

Course Specification
(4104 Computer Security)

Faculty: HICIT- **Higher Institute for Computers & Information Technology**

Programme(s) Title: Under graduate program in Computer Science

Major or minor element of programme: Compulsory

Department offering the programme: Department of Computer Science

Department offering the course: Department of Computer Science

Academic year / Class: 4th Year – 1st Semester

Main/Secondary: Main

Date of specification approval: 22/9/2015

A- Basic Information

Title: Computer Security

Code: 4104

Weekly Hours:

Lecture: 3

Exercise: -

Practical: 3

Total: 6

B- Professional Information

1 - Course Objectives:

To give the student the knowledge and practice of how to secure various components of the computer system.

After completing this course, the student should be able to identify the various threats to computer system and information exchanged over the network, and how to counter them, to be aware of various cryptosystems.

2- Program ILOs Covered by Course

Program Intended Learning Outcomes			
Knowledge and understanding	Intellectual Skills	Professional and practical skills	General and Transferable skills
a10, a18, a19	b1, b2, b16	c6, c9	

3- Intended learning outcomes of course (ILOs)

a- Knowledge and understanding:

- a1. Understanding the definition of the various threats, security services, protection techniques over the exchanged information.
- a2. Understanding the definition of the symmetric-key cryptosystems, asymmetric-key cryptosystems, and hybrid cryptosystems

b- Intellectual skills

- b1. Evaluate the computer assets and define security requirements.

- b2. Think over the security problems and schemes in various cryptosystems (symmetric-key cryptosystems, asymmetric-key cryptosystems, and hybrid cryptosystems).

c- Professional and practical skills

- c1. specify basic security issues.
c2. Apply counter measure for information exchange threats.

D- General and transferable skills

- d1. Work effectively as an individual and as a member of a team.
d2. Write Structural Report.

4- Contents

Topic	No. of Hours	Lectures	Practical
Introduction to computer security/database /program /O.S., network, and physical security.	12	6	6
Security threats, protection services, and protection mechanisms.	18	9	9
Symmetric-key Cryptosystems: Classical techniques/ Modern techniques	18	9	9
Public-key Cryptosystems	12	6	6
Hybrid Cryptosystems	18	9	9

5 -Teaching and learning methods

- 4.1 Lectures
4.2 Tutorial Exercises
4.3 Practical Lab
4.4 Discussions.

6 -Student assessment methods

- 5.1 Midterm Exam: To assess the knowledge and understanding achieved by the student during the previous weeks.
5.2 Final Exam: To evaluate what the student gain at the end of the course, and to assess: the knowledge and understanding, general skills, and intellectual skills.
5.3 Course Work &Quizzes: To keep the student always in the course, and to evaluate knowledge, understanding, intellectual, and transferable skills.

Assessment Schedule

Assessment	Week #
Mid Term Exam	8
Final Exam	16

Course Work &Quizzes	2-14
---------------------------------	-------------

Assessment Weight

Assessment	Weight %
Mid Term Exam	10%
Final Exam	80%
Course Work &Quizzes	10%
Total	100

Course Work &Quizzes: (Short Exams, Assignments, Researches, Reports, Presentations, Class/Project discussion)

7 -List of references

7.1 -Essential books (text books)

Cryptography and Network Security, Principles and practice, 2nd Edition
William Stalling, 1999

Cryptography and Network Security: Principles and Practice 6th Edition
by [William Stallings](#)

7.2 -Recommended books

Security in Computing, 3rd edition, Charles P. Pfleeger and Shari L. P. Pfleeger

7.3 -Periodicals, Web sites, ... etc

None

8- Facilities required for teaching and learning

MS Project SW Package for scheduling projects

MS Power Point SW Package for presentation

MS Word SW Package for system documentation preparation

9- Course Matrices

9.1 Course Content/ILOs Matrix

Contents	a1	a2	b1	b2	c1	c2	d1	d2
Introduction to computer security/database /program /O.S., network, and physical security.	√		√		√	√		
Security threats, protection services, and protection mechanisms.	√		√		√	√		
Symmetric-key Cryptosystems: Classical techniques/ Modern techniques		√	√	√	√	√		
Public-key Cryptosystems		√	√	√	√	√		
Hybrid Cryptosystems		√	√	√	√	√		

9.2 Learning Method /ILOs Matrix

Learning Methods	a1	a2	b1	b2	c1	c2	d1	d2
Lecture	√	√	√	√	√	√		
Tutorial Exercises			√	√	√	√		
Practical Lab			√	√	√	√		
Discussions.			√	√	√	√	√	√

9.3 Assessment Methods /ILOs Matrix

Assessment Methods	a1	a2	b1	b2	c1	c2	d1	d2
Midterm Exam	√	√	√	√	√	√		
Final Exam	√	√	√	√	√	√		
Course Work & Quizzes	√	√	√	√	√	√	√	√

Course coordinator: Dr. Magdy E.Elhennawy

Head of Department: Dr. Farouk A. Shabaan

Date : 22/9/2015

