هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

Course Specifications

Course Title:	Cryptographic
Course Code:	CYB 0104
Program:	Computer Science (Cybersecurity)
Department:	Applied Sciences
College:	Applied College
Institution:	Imam Muhammad Bin Saud Islamic University

Table of Contents

A. Course Identification

1. Credit hours: **3(2 theory , 2 lab)**
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: Third Semester
4. Pre-requisites for this course (if any)**:** CYB0101
5. Co-requisites for this course (if any)**:** None

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	3hours\week	100%
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	22
2	**Laboratory/Studio**	22
3	**Tutorial**	
4	**Others** (specify)	
	Total	44

B. Course Objectives and Learning Outcomes

1. Course Description

This course is designed to provide basic identification of replicating that covers classic encryption techniques, cluster encryption standards, data encryption, and basic concepts in the number. Theory. More replica blades such as AES, and flow encryption are covered. The course covers the general key encryption and RSA and some other public keys encryption systems such as Helman's exchange, encryption and elliptical curve system. Reserved retail functions are also covered for data safety in the course, by describing how the encryption block sequence can be used and understanding SSL and TLS. In addition, this course illustrate the Public channel cryptography and Modern Cryptography in information security field of study.

2. Course Main Objective

Give a deep understanding about the cryptography and the types used in different information. Understand the different between the symmetric and asymmetric encryption techniques. Also, students should differentiate between security transport and the modern cryptography.

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Understand the different cryptographic types.	ع1,ع3
1.2	To expose students to the importance of cryptographic.	ع3
1.3	Identify different types of cryptographic, classify the threats and develop a security model to prevent, detect and recover from the attacks.	ع2,ع5
2	**Skills :**	
2.1	Encrypt and decrypt messages using block ciphers, sign and verify messages using well known signature generation and verification algorithms.	م2,م1
2.2	Analyze existing authentication and key agreement protocols.	م5,م7
2.3	Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as Unix and Windows NT.	م6
3	**Values:**	
3.1	Implement hacking and encrypting to protect systems.	م7,ق1,ق2,ق3

C. Course Content

No	List of Topics	Contact Hours
1	Introduction	4
2	Hash Function	4
3	Authenticated encryption	4
4	Key Exchange	4
5	Asymmetric encryption and hybrid encryption	4
6	Public channel cryptography	5
7	Modern Cryptography	4
8	Signature proofs	5
9	Secure transport	5
10	User authentication	5
Total		44

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 and Understanding**		
1.1	Understand the different cryptographic types.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports.

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
		Quizzes Case studies and Analysis.	
1.2	To expose students to the importance of cryptographic.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
	Identify different types of cryptographic, classify the threats and develop a security model to prevent, detect and recover from the attacks.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.0	**Skills**		
2.1	Encrypt and decrypt messages using block ciphers, sign and verify messages using well known signature generation and verification algorithms.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.2	Analyze existing authentication and key agreement protocols.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.3	Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as Unix and Windows NT.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
3.0	**Values**		
3.1	Implement hacking and encrypting to protect systems.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	Week3,5	10%
2	Midterm	Week 7	20%
3	Lab Assignments group or individual /Class Assignments group or individual	Week4,7,9	15%
4	Lab Evaluations	All Semester	15%
5	Final	Week13	40%

***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 :

6 office hours per week.
3 hours of weekly meetings
Contact through the LMS
Communication/interact via e-mails with students

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Real world Cryptography,2021, by David Wong. The Mathematics of Encryption,2021, By Margaret Cozzens, Steven J. Miller
Essential References Materials	N/A
Electronic Materials	Online resources will be provided during class lectures.
Other Learning Materials	N/A

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Lecture room with Smart board Lab with 25 Pcs
Technology Resources (AV, data show, Smart Board, software, etc.)	PC and WiFi Internet access within the class room
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N\A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Student	Indirect using course evaluation survey
Quality of learning resources	Student and Faculty	Indirect using course evaluation and faculty survey

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	