Course Specifications

Course Title:	**Cyber Security Principles**
Course Code:	ICS-323
Program:	**Computer sciences**
Department:	**Computer science department**
College:	**College of science Al- Zulfi**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours: 3
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: Level six , 6th semester
4. Pre-requisites for this course (if any)**:** Algorithms and Data Structures (ICS 223)
5. Co-requisites for this course (if any)**:** Nil

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom		80%
2	Blended		10%
3	E-learning		10%
4	Correspondence		
5	Other		

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	Lecture	60
2	Laboratory/Studio	45
3	Tutorial	
4	Others (specify)	
	Total	
Other Learning Hours*		
1	Study	
2	Assignments	
3	Library	
4	Projects/Research Essays/Theses	
5	Others (specify)	
	Total	

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

The aim of this course is to facilitate understanding of the inherent strengths and limitations of cyber security principles that used as a tool for information security applications. Armed with this knowledge, student should be able to make informed decisions when building secure systems. The course covers various aspects of symmetric and asymmetric cryptography. While some topics will be dealt with in more detail, the course will attempt to provide a broad coverage of possibly all the core areas of cryptography. The students shall expected to implement and analyze some simple cryptographic schemes and read various articles. To understand the principles of encryption algorithms; conventional and public key cryptography. To have a detailed knowledge about authentication, hash functions and application level security mechanisms.

2. Course Main Objective

1	Develop an understanding of information assurance as practiced in computer systems and network applications
2	Gain familiarity with prevalent network and distributed system attacks and defenses against them
3	Develop an understanding of cryptography, how it has evolved, and some key encryption techniques used today.
4	Develop an understanding of security polices (such as authentication, integrity, and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	define the basic terminology , notation, and concepts of computer security.	
1.2	Assess the implications of cryptography in terms of privacy, security, and ethical issues	
1.3	Evaluate and compare encryption standards and techniques	
1...		
2	**Skills :**	
2.1	Compile, integrate and appraise various methods of encryption information.	
2.2	Measure and determine appropriate encryption standards and techniques to suite specific business and technological needs	
2.3	Analyze strengths and weaknesses in different systems.	
2...		
3	**Competence:**	
3.1	work cooperatively in a small group environment.	
3.2		

CLOs		Aligned PLOs
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Overview: computer security concepts, the OSI security Architecture, Security attacks, Security mechanisms, Model of network security.	4
2	Classical Encryption Techniques: Symmetric cipher model, substitution techniques, Transposition techniques, Rotor machines.	4
3	Block ciphers and DES: Block cipher principles, DES, the strength of DES, Differential and linear cryptanalysis, Block cipher design principles	4
4	Review of Mathematical concepts: Divisibility, Division algorithm, the Euclidean algorithm, Modular arithmetic, Groups, rings, fields. Finite Fields.	4
5	Advanced Encryption Standard: Finite Field Arithmetic, AES structures, AES transformation, AES key expansion.	4
6	Block cipher operation: Multiple and triple DES, ECB, CBC, CFB, OFB, Counter, and XTS mode of encryptions.	4
7	Stream ciphers: random bits generation, RC4, others stream ciphers.	4
8	Review of Number theory concepts: prime numbers, Fermat's and Euler's theorem, testing primality, Chinese remainder theorem, Discrete logarithms.	4
9	Public key Cryptography and RSA: principles of public key cryptosystems, The RSA algorithm.	4
10	Other public key cryptosystem: DH scheme, ElGamal cryptosystem.	4
11	Cryptographic Hash functions: Applications of Cryptographic hash functions, simple hash functions, SHA-3, Digital signatures. Applications in authentication.	12
12	Applications.	4
Total		

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of secure networking systems, and its underpinning science and mathematics;	Lectures Lab Demonstrations Case studies	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Asses the threats, vulnerabilities, and risks to a computer network		
1.3	Identify the standards of security		

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
	protocols for Emails, web security, and IP security.		
2.0	**Skills**		
2.1	Demonstrate creative and innovative ability in the synthesis of solutions and in formulating designs in secure computer network systems;	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems		
…			
3.0	**Competence**		
3.1	Set up, test and administer security systems for effective use;	Small group discussions. Whole group discussions. Brainstorming. Presentations	Observations Homework assignments Lab assignments Class Activities
3.2	Develop and implement a security plan as it relates to the network components of an organization		
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	11	15%
3	Homework assignments	Every week	10%
4	Presentation, class activities, and group discussion	After Every chapter	10%
5	E – Quiz	12	10%
6	Final written exam	16	40%
7	Total		100%
8			

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall 2016
Essential References Materials	C. Kaufman, Radia Perlman, Mike Speciner " Network Security, Private Communication in a Public World", Prentice Hall 2002
Electronic Materials	Video lectures
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classrooms and Laboratories, as those that are available at the college of science at AzZulfi.
Technology Resources (AV, Classrooms and Laboratories, as those that are available at the college of science at AzZulfi., etc.)	Classrooms and Laboratories, as those that are available at the college of science at AzZulfi.
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	None

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment.	Program Leaders	Direct
Quality of learning resources	Faculty	Indirect
Extent of achievement of course learning outcomes	Peer Reviewer	Direct
	Students'	
	Colleagues	
	Self-assessment	

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	