COURSE OUTLINE

(1) GENERAL

SCHOOL	SCHOOL OF SCIENCES		
ACADEMIC UNIT	DEPARTMENT OF MATHEMATICS		
LEVEL OF STUDIES	UNDERGRADUATE PROGRAM		
COURSE CODE		**SEMESTER**	**F**
COURSE TITLE	CRYPTOGRAPHY		
INSTRUCTOR	Panagiotis Nastou		
INDEPENDENT TEACHING ACTIVITIES		**WEEKLY TEACHING HOURS**	**CREDITS**
		4	6
COURSE TYPE	Special background		
PREREQUISITE COURSES:	NO		
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	GREEK		
IS THE COURSE OFFERED TO ERASMUS STUDENTS	YES		
COURSE WEBSITE (URL)	http://www.math.aegean.gr/index.php/en/academics/undergraduate-programs		

(2) LEARNING OUTCOMES

Learning outcomes
In this course the students are introduced to the basic complexity theory and how computational difficulty in solving problems can be exploited to build secure cryptographic protocols. The lectures are, then, focused on some elementary cryptographic schemes like Caesar's cipher, general substitution ciphers, polyalphabetic ciphers and how they can be broken efficiently. Then the students are introduced to Shannon's cryptographic principles of confusion and diffusion and how they lead to the Feistel-based block ciphers. Then, as case studies, the block ciphers DES, CAST-128 and AES are presented along with analysis of their security properties. In the middle of the course, the students are introduced to public key cryptography and the RSA, ElGamal scheme and the foundations of Elliptic Curve Cryptography as well as the state of the art in the cryptanalysis of RSA and ECC. The aim of this course is mainly to introduce the students into the basic concepts of cryptography and cryptanalysis. At the end of the course, they could develop and analyse certain cryptographic systems and they could be ready to use and modify certain cryptanalysis techniques.
General Competences
Working independently. Team work. Working in an interdisciplinary environment. Working in an international environment.

(3) SYLLABUS

Algorithms and Cryptography. An introduction to the Complexity Theory: fast tractable problems and the class P, hard computational problems and the class NP, NP-complete problems and the question if P is not equal NP.

Security Assessment Models. Design Secure Cryptographic Systems. Cryptography and Cryptanalysis. Information Theory: Probabilities, Entropy and Mutual Information.

Information Leakage by cipher. Perfect Secrecy. Redundancy of a Language. Key Equivocation. Counting average number of spurious keys. Unicity Distance. Stream and block Cryptographic algorithms.

Cryptographic Operations. Transposition Cipher. Shift Cipher, and the Caesar Cipher. Substitution cipher. Security of the Mono-alphabetic Substitution. Affine Cipher and its Cryptanalysis.

Vigenere Cipher and its Cryptanalysis: Kassiski test and Index of Coincidence. One time pad. Vernam Cipher. Hill Cipher and its Cryptanalysis. Cryptographic product.

Shared Key Ciphers. Substitution Permutation Networks (SPN). Sbox Design. Principles of Diffusion and confusion. Block Ciphers.

Feistel Networks and its security. DES and AES structure presentation. Block Ciphers Interconnection. Triple encryption and the meet-in-the-middle attack. Key Scheduling Algorithms. Linear and Differential Cryptanalysis.

Public Key Cryptography Schemes. RSA, public and private key pair generation, Square and Multiply Algorithm. Factoring Algorithms: Pollard-(p-1), Pollard-ρ, Dixon's Random Squares Algorithm, the Decryption Exponent Algorithm.

ElGamal Cryptographic System on Zp. Discrete Logarithm Problem and Algorithms for solving it: Baby-Step-Giant-Step and Pollard Rho Algorithm.

ElGamal Cryptographic System on Elliptic Curves. Elliptic Curve generation algorithms, basic Algebraic operations and their implementation algorithms. The Discrete Logarithm Problem on Elliptic Curves.

The concept and the use of Digital Signature Schemes.

TEACHING MATERIAL DISTRIBUTION	The teaching material of the course is uniformly distributed during the semester.

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY	Face-to-face
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY	• Use of ICT in teaching • Communication with students via e-mail • Uploading course material on moodle system.
TEACHING METHODS	

Activity	***Semester workload***
Lectures	52
Independent study	98
Course total (25 per ECTS)	***150***

COURSE COMMITMENTS	Attending course is not obligatory.
STUDENT PERFORMANCE EVALUATION	Student's evaluation is done in Greek through a written examination which includes short-answers questions and problem solving. For students with disabilities, evaluation takes place via oral exams.

(5) ATTACHED BIBLIOGRAPHY

1. Contemporary Cryptography, Stefanos Gritzalis, Papasotiriou Editions, March 2011.
2. Various Papers published in international conferences and journals.