Module (Course Syllabus) Catalogue

2022-2023

College/ Institute	Erbil Technical Engineering	
Department	Information System Engineering	
Module Name	Information Security	
Module Code	IS	
Degree	Technical Diploma ☐ Bachler ☑ High Diploma ☐ Master ☐ PhD ☐	
Semester	8	
Qualification	PhD	
Scientific Title	Lecturer	
ECTS (Credits)	6	
Module type	Prerequisite ☐ Core ☑ Assist. ☐	
Weekly hours	4	
Weekly hours (Theory)	(2)hr Class	( )Total hrs Workload
Weekly hours (Practical)	(2)hr Class	( )Total hrs Workload
Number of Weeks	15	
Lecturer (Theory)	Dr. Sara Raouf Muhamad Amin	
E-Mail & Mobile NO.	Sara.muhamad@epu.edu.iq 07504881488	
Lecturer (Practical)	Mr. Ahmad Kaka Amin	
E-Mail & Mobile NO.	+964 750 7703575	
Websites		

Course Book

<table>
<tr><td>Course Description</td><td colspan="5">In this course students will study how can secure information through transition. Information security is the theory and practice of only allowing access to information to people in an organization who are authorized to see it. During that year students will learn a plenty numbers of algorithms for encrypting and decrypting data.</td></tr>
<tr><td>Course objectives</td><td colspan="5">1. Learning security fundamentals and some historic and modern encryption methods.
2. Knowing how to protect the computers against viruses via anti-virus programs.
3. Having good information about firewalls, internet security, viruses and anti-viruses.</td></tr>
<tr><td>Student's obligation</td><td colspan="5">The attendance of students in lectures will have extra credit. He / she is required to continuously follow the lectures, submits homework and assignments. Expect quizzes any time. This is part of the assessment defined in section Assessment scheme.</td></tr>
<tr><td>Required Learning Materials</td><td colspan="5">Java or C++ or any Programming Language and a computer device</td></tr>
<tr><td rowspan="6">Evaluation</td><td colspan="2">Task</td><td>Weight (Marks)</td><td>Due Week</td><td>Relevant Learning Outcome</td></tr>
<tr><td colspan="2">Paper Review</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Assignment</td><td>Homework</td><td>5</td><td></td><td></td></tr>
<tr><td>Class Activity</td><td>2</td><td></td><td></td></tr>
<tr><td>Report</td><td>5</td><td>5</td><td>Academic writing</td></tr>
<tr><td>Seminar</td><td>5</td><td>5</td><td>presentation</td></tr>
</table>

		Essay			
		Project			
	Quiz		8	1	
	Lab activity		10		
	Midterm Exam theory practical		10 15	1	Student evaluation1
	Final Exam theory practical		20 20	1	Student evaluation2
	Total		100	18	
Specific learning outcome:	1- Our Course provides the students with a deep understanding of how modern cryptographic schemes work. 2- The difference between different types of attacks against ciphers 3- A few historical ciphers, and on the way we will learn about modular arithmetic, which is of major importance for modern cryptography as well 4- Why one should only use well-established encryption algorithms				
Course References:	1. Cryptography and Network Security: Principles and Practice, Global Edition, W. WILLIAM STALLINGS 2. Understanding Cryptography by Christof Paar · Jan Pelzl 3. An Introduction to Cryptography by Mohamed Barakat, Christian Eder, Timo Hanke September 20, 2018				

Course topics (Theory)	**Week**	**Learning Outcome**
An introduction to computer Security.	1	Why we need security?
Access Control	2	Authentication schema

Introduction to Number theory	3	Divisibility, Euclidean Alg., prime number and Modular arithmetic
Symmetric Ciphers Classical Encryption Techniques Substitution Techniques	4	Caesar Cipher Hill Cipher
Transposition Techniques Rotor Machine Steganography	5	Column transposition
Block Ciphers and Data Encryption Standard	6	Traditional block Cipher DES
Advance Encryption Standard	7	AES algorithm
Asymmetric Ciphers	8	Public key cryptography RSA
Digital Signatures	9	Digital signature application
System Security	10	Introduction to system security
Viruses Worms	11	Malicious Software
Network Security	12	Protocol stack, application layer
Final Exam	13	Final evaluation

Questions Example Design

Q1/ Define Information Security then write the basic principles of information security.

(15 marks)

Q2/ Fill in the following blanks.

1. _ _ _ _ _cipher is a mechanism of using a single key for encryption/decryption. The_ _ _ and the having the same size.
2. In the substitution cipher from 26 English alphabet we can create_ _ _ different keys.
3. For affine cipher we use two keys (a and b). The condition of choosing the key ‘a’ is _ _ _
4. Data Encryption Standard uses 16 rounds while Advanced Encryption Standard uses rounds _ _ _ _ .

(2 marks for each overall 20 marks)

Q3/ Using Columnar transposition with key (front) to decrypt the message "TNRGDMEIRERWIHAOTEGNE".

(15 marks)

Q4/ In the DES if you have

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

K1 = 000110 110000 001011 101111 111111 000111 000001 110010

Write the first two steps in the F box (f function).

(20 marks)

Q5/ A- find the values of these numbers after applying them on S-box

1. 110010
2. 100111
3. 010101
4. 111000

S-box S_1

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

(16 marks)

B- briefly write Encryption Process of a typical round of AES encryption.

(14 marks)

Lecturer Name: Dr. Sara Raouf Muhamad Amin

Extra notes:

External Evaluator

I confirm that the syllabus given in the attached course book is sufficient and covers the required areas needed for the students.

Mr. Omar Sheerko Mustafa
29/11/2020