Cryptography

Course code	student workload	credits (according to ECTS)	semester	frequency	duration
CIF61031	90 hours	4,5	Sem. 5 & 7	each odd-semester	16 meetings

1	Types of courses	contact hours	independent study	class size
	compulsory	63 hours	27 hours	40 students

5 Prerequisites for participation

Have completed Computational Mathematics

Have completed Information Security

2 Learning outcomes

IF-ILO-3

Graduates are able to develop professional careers in the field of computer science based on quality aspects, data-based decision making, be responsible, and make continuous improvements.

IF-ILO-7

Mastering the theoretical concept and principles of computer science, especially in the aspect of algorithms, programming, intelligent systems, information management, parallel and distributed computing, information security, human-computer interaction, software engineering, and fundamentals of computer systems and networks.

IF-ILO-11

Graduates are able to plan, develop, manage, and analyze the computer network-based system and the services running on top of them by considering the network security aspects.

3 Subject aims

Students are able to understand the mathematical basis used in cryptography

Students are able to understand the concept of cryptographic algorithms

Students are able to apply the basic concepts of cryptography to software

4 Teaching methods

lectures, case study, class discussion, presentation

6 Assessment methods

assignment, mid-term examination, end-term examination, project evaluation, practical-skill assessment

8 This module is used in the following degree programmes as well

10 Responsibility for module

11 Other information

Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) oleh Alfred J. Menezes,Paul C. van Oorschot), Scott A. Vanstone