Department of Computer Science

University of Cihan

Subject: Information Security

Course Book – Year 4th / 1st semester

Lecturer's name: Wafaa Mustafa Hameed

Academic Year: 2023-2024

Course Book

1. Course name	Information Security I
2. Lecturer in charge	Wafaa Mustafa
3. Department/ College	Department of Computer Science
4. Contact	e-mail: wafaa.mustafa@sulicihan.edu.krd Tel:
5. Time (in hours) per week	Theory: 2 Practical: 2
6. Office hours	Saturday: 9-11
7. Course code	
8. Teacher's academic profile	**https://uni.sulicihan.edu.krd/qa/profile/wafaa.mustafa/**
9. Keywords	Encryption , decryption, symmetric , Asymmetric, DES,AIS, Modular arithmetic

10. Course overview:

The ability to secure information within a modern enterprise—large or small—is a growing challenge. Threats to information security are global, persistent, and increasingly sophisticated. Long gone are the days when managers could hope to secure the enterprise through ad hoc means. Effective information security at the enterprise level requires participation, planning, and practice. It is an on-going effort that requires management and staff to work together from the same script. It is important to note as well that effective security is not achieved in stovepipes. Ineffective physical security, for example, can undermine otherwise effective information system security, and vice versa. Effective security at the enterprise level requires the effective interaction of physical security, information security, personnel security, and so on—indeed, all branches of security must interact effectively as a system to achieve overall enterprise security. This course is designed to teach mid-level security practitioners how to engage all functional levels within the enterprise to deliver information system security. To this end, the course addresses a range of topics, each of which is vital to securing the modern enterprise. These topics include inter alia plans and policies, enterprise roles, security metrics, Each piece of the puzzle must be in place for the enterprise to achieve its security goals; adversaries will invariably find and exploit weak links.

11. Course objective:

After going through this Course the students learn basics of information security, in both management aspect and technical aspect. Students understand of various types of security incidents and attacks, and learn methods to prevent detect and re act incidents and attacks. Students will also learn basics of application of cryptography which are one of the key technologies to implement security functions. At the last session, teams of students will make presentation of their study project for a topic related to information security.

12. Student's obligation

All students are normally required to attend the lectures; take part in lectures through solving an examples and exercises on the whiteboard or as quizzes, write a summery for the Previous lectures or report about the subject and they will get marks for each activity.

13. Forms of teaching

Different forms of teaching will be used to achieve the objectives, such as Data show, white board with different colour of marker, lecture notes beside the source book and computers for the practical part.

14. Assessment scheme

midterm exam	Classroom participation, Quizzes and reports	Final exam
40% (25 theoretical exam,15 practical exam)	10%	50% (35 theoretical exam, 15 practical exam)

15. Student learning outcome:

1. To become able to explain various Information security threat and controls for it.
2. To become able to analyse a security incidents and design countermeasures.
3. To become able to explain information security incident response.
4. To become able to explain the usage of Common Key cryptography and Public Key cryptography.
5. To become able to explain the mechanism to protect confidentiality and completeness of data.
6. To be able to apply arithmetical models.
7. Understand different encryption algorithms.

16. Course Reading List and References:

Key references	Useful references	Magazines and review(internet)
Information security Principles and practice, Mark stamp,San Jose State University, Published by JohnWiley & Sons, Inc., Hoboken, New Jersey. Published simultaneously in Canada.	Cryptography and Network Security *Principles and Practice* Sixth Edition, William Stallings, Copyright © 2014, 2011, 2006 Pearson Education, Inc**.,**	

17. Course Topics		
Week	**Theoretical**	**Practical**
1	Introduction, security attack, passive attack, active attacks,	convert strings and characters to ASCII and vice versa
2	Security mechanisms, security services, what is information security, CIA	*
3	Interruption, interception, Modification, fabrication, Cryptography, interceptor (intruder)	*
4	What is a cipher, cryptography, encryption algorithms,	*
5	Substitution ciphers*, the caesar cipher*, caesar full translation chart*, permutation or scramble ciphering*	Based on *
6	Vigenère ciphering*,	Based on *
7	One time pad(Vernam Cipher)	Based on *
8	More examples for the pervious encryption algorithms* & (quiz)	Based on *
9	Transposition Cipher(Columnar transposition)*	Based on *
10	XOR algorithm*	Based on *
11	DES algorithma*	Based on *
12	DES algorithms*	Based on *
13	AES algorithm*	Based on *
14	Reptition	

18. Overview: Asst.Prof.Dr.Lway Faisal Abdulrazak