Module	**Blockchain Cryptography Basics**
Lecturer	Prof. Dr.-Ing. Sebastian Gajek
Language	English
Teaching Method	Lecture + practical exercises
Credit Points / Duration	0.25 ECTS / 4 Lectures of 90 minutes each
Attendance Requirements	Some basic math skills
Goals / Skills	Blockchain technologies make heavily use of cryptography to achieve a consensus, be it in a Proof-of-Work or Proof-of-Stake protocol as in Bitcoin or Ethereum. In order to understand the key principals behind the protocols, we explore the magic behind hash functions and digital signatures. Specifically, we dive into the mechanics of Elliptic Curve DSA (ECDSA) and the Keccak hash function family. The students will not only learn how the cryptographic primitives work, but also understand why they are secure.
Content	1. Short intro to Blockchain 2. Motivation for Hash Functions/Signatures 3. Math Basics (Groups, Elliptic Curves) 4. ECDSA 5. Keccak Hash Family
Media Used	Electronic presentation, blackboard illustrations, discussion, practical exercises
Suggested Reading	Jonathan Katz and Yehuda Lindell: Introduction to Modern Cryptography (2nd Edition)