CPIT-425 Syllabus

Catalog Description

CPIT-425 Information Security
Credit: 3 (Theory: 3, Lab: 0, Practical: 1)
Prerequisite: CPIT-370
Classification: Department Required

The objective of this course is to provide basic knowledge about the technical and operational issues of modern cryptosystems and the related standards. Topics include threats to network security and schemes for breaking security, classical encryption techniques, block ciphers and stream ciphers, DES and triple DES, AES, block cipher operation modes, asymmetric ciphers: RSA, Diffie-Hellman key exchange, ElGamal cryptosystem, hash functions, MAC functions, digital signature, key management and distribution, X.509 certificates, transport level security: SSL and TLS, Intrusion, and types and configurations of firewalls.

Class Schedule

Meet 50 minutes 3 times/week or 80 minutes 2 times/week

Lab/Tutorial 90 minutes 1 times/week

Textbook

William Stallings, , "Cryptography and Network Security", Pearson; 8 edition (2016-02-24)

ISBN-13 9780134444284 **ISBN-10** 0134444280

Grade Distribution

Week	Assessment	Grade %
4	Graded Lab Work 1	4
5	Graded Lab Work 2	4
6	Exam 1	20
7	Graded Lab Work 3	4
8	Graded Lab Work 4	4
11	Graded Lab Work 5	4
11	Exam 2	20
14	Group Project	10
16	Exam	30

Last Articulated

December 18, 2017

Relationship to Student Outcomes

a	b	c	d	e	f	g	h	i	j	k	l	m	n
	x							x	x			x	

Course Learning Outcomes (CLO)

By completion of the course the students should be able to

1. Identify the security attacks. (b)
2. Examine the symmetric encryption scheme. (i)
3. **Apply traditional cipher techniques for encrypting and decrypting textual messages. (j)**
4. Develop programs to encrypt and decrypt text messages using some traditional ciphers. (j)
5. Analyze the internal operation and properties of modern encryption standards (DES and AES). (m)
6. **Distinguish the block cipher modes of operation. (m)**
7. Examine the public-key encryption scheme. (i)
8. **Analyze the operation and properties of some strong public-key algorithms (RSA, Diffie-Hillman and ElGamal Cryptographic System). (m)**
9. Develop programs to use RSA, Diffie-Hillman, and ElGamal algorithms for cryptographic applications. (i)
10. **Differentiate different algorithms to provide message authentication and digital signature. (m)**
11. Develop programs to produce and verify the digital signature of a message based on the RSA and ElGamal. (j)
12. Determine the centralized and decentralized key distribution schemes. (m)
13. Determine the use of X.509 public-key certificates. (m)
14. Differentiate the transport layer security protocols. (m)
15. **Identify and configure firewalls. (b)**

Coordinator(s)

Dr. Suhair Alshehri, Associate Professor

CPIT-425 Syllabus

Topics Coverage Durations

Topics	Weeks
Computer Security Overview	1
Classical Symmetric Cipher Encryption Techniques	1
Classical Block Cipher Encryption Techniques	1
Advanced Encryption Standard	1
Other Symmetric Block Cipher Encryption Techniques	1
Public-Key Cryptosystems	1
Other Public-Key Cryptosystems	1
Cryptograhic Hash Functions	1
Message Authentication Codes	1
Digital Signatures	1
Key Distributions	1
Key Management	1
Transport-Level Security	1
Firewall Basics	1
Firewall Configurations	1