ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD
(Department of Computer Science)

WARNING

1. **PLAGIARISM OR HIRING OF GHOST WRITER(S) FOR SOLVING THE ASSIGNMENT(S) WILL DEBAR THE STUDENT FROM AWARD OF DEGREE/CERTIFICATE, IF FOUND AT ANY STAGE.**
2. **SUBMITTING ASSIGNMENTS BORROWED OR STOLEN FROM OTHER(S) AS ONE'S OWN WILL BE PENALIZED AS DEFINED IN "AIOU PLAGIARISM POLICY".**

Course: Data & Network Security (3484) **Semester: Autumn, 2013**
Level: Bachelor **Total Marks: 100**

ASSIGNMENT No. 1

All questions carry equal marks.

Q.1 Describe the major security problems in view of data and network. Also a research in finding the solution for these problems.

Q.2 Describe security attack. How these attacks will be tackled and deterred? Elaborate.

Q.3 The basic security goals are confidentiality, Integrity and availability (CIA). Describe the issues and problems in achieving these goals.

Q.4 What are the role of security professional in the development of security standards and guidelines for a secure system?

Q.5 What is the role of different communication protocols in the realm of security in the information system?

ASSIGNMENT No. 2
Total Marks: 100

All questions carry equal marks.

Q.1 Describe the major problems that are associated with the physical security of system. Also describe their solution as a security professional.

Q.2 What is cryptography? Also describe the process of cryptanalysis.

Q.3 Check sum, hash function and digital signature provide security up to good level. How? Justify it.

Q.4 Do a research and find the basic terminology of cryptographic algorithms.

Q.5 Discuss the various attacks on information and system security. Describe their effectiveness and payoff.

3484 Data & Network Security

Recommended Book: **Principles of Computer Security by Wm. Arthur Conklin, Gregory B. White, Chuck Cothren**

Course Outline:

Unit 1: Introduction and Security Trends
The Security Problem, Security Incidents
Threats to Security, Security Trends
Avenues of Attack, Types of Attacks

Unit 2: General Security Concepts
Basic Security Terminology, Security Basics
Access Control, Security Models
Confidentiality Models, Integrity Models

Unit 3: Operational / Organizational Security
Security Operations in an Organization
Standards and Guidelines
The Security Perimeter, Physical Security

Unit 4: Standards and Protocols
PIKX/PKCS, PKIK Standards
PKCS, X.509, SSL/TLS, ISAKMP, CMP, XKMS

Unit 5: The Impact of Physical Security on Network Security
The Problem, Physical Security Safeguards
Policies and Procedures, Access Controls, Authentication

Unit 6: Conventional Encryption
Conventional Encryption Model, Classical Encryption Techniques
The Data Encryption Standard (DES), Triple DES
Placement of Encryption Function, Traffic Confidentiality

Unit 7: Authentication and Digital Signatures
Authentication requirements, Authentication Functions
Cryptographic Check sums, Hash Functions
Digital Signature

Unit 8: Cryptographic Algorithms
The MD5 Messages Digest Algorithm
The Secure Hash Algorithm (SHA)

Unit 9: Attacks and Malware
Attacking Computer Systems and Networks
Denial-of-Service Attacks, Backdoor and Trapdoors, Sniffing, Spoofing
Man-in-the-Middle Attacks, Reply Attacks, TCP/IP Hijacking
Attacks on Encryption, Password Guessing, Software Exploitation
Social Engineering, Malware.