

# TEMPLATE FOR COURSE SPECIFICATION

## HIGHER EDUCATION PERFORMANCE REVIEW: PROGRAMME REVIEW

### COURSE SPECIFICATION

This Course Specification provides a concise summary of the main features of the course and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the learning opportunities that are provided. It should be cross-referenced with the programme specification.

1. Teaching Institution	AL-Nahrain University
2. University Department/Centre	Computer science
3. Course title/code	Computing Security I
4. Program (s) to which it contributes	BSc
5. Modes of Attendance offered	Full time
6. Semester/Year	First semester/Forth year
7. Number of hours tuition (total)	3 hours (3 Lec)
8. Date of production/revision of this specification	1-9-2022
9. Aims of the Course:-	
The main aim of the course is to introduce the students to the principles of comouting security. It focuses on explain the abbreviations of the computing security, also explain the using techniques for achiving the best data security.	
In this semester, focuses on the common techniques for authentication, and Encryption, the types of the hachers and the techniques that used by the hachers.	

## 10. Learning Outcomes, Teaching ,Learning and Assessment Method

### A- Knowledge and Understanding

- A1. To teach students how the analysis and conclude the new methods for the security.
- A2. To teach students how to improve the current methods for security.
- A3.

### B. Subject-specific skills

- B1. To teach students the working of the common method of security that currently used.
- B2. To teach students the working of the methods of security and explain the weak points for each method.
- B3.To try the improving the security algorithms.

### Teaching and Learning Methods

Book, Lectures & homeworks.

### Assessment methods

Exams , Quizzes, and homeworks.

### C. Thinking Skills

- C1.try to explain the methods of security and how exploited by hackers in reality.
- C2.try to asked some questions that answers by a next lectures.
- C3.
- C4.

### D. General and Transferable Skills (other skills relevant to employability and personal development)

- D1. The student able to solve a real security problem.
- D2. Reads a good articles for this topics from the Internet.
- D3.

11. Course Structure					
Week	Hours	ILOs	Unit/Module or Topic Title	Teaching Method	Assessment Method
1	3		Data Security Principles 1. Security 2. Confidentiality 3. Integrity 4. Availability 5. Authentication 6. Accountability (Non-Repud	* Lecture	*Quiz & activity
2	3		Security Attack 1. Passive Attacks 2. Active Attacks	* Lecture	*Quiz & activity
3	3		-Basic Terminology -Basic Cryptographic Algorithms	* Lecture	*Quiz & activity
4	3		* Mathematics •Greatest Common Divisor(GCD) •(LCM) Least Common Multiple •Modular •Euler Function : •Inverse Algorithm (inv)	* Lecture	*Quiz & activity
5	3		* Block cipher Historically Symmetric Cipher Model Feistel Mode	* Lecture	*Quiz & activity
6	3		Confusion and Diffusion Substitution ( S-boxes) Permutation (P-boxes) Substitution-Permutation Network	* Lecture	*Quiz & activity

7	2		EXAM1	-	-
8	3		<p>Block Cipher Mode</p> <ul style="list-style-type: none"> <li>• ECB Operation Mode</li> <li>• CBC Operation Mode</li> <li>• Cipher FeedBack (CFB)</li> <li>• Output Feedback Mode (OFB)</li> </ul>	* Lecturer	*Quiz & activity
9	3		<p>Stream cipher</p> <ul style="list-style-type: none"> <li>• Stream Cipher Structure</li> <li>• Important element for design a stream cipher</li> <li>• Types of stream ciphers <ul style="list-style-type: none"> <li>▪ Synchronous stream ciphers</li> <li>▪ Self-synchronizing stream ciphers</li> </ul> </li> </ul>	* Lecturer	*Quiz & activity
10	3		<p>* Public-Key Cryptography</p> <p>Public-Key Characteristics</p> <p>Public-Key Applications</p> <p>Security of Public Key Schemes</p> <p>RSA description and algorithm</p> <p>Key Generation Algorithm</p> <p>Examples</p> <p>VIRUSES and OTHER MALICIOUS CONTENT</p> <p>Introduction</p> <p>Trapdoor</p> <p>Logic Bomb</p> <p>Trojan Horse</p> <p>Zombie</p>	* Lecturer	*Quiz & activity

			Bacteria Viruses Virus Operation.		
11	3		* Types of Viruses Boot Sector Viruses Executable Viruses Macro Viruses E-Mail Viruses Anti-Virus Software • first-generation • second-generation • third-generation fourth-generation Chapter Seven : Firewall Firewall Definition: Firewall Concept, Conditions, • <i>Firewall Concept.</i> • <i>Firewall Conditions.</i>	* Lecturer	*Quiz & activity
12	3		* Data Hiding Steganography and Watermarking The Need for Data Hiding Issues in Data Hiding Steganography	* Lecturer	*Quiz & activity
13	3		* Steganography types: 1- Pure Steganography: 2- Secret Key Steganography. 3 Public Key Steganography. Least significant bit (LSB) insertion. Watermarks	* Lecturer	*Quiz & activity
14	2		EXAM 2	-	-

## 12. Infrastructure

Required reading: <ul style="list-style-type: none"><li>· CORE TEXTS</li><li>· COURSE MATERIALS</li><li>· OTHER</li></ul>	<b>Cryptography And Network Security Principles And Practice</b> Fifth Edition William Stallings 2015
Special requirements (include for example workshops, periodicals, IT software, websites)	
Community-based facilities (include for example, guest Lectures , internship, field studies)	