هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title:	**Applied Cryptography**
Course Code:	**IS1769**
Program:	**Computer Information Systems**
Department:	**Computer Information Systems**
College:	**Computer Science & Information Technology**
Institution:	**Al-Baha University**
Version:	**1**
Last Revision Date:	**29/03/2023**

Table of Contents:

A. General information about the course:

Course Identification					
1. Credit hours:	3 Credit Hours (3, 0, 0) (Lecture, Lab, Tutorial) (3 Contact Hours)				
2. Course type					
a.	University ☐	College ☐	Department☒	Track☐	Others☐
b.	Required ☐	Elective☒			
3. Level/year at which this course is offered:	Elective course (12th Level/4th Year)				

4. Course general Description

The Applied Cryptography module is designed to provide Information Systems students with a practical understanding of cryptography and its applications in securing data. The course will cover various cryptographic concepts and techniques, including symmetric and asymmetric encryption, hashing, digital signatures, and key management. Emphasis will be placed on the application of these techniques to real-world scenarios, such as secure data storage, secure communication, and secure authentication. The course will also cover various frameworks and standards that can be used to ensure cryptographic security in information systems, such as SSL/TLS, AES, RSA, and SHA. By the end of the course, students will be equipped with the knowledge and skills necessary to implement effective cryptographic solutions to protect data privacy and integrity.

5. Pre-requirements for this course (if any): **IS1512- Information Systems Security**

6. Co- requirements for this course (if any): None

7. Course Main Objective(s)

1. Understand the fundamentals of cryptography and its role in ensuring data privacy and integrity.
2. Identify and evaluate different types of cryptographic algorithms and protocols.
3. Analyze cryptographic attacks and countermeasures to ensure secure data communication and storage.
4. Examine the practical application of cryptography in information systems and evaluate their effectiveness in protecting data.
5. Recognize the legal and ethical considerations surrounding the use of cryptography and its impact on privacy and security.
6. Evaluate the suitability of different cryptographic frameworks and standards for specific information system architectures.
7. Demonstrate the ability to design, implement, and evaluate cryptographic solutions in real-world scenarios.
8. Collaborate effectively in teams to identify and solve cryptographic challenges.
9. Communicate technical concepts related to cryptography clearly and effectively in oral and written formats.

10. Continuously reflect on and improve their own learning, particularly in relation to emerging trends and technologies in the field of cryptography.

1. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	30	100%
2.	E-learning		
3.	Hybrid • Traditional classroom • E-learning		
4.	Distance learning		

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	30
2.	Laboratory/Studio	
3.	Field	
4.	Tutorial	
5.	Others (specify)	
	Total	30

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Explain the core concepts and principles of cryptography and their application in securing data privacy and integrity.	K1	- Lectures - Case studies	- Midterm - Assignments - Final Exam
1.2	Describe the different types of cryptographic algorithms and protocols, including their strengths and weaknesses.	K2	- Lectures - Case studies	- Midterm - Assignments - Final Exam
1.3	Evaluate the effectiveness of cryptographic techniques and protocols in securing information systems against attacks.	K3	- Lectures - In-class discussions - Case studies	- Assignments - Final Exam
1.4	Compare and contrast different cryptographic frameworks and standards and their suitability for specific information system architectures.	K3	- Lectures - In-class discussions - Case studies	- Assignments - Final Exam
2.0	Skills			
2.1	Design and implement effective cryptographic solutions for a variety of information system scenarios, including secure data storage, communication, and authentication.	S1	- Lectures - In-class discussions - Case studies	- Group project - Final exam
2.2	Use relevant cryptographic tools and software to implement and evaluate cryptographic solutions.	S2	- Lectures - Case studies	- Group project
2.3	Analyze cryptographic challenges, identify appropriate solutions, and collaborate effectively in teams to solve cryptographic problems.	S3	- Lectures - In-class discussions	- Assignments
3.0	Values, autonomy, and responsibility			
3.1	Apply critical thinking skills to evaluate the effectiveness of cryptographic solutions and make informed decisions about their use in information systems.	V1	- In-class discussions - Case studies	- Assignments - Group project
3.2	Continuously reflect on and improve their own learning in the field of cryptography.	V2	- Assignments - Group project	- Assignments - Group project

Note: The Course Exit Survey will be used as an indirect Assessment Tool to evaluate the CLO.

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to cryptography: history, definitions, and applications	2
2	Symmetric encryption: principles, algorithms, and applications	4
3	Asymmetric encryption: principles, algorithms, and applications	4
4	Digital signatures: principles, algorithms, and applications	4
5	Cryptographic tools and software: OpenSSL, GnuPG, and other relevant tools	4
6	Cryptographic challenges and attacks: cryptanalysis, side-channel attacks, and implementation attacks	3
7	Cryptographic standards and frameworks: SSL/TLS, IPsec, and other relevant standards	3
8	Cryptography in information systems: secure data storage, communication, and authentication	3
9	Cryptography in practice: case studies and real-world applications	3
Total		30

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment	3 & 6	15%
2.	Midterm	5	15%
3.	Group-project	7	10%
4.	Final Exam	12	60%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	• Paar, C., & Pelzl, J. (2022). Understanding cryptography: A textbook for students and practitioners (2nd ed.). Springer. • Schneier, B., Ferguson, N., & Kohno, T. (2015). Cryptography engineering: Design principles and practical applications (2nd ed.). John Wiley & Sons • Trappe, W., & Washington, L. C. (2020). Introduction to cryptography with coding theory (3rd ed.). Pearson.
Supportive References	• Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography. Available online: https://toc.cryptobook.us/ • Aumasson, J. P. (2017). Serious cryptography: A practical introduction to modern encryption. No Starch Press.
Electronic Materials	• Cryptography I and Cryptography II courses on Coursera: Two free courses offered by Stanford University and taught by Dan Boneh. They provide a comprehensive introduction to cryptography, covering both theoretical and practical aspects.

	(https://www.coursera.org/learn/crypto/, https://www.coursera.org/learn/crypto2) • Crypto101: A free online course offered by the Open Crypto Audit Project. It covers the basics of cryptography, with a focus on practical applications. (https://www.crypto101.io/) • NIST Cryptographic Toolkit: A collection of cryptographic standards and guidelines from the National Institute of Standards and Technology (NIST). It provides information on industry best practices and the latest developments in the field. (https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines)
Other Learning Materials	• Saudi Digital Library (SDL).

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	A classroom or lecture hall with a whiteboard for 25 students.
Technology equipment (projector, smart board, software)	• A digital image projection system with a connection to a desktop computer and laptop computer. • High speed Internet connection. • An instructor computer station.
Other equipment (depending on the nature of the specialty)	None

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	• Students • Faculty • Course Coordinator	• Surveys (indirect). • Direct feedback from students. Comprehensive Course report (where we can find information about teaching difficulties and action plan, …)
Effectiveness of students assessment	• Students • Faculty • Exam Evaluation Committee • Course Coordinator	• Surveys (indirect). • Direct feedback from students. Exam evaluation by the Exam Evaluation Committee (indirect)
Quality of learning resources	• Students • Faculty • Course Coordinator	• Surveys (indirect) Comprehensive Course report (where we can find information about difficulties and challenges about learning resources as well

Assessment Areas/Issues	Assessor	Assessment Methods
		as consequences and action plan, …)
The extent to which CLOs have been achieved	• Faculty • Program Leader • Course Coordinator	• Student Results (direct) Comprehensive Course report (where we can find the CLO assessment results)
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	Curriculum Committee Meeting
REFERENCE NO.	
DATE	March 30, 2023