UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Uvod v kriptografijo in prostorsko geometrijo
Course title:	Introduction to Criptography and Spatial Geometry

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Informatika v sodobni družbi, visokošolski strokovni študijski program prve stopnje	-	Drugi ali tretji	Četrti ali šesti
Informatics in Contemporary Society, first cycle Professional Study Programme	-	Second or third	Fourth or sixth

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	1-ISD-VS-IP-UKPG-2020-05-14

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

Nosilec predmeta / Lecturer:	pred. mag. Matjaž Praprotnik

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

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisits:**
Pogoj za vključitev v delo je vpis v 2. oz. 3. 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. Student has to pass all requirements given at the exercises before examination.

Vsebina:	**Content (Syllabus outline):**
• *Prostorska geometrija:* Vektorska algebra, točke v prostoru, koordinatni sistemi, vektorske operacije v koordinatnih sistemih, matematični zapis krivulj, ploskev, teles in zlepkov v ravnini in prostoru, geometrija s topologijo, projektivna geometrija. Geometrija in računalnik, prostorski podatki in informacije, podatkovne zbirke. • Matematični temelji kriptografije:	• Spatial geometry: Vector algebra, points in the space, coordinate systems, vector operations in coordinate systems, mathematical expresions of curves and surfaces in plane and space, geometry with topology, projective geometryGeometry and computers, spatial data, databases. • Mathematical fundamentals of cryptography:

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, identifikcija, autentifikacija, 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), generiranje naključnih števil in eliptične krivulje, teoretična varnost teh algoritmov.	Complexity theory, basic number theory, factorization of integers, generation of prime numbers, discrete algorithms in finite fields, probablity. • Introduction to cryptography: History of cryptography, cryptographic techniques and protocols, (key generation and exchange, indentification, autentification, 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), random numbers, elliptic curves, theoretical security of these algorithms.

Temeljni literatura in viri / Readings:

- Vidav, I. (1991). *Višja matematika I.*
- Stinson, D. & Paterson, M. (2019). *Cryptography: Theory and Practice* (4th ed.). New York: CRC press.
- Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. (2001). *Handbook of Applied Cryptography*. New York: CRC Press.
- Galbraith, S. (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press.

Cilji in kompetence:	**Objectives and competences:**
Učna enota prispeva k razvoju naslednjih splošnih in predmetno-specifičnih kompetenc: • poznavanje in razumevanje širokega nabora aplikacij informacijsko komunikacijske tehnologije v sodobni družbi • poznavanje in razumevanje interakcij med informacijsko komunikacijsko tehnologijo in sodobno družbo • razvoj in uporaba informacijsko komunikacijske tehnologije, sposobnosti in spretnosti v lokalnem in mednarodnem okolju • prizadevanje za kakovost strokovnega dela skozi avtonomnost, (samo)kritičnost, (samo)refleksivnost in (samo)evalviranje v strokovnem delu	The instructional unit contributes to the development of the following general and subject-specific competences: • knowledge and understanding of a wide range of applications of information communication technology in the modern society • knowledge and understanding of interactions between ICT and the modern society • development and the use of ICT, abilities and skills in local and international environment • striving to achieve quality of professional work through autonomy, (self) criticism, (self) reflexivity and (self) evaluation in professional work • ability to flexibly apply knowledge in practice

• sposobnost fleksibilne in aplikativne uporabe teoretičnega znanja • poznavanje tehnologij za spletno programiranje na strani klienta in strežnika ter razvoj aplikacij • sposobnost zapisati problem v obliki algoritma in pretvorba algoritma v računalniški program z uporabo sodobnih programskih orodij • razumevanje in uporaba računalniških sistemov in arhitektur	• knowledge of client and server side web programming technologies and applications development • the ability to write the problem in the form of an algorithm and converting the algorithm into a computer program using modern programming tools • understanding and use of computer systems and architectures

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Študent/študentka:* • spozna matematične temelje za opisovanje prostorskih informacij, ki so nujno potrebni za sposobnost ravnanja s prostorskimi podatki in izdelavo spletnih ter mobilnih rešitev, ki temeljijo na prostorskih podatkih • 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:* • gets mathematical basis for modelling the spatial data, which are necessary to be able to manage the spatial data and to develop web and mobile applications which rely on spatial data • acquire mathematical introduction into cryptography which is necessary to understand the concepts of cryptographic security • acquire 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. Ustnega izpita ni potrebno opravljati, kadar študent s pisnim izpitom zbere vsaj 85 % 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. Students who have gained at least 85 % with written exam are exempted from the oral examination.

Reference nosilca / Lecturer's references:

- PRAPROTNIK MATJAŽ (2016) Učinkovito generiranje eliptičnih krivulj za potrebe parjenj : magistrsko delo, Ljubljana.
- PRAPROTNIK MATJAŽ (2001) Kriptoanaliza urno-kontroliranega pomičnega registra : diplomsko delo, Ljubljana.