HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

ACA - Angewandte Kryptanalyse

ACA - Applied Cryptanalysis

General information	
Module Code	ACA
Unique Identifier	ApplCryptAna-01-MA-M
Module Leader(s)	Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de)
Lecturer(s)	Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de)
Offered in Semester	Wintersemester 2025/26
Module duration	1 Semester
Occurrence frequency	Regular
Module occurrence	In der Regel im Wintersemester
Language	Englisch
Recommended for international students	Yes
Can be attended with different study programme	No

Curricular relevance (according to examination regulations)
Study Subject: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Study Specialization: Elektrische Energietechnik Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Study Specialization: Kommunikationstechnik und Embedded Systems Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Study Specialization: Mechatronik Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Sc. - MCS - Computer Science (PO 2023, V1) Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Sc. - MIE - Information Engineering (PO 2022, V3) Module type: Wahlmodul Semester: 1, 2, 3

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
Students know selected cryptographic primitives as well as algorithms and can apply them in practice. They also know selected attack techniques and can apply them. This enables students to make a well-founded assessment of the security of the algorithms. On this basis, they can assess the security of security protocols used in practice.
Students master the ways of thinking used in modern cryptography. They deepen their knowledge in the field of mathematics and improve their programming skills by solving problems in cryptography.
They learn to discuss and debate problems of information security and cryptography for practical use with their fellow students.

Students critically reflect on the role of cryptanalysis within the broader context of IT security and responsible research practice. They justify their methodological approach to open-ended problems based on theoretical knowledge from cryptography and computer science. Through the analysis and application of attack techniques, they develop a realistic and professional understanding of the limits and responsibilities of designing secure systems. They are able to communicate their findings and reasoning to both technical and interdisciplinary audiences, and reflect on the societal implications of cryptographic (in)security, such as privacy, surveillance, and digital trust.

Content information

Content	Modern cryptography has become an integral part of our everyday lives. Everyone uses various Internet services, online banking, contactless payment, etc. on a daily basis and therefore services that would not be possible without cryptography. In addition to encrypting confidential information, cryptography has been reliably guaranteeing other security goals such as authenticity, integrity and non-repudiation for decades. Cryptanalysis is the science and practice of analysing and breaking cryptographic systems, for example to decrypt confidential information without knowledge of the secret key. In addition to analysing encryption schemes, cryptanalysis also includes other cryptographic mechanisms in order to identify and exploit their vulnerabilities. In this course, selected attack techniques against modern cryptographic methods (e.g., factoring or side-channel attacks), with a focus on encryption methods, are presented, discussed and applied. What options do attackers have to break RSA? How can schemes based on discrete logarithms, like the Diffie-Hellman key exchange, be attacked? And what does all of that effect the security of security protocols like TLS? These and many more questions will be answered in this course which will lead to a better understanding of what the term "secure encryption" means. Knowledge of the possibilities of attacks is a prerequisite for the secure practical use of cryptographic algorithms in security protocols or for their implementation.
Literature	Aumasson J.-P.: Serious Cryptography – A Practical Introduction to Modern Encryption, 2nd Edition, No Starch Press, 2025. Ferguson, N., B. Schneier and T. Kohno: Cryptography Engineering – Design Principles and Practical Applications, Wiley, 2010. Hoffstein, J., J. Pipher und J. H. Silverman: An Introduction to Mathematical Cryptography, 2nd Edition, Springer, 2014. Katz, J. und Y. Lindell: Introduction to Modern Cryptography, 3rd Edition, CRC Press, 2020. Knospe, H.: A Course in Cryptography, American Mathematical Society, 2019. Paar C. und J. Pelzl: Understanding Cryptography. A Textbook for Students and Practitioners, Springer, 2009. Stamp, M. und R. M. Low: Applied Cryptanalysis. Breaking Ciphers in the Real World, Wiley, 2007. Von zur Gathen, J.: CryptoSchool, Springer, 2015.

Teaching formats of the courses

Teaching format	SWS
Labor	2
Lehrvortrag	2

Workload

Number of SWS	4 SWS
Credits	5,00 Credits
Contact hours	48 Hours
Self study	102 Hours

Module Examination	
Examination prerequisites according to exam regulations	None
ACA - Laborprüfung	Method of Examination: Laborprüfung Weighting: 0% wird angerechnet gem. § 11 Absatz 2 PVO: Yes Graded: No Remark: Participation in 80% of the lab exercises.
ACA - Klausur	Method of Examination: Klausur Duration: 120 Minutes Weighting: 100% wird angerechnet gem. § 11 Absatz 2 PVO: No Graded: Yes Remark: In addition to the contents of the lectures, all contents of the lab exercises are also relevant for the exam.

Miscellaneous	
Recommended Prerequisites	Knowledge of cryptography from other courses is advantageous, but not a prerequisite for participation in the course. Students should be familiar with fundamental concepts from discrete mathematics and number theory, such as modular arithmetic, prime numbers, greatest common divisors, and basic group theory. A basic understanding of algorithms and their complexity is expected. Prior exposure to concepts like modular exponentiation, Euclidean algorithm, and finite fields is helpful but not mandatory. Students should have basic programming experience in any general-purpose language (e.g., Python, Java, C, etc.). No prior experience with SageMath or Jupyter Notebooks is required. Familiarity with basic control structures (loops, conditionals, functions) is expected, as cryptanalytic techniques will be implemented and explored in an interactive programming environment.