1.	**Course title**	Provable security
2.	**Course code**	БК-И-03
3.	**Semester**	10
4.	**Unit offering the course**	Faculty of Computer Science and Engineering
5.	**ECTS**	6
6.	**Goals of the study programme**	
	To understand:§ The principles of security proofs§ Typical security models for various primitives§ Basic security reductions§ Necessary and sufficient assumptions for proofsTo become able to:§ Given a proof strategy, compute success of reduction§ Design a proof strategy from scratch§ Write full basic proofs§ Assess the soundness of a proof, spot irregularities§ Draw conclusions about impact of a proof	
7.	**Contents of the study programme**	
	1. Introduction to provable security2. The method of provable security3. Adversarial models4. Security assumptions and security reductions5. Game-based security6. Pseudo-random permutations and pseudo-random functions. One way functions7. Techniques of proving security in symmetric crypto8. Techniques of proving security in public key crypto	