|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. Course title:** Information and data security | | | | |
|  | | | | |
| **2. Code:** | | **3. Type (lecture, practice etc.):** lecture | | |
|  | | | | |
| **4. Contact hours:** 3 hoursper week | | **5. Number of credits (ECTS):** 3 | | |
|  | | | | |
| 6. Preliminary conditions (max. 3): | | | | |
|  | | | | |
| **7. Announced:** fall semester, spring semester, both | | | | |
|  | | | | |
| **8. Limit for participants:** 150 | | | | |
|  | | | | |
| **10. Responsible teacher (faculty, institute and department):**  Dr. Mátyás Koniorczyk (Faculty of Science, Institute of Mathematics and Informatics, Department of Applied Mathematics) | | | | |
|  | | | | |
| 11. Teacher(s) and percentage: | | ? | | 100% |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | | | | |
| **12. Language:** English | | | | |
|  | | | | |
| 13. Course objectives and/or learning outcomes:  Objectives:  The aim of the course is to understand the importance, basic concepts and techniques of information and data security, cybersecurity and cryptography.  Learning outcomes: students completing the course will  *have a knowledge* on the basic concepts of information and data security, cybersecurity and cryptography.They use the suitable professional vocabulary of the topic.  They will be *able* to apply and evaluate solutions related to the topic.  They will be *open* and *intend* to extend their knowledge in the field, respect the rules of cybersecurity. | | | | |
|  | | | | |
| 14. Course outline   1. Basics of information and data security. Legal aspects of information and data security. 2. Cryptography and cryptology. Areas and methods of the field. 3. Symmetric-key cryptography DES and AES. 4. Basics of public-key cryptography. RSA. 5. Discrete logarithm-based ciphers. Diffie-Hellman key exchange 6. Digital signatures and authentication. Hash functions. 7. Protocols 8. Examples: the ssh protocol 9. Examples: encrypted webpages 10. Network security. Firewalls and their use. 11. Security of wireless networks. 12. Selected topics in cybersecurity. 13. Selected topics in cybersecurity. | | | | |
|  | | | | |
| **15. Mid-semester works**  Lectures have to be attended. | | | | |
|  | | | | |
| **16. Course requirements and grading**  The semester concludes in a standard colloquium. | | | | |
|  | | | | |
| 17. List of readings   1. Christof Paar, Jan Pelzl: Understanding Cryptography. A Textbook for Students and Practitioners, Springer Berlin-Heidelberg, 2010. ISBN: 978-3-642-44649-8 (Print) 978-3-642-04101-3 (Online) 2. James Graham, Ryan Olson, Rick Howard (eds.:) Cyber Security Essentials, Auerbach Publications; 1 edition (2010). | | | | |
|  | | | | |
| 18. Recommended texts, further readings   1. Bruce Scheiner: Applied Cryptography, 2nd ed., Wiley 2015, Print ISBN: 9780471128458 Online ISBN: 9781119183471 2. Wiliam Stallings: Cryptography and Network Security: Principles and Practice (7th Edition), Pearson, 2016., ISBN: 0134444280 | | | | |
|  | | | | |
| **Date** | 13 April, 2017 | **Prepared by** |  | |
| Dr. Mátyás KONIORCZYK  responsible teacher | |
|  | | | | |
| **Endorsed by** | | |  | |
| XXX program supervisor | |