1.	**Course title**	Cryptographic engineering
2.	**Course code**	БК-И-05
3.	**Semester**	9
4.	**Unit offering the course**	Faculty of Computer Science and Engineering
5.	**ECTS**	6
6.	**Goals of the study programme**	
	You learn the difference of implementations of security from secure implementationsYou learn how to implement a cipher on constrained platform i.e. a microcontroller and on an FPGA platformYou learn the practical side-channel cryptanalysis of various crypto implementations	
7.	**Contents of the study programme**	
	1. Introduction to techniques for fast and secure implementation of cryptographic software2. Modular arithmetics and finite field arithmetics3. Implementation aspects of symmetric key cryptography (AES, SHA)4. Implementation aspects of public key cryptography (RSA, ECC)5. Implementation aspects of lightweight cryptography6. Secure implementation of cryptographic primitives7. Side-channel attacks and countermeasures8. Cryptographic software packages	