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 in univerzitetni študijski program prve stopnje	-	Drugi ali tretji	Četrti ali šesti
Informatics in Contemporary Society, first cycle Professional Study Programme and Academic Study programme	-	Second or third	Fourth or sixth

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	1-ISD-VS,UN-IP-UKPG-2016-10-01

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

Nosilec predmeta / Lecturer:	

Jeziki / Languages:	**Predavanja / Lectures:**	Slovenski, angleški / Slovene, English
	Vaje / Tutorial:	Slovenski, angleški / Slovene, 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 opravljen izpit iz predmeta Matematika 1 in Matematika 2. Študent/študentka mora pred pristopom k izpitu opraviti vse obveznosti na vajah.	Condition for participation is enrolment into 2nd or 3rd year of study and passed exam from Mathematics 1 and Mathematics 2. Student has to pass all requirements given at the exercises before examination.

Vsebina:	**Content (Syllabus outline):**
• Prostorska geometrija: geometrija in računalnik, vektorska algebra, točke v prostoru, koordinatni sistemi, vektorske operacije v koordinatnih sistemih, geometrija s topologijo, matematični zapis posebnih krivulj, zlepki, ploskve in telesa v ravnini in prostoru, prostorski podatki in informacije: mape, slike, podatkovne zbirke.	• Spatial geometry: geometry and computers, vector algebra, points in the space, coordinate systems, vector operations in coordinate systems, geometry with topology, mathematical expresions for special curves, splines, surfaces and bodies in plane and space. Spatial data, maps, figures, data sets.

• Matematični temelji kriptografije: teorija kompleksnosti, osnove teorije števil, problem iskanja razcepa števil, problem generiranja praštevil, diskretni algoritmi v končnih obsegih, naključna in psevdonaključna števila. • Uvod v kriptografijo:kriptografske tehnike in protokoli (generiranje in izmenjava ključev, identifikacija, autentifikacija, izmenjava skrivnosti, kriptografska zaščita podatkovnih zbirk), kriptografski algoritmi (DES, RSA algoritem, podpisne sheme, zgoščevalne funkcije, identifikacijske sheme), teoretična varnost teh algoritmov.	• Mathematical basics of cryptography: complexity theory, basics from number theory, factorization of integers, prime number generation, discrete algorithms in finite fields, random and pseudo random numbers. • Introduction to cryptography: cryptographic techniques and protocols, (key generation and exchange, indentification, autentification, secret exchange, criptographic protection of data basis), cryptographic algorithms (DES, RSA, digital signature scheme, hash functions, indentification schemes), theoretical security of these algorithms.

Temeljni literatura in viri / Readings:

- FRANK, ANDREW U. (2006): Practical Geometry - The Mathematics For Geographic Information Systems. Rokopis (dostopno na ftp://ftp.geoinfo.tuwien.ac.at/wilke/BUP_Skriptsammlungen/GeoInfo/Books/%5BFrank%5D_Practical_Geometry.pdf)
- HOFFSTEIN, JEFFREY, PIPHER, JILL IN SILVERMAN, JOSEPH H. (2008): An Introduction to Mathematical Cryptography, Springer-Verlag – Undergraduate Texts in Mathematics.
- SCHNEIER, BRUCE (1996): Applied cryptography : protocols, algorithms, and source code in C, John Wiley & Sons, New York.

Cilji in kompetence:	**Objectives and competences:**
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, (samo)refleksivnost in (samo) evalviranje v strokovnem delu • sposobnost fleksibilne uporabe znanja v praksi • sposobnost logičnega sklepanja, ocenjevanja velikostnega reda	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 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

rezultata, natančnosti izražanja, pisanja in razmišljanja

Predmetno-specifične kompetence:

- poznavanje matematičnega modela prostorskih podatkov
- sposobnost izvajanja računskih operacij in analiz nad prostorskimi podatki
- poznavanje matematičnih temeljev kriptografske varnosti
- poznavanje glavnih algoritmov in tehnik iz kriptografije

estimate the order of magnitude of the result, to be precise in at expressions, writing and thinking

Subject-specific competences:

- familiarity with the mathematical spatial data model
- ability to carry out computational operations and analyses of spatial data
- familiarity with mathematical basics of cryptographic security
- familiarity with the main algorithms and cryptographic techniques

Predvideni študijski rezultati:

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

Intended learning outcomes:

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:

- 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
- vaje v računalniški učilnici: pri teh vajah bodo študentje spoznali in preizkusili konkretne algoritme in programske rešitve za posamezno področje. te vaje bodo potekale v manjših skupinah, tako da bo imel vsak študent na razpolago en računalnik
- domače naloge in projektna naloga – z njimi bo študent preko samostojnega dela utrdil vse znanje, ki ga je pridobil na predavanjih in vajah

Learning and teaching methods:

- 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
- computer lab work where they will acquire and test some concrete algorithms for specific area. This work will take place in small groups with one computer available for each student
- 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

- *kolokviji:* z njimi bodo študentje stimulirani, da sproti študirajo snov, ki bo obravnavana na predavanjih in vajah	at lectures and tutorials simultaneously

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
- ustni izpit	30	- oral exam
- pisni izpit ali sprotno delo: kolokviji, kvizi, domače naloge	70	- written exam or intermediate work: mid-term examinations, quizzes, homeworks
Kdor s sprotnim delom ali s pisnim izpitom zbere vsaj 51 % možnih točk, lahko pristopi k ustnemu izpitu.		As a prerequisite for the oral examination student must gain at least 51 % of possible points with intermediate work or with written exam.
Ustnega izpita je oproščen, kdo s pisnim izpitom ali sprotnim delom zbere vsaj 70 % točk in je bil vsaj 50 % na predavanjih.		Students who have gained at least 70 % with intermediate work or written exam and have participated at least 50 % of lectures are exempt from the oral examination.