UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Uvod v kriptografijo
Course title:	Introduction to Cryptography

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Računalništvo in spletne tehnologije, visokošolski strokovni študijski program prve stopnje	-	Drugi	Tretji
Computer Science and Web Technologies, first cycle Professional Study Programme	-	Second	Third

Vrsta predmeta / Course type Obvezni / Obligatory

Univerzitetna koda predmeta / University course code: 2-RST-VS-UK-2022-12-16

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	-	45	-	-	105	6

Nosilec predmeta / Lecturer:

Jeziki / Languages:		
	Predavanja / Lectures:	Slovenski / Slovenian, Angleški / English
	Vaje / Tutorial:	Slovenski / Slovenian, Angleški / English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Pogoj za vključitev v delo je vpis v 2. letnik študija in opravljena izpita Matematika 1 in Matematika 2. Študent/študentka mora pred pristopom k izpitu opraviti vse obveznosti na vajah.	Enrolment into the second year of the study and passed exams Mathematics 1 and Mathematics 2. Before examination, a student must complete all assignments given at the exercises.

Vsebina: **Content (Syllabus outline):**

- *Matematični temelji kriptografije*: Teorija kompleksnosti, osnove teorije števil, problem iskanja razcepa števil, problem generiranja praštevil, diskretni algoritmi v končnih obsegih, verjetnost.
- *Uvod v kriptografijo:* Zgodovina kriptografije, kriptografske tehnike in protokoli (generiranje in izmenjava ključev, identifikacija, avtentikacija, izmenjava skrivnosti, kriptografska zaščita podatkovnih zbirk).
- *Kriptografski algoritmi:* DES (Data Encryption Standard) in AES (Advanced Encryption Standard) algoritma, RSA (Rivest-Shamir-Adleman) in ElGamalov algoritem, podpisne sheme, zgoščevalne funkcije, identifikacijske sheme, *eliptične krivulje(ECC)*.
- *Generiranje naključnih števil*.
- *Teoretična varnost algoritmov*.

- *Mathematical fundamentals of cryptography:* Complexity theory, basic number theory, factorization of integers, generation of prime numbers, discrete algorithms in finite fields, probablitiy.
- *Introduction to cryptography:* History of cryptography, cryptographic techniques and protocols (key generation and exchange, identification, authentication, secret exchange, cryptographic protection of databases).
- *Cryptographic algorithms:* DES (Data Encryption Standard) and AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) and ElGamal), digital signature scheme, hash functions, indentification schemes, *elliptic curves (ECC)*
- *Random numbers.*
- *Theoretical security of algorithms*

Temeljni literatura in viri / Readings:

- Galbraith, S. (2012). Mathematics of Public Key Cryptography. Cambridge University Press.
- Grimmett, G. D. & Stirzaker, D. R. (2001). Probability and Random Processes (3rd ed.). Oxford University Press.
- Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. (2001). Handbook of Applied Cryptography. New York: CRC Press.
- Stinson, D. & Paterson, M. (2019). Cryptography: Theory and Practice (4th ed.). New York: CRC press.
- Vidav, I. (2017). Algebra. DMFA.

Cilji in kompetence:

Učna enota prispeva k razvoju naslednjih splošnih in predmetno-specifičnih kompetenc:

Splošne kompetence:
- poznavanje osnov računalništva in informacijske tehnologije
- poznavanje in razumevanje procesov, ki jih je mogoče informacijsko podpreti z uporabo spletnih tehnologij, ter sposobnost za njihovo analizo, sintezo in predvidevanje rešitev ter njihovih posledic
- poznavanje pomena kakovosti in prizadevanje za kakovost strokovnega dela skozi avtonomnost, samoiniciativnost, (samo)kritičnost,

Objectives and competences:

The instructional unit contributes to the development of the following general and subject-specific competences:

General competences:
- familiarity with the basics of computer science and information technology
- familiarity with and understanding of processes allowing information-aided use of web technologies, and the ability to analyse and synthesize them as well as predict solutions and their consequences
- familiarity with the importance of quality, striving to maintain the quality of professional work through practicing autonomous behaviour, showing

(samo)refleksivnost in (samo) evalviranje v strokovnem delu • sposobnost fleksibilne uporabe znanja v praksi • sposobnost logičnega sklepanja, ocenjevanja velikostnega reda rezultata, natančnosti izražanja, pisanja in razmišljanja *Predmetno-specifične kompetence:* • poznavanje matematičnih temeljev kriptografske varnosti • poznavanje glavnih algoritmov in tehnik iz kriptografije	initiative, as well as through (self-) criticism, (self-)reflection and (self-) evaluation • ability to use the acquired knowledge in practice in a flexible manner • ability to make logical conclusions, to estimate the order of magnitude of the result, to be precise in at expressions, writing and thinking *Subject-specific competences:* • familiarity with mathematical basics of cryptographic security • familiarity with the main algorithms and cryptographic techniques

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Študent/študentka:* • dobro spozna matematične temelje kriptografije, ki so nujni za razumevanja koncepta računalniške kriptografske varnosti • spozna tudi ključne algoritme in tehnike in njihovo teoretično varnost	Knowledge and understanding: *The student:* • acquires mathematical introduction into cryptography which is necessary to understand the concepts of cryptographic security • acquires the most important cryptographic algorithms and techniques and their theoretical security

Metode poučevanja in učenja:	**Learning and teaching methods:**
• predavanja z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • vaje: na teh vajah bodo reševali manjše primere, s katerimi bodo utrjevali snov s predavanj • domače naloge in projektna naloga – z njimi bo študent preko samostojnega dela utrdil vse znanje, ki ga je pridobil na predavanjih in vajah • kolokviji: z njimi bodo študentje stimulirani, da sproti študirajo snov, ki bo obravnavana na predavanjih in vajah	• lectures with active student participation (explanation, discussion, questions, examples, problem solving) • tutorials where students will rehearse, revise and lit up notions, methods encountered at lectures • home work and project work: with them will students by individual work consolidate knowledge obtained at lectures and tutorials • mid-term examinations will stimulate students to study the matter dealt with at lectures and tutorials simultaneously

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): • ustni izpit • pisni izpit Namesto pisnega izpita lahko študent opravi obveznosti predmeta z domačimi nalogami in sprotnim delom (kolokviji, kvizi). Za pristop k ustnemu izpitu je potrebno s pisnim izpitom ali s sprotnim delom zbrati vsaj 51% možnih točk.	 30 70	Type (examination, oral, coursework, project): • oral exam • written exam Written exam can be replaced with homeworks and intermediate work (mid-term examinations, quizzes). As a prerequisite for the oral examination student must gain at least 51 % of possible points with intermediate work or with written exam. .