Applied Cryptography

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE		
COURSE UNIT CODE	**CSCYB103**	**SEMESTER OF STUDY**	1st
COURSE TITLE	**Applied Cryptography**		
COURSEWORK BREAKDOWN		**TEACHING WEEKLY HOURS**	**ECTS Credits**
	Lectures	3	
	Tutorials	1	
		4	**8**
COURSE UNIT TYPE	Compulsory, Specialized general knowledge		
COURSE DELIVERED TO ERASMUS STUDENTS	YES		
MODULE WEB PAGE (URL)	https://eclass.uniwa.gr/courses/CSCYB105/		

2.LEARNING OUTCOMES

Learning Outcomes

- An introduction on cryptographic definitions and notions
- Familiarization with security issues
- Understanding of the cryptographic protocols capabilities
- The skills to select the most adequate cryptographic solutions for given security problem.

General Skills

- *Search for optimal cryptographic solutions*
- *Independent work*

3.COURSE CONTENTS

The description contains the material to be covered during 13 sessions.

1) Introduction to cryptography. History of cryptography and definitions
2) Mathematical background. Modular computations, Boolean functions, birthday paradox
3) Pseudorandom generators and stream ciphers
4) Pseudorandom functions. Block ciphers (AES) and modes of operation (CBC,CTR).
5) One way functions and hash functions (SHA-2, SHA-3).
6) Message Authentication codes. HMAC and ECBC.
7) Authenticated encryption with associated data (GCM).
8) Public key cryptography. RSA and secure implementations. The problem of factorization
9) El Gamal and elliptic curves. The discrete logarithm problem.
10) Digital signatures. Digital signature algorithm, EdDSA.
11) Attacks against symmetric and public key encryption protocols
12) Key Encapsulation Mechanism, Key encryption, Diffie-Hellman Key agreement, and authentication protocols

13)	Advanced cryptography: MPC, ORAM, Homomorphic encryption

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open e-Class system, with uploaded notes, lectures, exercises for practice and communication with students.
TEACHING METHODS	
ASSESSMENT METHODS	I. A written final examination (60%) and II. Research work (40%)

Method description	*Semester Workload*
Lectures	39
Tutorials	39
Research work	50
Self study	60
Total course hours (25 h workload per ECTS)	***188***

5.RESOURCES

Essential

- *Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell (2nd Edition!)*
- *Cryptography Made Simple. Nigel Smart. Springer*

Recommended

- *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*
- *ENISA, Algorithms, key size and parameters, report – 2014*
- *ECRYPT – CSA, Algorithms, Key Size and Protocols Report (2018)*

3. DATABASE SYSTEMS SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE		
COURSE UNIT CODE	**CSCYB205**	**SEMESTER OF STUDY**	2nd
COURSE TITLE	**Database Systems Security**		

COURSEWORK BREAKDOWN	**TEACHING WEEKLY HOURS**	**ECTS Credits**
Lectures	3	
Tutorials	2	
	5	**7**

COURSE UNIT TYPE	Compulsory, Specialized general knowledge
PREREQUISITES :	NONE

LANGUAGE OF INSTRUCTION/EXAMS:	GREEK, ENGLISH
COURSE DELIVERED TO ERASMUS STUDENTS	YES
MODULE WEB PAGE (URL)	

2. LEARNING OUTCOMES

Learning Outcomes

- To understand the risks that exists in data publishing
- To know the existing options for secure databases
- To design more secure databases

General Skills

- To be able to protect client’s data from attacks
- To understand the main concept of big data and the trends and security risks of the modern applications
- To know which data should be protected

3.COURSE CONTENTS

The description contains the material to be covered during 13 sessions.

- Discretionary and mandatory access control
- Security protection capabilities of the SQL language
- Privacy protection for relational, spatial and graph data
- Privacy protection of data changing over time
- Digital watermarking and fingerprinting in relational databases.
- Encrypted databases and retrieval of encrypted data
- Security in statistical and distributed databases
- Big data security
- Data security and privacy protection in online social networks.
- Big data integration and security

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.
TEACHING METHODS	

Method description	***Semester Workload***
Lectures	39
Tutorials	26
Research work	50
Self study	60
Total course hours (25 h workload per ECTS)	***175***

ASSESSMENT METHODS	I. A written final examination (20%) and II. Research work (80%)

5.RESOURCES

Essential

- *Privacy Preserving Data Publishing: An Overview, Synthesis Lectures on Data Management, 2010, Raymond Chi Wing Wong, Ada Wai Chee Fu*
- *Συστήματα Διαχείρισης Βάσεων Δεδομένων, 3η Έκδοση, Ramakrishnan Raghu, Gehrke Joahannes . (Κεφάλαιο 24)*
- *Θεμελιώδεις αρχές συστημάτων βάσεων δεδομένων, Elmasri Ramez, Navathe Shamkant B.B (Κεφάλαιο 17)*
- *Rakesh Agrawal and Jerry Kiernan. 2002. Watermarking relational databases. In Proceedings of the 28th international conference on Very Large Data Bases*

Recommended

- *Chen, Bee Chung & Kifer , Daniel & LeFevre, Kristen & Machanavajjhala , Ashwin. (2009). Privacy Preserving Data Publishing. Foundations and Trends in Databases.*
- *Fung, Benjamin & Wang, ke & Chen, Rui & Yu, Philip. (2010). Privacy Preserving Data Publishing: A Survey of Recent Developments. ACM Comput . Surv .. 42.*
- *Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, Raju Halder, Shantanu Pal and Agostino Cortesi*