SIR SYED UNIVERSITY OF ENGINEERING & TECHNOLOGY
COMPUTER ENGINEERING DEPARTMENT

COURSE INFORMATION SHEET
(For Theory Based Course)

Session:	Fall-2023
Course Title:	Cryptography and Network Security
Course Code:	CE-408T
Credit Hours:	3+0
Semester:	8th
Pre-Requisites:	MS-204 Discrete Mathematics / CE-402 Computer Communication and Networks
Instructor Name:	Najam ul Islam Farooqi, Dr. Rukaiya, Shama Qasim
Email and Contact Information:	mfarooqui@ssuet.edu.pk, rukaiya@ssuet.edu.pk, shbano@ssuet.edu.pk
WhatsApp Group	CE-408 CNS
Office Hours:	8:30 am – 5:00 pm

COURSE OBJECTIVE:
The objective of this course is to introduce concepts related to cryptography and Network Security. Different security algorithms and mechanisms will be presented and solutions to security threats will be discussed.

COURSE OUTLINE:
Introduction to data and network security, goals, threats and attacks, Kill chain models, Advanced Persistent Threats, Security mechanisms, Difference between Cryptography and cryptanalysis, Traditional substitution and transposition cipher, Modern symmetric-key cryptography, Simplified DES, DES design principals, Double DES, Triple DES, Concept of Block chain with its applications, and Block cipher modes of operation, Raijndael Algorithm, Mechanism of encryption in AES, Principles of Public Key Cryptosystem, RSA Algorithm, Diffie-Hellman Key Exchange, Application of cryptographic Hash functions, Secure Hash Algorithm (SHA), Key management and distribution, Network Security Mechanisms, IPSec, Virtual Private Network, Firewalls and Intrusion Detection and Prevention Systems

COURSE LEARNING OUTCOMES (CLOs) and its mapping with Program Learning Outcomes (PLOs):

CLO No.	Course Learning Outcomes (CLOs)	PLOs	Bloom's Taxonomy
1	**Explain** fundamental security objectives, security attacks, services, and mechanisms.	**PLO_1** (Engineering knowledge)	**C2** (Understanding)
2	**Apply** various algorithms and security mechanisms to provide confidentiality, integrity, and authentication.	**PLO_3** (Design/Development of Solutions)	**C3** (Applying)
3	**Identify** appropriate techniques to analyze the problems in the discipline of network security.	**PLO_2** (Problem Analysis)	**C4** (Analyzing)

SIR SYED UNIVERSITY OF ENGINEERING & TECHNOLOGY
COMPUTER ENGINEERING DEPARTMENT

COMPLEX ENGINEERING PROBLEM/ACTIVITY:

Complex Engineering Problem Details	**Included:** Yes Nature and details of Complex Engineering Problem (CEP): It will be based on CLO3; students will be asked to develop a "Network Security Solution to a given scenario". To investigate the problem, students must use in-depth knowledge related to the concepts: Network Security Mechanisms **Attributes could be: WP1, WP3, WK8, WA4** WP1: Depth of knowledge required WP3: Depth of analysis required WK8: Research Literature WA4: Investigation Assessment in: Assignment # 03
Complex Engineering Activity Details	**Included:** Not included

RELATIONSHIP BETWEEN ASSESSMENT TOOLS AND CLOs:

Assessment Tools	CLO-1 (Marks 27)	CLO-2 (Marks 42)	CLO-3 (Marks 21)
Quizzes	7.4% (02)	9.5% (04)	19% (04)
Assignments	7.4% (02)	9.5% (04)	19% (04)
Midterm Exam	29.6% (12)	28.6% (18)	-
Final Exam	55.6% (15)	52.4% (22)	62% (13)

GRADING POLICY:

Assessment Tools	Percentage
Quizzes	10%
Assignments	10%
Midterm Exam	30%
Final Exam	50%
TOTAL	**100%**

Recommended Book:

- Stallings, William. Cryptography and Network Security: Principles and Practice, 8th Edition, published by Pearson Education, 2020, ISBN 978-0-13-670722-6

Reference Books:

- Forouzan, Behrouz A. Cryptography and Network Security, January 2010 Edition 2nd, Published by Tata McGraw-Hill, ISBN- 10: 0073327530

SIR SYED UNIVERSITY OF ENGINEERING & TECHNOLOGY
COMPUTER ENGINEERING DEPARTMENT

LECTURE PLAN

Course Title: Cryptography and Network Security
Course Code: CE-408T

Week No.	Week Dates	Topics	Required Reading	Key Date
1	03-10-2023 to 06-10-2023	**Chapter 1:** Computer and Network Security Concept	Sta:Pg. 21 Foro-chap 1:pg 1-32	
		Security attacks	Sta:Pg. 27 Foro-chap 1:pg 3-5	
		Security Mechanisms	Sta:Pg. 29 Foro-chap 1:pg 6-8	
2	09-10-2023 to 13-10-2023	**Chapter 3:** Classical Encryption Techniques	Sta:Pg. 86 Foro-chap 3:pg 55-60	**Assignment#01**
		Traditional substitution ciphers (Mono-alphabetic)- Additive Ceasar cipher	Sta:Pg. 92-94 Foro-chap 3:pg 61-64	
		Mono-alphabetic Ciphers Cont. Multiplicative cipher	Sta:Pg. 98 Foro-chap 3:pg 65-66	
		Affine Ciphers	Sta:Pg. 99 Foro-chap 3:pg 66-68	
3	16-10-2023 to 20-10-2023	Traditional substitution ciphers (Poly alphabetic)	Sta:Pg. 107 Foro-chap 3:pg 69-80	**Quiz#01**
		Traditional transposition ciphers	Sta:Pg.108 Foro-chap 3:pg 81-86	
		Chapter 4: Block Cipher and Data Encryption Standards	Sta:Pg.119 Foro-chap 6:pg 159	
		Simplified DES key generation	Power point lecture 5	
		Simplified DES encryption, decryption	Power point lecture 5	
4	23-10-2023 to 27-10-2023	Data encryption standard DES design principals & Algorithm, key generation	Sta:Pg. 129 Foro-chap 6:pg 160-173	
		DES Encryption, Decryption	Sta:Pg. 131 Foro-chap 6:pg 160-173	
5	30-10-2023 to 03-11-2023	**Chapter 6**: Advance Encryption Standard	Sta:Pg. 172-178 Foro-chap 7:pg 191-192	**Assignment#02**
		AES Key Generation	Sta:Pg. 190-192 Foro-chap 7:pg 193-195, pg 207-211	
		AES Encryption	Sta:Pg. 179-189 Foro-chap 7:pg 195-201	
6	06-11-2023 to 10-11-2023	Multiple Encryption and Triple DES	Sta:Pg. 202 - 207 Foro-chap 6:pg 181-185	
		Chapter 7: Block Cipher Operation	Sta:Pg. 208 Foro-chap 8:pg 225	
		Modes of Block Cipher	Sta:Pg. 213-221 Foro-chap 7:pg 226-238	
7	13-11-2023 to 17-11-2023	**Chapter 9:** Public-key cryptography	Sta:Pg. 284-293	
		RSA	Foro-chap 10:pg 301-305	
		RSA Continue	Sta:Pg. 294-294 Foro-chap 10:pg 301-305	
8	**Midterm Examination (20-11-2023 to 24-11-2023)**			
9	27-11-2023 to	**Chapter 10**: Other Public Key Crypto System	Sta:Pg. 314-316	

SIR SYED UNIVERSITY OF ENGINEERING & TECHNOLOGY
COMPUTER ENGINEERING DEPARTMENT

	01-12-2023	Diffie-Hellman Key Exchange		**Quiz#02**
		Chapter 11: Cryptographic Hash Functions,	Sta:Pg. 340-347 Foro-chap 12:pg 363-367	
		SHA- I	Sta:Pg. 340-347 Foro-chap 12:pg 363-367	
10	04-12-2023 to 08-12-2023	Block chain, Methods and its applications	Online resource	**Assignment#03**
		Chapter 13: Digital signatures	Sta:Pg. 420-426 Foro-chap 13:pg 389-394	
		RSA and DSS approach	Sta:Pg. 426-430 Foro-chap 13:pg 396-400	
11	11-12-2023 to 15-12-2023	**Chapter 15:** User Authentication Protocol	Sta:Pg. 474	
		Remote User Authentication Principles	Sta:Pg. 474-478	
		Kerberos	Sta:Pg. 482-495 Foro-chap 15:pg 443-447	
12	18-12-2023 to 22-12-2023	**Chapter 19**: Electronic Email Security, Email threats, comprehensive email security	Sta:Pg. 613-624 Foro-chap 16:pg 467	
		S/MIME/TLS	Sta:Pg. 627-638 Foro-chap 16:pg 492-499	
		Pretty Good Privacy (PGP), PGP Services	Sta:Pg. 638-639 Foro-chap 16:pg 470-472	
13	25-12-2023 to 29-12-2023	**Chapter 20:** IP Security	Sta:Pg. 662-667 Foro-chap 18:pg 552-562	**Quiz#03**
		Services and Policies, IP Security Header	Sta:Pg. 673-680	
		Internet Key Exchange	Sta:Pg. 684-692 Foro-chap 18:pg 563-566	
14	01-01-2024 to 05-01-2024	**Chapter 23**: Firewalls	Online resource	
		Firewall characteristics and access policy	Online resource	
15	08-01-2024 to 12-01-2024	Types of firewalls	Online resource	
		Firewall location and configuration	Online resource	
		Revision	-	
16	15-01-2024 to 19-01-2024	Make Up Class for 16 Week may be adjusted before Midterm	-	-
Final Examination (22-01-2024 to 26-01-2024)				

Sta: William Stallings, Foro: Behrouz A. Forouzan

Name & Signature: _____ Date: _____
(Najam ul Islam Farooqui)

Name: & Signature: _____ Date: _____
(Head of Department)