Course Title	Cryptography				
Course Code	CYS625				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year/1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course introduces fundamental concepts of cryptography and its uses in cyber and information security. Beyond the basic uses for keeping information secret and the different methods available, additional forms, such as hashes, digital signatures, non-repudiation and steganography, are introduced.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the underlying principles of cryptography, clear text, plain text, algorithms, and keys. • Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them. • Classify and describe a number of different encryption algorithms and the way that they work. • Describe the mathematical principles behind encryption and the mathematical properties of ciphertext. • Describe and evaluate different methods used to crack encryption. • Explain the different uses of encryption methods and the security objectives that they meet.				
Prerequisites	None	Co-requisites	CYS600		

Course Content	Introduction: History of cryptography, early forms, cryptosystem strength, Caesar cipher, one time pad, steganography. Principles: basic cryptographic functions – substitution ciphers and transposition ciphers, symmetric and asymmetric algorithms, block and stream ciphers, hybrid systems. Symmetric systems: DES, 3-DES, AES, IDEA, Blowfish, RC4-5-6, Twofish, Serpent, others, uses and cryptographic services provided. Asymmetric systems: Diffie-Hellman algorithm, RSA, El Gamal, Elliptic Curve systems, zero knowledge proof, SSL/TLS, PGP, S/MIME, Bitcoin. Public key systems: one-way algorithms, public and private keys, public key infrastructure, certificate and trust authorities, distributed trust systems. Other cryptographic services: message and file integrity, hashing, digital certificates, digital signatures, key management. Attacks: known and chosen plaintext attacks, ciphertext attacks, analytical attacks, frequency analysis, statistical attacks, social engineering attacks. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the uses of cryptography in real systems.
Teaching Methodology	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
Bibliography	*"Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series)"*, by Jonathan Katz and Yehuda Lindell *"Understanding Cryptography: A Textbook for Students and Practitioners"*, by Christof Paar and Jan Pelzl *"Applied Cryptography: Protocols, Algorithms and Source Code in C"*, by Bruce Schneier *"Modern Cryptanalysis: Techniques for Advanced Code Breaking"*, by Christopher Swenson

Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English