Institute of Computer Science/Information Technology (ICS&IT)
Faculty of Management Sciences & CS/IT (FMCS)
The University of Agricultural Peshawar

Program:	BS(CS)-4
Course Title:	Information Security
Course Code:	CC-501
Course Hours:	03
Total Weeks:	16
Total Credit Hours:	48

Course Objective

Often there has been a need to protect information from 'prying eyes'. In the electronic age, information that could otherwise benefit or educate a group or individual can also be used against such groups or individuals. Industrial espionage among highly competitive businesses often requires that extensive security measures be put into place. And, those who wish to exercise their personal freedom, outside of the oppressive nature of governments, may also wish to encrypt certain information to avoid suffering the penalties of going against the wishes of those who attempt to control. So this course will help to secure information from eavesdroppers.

Week-1

- Introduction to information security
  - Concept of Confidentiality, integrity, availability, authenticity and accountability.
  - Threats and attack
- Basic concepts
  - Malware
    - Virus, Worms, Anti-malware
  - Hacking, Intruder

Week-2

- Security Basic
- Security approach
- Security Attack
  - Active Attack Vs Passive Attack
- Types of Security Threat
  - Interception
  - Interruption
  - Modification
  - Fabrication

Week-3

- Cryptanalysis

- Brute force Attack
- Cryptanalytic Attack
  - Chosen Plain Text
  - Chosen Cipher Text
  - Chosen Text
  - Cipher Text only
  - Known plain text

Week-4

- Types of Cryptography
  - Symmetric Encryption
    - Substitution
      - Ceaser cipher, Mono alphabetic, Play fair, Hill cipher
      - Poly alphabetic
        - Vegner cipher
        - Vernam
    - Transposition
    - Steganography
  - Public Key Cryptography
  - Hash Algorithm

Week-5

- Famous Algorithm of Private Key Cryptography (DES & IDEA)
- DES (Data Encryption Standard)
  - Initial & Final Permutation
  - DES Round
  - Per-Round Key generation
  - Mangler function

Week-6

- Using Secret/Private Key Cryptography to Encrypt Large Messages
  - Electronic Code Book
  - Cipher Block Chaining

Week-7

- Modular Mathematics
  - Method to Encrypt messages
- Congruence
- Totient function

Week-8

- RSA Public Key System
- Deffie-Hellman Algorithm

Week-9

- Authentication
  - Password Based
  - Address Based
  - Cryptographic Based

Week-10
- Hash Algorithm/Message Digest
  - MD2
  - MD4

Week-11
- Digital Signature
- Trusted Intermediaries
- Key Distribution Protocol

Week-12
- Digital Certificate
- Certification Authority
- Certificate Revocation List(CRL)

Week-13
- Kerberos
  - Notation
  - Simple Authentication
- Establish Secure Channels

Week-14
- Assumption of Kerberos and ticket
- Attacks against IP

Week-15-16
- Firewalls
  - Packet Filter
  - Application level Gateway
  - Hybrid

Total Marks: 100

Recommended Text Book:

Cryptography and Network Security: Principles and Practice
By: William Stallin