaj,

izpit iz teorije

ocene: 1-5 (negativno), 6-10 (pozitivno) (po Statutu UL)

50%

50%

Type (examination, oral, coursework, project):

2 midterm exams instead of written exam, written exam

oral exam

grading: 1-5 (fail), 6-10 (pass) (according to the Statute of UL)

**Reference nosilca / Lecturer's references:**

Marko Petkovšek:

PETKOVŠEK, Marko, ZAKRAJŠEK, Helena. Enumeration of l-graphs: Burnside does it again. *Ars mathematica contemporanea*, ISSN 1855-3966. [Tiskana izd.], 2009, vol. 2, no. 2, str. 241-262. [COBISS.SI-ID 15497049]

ABRAMOV, Sergei A., PETKOVŠEK, Marko. On the bottom summation. *Programming and computer software*, ISSN 0361-7688, 2008, vol. 34, no. 4, str. 187-190. [COBISS.SI-ID 15287385]

PETKOVŠEK, Marko. Symbolic computation with sequences. Programming and computer software, ISSN 0361-7688, 2006, vol. 32, no. 2, str. 65-70. [COBISS.SI-ID 15287129]

Primož Potočnik:

POTOČNIK, Primož, SPIGA, Pablo, VERRET, Gabriel. On the nullspace of arc-transitive graphs over finite fields. Journal of algebraic combinatorics, ISSN 0925-9899, 2012, vol. 36, no. 3, str. 389-401. [COBISS.SI-ID 16162137]

POTOČNIK, Primož. B-groups of order a product of two distinct primes. Mathematica slovac, ISSN 0139-9918, 2001, vol. 51, no. 1, str. 63-67. [COBISS.SI-ID 10617433]

POTOČNIK, Primož, VERRET, Gabriel. On the vertex-stabiliser in arc-transitive digraphs. Journal of combinatorial theory. Series B, ISSN 0095-8956, 2010, vol. 100, iss. 6, str. 497-509. [COBISS.SI-ID 15680601]

Arjana Žitnik:

JURIŠIĆ, Aleksandar, TERWILLIGER, Paul, ŽITNIK, Arjana. The Q-polynomial idempotents of a distance-regular graph. Journal of combinatorial theory. Series B, ISSN 0095-8956, 2010, vol. 100, iss. 6, str. 683-690. [COBISS.SI-ID 15688537]

KAVČIČ, Urška, MUCK, Tadeja, LOZO, Branka, ŽITNIK, Arjana. Readability of multi-colored 2D codes. Technics technologies education management, ISSN 1840-1503, 2011, vol. 6, no. 3, str. 622-630, ilustr. [COBISS.SI-ID 2673008]

CONDER, Marston D. E., PISANSKI, Tomaž, ŽITNIK, Arjana. GI-graphs: a new class of graphs with many symmetries. Journal of algebraic combinatorics, ISSN 0925-9899, 2014, vol. 40, iss. 1, str. 209-231. [COBISS.SI-ID 16969561]