FUTURE UNIVERSITY IN EGYPT جامعة المستقبل

Faculty of Computers and Information Technology

Computers and Information Security

Information :

Course Code :	DM426	**Level :**	Undergraduate	**Course Hours :**	3.00- Hours
Department :	Department of Computer Science				

Instructor Information :

Title	Name	Office hours
Associate Professor	Soha Safwat Labib Hana	1
Assistant Lecturer	Mahmoud Magdy Mohamed Abdo	1
Teaching Assistant	Tasneem Hatem Ali Mohamed Zein Eldeen	
Teaching Assistant	Nadeen Ramadan Youssef Morsi Youssef	
Teaching Assistant	Aya Mohamed Ahmed Morsy Farag	

Area Of Study :

Apply the basic concepts of process and thread.
Use effectively communication skills.
Understand knowledge that enhances skills in cryptography.
Use and adopt fundamental and advanced mathematics of security systems.
Comprehend deeply the basic concepts, techniques and methods to implement ciphering algorithms to be ready for further and continuous learning

Description :

Introduction, Identification and authentication, Authorization rules. Data classification. Basic data encryption and decryption techniques, Different types of ciphers, characteristics of good ciphers crypt analysis, Public-key system, single key system and data encryption standards, Threats, Safeguards and security objectives, security with some existing systems, Security level. Computer virus protection, Privacy and data protection, designing of secure system. Discussions of the need for network security, describe various threats, attach types and hashers. Explain authentication, encryption. & encryption standard. Secret- key, public nay algorithm authentication protocols, digital certificate. Virtual private network (VPN), secure sockets layer (SSL)

Course outcomes :

a.Knowledge and Understanding: :	
1 -	Discuss the fundamental mathematics required to design the cryptography and cryptanalysis techniques
2 -	Explain the principles and algorithms of data cryptanalysis to break the code against some conventional ciphering algorithms to get plaintext from cipher text
3 -	Discuss the fundamental topics of conventional and public key encryption to get cipher text from the plaintext
4 -	Identify the legal, professional and moral aspects related to DMT
b.Intellectual Skills: :	
1 -	Analyze different computer science problems of information security

2 -	Select appropriate methodologies and techniques for cryptographic systems
3 -	Classify methods, techniques and algorithms that solve Web security problems
c.Professional and Practical Skills: :	
1 -	Apply effective information to implement cryptographic algorithms using appropriate programming languages
2 -	Deploy effective supporting tools to apply conventional and public key encryption algorithms to get cipher text from plaintext
3 -	Create technical reports according to professional standards to acquire and manage different information about the implementation of cryptanalysis algorithms using scientific literature and web sources
d.General and Transferable Skills: :	
1 -	Work on a team to develop solutions for operating systems problems
2 -	Apply communications skills in presentation and report writing for operating systemsôconcepts and modules

ABET Course outcomes :	
1 -	Apply the basic concepts of process and thread
2 -	Demonstrate adequate understanding of cryptography concepts and techniques
3 -	Demonstrate adequate understanding of the fundamental concepts, techniques, and safeguards targeting computing systems security
4 -	Comprehend the basic concepts, techniques and methods to implement ciphering algorithms to be ready for further and continuous learning
5 -	Communicate effectively

Course Topic And Contents :

Topic	No. of hours	Lecture	Tutorial / Practical
Information Security Basics and OSI Security Architecture	4	2	2
Introduction to Cryptography and Cesar ciphering	4	2	2
Monoalphabetic ciphering algorithm	4	2	2
Playfair ciphering algorithms and their cryptanalysis techniques	4	2	2
Polyalphabetic ciphering algorithm	4	2	2
Fence ciphering algorithm	4	2	2
Columnar transposition ciphering algorithm	4	2	2
Block Ciphers: Data Encryption Standard(P1)	4	2	2
Mid Term Exam	2		
Block Ciphers: Data Encryption Standard(P2)	4	2	2
Public key encryption algorithms (P1)	4	2	2
Public key encryption algorithms (P2)	4	2	2
Student Presentations	4	2	2
Final Exam	2		

Teaching And Learning Methodologies :
Interactive Lectures including Discussions
Practical Lab Sessions

Self-Study (Project / Reading Materials / Online Material / Presentations)
Case Studies
Problem Solving

Course Assessment :

Methods of assessment	Relative weight %	Week No	Assess What
Assignments	3.00	4	
Final Exam	40.00	14	
Individual Projects	4.00		
Midterm Exam (s)	20.00	9	
Practical Exam	10.00	13	
Presentations	4.00	12	
Quizzes	10.00	5	
Research and Reporting	4.00		
Team Work Projects	5.00		

Course Notes :

An Electronic form of the Course Notes and all the slides of the Lectures is available on the Students Learning Management System (Moodle)

Web Sites :

Journal of Information Security and Applications - Elsevier
https://www.journals.elsevier.com/journal-of-information-security-and-applications