Course title	**APPLICATIONS OF CRYPTOGRAPHY**		
Course code	DET038		
Type of course	Elective – lectures and laboratory work		
Level of course	Advanced level course		
Year of study	First (I)	**Semester/trimester**	Second (2.)
ECTS (Number of credits allocated)	6 ECTS (Lectures 30 hours – 1 ECTS; laboratory work 30 hours – 1 ECTS; office hours, project assignment and independent study 120 hours – 4 ECTS)		
Name of lecturer	Ph.D. Tonko Kovačević, college professor		
Learning outcomes and competences	Students are trained for independent work in the practical application of cryptographic systems to protect the data and resources in information and communication systems.		
Prerequisites	None		
Course contents	Introduction to information security and cryptography. Basic concepts, basic security threats and security objectives. Cryptography based on symmetric (secret) key. Classical (historical) cryptosystems: permutation and substitution ciphers, Vigenere Code, Vernam code. Modern ciphers (DES, AES). Block and stream cipher (RC4). Generators of pseudo-random numbers. The main modes of modern codes (ECB, CBC, CFB, OFB, CTR mode). Cryptography based on asymmetric (public) key. RSA cryptosystem. Diffie-Hellman protocol for establishing a secret key. Authentication functions (cryptographic "hash" functions and MAC algorithms) and their applications. Advanced cryptographic protocols. Cryptography IPSec protocol. Web Security - Secure Socket Layer (SSL). Security of wireless networks (Wi-Fi security). Advanced authentication messages in wireless networks. Mechanisms for distributing cryptographic keys. Digital signatures and certificates. PKI infrastructure. The application of cryptography to protect databases.		
Recommended reading	*1.* J. Sen, *Applied Cryptography and Network Security*, InTech, 2012. 2. W. Stallings: *Cryptography and Network Security. Principles and Practice*, Prentice Hall, 2005.		
Supplementary reading	1. J. Menezes, P. C. Oorschot, S. A. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996. 2. A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007. 3. D. Stinson, *Cryptography Theory and Practice, 3rd Edition*, CRC Press 2005.		
Teaching methods	• Lectures, laboratory work and office hours		
Assessment methods	• End-of-semester tests • Seminar paper • Course attendance • Laboratory work		
Language of instruction	• Croatian • English		
Quality assurance methods	In accordance with: The Quality Assurance in Science and Higher Education Act, University of Split Book of Regulations, University Department of Professional Studies Rules of Procedure, and Ordinance on Teacher Professionalism, Quality Assurance and Evaluation		