

**AL-MANSOUR UNIVERSITY COLLEGE**  
**Dept. of Computer Science & Information Systems**

**Subject** : Computer Security

**Year** : Fourth

**Weekly hours:** 2 Theoretical + 2 Lab

| <b>N</b> | <b>CONTENTS</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>H</b> |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1        | <b><u>Data Security</u></b> <ul style="list-style-type: none"><li>- Introduction</li><li>- Key Areas of Risks</li><li>- Management of Data Security</li><li>- Physical security</li><li>- Logical Access control</li><li>- Backup and disaster</li><li>- Telecommunication security</li><li>- Application Development</li><li>- Data Base Security</li><li>- Office systems</li></ul>                                                                                             | 10       |
| 2        | <b><u>Computer Security :an overview</u></b> <ul style="list-style-type: none"><li>- Introduction</li><li>- Kinds of threats to the Security of computer</li><li>- Characteristics of computer intrusion</li><li>- Second service problems</li><li>- Types of problems that can block a computing systems</li><li>- Types of attacks &amp; controls</li><li>- Method of defenses</li></ul>                                                                                        | 6        |
| 3        | <b><u>Basic Encryption and Decryption</u></b> <ul style="list-style-type: none"><li>- Terminology and Background</li><li>- Mono alphabetic ciphers (substitutions)</li><li>- Poly alphabetic ciphers</li><li>- Transposition ciphers (simple and double)</li><li>- Stream and Block ciphers</li><li>- One-time pads</li><li>- Confusion &amp; Diffusion</li><li>- Shannon's five criteria</li><li>- The concept of randomness</li><li>- Statistical test for randomness</li></ul> | 12       |
| 4        | <b><u>Secure Encryption Systems</u></b> <ul style="list-style-type: none"><li>- Complexity</li><li>- Properties of Arithmetic</li><li>- Public key system</li><li>- Kerkle-Hellman Knapsacks</li><li>- RSA system</li><li>- DES</li><li>- Characteristics of good cipher</li></ul>                                                                                                                                                                                                | 14       |

|                         |                                                                                                                                                                                                                                                           |    |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 5                       | <b><u>Security Involving Programs</u></b> <ul style="list-style-type: none"> <li>- Information Access problems</li> <li>- Service problems</li> <li>- Program Development controls against programs attacks</li> <li>- Administrative controls</li> </ul> | 4  |
| 6                       | <b><u>Protection Services for users of operating system</u></b> <ul style="list-style-type: none"> <li>- Protected objects</li> <li>- Security Method of operating system</li> <li>- Protection of memory and addressing</li> </ul>                       | 10 |
| 7                       | <b><u>Personal Computer Security</u></b> <ul style="list-style-type: none"> <li>- Contributors to security problems</li> <li>- Security measures</li> <li>- Protection for files</li> <li>- Copy protection</li> </ul>                                    | 4  |
| Total theoretical hours |                                                                                                                                                                                                                                                           | 60 |

### **References :**

1. Deborah Russell and G.t Gangemi, ( 2002 ), Computer Security Basics.
2. R. Shinner, ( 1996 ), Applied Cryptography, Second edition, John Wiley & Sons Infoundationsw, New York.
3. H. Beker & F. Piper, ( 1982 ), Cipher Systems, Noth wood publication.