Department of Computer Science

College of Science

University of Salahaddin

Subject: Information SecurityII

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

Lecturer's name: **Newroz Nooralddin Abdulrazaq**

Academic Year: 2022/2023

Course Book

1. Course name	Information SecurityII
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	**Tuesday**: 8:30 am –10:30 (Theoretical-CS branch , 10:30– 12:30 pm (Theoretical-IT-branch) + **Wednesday**: 8:30 am -12:30 pm (Practical CS Branch-2Groups) + **Thursday** : 8:30 am -12:30 pm (Practical IT 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. Confidentiality: Modern Cryptography- Symmetric Key Cryptography.
2. Number theory for Modern Cryptography
4. Confidentiality: Modern Cryptography- Public Key Cryptography.
5. key Management.
7. Hash Function & Digital Certificate.
8. Network Security.

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: -

- **Second 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 use the techniques and methods learned in this course to encrypt and decrypt Messages using Modern Cryptography.

2- Student will learn how to manage keys in Moder era of Cryptography.

3- Student will learn general definitions and how the data transmitted and protected during Network interconnection

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, + Symmetric Key Cryptography + Key Expansion in AES Week 2: Encryption and Decryption message using AES Technique. Week 3-4: Number Theory related to modern Cryptography: General definitions + Modular exponential methods + Fermat Theorem + Euler Theorem. Week 5-7: Confidentiality: Public key cryptography techniques: Knapsack + RSA + ElGamal Cryptosystem Week8: Midterm Exam Week9: Key Distribution and Managements: Diff-Hellman key exchange Week 10-11: Message Authentication Hash function + Digital Certificate Week 12-15: Network Security: Secure socket layer + Transport Layer Security + Electronic Mail Security + IP Security + Firewall	Newroz N. Abdulrazaq (2 hrs)
18. Practical Topics (If there is any)	
Harness one of the programming language to implement number theory and Modern cryptography techniques.	Newroz N. Abdulrazaq (2 hrs)

19. Examination: Use Techniques, Methods, Models

Question: Define Hash Function and what is MD5?

Multiple Choices Questions:

1- Network Security provides authentication and access control for resources.

a) True b) False

2- In TLS padding cann be upto a maximum of –

a) 79 bytes b) 127 bytes c) 255 bytes d) none of the mentioned

Question: **Encrypt** (Kurdistan) using RSA cipher with keys p= 11 and q=19?

21. Peer review