UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-514DL	Cryptography and Network Security	10
Prerequisites	**Department**	**Semester**
None	Computer Science	Fall
Type of Course	**Field**	**Language of Instruction**
Required	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr Ioanna Dionysiou	1st
Mode of Delivery	**Work Placement**	**Corequisites**
Distance Learning	N/A	N/A

Course Objectives:

The main objectives of the course are to:

- appreciate the need for network security practices and information protection.
- provide students with deep knowledge on principles and practice of cryptography.
- provide students with deep knowledge on principles and practice of classical computer and network security paradigms.
- expose students to techniques to detect and manage security threats by means of contemporary host-based and network-based intrusion detection/prevention tools, physical security measures, auditing, logging.
- build foundations to assess contemporary security policies and security mechanisms within organizations and illustrate the balance of the managerial, technical, and legal aspects of network security.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. explain the principles of cryptography.
2. discuss the practical use of cryptography in symmetric/asymmetric encryption, hash functions, MAC, and digital signatures.
3. discuss key management schemes for master, public, and session keys.
4. discuss and explain network authentication protocols (Kerberos, PKI), Web security paradigms (TLS, SSH), and IP Security.
5. identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic network defense tools

6. identify various types of malicious software and use countermeasure defense/detection tools
7. discuss sector-specific frameworks, including policies, mechanisms, and standards, where applicable
8. appreciate the importance of ethics as a network security practitioner
9. use existing technologies and libraries to achieve security goals

Course Content:

1. Overview of Computer and Network Security Concepts
2. Classical Encryption Techniques
3. Symmetric Ciphers
4. Asymmetric Ciphers
5. Cryptographic Data Integrity Algorithms
6. Key Management and Distribution
7. User Authentication
8. Network Security Services
9. Malicious Software and Countermeasure Defenses
10. Security Management
11. Security Management Case Studies
12. Legal And Ethical Issues

Learning Activities and Teaching Methods:

Lectures, Labs, Assignments, Case studies.

Assessment Methods:

Lab Assignments
Presentation
Final Exam

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Cryptography and Network Security: Principles and Practice, Global Edition	W. Stallings	Pearson	2018	9781292158594
Computer Security: A Hands-on Approach 2nd Edition	Wenliang Du	Wenliang Du	2019	9781733003926
Computer Security: Principles and Practice, Global Edition	W. Stallings, L. Brown	Pearson	2018	9781292220635

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition	R. Anderson	John Willey and Sons	2008	0470068523