COURSE OUTLINE

Subject Title: Cryptography and Network Security	**Teacher's Name:** Risala Tasin Khan, Ph.D
Course Code: IT-4257	**Designation:** Professor
Credit Hour: 3	**E-mail:** risala@juniv.edu
Contact Hour:1.2+1.2	**Advising Hour:** Office Time on Monday, Tuesday and Thursday

Course Objectives:

1. To introduce basic computer security methods and practices, and their appropriate application.
2. To provide a general understanding of cryptography and network security.
3. To expose the students to the role for security audit.
4. To highlight recent advances in security and privacy.

Course Outcome:

CO	Description	Domain/ level of learning taxonomy
CO1	**Explain** terms related to important computer security and privacy techniques	Cognitive / L2, Affective / L2
CO2	**Understand** security threats, apply principles and practices of computer security to solve them	Cognitive / L3, Affective / L3
CO3	**Identify** vulnerability of systems, assess relevant risks and propose solutions to solve the problems	Cognitive / L4, Affective / L3
CO4	**Learn** to clearly communicate to point out legal and ethical issues in computer security	Cognitive / L4, Affective / L4

Text Books:

1. Behrouz A Forouzan , “Cryptography and Network Security”, Tata McGraw Hill Education Pvt. Ltd., New Delhi
2. William Stallings, “Cryptography and Network Security, fourth edition, Prentice Hall, New Delhi

Distribution (Planning) of the Course Contents:

Lecture No.	Contents
Lec:1-2	Basic idea of Security ➢ Key idea of computer security ➢ CIA Triad ➢ Goal of Information Security ➢ Basic idea of Risk, Vulnerability, and Threat ➢ Security Control ➢ DAD Triad ➢ Data security states ➢ OSI Security Architecture ➢ Security Services
Lec:3-5	Mathematics of Network Security ➢ Fundamental knowledge on different mathematical terms ➢ Basic knowledge on GCD and LCM ➢ Extended Euclidean Algorithm ➢ Linear Diophantine Equation ➢ Congruence Relation ➢ Modular Arithmetic ➢ Multiplicative Inverse ➢ Modular Inverse ➢ Set of additive and multiplicative inverse
	QUIZ-1
Lec-7-8	Cryptography Basic ➢ Cryptographic concept ➢ Symmetric and Asymmetric Cryptography ➢ Hashing Algorithm ➢ Data Encryption Standards ➢ Digital Signature ➢ Cryptographic Attacks
Lec-9-11	Classical Encryption Techniques

	➢ Symmetric Cipher Model ➢ Cryptanalytic and Brue-Force Attack ➢ Substitution Technique ➢ Transposition Ciphers
Quiz 2	
Lec-13-14	Digital Signature and Hash Function ➢ Digital Signature Basics and Process ➢ Service Provided by Digital Signature ➢ Digital Signature vs Cryptosystem ➢ MAC vs Digital Signature ➢ Cryptographic Hash Function ➢ Application of Hash Function ➢ Properties of Hash Function ➢ Simple Hash Function ➢ MAC vs Hash Coding
Lec-15-16	Authentication and Authorization ➢ Some Basic Terminology ➢ Different types of Authentication ➢ Authentication vs Authorization ➢ Message vs Entity Authentication ➢ Message Authentication using MAC ➢ Message Authentication using Hash Function ➢ Authentication Factors ➢ Different types of Password Authentication ➢ Possible Attacks on Password Verification ➢ Authentication by Inherence Factor ➢ Biometric in details
Lec-17-19	Key Management and Certifications ➢ Problems with Trusted Third Party ➢ Key Distribution Center ➢ Protocols of creating session key using KDC ➢ Using multiple KDCs ➢ Kerberos ➢ Symmetric Key Agreement ➢ Public Key Distribution ➢ Digital Certificate ➢ X.509 Digital Certificate ➢ Certificate Authority ➢ Public Key Infrastructure (PKI)

Quiz-3	
Lec-21-22	DES and RSA Cryptosystem ➢ Introduction to Modern Block Cipher and their characteristics ➢ Components of modern block cipher ➢ Product Cipher ➢ Feistel and non-Feistel cipher ➢ Short history of DES ➢ Basic structure of DES ➢ Round key generation process ➢ Discussion on RSA cryptosystem
Lec-23-24	E-mail Security ➢ E-mail Security Threats ➢ E-mail Security Solutions ➢ PGP ➢ S/MIME
Lec-25	Firewall Design Principles ➢ Firewall Architecture and their limitation ➢ The DMZ firewall and its limitation
Lec-26	Web Security and IPSec ➢ Overview of Web Security ➢ IPSec ➢ SSL/TLS ➢
Lec-27	Vulnerability Assessment ➢ Overview of network vulnerability ➢ Port Scanner ➢ Password Cracker

--- --- --- --- --- ---

Signature of the Faculty