UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Uporabna kriptografija
Course title:	Applied Cryptography

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Kibernetska varnost, magistrski študijski program druge stopnje	-	Prvi	Drugi
The second cycle masters study programme Cyber Security	-	First	Second

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	5-KV-MAG-IP-UK-2022-06-10

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
20	/	30	/	/	100	5

Nosilec predmeta / Lecturer:	Izr. prof. dr. Borut Lužar

Jeziki / **Languages:**	**Predavanja / Lectures:**	Slovenski / Angleški
	Vaje / Tutorial:	Slovenski / Angleški

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**

Pogoj za vključitev v delo je poznavanje osnov algebre, verjetnostnega računa in statistike.	Fundamental knowledge of algebra, probability and statistics.

Vsebina:	**Content (Syllabus outline):**
• Uvod v kriptografijo (osnove, Kerckhoffs-ov princip, kriteriji varnosti, tipi napadov). • Simetrične šifre (temeljni principi, bločne šifre (AES), tokovne šifre (RC4, ChaCha20), načini šifriranja, primeri uporabe). • Zgoščevalne funkcije (kriptografske zgoščevalne funkcije (SHA256), MAC, avtentikacija in šifriranje (AES-GCM), primeri uporabe). • Asimetrične šifre oz. javna kriptografija (temeljni principi, RSA in teorija števil, Eliptične krivulje in končni obsegi, primeri uporabe). • Digitalni podpisi (DSA, ECDSA, primeri uporabe). • Protokoli za dogovor o ključu in upravljanje s ključi (klasifikacija, Diffie-Hellman, Kerberos, STS, PKI, digitalna potrdila, kriptografija na podlagi identitete, primeri uporabe). • Generatorji naključnih števil (temeljni principi, primeri uporabe). • Uporaba kriptografije v praksi (TLS/SSL, WPA, GSM, 2FA – FIDO, P2PE in E2EE, Blockchain).	• Introduction to cryptography (basic principles, Kerckhoffs-ov principle, security criteria, types of attack). • Symmetric-key encryption (basic principles, block ciphers (AES), stream ciphers (RC4, ChaCha20), modes of operation, use cases). • Hash functions (cryptographic hash functions (SHA256), MAC, authenticated encryption (AES-GCM), use cases). • Public-key encryption (basic principles, RSA and number theory, Elliptic curves and finite fields, use cases). • Digital signatures schemes (DSA, ECDSA, use cases). • Key establishment protocols and key management (classification, Diffie-Hellman, Kerberos, STS, PKI, digital certificates, identity-based cryptography, use cases). • Random number generators (basic principles and examples of RNG, use cases).) Deployed cryptography (TLS/SSL, WPA, GSM, 2FA – FIDO, P2PE, and E2EE, Blockchain).

Temeljni literatura in viri / Readings:

- D. Stinson: Cryptography - Theory and Practice, 4th edition, CRC Press, 2018.
- J. Katz, Y. Lindell: Introduction to Modern Cryptography, 3rd edition, Chapman & Hall/CRC Cryptography and Network Security Series, 2020.
- S. D. Galbraith: Mathematics of Public Key Cryptography, Cambridge University Press, 2012.
- N. Ferguson, B. Schneier, T. Kohno: Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.
- B. Schneier: Applied cryptography: protocols, algorithms, and source code in C. New York: John Wiley & Sons, 1996.
- A. J. Menezes, P. C. Van Oorschot, S. Vanstone: Handbook of Applied Cryptography. New York: CRC Press, 1996.

- J. W. Lawrence, F. A. Zorzitto: Abstract Algebra - A Comprehensive Introduction, Cambridge University Press, 2021.

Cilji in kompetence:

Splošne kompetence:

- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.
- Sposobnost pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti.
- Poznavanje pomena kakovosti in prizadevanje za kakovost strokovnega dela skozi avtonomnost, samoiniciativnost, (samo)kritičnost, (samo)refleksivnost in (samo)evalviranje.

Predmetno-specifične kompetence:

- Poznavanje temeljnih principov kriptografije.
- Poznavanje kriptografskih algoritmov in njihove uporabe.
- Sposobnost primerjave in izbire primernih kriptografskih algoritmov za praktično uporabo.

Objectives and competences:

General competences:

- The ability of flexible usage of the acquired knowledge on cyber security in practice.
- The ability to obtain, select, analyse information, as well as to interpret them to comprehensively solve problems, challenges and incidents in the field of cyber security.
- Knowledge of the importance of quality and striving for the quality of professional work through autonomy, self-initiative, as well as (self-) criticism, (self-) reflection, and (self-) evaluation.

Subject-specific competences:

- Knowledge of cryptography principles.
- Knowledge of cryptographic algorithms and use cases.
- Ability to compare and choose suitable cryptographic algorithm for practical use

Predvideni študijski rezultati:

Študenti bodo:

- sposobni razumeti ključne kriptografske principe in tehnike.
- spoznali moderne kriptografske algoritme.
- znali uporabiti ustrezne kriptografske algoritme v praksi.
- znali ovrednotiti varnost uporabljenih kriptografskih algoritmov.

Intended learning outcomes:

Students will:

- be able to understand cryptographic principles and technics.
- get acquainted with modern cryptographic algorithms.
- know how to use suitable cryptographic algorithms for given use cases.
- know how to assess the security of used cryptographic algorithms.

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri); • *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih in kjer rešujejo različne konkretne probleme.	• *Lectures with active participations by the students* (explanation, discussion, questions, cases); • *Tutorials*, where students will recall, reinforce, and shed light on the concepts and methods introduced at lectures and where they will solve various concrete problems.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
• Domače naloge	50 %	Home assignments
• Projektna naloga	50%	Project assignment

Reference nosilca / Lecturer's references:

- B. Lužar, M. Mockovčiaková, R. Soták: Note on list star edge-coloring of subcubic graphs, J. Graph Theory 90(3) (2019), 304-310.
- F. Dross, B. Lužar, M. Maceková, R. Soták: Note on 3-choosability of planar graphs with maximum degree 4, Discrete Math. 342(11) (2019), 3123-3129.
- B. Lužar, M. Mockovčiaková, P. Ochem, A. Pinlou, R. Soták: On non-repetitive sequences of arithmetic progressions: the cases $k \in \{4,5,6,7,8\}$, Discrete Appl. Math. 279 (2020), 106-117.
- M. Šurimová, B. Lužar, T. Madaras: Adynamic coloring of graphs, Discrete Appl. Math. 284 (2020), 224-233.
- K. Rojko, B. Bratić, B. Lužar: The Bologna reform's impacts on the scientific publication performance of Ph.D. graduates - the case of Slovenia, Scientometrics 124 (2020), 329-356.
- P. Holub, B. Lužar, E. Mihaliková, M. Mockovčiaková, R. Soták: Star edge-coloring of square grids, Appl. Math. Comput. 392 (2021), 125741.
- A. Hinz, B. Lužar, C. Petr: The Dudeney-Stockmeyer Conjecture, Discrete Appl. Math. (2021).
- B. Lužar, E. Máčajová, M. Škoviera, R. Soták: Strong edge colorings of graphs and the covers of Kneser graphs, J. Graph Theory (2022).
- K. Rojko, B. Lužar: Scientific performance across research disciplines: Trends and differences in the case of Slovenia, J. Informetrics 16(2) (2022), 101261.
- H. La, B. Lužar, K. Štorgel: Further extensions of the Grötzsch Theorem, Discrete Math. 345 (2022), 112849.