| UČNI NAČRT PREDMETA / COURSE SYLLABUS | | | |
|---|---|---|---|
| **Predmet:** | Kriptografija in računalniška varnost | | |
| **Course title:** | Cryptography and computer security | | |

| **Študijski program in stopnja**<br>**Study programme and level** | **Študijska smer**<br>**Study field** | **Letnik**<br>**Academic year** | **Semester**<br>**Semester** |
|---|---|---|---|
| Interdisciplinarni magistrski študijski program Računalništvo in matematika | ni smeri | 1 ali 2 | prvi ali drugi |
| Interdisciplinary Masters study programme Computer Science and Mathematics | none | 1 or 2 | first or second |

| | |
|---|---|
| **Vrsta predmeta / Course type** | izbirni |
| | |
| **Univerzitetna koda predmeta / University course code:** | M2837 |

| **Predavanja**<br>**Lectures** | **Seminar**<br>**Seminar** | **Vaje**<br>**Tutorial** | **Klinične vaje**<br>**work** | **Druge oblike študija** | **Samost. delo**<br>**Individ. work** | **ECTS** |
|---|---|---|---|---|---|---|
| **45** | **10** | **20** | | | **105** | **6** |

| | |
|---|---|
| **Nosilec predmeta / Lecturer:** | prof. Aleksandar Jurišić |

| | | |
|---|---|---|
| **Jeziki / Languages:** | **Predavanja / Lectures:** | slovenski/Slovene, angleški/English |
| | **Vaje / Tutorial:** | slovenski/Slovene, angleški/English |

| **Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:** | **Prerequisites:** |
|---|---|
| | |
| **Vsebina:** | **Content (Syllabus outline):** |

| | |
|---|---|
| Informacijska/računalniška varnost opisuje vse preventivne postopke in sredstva s katerimi zagotovimo dostop do informacijskih sistemov in njihove vsebine ter preprečimo njihovo nepooblaščeno uporabo. Med preventivnimi ukrepi nudi kriptografija največjo varnost oziroma zaščito glede na svojo prilagodljivost digitalnim medijem in s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, digitalno overjanje/ podpisovanje, digitalni denar, in drugi kriptografski protokoli, obseg: matematika, računalništvo, elektrotehnika, finance, politika, obramba, itd.). Vsebina bo med drugim zajemala naslednje teme:• Simetrična kriptografija– Klasični tajnopisi in zgodovina kriptografije– Kerckhoffov princip in stopnje napadov na kriptosisteme.– Shannonova teorija informacij in entropija (popolna, računska in dokazljiva varnost)– Bločne šifre (DES/IDEA, AES in finalisti, linearna in diferenčna analiza)– Tokovne šifre/PRNG (RC4, LFSR in Berlekamp-Masseyjev algoritem, ...),– Kriptoanaliza in statistične metode– Zgoševalne funkcije (MD/SHA, HMAC ...) in kode za avtentikacijo (MAC), napadi s paradoksom rojstnih dni, novi napadi, ...• Kriptografija javnih ključev oziroma asimetična kriptografija– Popolna varnost (računska, brezpogojna, dokazljiva)– Kriptosistemi z javnimi ključi, enosmerne funkcije in z njimi povezani problemi iz teorije števil (testiranje praštevilskosti, faktorizacija števil, diskretni logaritem)– Digitalni podpisi (RSA, DSA, enkratni, slepi, skupinski, itd.)– Protokoli za dogovor o ključu (Diffie-Hellman, ElGamal, Kerberos, STS)– Sheme za identifikacijo oseb in naprav (izziv/odgovor ...)– Drugi protokoli (grb/cifra po telefonu, mentalni poker, sheme za deljenje skrivnosti, kode za overjanje, časovni žigi, vizualna kriptografija, dokaz brez razkritja znanja)– Kvantna kriptografija• Računalniška varnost– Varnost programov (hrošči, virusi, zlonamerna koda)– Varnost podatkovnih baz (anonimizacija)– Varnost | Information/Computer Security describes all preventive measures, procedures and means to ensure access to Information Systems and their contents in order to prevent their unauthorized use. Cryptography provides maximum security while at the same time preserve the flexibility of digital media. It forms the foundation of Information Society (objectives: privacy, data integrity, digital authentication/signatures, digital cash, and other cryptographic protocols, it covers: Mathematics, Computer Science, Electrical Engineering, Finances, Policy, Defense, etc.). The course will cover the following topics:<br>• Symmetric cryptography<br><br>– Classical Ciphers and History of Cryptography<br><br>– Kerckhoff Principle and various attacks on cryptosystems<br><br>– Shannon Theory of Information and Entropy (Perfect, Computational and Provable Security)<br><br>– Block Ciphers (DES/IDEA, AES and finalists, Linear and Differential Analysis)<br><br>– Stream Ciphers/PRNG (RC4, LFSR and Berlekamp-Massey algorithm,...),<br><br>– Cryptoanalysis, Statistical Methods<br><br>– Hash Functions (MD/SHA, HMAC...)<br><br>and Authentication Codes (MAC),<br><br>Birthday Paradox Attacks, new attacks,...<br><br>• Public-key cryptography (Asymmetric Cryptography)<br><br>– Perfect Security (Computational,<br><br>Unconditional and Provable Security)<br><br>– Public-Key Cryptosystems, One-Way |

| | | |
|---|---|---|
| operacijskih sistemov (MS Win, Unix/Linux, liveCD)– Varnost mrežnih komunikacij (požarni zidovi, VPN, IPSec, SSL)– Zasebnost v računalništvu (žetoni/pametne kartice, RFID kartice)– Upravljanje s ključi (certifikati, CA, PKI, X.509)– Učinkovite in varne implementacije kriptosistemov (napadi s stranskim kanalom in obramba pred njimi)– Upravljanje varnosti v praksi (varnostne politike, nadzor)– Patenti in standardi (ISO, IEEE, IETF) | | Functions and related problems in Number Theory (Primality Testing, Integer<br><br>Factorization, Discrete Logarithem Problem)<br><br>– Digital Signatures (RSA, DSA, one-time, blind, group etc.)<br><br>– Key Agreement Protocols (Diffie-Hellman, ElGamal, Kerberos, STS)<br><br>– Identification Schemes for humans and devices (challenge/response...)<br><br>– Other protocols (head/tail over the phone, mental poker, Secret Sharing Schemes, Authentication Schemes, Timestamps, Visual Cryptography, Zero-Knowledge Proofs)<br><br>– Quantum Cryptography<br><br>• Computer/information security<br><br>– Security of programs (bugs, viruses,<br><br>malicious code)<br><br>– Security of databases (anonymization)<br><br>– Security of OS (MS Win, Unix/Linux, liveCD)<br><br>– Security of network communication<br><br>(firewalls, VPN, IPSec, SSL)<br><br>– Privacy in Computer Science (tokens/smart cards, RFID cards)<br><br>– Key management (certificates, CA, PKI, X.509)<br><br>– Efficient and secure implementations of cryptosystems (sidechanell<br><br>attacks and defenses against them) |

| | |
|---|---|
| | – Real time security management<br><br>(security policy, monitoring)– Patents and standards (ISO, IEEE, IETF) |

**Temeljni literatura in viri / Readings:**

– D. Stinson, Cryptography: Theory and Practice, tretja izdaja, Chapman and Hall/CRC, 2006.– A. Menezes, P. van Oorschot in S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997 (peti ponatis 2001).– C.P. Pfleeger in S.L. Pfleeger, Security in Computing, četrta izdaja, Prentice Hall, 2006.

| **Cilji in kompetence:** | **Objectives and competences:** |
|---|---|
| Študent se spozna z osnovami kriptografije in računalniške varnosti. | Introduction to Cryptography and Computer Security. |

| **Predvideni študijski rezultati:** | **Intended learning outcomes:** |
|---|---|
| Po uspešnem zaključku tega predmeta bo študent:<br>- razumel osnovne probleme računalniške varnosti in v podrobnosti delovanje najbolj znanih<br><br>kriptosistemov sistemov ter bo sposoben povezovati obe področji, predlagati rešitve in<br><br>implementirati oziroma vzdrževati kriptografske sisteme,<br><br>- znal uporabiti oz. bil sposoben opredeliti (definirati) problem, pravilno ovrednotiti s<br><br>strokovnega vidika (tako s kriptografskega kot varnostnega) ter predlagati/ovrednotiti | After successful completition of this course the students will be able to:<br>- master the basic problems of computer security and the detailed structure of the most famous<br><br>cryptosystems and will be capable to connect these areas, propose specific solutions and implement or maintain cryptosystems,<br><br>- apply, i.e., be able to define the problem, correctly evaluate it from a professional point of view (both<br><br>cryptographic and security) and to propose/evaluate an effective solution, |

| | |
|---|---|
| učinkovito<br><br>rešitev,<br><br>- razumel uglašenosti med teorijo in njeno rabo na konkretnih primerih računalniške varnosti.<br><br>Predmet je osnova za številne predmete, ki preučujejo računalniške sisteme in mreže,<br><br>(tele)komunikacijo, digitalno forenziko, elektronsko in mobilno poslovanje,... Med pridobljene<br><br>spretnosti štejejo teoretične osnove za inženirsko reševanje različnih praktičnih problemov, ki se pojavljajo v problemih iz računalniške varnosti in kriptografije. | - understand the connection between theory and practice applied to specific examples of computer<br><br>security.<br><br>This course is a foundation for several courses that study computer systems and networks,<br><br>telecommunications, digital forensics, electronic and mobile commerce, etc. Students will gain a<br><br>theoretical foundation for a variety of practical problems that are encountered in the field of computer security and cryptography. |

| **Metode poučevanja in učenja:** | **Learning and teaching methods:** |
|---|---|
| Predavanja, vaje, domače naloge, seminarji, konzultacije, laboratorijsko delo. Poseben poudarek je na sprotnem študiju in na skupinskem delu pri vajah in seminarjih. Ogledali si bomo tudi kakšen video. | Lectures, tutorials, assignments, seminars, office hours, lab work. There will be a special emphasis on real-time studies and team work (tutorials and seminars). We will occasionally watch a video material related to the course material. |

| **Načini ocenjevanja:** | Delež (v %) / Weight (in %) | **Assessment:** |
|---|---|---|
| Način (pisni izpit, ustno izpraševanje, naloge, projekt):<br>Sprotno preverjanje (domače naloge, kolokviji in projektno delo)<br><br>Končno preverjanje (pisni in ustni izpit)<br><br>Ocene: 6-10 pozitivno, 5 negativno (v skladu s Statutom UL) | 50%<br>50% | Type (examination, oral, coursework, project):<br>Continuing (homework, midterm exams, project work)<br><br>Final (written and oral exam)<br><br>Grading: 6-10 pass, 5 fail (according to the rules of University of Ljubljana) |

**Reference nosilca / Lecturer's references:**

Aleksandar Jurišić:

– JURIŠIĆ, Aleksandar, KOOLEN, Jack. A local approach to 1-homogeneous graphs. Designs, codes and cryptography, ISSN 0925-1022, 2000, let. 21, str. 127-147 [COBISS.SI-ID 10205017]

– JURIŠIĆ, Aleksandar, KOOLEN, Jack, TERWILLIGER, Paul. Tight distance-regular graphs. Journal of algebraic combinatorics, ISSN 0925-9899, 2000, vol. 12, no. 2, str. 163-197 [COBISS.SI-ID 10277465]

– JURIŠIĆ, Aleksandar. AT4 family and 2-homogeneous graphs. Discrete Mathematics, ISSN 0012-365X. [Print ed.], 2003, vol. 264, no. 1-3, str. 127-148 [COBISS.SI-ID 12515673]

– JURIŠIĆ, Aleksandar, KOOLEN, Jack. Distance-regular graphs with complete multipartite [mu]-graphs and AT4 family. Journal of algebraic combinatorics, ISSN 0925-9899, 2007, vol. 25, no. 4, str. 459-471 [COBISS.SI-ID 14370393]

– BROUWER, Andries E., JURIŠIĆ, Aleksandar, KOOLEN, Jack. Characterization of the Patterson graph. Journal of algebra, ISSN 0021-8693, 2008, vol. 320, iss. 5, str. 1878-1886 [COBISS.SI-ID 14632537]

– JURIŠIĆ, Aleksandar, KOOLEN, Jack. Classification of the family AT4(qs,q,q) of antipodal tight graphs. Journal of combinatorial theory. Series A, ISSN 0097-3165, 2011, vol. 118, iss. 3, str. 842-852 [COBISS.SI-ID 15875417]