Department of Computer Science

College of Science

University of Salahaddin

Subject: Information Security1

Course Book – *Year 4(CS and IT) branches*

Lecturer's name: Newroz Nooralddin Abdulrazaq

Academic Year: 2022/2023

Course Book

1. Course name	Information Security
2. Lecturer in charge	Newroz Nooralddin Abdulrazaq
3. Department/ College	Computer Science and Information Technology / Science
4. Contact	E-mail: Newroz.abudlrazaq@su.edu.krd Tel: +964(0)7504052680
5. Time (in hours) per week	Theory: 2 + Practical: 2
6. Office hours	**Sunday** : 8:30 am -12:30 pm Practical (Practical CS Branch-2Groups) + **Tuesday** : 8:30 am –10:30 (Theoretical-IT branch , 12:30– 2:30 pm (Theoretical-CS-branch)+ **Thursday** : 8:30 am - 12:30 pm Practical (Practical CS Branch-2Groups)
7. Course code	
8. Teacher's academic profile	» Final Grade: 60.58% (Rank: 3 in a class of 15 students) 07/1995 **Iraq. Secondary School Degree** ("Shikh Mahmood Alhafid"), Erbil; Iraq. » Final Grade: 80.66% PUBLICATIONS Qaradaghi, T.; Abdulrazaq, N. (2015), 'Comparison between Separable and Irreducible Goppa Code in McEliece Cryptosystem', World Academy of Science, Engineering and Technology, International Science Index 106, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9(10), 2065 - 2071. "Cryptosystem Based on Error Correcting Codes", Zanco Journal of Pure and Applied Sciences,

	Salahaddin University- Erbil 2016, Vol 22, No. 2, 99-109. "Evaluation Study of Original McEliece Cryptosystem Against Side Channel Attack" Journal of Zankoy Sulaimani-Part A- for Pure and Applied Science 2016. CONFERANCES "ICCNS 2015: 17th International Conference on Cryptography and Network Security, Istanbul, Turkey, October 26-27,2015" 'Comparison between Separable and Irreducible Goppa Code in McEliece Cryptosystem'.
9. Keywords	**Information Security- Computer Security- Security Components- Control Access Matrix- Authentication-Assurance- Threats- Cryptography- Cryptanalysis- Cryptosystem- Encryption- Decryption- Malware- Firewall- Password Management.**

Course Overview

Information security can be defined as the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. Or it Protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

cryptography is an essential component of computer security; it is by no means the only component. Cryptography provides a mechanism for performing specific functions, such as preventing unauthorized people from reading and altering messages on a network. However, unless developers understand the context in which they are using cryptography, and unless the assumptions underlying the protocol and the cryptographic mechanisms apply to the context, the cryptography may not add to the security of the system. The canonical example is the use of cryptography to secure communications between two low-security systems. If only trusted users can access the two systems, cryptography protects messages in transit. But if untrusted users can access either system (through authorized accounts or, more likely, by breaking in), the cryptography is not sufficient to protect the messages. The attackers can read the messages at either endpoint.

11. Course objective:

This course will provide students with an in-depth understanding the principles and of the many applications of Information Security including:

1. Components of information Security and Their Terminologies.
2. Authentication.
4. Information flow
6. Malicious Logics.
7. Basics of Number Theory.
8. Classical Cryptography.
9. Firewalls + AntiMalware + control access control.

12. Student's obligation

The students are obliged to attend the classes. Throughout the course students will be tested through quizzes, assignments, class test.

13. Forms of teaching

- Using Laptop with data show
- Using PowerPoint presentation
- Delivering the PPT slides to the students before giving the lecture.
- Interaction with the students inside the classroom.

14. Assessment scheme:

Assessments: -

- **First Semester exam**
  - Theoretical Monthly Exam % 12
  - Practical Monthly Exam % 30
  - Activity + Assignments+ Quiz 8% (practical & Theoretical)

Examinations

- Final exam %50

15. Student learning outcome:

1- Students will read, interpret, and use the vocabulary, symbolism, and basic definitions used in information security.

2- Students will use the facts, formulas, and techniques learned in this course to Polices of Confidentiality and integrity.

3- Students will use the techniques and methods learned in this course to encrypt and decrypt Messages.

16. Course Reading List and References:

1- Mark Stamp, Information Security: Principles And Practice (Third Edition), 2021.

2- William Stallings, Lawrie Brown, Computer Security Principles and Practice (Second Edition), 2012.

3- Wade Trap, Lawrence Washington, Introduction to Cryptography with Coding Theory (Second Edition), 2006.

17. The Topics:	**Lecturer's name**
Week 1: Introduction, General definitions, and Components of Computer Security, Security Threads, Security Attack, Security Goals, Mechanism and policy **Week 2**: Authentication (password + Biometrics + Two factor) **Week 3-4:** Number Theory related to Classical Cryptography: General definitions + Euclidean Algorithm + Inverse **Week 5-6**: Confidentiality: Classical cryptographic methods: Substitution Ciphers- Monoalphabetic cipher: Shift Cipher + Cryptanalysis using the frequency of the letters + Affine Cipher **Week7:** Midterm Exam **Week8:** Confidentiality: Classical cryptographic methods- Substitution Ciphers-- Polyalphabetic ciphers-Vigenere cipher+ Cryptanalysis knowing a part of plain& cipher text. **Week 9-10**: Playfair cipher + Classical cryptographic methods- Transposition Ciphers: Reverse cipher - Columnar transposition cipher. **Week 11:** Hill Cipher + Block Cipher (one Time pad)	Newroz N. Abdulrazaq (2 hrs)

Week12-13: Software Security: Malicious Logics + Firewalls + Antimalware **Week 14- 15**: Authorization: Control Access Matrix.	
18. Practical Topics (If there is any)	
Harness one of the programming language to implement number theory and classical cryptography techniques including: Euclidian Algorithm to find GCD between two numbers and inverse of arithmetic modular- select some techniques from classical ciphers- select some techniques from modern cryptosystem and how to work patch files.	Newroz N. Abdulrazaq (2 hrs)

19. Examination: Use Techniques, Methods, Models

Question: suppose that Alice provides an online chess playing service known as Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC where they are matched with another player of comparable ability.

a. Where (and why) is confidentiality important for AOC and its customers?

b. Why is integrity necessary?

c. Why is availability an important concern?

Multiple Choices

1- In symmetric cryptography, which of the following MUST be true:

a. Encryption and decryption take the same amount of time.

b. Different algorithms are used for encryption and decryption.

c. Cryptographic operations are one-way, and not reversible.

d. The same key is used for encryption and decryption.

Q) Encrypt (Kurdistan) using Affine cipher with keys alpha=7 and beta=11?

21. Peer review