UČNI NAČRT PREDMETA / COURSE SYLLABUS (leto / year 2017/18)			
Predmet:	Teorija kodiranja in kriptografija 2		
Course title:	Coding theory and cryptography 2		

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Interdisciplinarni magistrski študijski program Računalništvo in matematika	ni smeri	1 ali 2	prvi ali drugi
Interdisciplinary Master's study programme Computer Science and Mathematics	none	1 or 2	first or second

Vrsta predmeta / Course type	izbirni / elective
Univerzitetna koda predmeta / University course code:	M2844

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	**15**	**30**			**105**	**6**

Nosilec predmeta / Lecturer:	prof. dr. Sergio Cabello Justo, prof. dr. Arjana Žitnik

Jeziki / Languages:	**Predavanja / Lectures:**	slovenski / Slovene, angleški / English
	Vaje / Tutorial:	slovenski / Slovene, angleški / English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Vpis v letnik študija.	Enrolment in the programme.
Vsebina:	**Content (Syllabus outline):**

Vsebina je razdeljena na obvezni del, pri katerem se obravnava osnovne pojme in teoretične osnove teorije kodiranja in kriptografije, ter na izbirni del, pri katerem se obravnava izbrane aplikacije.Obvezni del: 1. Stiskanje podatkov (simbolno kodiranje, Shannonova teorija, Huffmanov kod, aritmetično kodiranje, slovarske metode) 2. Kriptografija (Osnovni pojmi: simetrični kriptosistemi,bločne in tokovne šifre, asimetrični kriptosistemi, zgoščevalne funkcije in kodi za avtentikacijo (MAC), digitalni podpis. Teoretične osnove: generatorji psevdonaključnih števil in enosmerne funkcije, njihove povezave in uporaba pri analizi varnosti kriptosistemov.) 3. Kodi, ki popravljajo napake (Shannonov izrek, zgornje in spodnje meje za število kodnih besed, linearni kodi) Pri izbirnem delu predavatelj izbere nakatere izmed naslednjih tem: izbrani kriptosistemi, izbrani kriptografski protokoli, učinkovite računanje nad končnimi obsegi, dokazi brez razkritja znanja, delitev skrivnosti, izbrani kodi (turbo kodi, paritetni kodi z nizko gostoto (LDCP), Goppa kodi), verjetnostne porazdelitve podatkov	The course is divided into core part, which treats the basics concepts and theoretical foundations and of coding theory and cryptography, and optional parts that include selected applications. Core part:1. Data compression (symbol coding, Shannon's theory, Huffman coding, arithmetic coding, dictionary methods) 2. Cryptography (Basic concepts: symmetric cryptosystems, block ciphers, stream ciphers, asymmetric cryptosystems, hash functions, message authentication codes, digital signatures. Theoretical foundations: pseudorandom generators, one-way functions, their relations and uses in security analysis.) 3. Error-correcting codes (Shannon’s theorem, upper and lower bounds on the number of codewords, linear codes) For the optional part the lecturer selects some of the following topics: selected cryptosystems, selected cryptographic protocols, efficient computation over finite fields, zero knowledge proof systems, secret sharing schemes, selected error-correcting codes (turbo codes, low density parity-check codes, Goppa codes), probabilsictic models of data

Temeljni literatura in viri / Readings:

O. Goldreich, The Foundations of Cryptography - Volumes 1 and 2, Cambridge University Press.

S. Goldwasser, M. Bellare, Lecture Notes in Cryptography, available online at http://www-cse.ucsd.edu/users/mihir/papers/gb.html.

D. R. Stinson, Cryptography. Theory and practice, 3rd ed., CRC Press, 2006.

D. Welsh, Codes and cryptography, Oxford: Clarendon Press, 1995.

J. Justesen, T. Hoeholdt, A course in error-correcting codes, European Math. Soc., 2004.

Raziskovalni članki po izboru predavatelja za izbirni del predmeta

Cilji in kompetence:	**Objectives and competences:**

Študent pridobi sposobnost kritične analize komunikacijskih kanalov s stališča informacijske varnosti, zanesljivosti prenosa in računske zahtevnosti.	Students acquire competency to analyze communication channels with respect to security of information, reliability of transmission and computational complexity.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: Uporaba kodiranja za različne namene (ekonomičnost, varnost, zanesljivost komunikacije). Prednosti in slabosti simbolnega kodiranja, tekočega kodiranja in slovarskih metod. Primerjava in načini uporabe simetričnih in asimetričnih kriptosistemov. Lastnosti in uporaba linearnih kodov. Dobre teoretične osnove teorije kodiranja in kriptografije ter razumevanje analize varnosti kriptosistemov. Poznavanje izbranih kriptosistemov, protokolov, kodov v uporabi. Uporaba: Varnost podatkov.Refleksija: Prednosti in slabosti različnih metod. Prenosljive spretnosti – niso vezane le na en predmet: Spoznanje matematičnih osnov uporabnega področja.	Knowledge and understanding: Applications of coding to achieve efficiency, security and reliability of communication. Strengths and weaknesses of symbol coding, stream coding, and dictionary methods. Comparison and applications of symmetric and asymmetric cryptosystems. Degrees of cryprographic security. Properties and use of linear codes. Good theoretical foundations in coding theory and cryptography and understanding of security analysis of cryptosystems. Knowledge of selected cryptosystems, protocols and codes in use. Application: Data security. Reflection: Strengths and weaknesses of different methods. Transferable skills: Learning mathematical foundations of an applied area.

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, seminar, vaje, domače naloge, konzultacije in samostojno delo študentov.	Lectures, seminar, recitation classes, coursework, consultations and independent work by the students.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): Sprotno preverjanje (domače naloge,	50% 50%	Type (examination, oral, coursework, project): Continuing (homework, midterm exams, project work) Final (written or oral exam)

kolokviji in projektno delo) Končno preverjanje (pisni ali ustni izpit) Ocene: 6-10 pozitivno, 1-5 negativno (v skladu s Statutom UL)		Grading: 6-10 pass, 1-5 fail (according to the rules of University of Ljubljana)

Reference nosilca / Lecturer's references:

Sergio Cabello:

CABELLO, Sergio, PADRÓ, Carles, SÁEZ, Germán. Secret sharing schemes with detection of cheaters for a general access structure. Designs, codes and cryptography, ISSN 0925-1022, 2002, vol. 25, no. 2, str. 175-188. [COBISS.SI-ID 13352281]

CABELLO, Sergio, ROTE, Günter. Obnoxious centers in graphs. SIAM journal on discrete mathematics, ISSN 0895-4801, 2010, vol. 24, no. 4, str. 1713-1730. [COBISS.SI-ID 15762265]

CABELLO, Sergio, GIANNOPOULOS, Panos, KNAUER, Christian, MARX, Dániel, ROTE, Günter. Geometric clustering: fixed-parameter tractability and lower bounds with respect to the dimension. ACM transactions on algorithms, ISSN 1549-6325, 2011, vol. 7, no. 4, article 43 (27 str.). [COBISS.SI-ID 16028761]

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 tehnologies 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]