ALLAMAIQBALOPENUNIVERSITY, 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 ASSIGNMENT(S) 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, 2012**
Level: Bachelor **Total Marks: 100**
Pass Marks: 40

ASSIGNMENT No. 1

Note: All questions carry equal marks.

Q. 1 Describe the vulnerability issues in security. Also describe modern types of security attacks.

Q. 2 a) Explain the methodology of various types of attacks and their countermeasures.
b) What is the effectiveness of Access Control List (ACL) in security management system?

Q. 3 Define the goals of security system. Also describe the purpose of various security models.

Q. 4 What are the different levels of security put into practice by security unit for full proof security to organization assests?

Q. 5 Elaborate the basics of Public-Key infrastructure X.509/Public-Key Cryptography Standards (PIKX/PKCS) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards in security perspectives.

ASSIGNMENT No. 2

Total Marks: 100

Note: All questions carry equal marks.

Q. 1 Organizational executive has decided to rewrite the policies and procedures for physical security. Considering physical security's impact on network security, write a memo to management giving several recommendations that world get user more involved with security.

Q. 2 Explain the concept of key space. How does it improve an algorithm's ability to protect data?

Q. 3 Explain why 3DES is stronger than regular DES?

Q. 4 Describe the purpose of transposition, shift, stream and block cipher. Give examples of each.

Q. 5 Describe the type of information that attackers might try to obtain if they were able to install a sniffer on a network.

3484 Data & Network Security Credit Hours: 3 (3+0)

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

Course Outline:
Unit No. 1 Introduction and Security Trends

The Security problem, Security Incidents
Threats to Security, Security Trends
Avenues of Attack, Types of Attacks

Unit No. 2 General Security Concepts

Basic Security Terminology, Security Basics
Access Control, Security Models
Confidentiality Models, Integrity Models

Unit No. 3 Operational/Organizational Security

Security Operations in an Organization
Standards, and Guidelines
The security Perimeter, Physical Security

Unit No. 4 Standards and Protocols

PIKX/PKCS, PKIK Standards
PKCS, X.509, SSL/TLS, ISAKMP, CMP, XKMS

Unit No. 5 The Impact of Physical Security on Network Security

The problem, Physical Security Safeguards
Policies and procedures, Access Controls, Authentication

Unit No. 6 Conventional Encryption

Conventional Encryption Model, classical Encryption Techniques
The Data Encryption Standard (DES), Triple DES
Placement of Encryption Function, Traffic Confidentiality

Unit No. 7 Authentication and Digital Signatures

Authentication requirements, Authentication Functions
Cryptographic check sums, Hash Functions
Digital Signature

Unit No. 8 Cryptographic Algorithms

The MD5 Messages Digest Algorithm
The Secure Hash algorithm (SHA)

Unit No. 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

=========