CPCS-425 Syllabus

Catalog Description

CPCS-425 Information Security
Credit: 3 (Theory: 3, Lab: 0, Practical: 0)
Prerequisite: CPCS-361 , CPCS-371
Classification: Elective

The objective of this course is to provide an introduction to information security in computer networks, with a focus on providing basic knowledge of the technical and operational issues of modern cryptosystems and their related standards. Topics include security threats and vulnerabilities, classical encryption techniques, block ciphers and stream ciphers, DES and triple DES, AES, Block cipher operation modes, asymmetric ciphers: RSA, Diffie-Hellman key exchange, hash functions, MAC functions, digital signature: digital Signature Standard DSS, key management and distribution, X.509 certificates, web security: SSL and TLS, email security (PGP), malicious software, and firewalls.

Class Schedule

Lab/Tutorial 90 minutes 1 times/week

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

Textbook

William Stallings, , "Cryptography and Network Security", Prentice Hall; 5 edition (2011)

ISBN-13 9780136097044 **ISBN-10** 0136097049

Grade Distribution

Week	Assessment	Grade %
6	Quiz 1	5
8	Exam 1	15
12	Exam 2	15
13	Quiz 2	5
14	Project (Individual)	10
15	Lab Exam	15
16	Exam	35

Last Articulated

May 2, 2016

Relationship to Student Outcomes

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

Course Learning Outcomes (CLO)

By completion of the course the students should be able to

1. Identify security challenges, threats, attacks and explain risk management process and steps (b)
2. Identify and apply classical encryption algorithms: substitution and permutation and approaches for possible attaks (j)
3. Develop codes to encrypt and decrypt text messages using some classical encryption techniques (caesar, vigenre,…) (c)
4. **Describe the block and internal operation, and properties of modern encryption standards (DES) and (AES) and describe the block cipher modes of operation (j)**
5. Develop codes to use DES algorithms for cryptographic applications. (j)
6. Define the public key cryptosystem concept and demonstrate the use of public-key cryptosystems for authentication, secrecy, and key exchange (a)
7. Describe the operation and properties of a strong public-key algorithm (RSA) (j)
8. Develop codes to use RSA algorithm for cryptographic applications (j)
9. Demonstrate the use of message authentication code (MAC) and hash functions for authentication (a)
10. Develop codes to apply MAC and hash function SHA-1 on simple text message for authentication and integrity purposes (k)
11. **Define digital signature purposes and requirements and describe the two digital signature schemes (RSA and DSS). (i)**
12. Develop codes to produce and verify digital signature of a message using RSA and DSS. (k)
13. Define the properties of a secure key and compare the centralized and decentralized key distribution schemes. (i)
14. **Describe the use of X.509 public-key certificates and define PKI and its contents (a)**
15. Generate X.509 certificates using software tools (k)
16. **Identify basic firewall system, packet filtering. List what Firewalls can and cannot block. (a)**
17. **Describe web security protocols (SSL and TLS) and current email security protocol (PGP)(S/MIME) (i)**
18. Describe Cloud computing elements, cloud secuirty and countermeasures and define cloud security as a service

CPCS-425 Syllabus

Topics Coverage Durations

Topics	Weeks
Introduction to Information Security	2
Classical Cryptography	2
Symmetric (Modern) Cryptography	2
Public-Key Cryprography	2
Message Authentication Techniques	1
Digital Signature	1
Key Management and Distribution	1
Firewalls	1
Web and Email Security	2
Cloud Security	1

Coordinator(s)

Dr. Khalid Alsubhi, Associate Professor