4

**Aktuelle Modulbeschreibung**

|  |  |
| --- | --- |
| **Module Number:** | **11859** |
| **Module Title:** | **Cryptography** |
|  | Kryptographie |
| **Department:** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member:** | * Prof. Dr. rer. nat. habil Meer, Klaus * Prof. Dr. rer. nat. habil. Köhler, Ekkehard |
| **Language of Teaching / Examination:** | English |
| **Duration:** | 1 semester |
| **Frequency of Offer:** | Every summer semester |
| **Credits:** | 8 |
| **Learning Outcome:** | The students should   * know relevant symmetric and asymmetric crypto systems * understand the mathematics relevant for desgining and analyzing crypto systems * be able to explain and use the most important approaches to cryptography * gain the ability to understand state-of-the-art scientific work in the area of cryptography |
| **Contents:** | * Mathematical Foundations relevant in the context of cryptography, including basic number theory, finite fields, polynomial rings, factorization * elementary crypto systems * Symmetric Cryptosystems DES and AES * public key cryptography, RSA - discrete logarithm, elliptic curve systems * secure signature and authentication methods * security of crypto systems * zero knowledge proofs * complexity theoretic aspects |
| **Recommended Prerequisites:** | Basic knowledge about discrete mathematics and linear algebra, for example as covered by the modules   * 11101: Linear Algebra and Analytical Geometry I * 11102: Linear Algebra and Analytical Geometry II   or   * 11112: Mathematics IT-1 (Discrete Mathematics) * 11113: Mathematics IT-2 (Linear Algebra) |
| **Mandatory Prerequisites:** | None |
| **Forms of Teaching and Proportion:** | * Lecture / 4 Hours per Week per Semester * Exercise / 2 Hours per Week per Semester * Self organised studies / 150 Hours |
| **Teaching Materials and Literature:** | **Books in English**   * G. Baumslag, B. Fine, M. Kreuzer, G. Rosenberger: A Course in Mathematical Cryptography, De Gruyter, 2015 * J. Hoffstein, J. Pipher, J.H. Silverman: An Introduction to Mathematical Cryptography, 2nd Edition, Springer 2014. * D.R. Stinson: Cryptography: Theory and Practice, CRC, 1995   **Books in German**   * V. Diekert, M. Kufleitner, G. Rosenberger: Diskrete Algebraische Methoden, De Gruyter 2013 |
| **Module Examination:** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination:** | * Written examination, 90 minutes, **OR** * Oral examination, 30 - 45 minutes, (in case of a small number of participants)   In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination:** | Performance Verification – graded |
| **Limited Number of Participants:** | None |
| **Part of the Study Programme:** | * M.Sc. / Angewandte Mathematik (research-oriented profile) / Prüfungsordnung 2008 * M.Sc. / Cyber Security (research-oriented profile) / Prüfungsordnung 2017 * Abschluss im Ausland / Informatik / keine Prüfungsordnung * M.Sc. / Informatik (research-oriented profile) / Prüfungsordnung 2008 - 2. SÄ 2017 * M.Sc. / Informations- und Medientechnik (research-oriented profile) / Prüfungsordnung 2017 * B.Sc. / Mathematik (research-oriented profile) / Prüfungsordnung 2007 * B.Sc. / Wirtschaftsmathematik (research-oriented profile) / Prüfungsordnung 2007 |
| **Remarks:** | * Study programme Cyber Security M. Sc.: Mandatory module in complex "Cyber Security Basics". * Study programme Applied Mathematics M. Sc.: This module is part of the complex "Mathematics Enhancement". * Study programme Information and Media Technology M. Sc.: This module is part of the complex "Fundamental Methods". * Study programme Computer Science M. Sc.: Compulsory elective module in "Mathematics" or in field of application "Mathematics". |
| **Module Components:** | * Lecture: Cryptography * Accompanying exercises * Related examination |
| **Components to be offered in the Current Semester:** | * no assignment |