

Faculty of Computers and Information Technology

Computer And Information Security

Information :

Course Code : ITC 426

Level : Undergraduate

Course Hours : 3.00- Hours

Department : Faculty of Computers and Information Technology

Instructor Information :

Title	Name	Office hours
Lecturer	Hussein Mohamed Mohamed Ali Harb	
Teaching Assistant	Donia Waleed Gamal Seddek Elsayed Hagag	

Area Of Study :

Understand types of threats to information system.
 Understand the requirements for the information security.
 Understand the different types of the cryptography techniques.
 Develop ciphering algorithms both conventional and public key based
 Develop cryptanalysis algorithm to cipher text to break the code against some conventional ciphering algorithms.
 Understands the concepts, and bases of Web security.

Description :

Basic concepts of information and network security; Classical encryption techniques; Modern block ciphers and the data encryption standards; Block cipher cryptanalysis and usage; Modern stream ciphers; Number theory; Public key cryptography; Key certificates and management; Message authentication and hash functions; Hash algorithms; Digital signature and authentication protocols; Electronic mail security; IP security; Web security; Firewalls; Introduction to digital steganography and watermarking techniques.

Course outcomes :

a.Knowledge and Understanding: :

1 -	Identify contemporary issues in information security
2 -	Define information security risks.
3 -	Define the three aspects of information security: services, mechanisms and attacks
4 -	Describe cipher principles
5 -	Discuss the cryptographic systems
6 -	Describe the basic operations and applications of firewalls, Intrusion Detection

b.Intellectual Skills: :

1 -	Evaluate classical techniques of information security
2 -	Evaluate cryptographic systems algorithms
3 -	Identify the impact of different security breaches on Information security
4 -	Explain the guidelines and procedures of Information security investigations

5 -	Perform comparisons between (methods, techniques...etc) related to information security
6 -	Identify countermeasures and review techniques appropriate to the management of information security risks

c. Professional and Practical Skills: :

1 -	Institute Information security program management
2 -	Use appropriate programming languages
3 -	Implement cryptographic systems algorithms
4 -	Implement different ciphers on Software

d. General and Transferable Skills: :

1 -	Work in stressful environment and within constraints
2 -	Communicate effectively
3 -	Demonstrate efficient IT capabilities
4 -	Lead and motivate individuals
5 -	Manage tasks and resources

Course Topic And Contents :

Topic	No. of hours	Lecture	Tutorial / Practical
Information security bases and OSI Security Architecture	4	2	2
Introduction to Cryptography and Cisar ciphering	4	2	2
Monoalphabetic and Playfair ciphering algorithms and their cryptanalysis techniques	4	2	2
Polyalphabetic, Vigenere ciphering and Kasiski method	4	2	2
Midterm Exam I	3	1	2
Autokey Cipher, Vernam Cipher, Transposition Ciphers, Rail Fence cipher	4	2	2
Row Transposition Ciphers, Product Ciphers, Rotor Machine Principles, Steganography	4	2	2
Block Ciphers and the Data Encryption Standard	4	2	2
Differential & Linear Cryptanalysis	4	2	2
Midterm Exam II	3	1	2
Intrusion Detection Systems	4	2	2
Security in cloud computing	4	2	2
The AES Cipher	4	2	2
Web Security	4	2	2
Revision	4	2	2
Final Exam	4	2	2

Teaching And Learning Methodologies :

Lectures
Exercises
Practical training

Presentation

Open Discussion

Projects

E. Learning

Web-Site searches

Self Studies

Course Assessment :

Methods of assessment	Relative weight %	Week No	Assess What
current discussion and class activities	10.00	3	the student progress and attitude
final written	40.00	16	the ability to understand, remember and assess
practical exam	30.00	14	the practical skills in providing solutions
written mid-term exam 1	10.00	5	student progress along mid-semester
written mid-term exam 2	10.00	10	student progress along mid-semester

Course Notes :

PowerPoint presentations, and pdf files

Recommended books :

ÇArthur E. Hutt, Douglas B. Hoyt, Seymour Bosworth. "Computer Security Handbook", third edition, John Wiley & Sons, Inc, 1995.

ÇRick Lehtinen. "Computer Security Basics", second edition, O'Reilly Media, Inc, 2006.

Web Sites :

prezi.com