Cryptography

**Course Description**

This course covers basic and targeted in-depth knowledge of cryptographic processes and the practical use of cryptographic systems. After an overview of cryptographic methods, hash functions, symmetric methods, and asymmetric methods are presented. The theoretical basics of selected procedures are taught and practically explained using simple examples. In addition, areas of application and application scenarios for cryptographic procedures are presented.

**Contents**

1. Protection Goals, Vulnerabilities, and Threats
   1. Protection Goals
   2. Vulnerabilities and Threats
2. Foundations of Cryptology and its Core Components
   1. Encoding
   2. Symmetrical Encryption
   3. Asymmetric Encryption
   4. One-way Functions and Cryptographic Hash Functions
3. Basic Cryptographic Applications
   1. Key exchange and Hybrid Processes
   2. Digital Signature
   3. Message Authentication Code
   4. Steganographic Methods
4. Authentication
   1. Passwords and Public-Key-Certificates
   2. Challenge-Response-Procedure and Zero-Knowledge-Procedure
   3. Biometric Methods
   4. Authentication in Distributed Systems
   5. Identities Through Smartcards
5. Security of Single Computers
   1. Malware and Cookies
   2. Some Special Features of Operating Systems
   3. Web Server Security
6. Security in Communication Networks
   1. Security Problems and Defense Concepts
   2. Internet Standards for Communication Security
   3. Identity and Anonymity
   4. Security in Mobile and Wireless Communications
7. Security in E-Commerce
   1. Email Security
   2. Online Banking and Online Payments
   3. Electronic Money
8. Secure Software Development
   1. Threat Modeling
   2. Secure Software Design
   3. Techniques for Safe Programming