Country	Institution	Course	ECTS
BULGARIA	Vasil Levski National Military University	**Cryptography**	**5.0**

Service	Minimum Qualification for Lecturers
All	• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG 6001 Level 2. • Adequate pedagogical and psychological competences. • Thorough knowledge of the topic taught.
Languages **English, Bulgarian**	

Prerequisites for international participants:	Goal of the Course:
• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. • The end of the 1st year of higher education.	• Investigate the security of encrypted data in communication and information systems. • Explore the role of hackers and code breakers influenced cryptography in modern secure communication. • To get an opportunity to try encrypting data yourself by completing cryptography challenge.

Learning outcomes		
	Knowledge	• The concepts used in early substitution and translation ciphers. • Symmetric key encryption systems and public key encryption systems. • Mathematical background of cryptography. • Stream ciphers. Pseudo-randomness and how to use it for encryption. • Essential techniques for survival and materials used for survival. • Block ciphers and some classic block-cipher constructions (DES, 3DES and AES). • Public-key cryptography. Public key encryption systems: one based on RSA functions and the other based on the Diffie-Hellman protocol.
	Skills	• Apply some early substitution and translation ciphers. • Distinguish symmetric key encryption systems from public key encryption systems. • Assess simple cryptographic methods from a practical viewpoint. • Apply some cryptographic ciphers by yourself to simple data.
	Competences	• Describe the concepts used in early substitution and translation ciphers. • Demonstrate the use of symmetric key encryption systems and public key encryption systems, and describe its advantages and disadvantages. • Assess simple cryptographic methods from a theoretical and practical viewpoint.

Verification of learning outcomes

- **Tests**: At the end of each topic of the course students must complete specific practice quiz.
- **Project:** Self design of some simple cryptographic cipher.

Course Details		
Main Topic	**Recommended WH**	**Details**
Introduction to Cryptography	10	• What is Cryptography and Cryptanalysis? • History of Cryptography. • Information Theoretic Security and the One Time Pad. • Encryption Systems. • Practice Quiz 1.
Mathematical Background to Cryptography	10	• Algebraic sets, groups and fields. • Galois Fields. • Extended Euclidian Algorithm. • Linear Recurrences. • Practice Quiz 2.
Symmetric key algorithms	12	• Pseudo-randomness. • Stream Ciphers. • Block Ciphers. • Practice Quiz 3.
Asymmetric key algorithms	12	• Public Key Encryption Systems Based on the Diffie-Hellman Protocol. • RSA Public Key Cryptographic System. • Other Public Key Encryption Systems. • Practice Quiz 4.
Additional hours to increase the learning and skills outcomes		
Self-Project	16	• Enhancing knowledge by studying specific cryptographic topics. • Enhancing skills by designing a simple cryptographic cipher.
Total	60	

This study course description is created and revised at “Computer Systems and Technology” Department and accepted at Faculty council.

Developed by:

prof. eng. ScD, PhD Zhaneta Savova

REFERENCES:

1. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.
2. Metcalf, Leigh, and William Casey. Cybersecurity and applied mathematics. Syngress, 2016.
3. Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2010.
4. Stallings, William, et al. Computer security: principles and practice. Upper Saddle River, NJ, USA: Pearson Education, 2017.
5. Yan, Song Y., Song Y. Yan, and Lagerstrom-Fife. Cybercryptography: Applicable Cryptography for Cyberspace Security. Springer International Publishing, 2019.