Course Description Form

1. Course Name:
Computing Security I
2. Course Code:
COMP300
3. Semester / Year:
Second semester/ four year
4. Description Preparation Date:
1-10-2025
5. Available Attendance Forms:
Full Time
6. Number of Credit Hours (Total) / Number of Units (Total)
60 h(30 theoretical +30 practical) /4 units
7. Course administrator's name (mention all, if more than one name)
Name: Asst. Prof. Dr. Dalal N. Hamood Email: dalal.naeem@nahrainuniv.edu.iq Assist Lecturer Ibtihal Abbass Lecturer Assad
8. Course Objectives

Course Objectives	The main aim of the course is to introduce the students to the principles of computing security. It focuses on explain the abbreviations of the computing security, also explain the using techniques for achieving the best data security. In this semester, focuses on the common techniques for authentication, and Encryption, the types of the hackers and the techniques that used by the hackers.

9. Teaching and Learning Strategies	
Strategy	Book, Lectures, Quizzes, Exam & homework's.

10. Course Structure

Week	Hours	Required Learning Outcomes	Unit or subject name	Learning method	Evaluation method
1	2		* **1.**Data Security Principles 1. Security 2. Confidentiality	* Lecturer	Quiz & activity

			3. Integrity 4. Availability 5. Authentication 6. Accountability (Non-Repudiation)		
2	2		Security Attack 1. Passive Attacks 2. Active Attacks	* Lecturer	Quiz & activity
3	2		**1-**Basic Terminology 1-Basic Cryptographic Algorithms	* Lecturer	Quiz & activity
4	2		* Mathematics • Greatest Common Divisor(GCD) • (LCM) Least Common Multiple • Modular • Euler Function : • Inverse Algorithm (inv)	* Lecturer	Quiz & activity
5	2		* Block cipher Historically Symmetric Cipher Model Feistel Mode	* Lecturer	Quiz & activity
6	2		Confusion and Diffusion Substitution (S-boxes) Permutation (P-boxes) Substitution-Permutation Network	* Lecturer	Quiz & activity
7	2		EXAM1	* Lecturer	Quiz &

					activity
8	2		Block Cipher Mode • ECB Operation Mode • CBC Operation Mode • Cipher FeedBack (CFB) • Output Feedback Mode (OFM)	* Lecturer	Quiz & activity
9	2		Stream cipher • Stream Cipher Structure • Important element for design a stream cipher • Types of stream ciphers ▪ Synchronous stream ciphers ▪ Self-synchronizing stream ciphers	* Lecturer	Quiz & activity
10	2		* Public-Key Cryptography Public-Key Characteristics Public-Key Applications Security of Public Key Schemes RSA description and algorithm Key Generation Algorithm Examples VIRUSES and OTHER MALICIOUS CONTENT Introduction Trapdoor Logic Bomb Trojan Horse	* Lecturer	Quiz & activity

			Zombie Bacteria Viruses Virus Operation.		
11	2		* 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, • *Firewall Concept.* • *Firewall Conditions.*	* Lecturer	Quiz & activity
12	2		* Data Hiding Steganography and Watermarking The Need for Data Hiding Issues in Data Hiding Steganography	* Lecturer	Quiz & activity
13	2		* Steganography types: 1- Pure Steganography: 2- Secret Key Steganography. 3 Public Key Steganography. Least significant bit (LSB) insert Watermarks	* Lecturer	Quiz & activity
14	2		EXAM 2	* Lecturer	Quiz & activity

11. Course Evaluation

Mid 10
Quizzes 10
HW 10
Activities (or report) 10

Final exam 50 Final Lab 10	
12. Learning and Teaching Resources	
Required textbooks (curricular books, if any)	
Main references (sources)	**Cryptography And Network Security Principles And Practice** Fifth Edition William Stallings 2015
Recommended books and references (scientific journals, reports…)	
Electronic References, Websites	