COURSE CODE	12140527	**COURSE LEVEL**	Graduate
COURSE TITLE	Cryptography and Network Security		
COURSE TYPE			
LECTURER(S)	Anas Melhem		
CREDIT VALUE	3		
PREREQUISITES			
COREQUISITES	None		
DURATION OF COURSE	1 Semester		
WEB LINK			

CATALOGUE DESCRIPTION This the course on Cryptography and Network Security, objectives are: Classical encryption techniques, Block ciphers and the Data Encryption Standard, Basics of finite fields, Advanced Encryption Standard, Contemporary symmetric ciphers, Confidentiality using symmetric encryption, Basics of number theory, Key management, Public key cryptosystems, Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols, Network security practice, Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls

AIMS & OBJECTIVES The aim of the course is to introduce the student to the fundamentals of cryptography and network security.

GENERAL LEARNING OUTCOMES (COMPETENCES) On successful completion of this course, all students will have developed knowledge and understanding of: Classical encryption techniques, Block ciphers and the Data Encryption Standard, Basics of finite fields, Advanced Encryption Standard, Contemporary symmetric ciphers, Confidentiality using symmetric encryption, Basics of number theory, Key management, Public key cryptosystems, Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols, Network security practice, Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls

On successful completion of this course, all students will have developed their skills in: the programming of symmetric and/or asymmetric ciphers and their use in the networks.

On successful completion of this course, all students will have developed their appreciation of and respect for values and attitudes regarding the issues of: Cryptography; Block and stream ciphers; Symmetric and asymmetric ciphers; Network security; Cooperation and teamwork ; Unsupervised learning

GRADING CRITERIA Will be decided according to student performance.

RELATIONSHIP WITH OTHER COURSES The course is based on the majority of the undergraduate courses related to algorithms, programming, computer organization, and networking
ASSIGNMENTS There will be a term project.
METHOD OF ASSESSMENT •30% Midterm •40% Final •30% Assignment
TEXTBOOK W. Stallings, Cryptography and Network Security, Principles and Practices, 3rd Ed., Prentice Hall, 2003, ISBN 0-13-111502-2
SEMESTER OFFERRED 2017-18 Summer Semester

CONTENT & SCHEDULE

- Classical encryption techniques,
- Block ciphers and the Data Encryption Standard,
- Basics of finite fields,
- Advanced Encryption Standard,
- Contemporary symmetric ciphers,
- Confidentiality using symmetric encryption,
- Basics of number theory,
- Key management,
- Public key cryptosystems,
- Message authentication,
- Hash functions and algorithms,
- Digital signatures and authentication protocols,
- Network security practice,
- Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls

PLAGIARISM AND OTHER FORMS OF CHEATING

Plagiarism is intentionally failing to give credit to sources used in writing regardless of whether they are published or unpublished. Plagiarism (which also includes any kind of cheating in exams) is a disciplinary offence and will be dealt with accordingly. Copying will also be dealt with similarly.

Last modified 23/06/2018