MSA UNIVERSITY
FACULTY OF ENGINEERING
MODULE OUTLINE

Module Code	**: ECE 5432**
Title	**: Cryptography**
Level	**: 3**
Credit Hours	**: 3**
Prerequisites	**: ECE 435**

AIMS

The objective of this course is to provide a foundation of cryptography in an applied manner so that students can grasp its importance in relation to the rest of information security. The course covers principles of number theory and cryptographic algorithms and cryptanalysis. Topics include: steganography, block and stream ciphers, secret key encryption (DES, AES, RC-n), primes, random numbers, factoring, and discrete logarithms; Public key encryption (RSA, Diffie-Hellman, Elliptic curve cryptography); Key management, hash functions (MD5, SHA-1,RIPEMD-160, HMAC), digital signatures, certificates and authentication protocols. Cryptanalytic methods (known, chosen plaintext etc.) for secret and public key schemes

SYLLABUS

Topics
Introduction; History of Cryptography; Steganography.
Cryptology and simple cryptosystems; Shift, Affine, Hill Ciphers; Enigma
Conventional encryption techniques; Stream and block ciphers; DES;
DES continued; Linear and Differential Cryptanalysis; Hash functions;
More on Block Ciphers; The Advanced Encryption Standard
Hash Functions and their Implementation
Number Theory and Algorithm Complexity; Public Key Encryption - RSA
Public key Encryption using Discrete Logarithms
Elliptic Curve Cryprography
Digital signatures and the digital signature standard
Key Management Schemes
Identification Schemes and Biometrics

LEARNING OUTCOMES

Knowledge

After completing this course students well be able to:

1. Grasp the importance of cryptography in relation to the rest of information security
2. Understand principles of number theory and cryptographic algorithms and cryptanalysis
3. Learn how various cryptographic schemes work

Skills

After completing this course students well be able to:

1. Measure the running time of an algorithm and understand the notion of reducing one problem to another
2. Analyze security of a cryptographic scheme and determine whether or not it is secure

Teaching/Learning Strategies

- Lectures
- Tutorials
- Laboratories
- Individual/Group Project

Learning Materials

Reference Text:

- Katz , Jonathan, and Yehuda Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC ,2008.

Supplementary Readings:

- Douglas R. Stinson, Cryptography: Theory and Practice, 3rd ed. , Chapman & Hall/CRC ,2005.
- William Stallings, Cryptography and Network Security, 4th.Ed, Prentice Hall PTR, 2006

Assessment Scheme

- Weekly Written Assignments (12 Assignments).
- Class Written Tests (2.5-hr Tests)
- Individual/Team Course Project
- Unseen Written Mid-Term Exam (1.5-hr. Exam).
- Unseen Written Final-Exam (3-hr. Exam).

Assessment Pattern

• Assignments	15%
• Tests and Quizzes	15%
• Projects and Reports	10%
• Mid-Term Exam	20%
• Final Exam	40%
Total	**100%**

Learning Unit Contact Hours

• Lectures	3	hrs / week
• Tutorials	1.5	hrs / week
• Total class contact hours	63	hrs/semester
• Total self study hours	45	hrs/semester
• Total study hours	108	hrs/semester

Module Leader:

Dr. Farah Raad