Network Security

Code	Credit Hours
CS-381	3+1

Course Description:

This course is the combination of techniques and tools, which is used to secure networks, applications, and resources of an organization. It will also help students understand the tools and building-blocks of security such as cryptography and security protocols.

The successful completion of this course will enable the students to practically use cryptographic algorithms and protocols to secure local resources, network traffics, and distributed applications. It will also help them to identify vulnerabilities in networks and patch them.

Textbook:

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, published by Pearson Education, Inc., publishing as Prentice Hall, 2022.

Reference Books:

1. B. A. Forouzan, D. Mukhopadhyay*, Cryptography and Network Security*, 2nd Edition, Mc-Graw Hill.

2. B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd Edition, Wiley.

3. W. Stallings, *Network Security Essentials: Applications and Standards*, 6th Edition, published by Pearson Education, Inc., 2016.

4. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. (Online at http://www.cacr.math.uwaterloo.ca/hac/)

Prerequisites:

N/A

Assessment System for Theory:

Quizzes	10%
Assignments	10%
Projects	10%
Mid Terms	30%
ESE	40%

Assessment System for Lab:

Quizzes	10%
Assignments	0%
Lab Work and Report	70%
Lab ESE/Viva	20%

Teaching Plan:

Week No	Topics	Learning Outcomes
1	Introduction to Network Security Course	Computer Security Concepts, Security Architecture Security Attacks, Security Services, Security Mechanisms
2-5	Classical Cryptography and Block Ciphers	In this section, the following topics are covered: • Block Cipher vs Stream Cipher • Data Encryption Standard (DES) • Advanced Encryption Standard (AES) • Modes of Operation
6-8	Public Key Cryptography, Integrity and Authentication, Key Management and Distribution	In this section, the following topics are covered: • The RSA Algorithm • Hash Functions and Message Authentication Codes (MACs) • Public Key Distribution and Infrastructure (PKIX) and X.509 certificates
9	**MID SEMESTER EXAM**	
10-12	Secure Virtual Networks	Various protocols are explored in detail including IPsec (for VPN), SSL, and SET
13	Email Security	PGP and S/MIME are briefly covered
14-15	IDS and Firewalls	The different types of firewalls and approaches to intrusion detection are examined
16-17	Mobile and Radio Networks Security	In this section, the threats and countermeasures for different radio and mobile networks are considered
18	**END OF SEMESTER EXAM**	

Practical Plan:

Experiment No	Description
1	Network Packet Analysis Using Wireshark
2	Encryption and Decryption using Vigenère Cipher
3	Decrypting HTTPS on Windows in Wireshark
4	Implementation of Data Encryption Standard (Part 1)
5	Implementation of Data Encryption Standard (Part 2)
6	Implementation of Advanced Encryption Standard (AES)
7	Malware Creation Using Batch Scripting
8	RSA Key Generation and Encryption/Decryption
9	Ensuring the Integrity of a Message
10	Digital Certificates
11	Investigation of Penetration Testing (Open-Ended Lab) (Part 1)
12	Investigation of Penetration Testing (Open-Ended Lab) (Part 2)
13	How To: Crack WEP/WPA password using Aircrack-ng
14	Email Encryption using Pretty Good Privacy (PGP)
15	Semester Project (CEP) (Part 1)
16	Semester Project (CEP) (Part 2)