UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Aplikativna kriptografija
Course title:	Applied 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 ali tretji	Četrti ali šesti
Computer Science and Web Technologies, first cycle Professional Study Programme	-	Second or third	Fourth or sixth

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	2-RST-VS-IP-AKrip-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:**
Opravljen izpit Uvod v kriptografijo in prostorsko geometrijo.	Passed exam Introduction to Cryptography and Spatial Geometry.

Vsebina:	**Content (Syllabus outline):**
• *Uvod*: Uvod v kriptografijo, simetrična in asimetrična kriptografija, javna kriptografija, RSA, Eliptične krivulje, digitalni podpisi. • Generatorji naključnih in psevdo naključnih števil (Blum Blum Shub, Yarow), statistični testi, (Diehard).. Distribucija ključev, protokoli za dogovor o ključu (Diffie-hellman, STS, Kerberos, TLS). Infrastruktura javnih	• *Introduction:* Introduction cryptography, symmetric and asymmetric cryptography, public key cryptography, RSA, Elliptic curves digital signatures. • Random and pseudo random number (*Blum Blum Shub, Yarow)* generators, statistical test (Diehard). Key distribution, key agreement protocols (Diffie-Hellman, STS, Kerberos, TLS). Public Key Infrastructure (PKI), lifecycle of keys,

ključev (PKI) , življenjski cikel ključev, certifikati, certifikatne agencij, časovno žigosanje. • *Drugi kriptografski protokoli:* sheme za deljenje skrivnosti, sheme za identifikacijo oseb in naprav (izziv/odgovor, dokaz brez razkritja znanja,...), grb/cifra po telefonu, miselni poker, kriptografija na podlagi identitete, verižni podpisi in večpartitni protokoli.	digital certificates, certificate authorities, timestamping. • *Other Cryptographic Protocols:* Secret sharing schemes, identification schemes (challenge/response, zero-knowledge proofs...), head/tails over phone, mental poker, identify based cryptography, ring signatures, multiparty protocols.

Temeljni literatura in viri / Readings:

- Ferguson, N., Schneier, B. & Kohno T. (2010). *Cryptography Engineering – Design Principles and Practical Applications*. Wiley Publishing Inc.
- Stinson, D. & Paterson, M. (2019). *Cryptography: Theory and Practice* (4th ed.). CRC Press.
- Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. (2001). *Handbook of Applied Cryptography.* New York: CRC Press.
- Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C.* New York: John Wiley & Sons.

Cilji in kompetence:	**Objectives and competences:**
Učna enota prispeva k razvoju naslednjih splošnih in predmetno-specifičnih kompetenc: *Splošne kompetence:* • usposobljenost za izvajanje vseh faz razvoja spletnih in mobilnih aplikacij: načrtovanje, razvoj, zagon, prodaja, vzdrževanje • obvladovanje postopkov zagotavljanja varnega in stabilnega delovanja spletnih in mobilnih aplikacij in sprotnega odpravljanja napak • sposobnost varnega in namenskega koriščenja najzahtevnejših spletnih storitev *Predmetno-specifične kompetence:* • poznavanje najpogostejših groženj varnosti in uporaba praktičnih postopkov za zagotavljanje varnosti informacijskega sistema • poznavanje glavnih algoritmov in tehnik iz kriptografije	*The instructional unit contributes to the development of the following general and subject-specific competences:* *General competences:* • competence to carry out all phases of development of web and mobile applications: planning, development, start-up, sales, maintenance • managing of all procedures of providing safe and stable web and mobile applications operation, and timely fixing of errors • ability to safely and purposefully use the most complex web services *Subject-specific competences:* • familiarity with the most frequent security threats and the use of practical procedures ensuring information system securit • familiarity with the main algorithms and cryptographic techniques

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Študent/študentka:* • pozna ključne algoritme in tehnike s področja kriptografije • pozna jih z vidika teoretične varnosti kakor tudi z vidika praktičnega zagotavljanja varnosti s programskimi rešitvami, ki temeljijo na teh teoretičnih konceptih	Knowledge and understanding: *The student:* • is familiar with algorithms and techniques relating to the field of cryptography and • her/his knowledge shall encompass theoretical security aspects as well as aspects related to providing security in practice based on the theoretical concepts

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • *vaje* v računalniški učilnici: pri teh vajah bodo študentje spoznali in preizkusili konkretne kriptografske algoritme in programske rešitve za posamezen algoritem oz. tehniko. 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	• *lectures* with active student participation (explanation, discussion, questions, examples, problem solving) • *tutorials* in computer lab (laboratory practice) allow the students to get to know and test specific cryptographic algorithms and program solutions for individual algorithm or technique. The tutorials will be performed in small groups, allowing each student to have access to own computer • *home assignments* and *project* will allow students to strengthen knowledge acquired during lectures and tutorials through individual work

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
• projektna naloga • zagovor in predstavitev projektne naloge	70 30	• project assignment • defense and presentation of project assignment

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.