NATIONAL UNIVERSITY OF ENGINEERING
COLLEGE OF SCIENCES

COMPUTER SCIENCE PROGRAM

CM04A – CRYPTOGRAPHY AND SECURITY

I. GENERAL INFORMATION

CODE	: CM04A Cryptography and Security
SEMESTER	: 8-10
CREDITS	: 5
HOURS PER WEEK	: 6 (Theory, Practice, Laboratory)
PREREQUISITES	: CC411 Computer and Information Security
CONDITION	: Elective

II. COURSE DESCRIPTION

The course prepares students for understanding and applying cryptographic algorithms and techniques for designing secure network systems. Students apply symmetric cyphering techniques, public key encryption systems, hash function for developing different cryptographic systems depending on the characteristics of the network to be secured. Students also analyze network security applications such as digital signature, electronic mail security, Intenet security, web security. Computer software applications are used for implementing and analyzing different cryptographic systems.

III. COURSE OUTCOMES

At the end of the course students:

1. Understand the importance of cryptography for designing secure computer and communication networks ensuring data confidentiality and integrity, authentication and no-repudiation.
2. Apply symmetric cyphering algorithms and techniques for designing cryptographic systems, and analyzing their strength and robustness.
3. Develop public key encryption systems using hush functions for message authentication and integrity analysis.
4. Apply cryptography methods for network security: digital signature, public key infrastructure, electronic mail security, Internet security, web security.

IV. LEARNING UNITS

1. INTRODUCTION

Computer and communications network security. Security trends. OSI security architecture. Security attacks. Security services. Security mechanisms. A model for network security. Encryption and cyphering. Symmetric cyphering. Key terms.

2. SYMMETRIC CYPHERING

Classical encryption techniques. Symmetric cypher model. Substitution techniques. Rotor machines. Steganography.

Block cypher and data encryption model. Block cypher principles. Data encryption standard DES. Strength of DES. Differential and linear cryptanalysis. Block cypher design.

Finite fields. Groups, rings and fields. Modular arithmetic. Euclidean algorithm. Finite fields of the form GF(2n).
Advanced encryption standards AES. Evaluation criteria for AES. AES cypher. Confidentiality using symmetric encryption. Encryption function. Traffic confidentiality. Key distribution. Random number generation.

3. PUBLIC KEY ENCRYPTION AND HASH FUNCTIONS

Number theory. Fermat and Euler theorems. Testing for primality. Chinese remainder theorem. Discrete logarithms.
Public key cryptography and RSA. Public key crypto-systems. RSA algorithm. Complexity of algorithms.
Key management. Diffie-Hellman key exchange. Elliptic curve arithmetic. Elliptic curve cryptography.
Message authentication and Hash functions. Authentication requirements. Authentication functions. Message authentication codes. Hash functions. Security of Hash functions and Macs.
Hash and MAC algorithms. Secure Hash algorithm. Whirlpool. HMAC. CMAC.
Digital signature and authentication protocols. Digital signature standards.

4. NETWORK SECURITY APPLICATIONS

Authentication applications. Kerberos. X.509 authentication service. Public key infrastructure.
Electronic mail security. Pretty good privacy. S/MIME. Data compression using ZIP. Radix-64 conversion. PGP random number generation.
IP security. Architecture. Authentication header. Security payload encapsulation. Security association combination. Key management.
Web security. Security considerations. Secure Socket Layer SSL. Transport Layer Security TLS. Secure electronic transaction.

V. METHODOLOGY

The course takes place in theory, practice and computer laboratory sessions. In theory sessions, the instructor presents the methods for cryptographic cyphering and network security. In practice session, instructor and students work together for analyzing and proposing solutions to different cryptography problems. In computer laboratory sessions, students implement algorithms for cryptographic cyphering, as well as test their strength.

VI. EVALUATION FORMULA

The final grade PF is calculated as follows:

$$PF = 0.20\ EP + 0.3\ EF + 0.20\ PR + 0.30\ LB$$

where:

PF: Final grade EP: Mid-term exam EF: Final exam
PR: Practice work: LB: Computer laboratory work

VII. BIBLIOGRAPHY

1. Cryptography and Network Security
   William Stallings
   Prentice Hall Editions, 2016
2. Serious Cryptography
   Jean Philippe Aumasson
   William Pollock Editions. 2016.