هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

2023

TP-153

Course Specification

(Bachelor)

Course Title: Cryptography	
Course Code: COMP-525	
Program: Bachelor in Computer Science	
Department: Computer Science	
College: College of Computer Science and Information Technology	
Institution: Jazan University	
Version: V2	
Last Revision Date: 07 January 2023	

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (03)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (Level 09/ Year 05)					

4. Course General Description:

This course delves into the evolution of cryptography from classical systems to modern applications. It begins with an exploration of symmetric ciphers, including block and stream ciphers. The course progresses to intricate aspects of asymmetric cryptography, encompassing public-key systems like RSA and Elliptic Curve Cryptography. It delves into secure communication protocols, such as SSL/TLS, alongside practical aspects of key management and distribution. The curriculum also introduces advanced topics, including the principles of quantum cryptography and the cryptographic underpinnings of blockchain technology.

5. Pre-requirements for this course (if any)**:**

Computer Security and Privacy (COMP-323)

6. Pre-requirements for this course (if any)**:**

No

7. Course Main Objective(s):

- Discuss the fundamental mathematical foundations and fundamental concepts of cryptography.
- To offer insights into different cryptographic algorithms and protocols and analyze their limitations and vulnerabilities.
- Describe the application of cryptographic algorithms in various interdisciplinary fields such as cybersecurity, data privacy, blockchain, and digital forensics.

- To introduce advanced topics in the domain of cryptography and security like quantum cryptography, lightweight cryptography, and blockchain technology.
- To familiarize students with the practical application of various cryptographic algorithms and protocols.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning (Self-Learning)		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	28
2.	**Laboratory/Studio**	28
3.	**Field**	--
4.	**Tutorial**	--
5.	**Others (specify)**	4
Total		60

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	Describe the fundamental mathematical foundations and cryptographic principles of cryptographic algorithms.	K1	• Lectures/Presentations • Media Lectures	• Mid-Term Exam • Assignment- 1 Final Theory Exam

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.2	Discuss the evolving trends in the domain of cryptography and security and its impact.	K2	• Lectures/Presentations • Media Lectures	• Assignment- 2 • Final Theory Exam
2.0	**Skills**			
2.1	Evaluate different cryptographic algorithms and protocols and analyze their limitations and vulnerabilities.	S2	• Lectures /Presentations • Media Lectures Tutorials	• Assignment - 1 • Final Theory Exam
2.2	Assess the workings of cryptographic algorithms and interdisciplinary cryptographic applications.	S2	• Lectures /Presentations • Media Lectures Tutorials	• Assignment - 1 • Assignment – 2 • Final Theory Exam
2.3	Apply various cryptographic algorithms and protocols in practical applications.	S1	• Lectures /Presentations • Media Lectures Tutorials	• Assignment -1 • Final Theory Exam
2.4	Implement basic cryptographic protocols using mathematical and algorithmic principles.	S3	• Lectures /Presentations • Lab Demonstration • Media Lectures Group discussion	• Lab Exam • Final Theory Exam
3.0	**Values, autonomy, and responsibility**			
3.1	Demonstrate the ability to work in a group for collective problem-solving and implementing cryptographic solutions.	V2	Group Discussion	• Assignment – 2

C. Course Content

No	List of Topics	Contact Hours
1.	Classical Encryption Techniques: Definitions, Symmetric cipher model, Cryptographic systems, Cryptanalysis and Brute-Force Attack, Types of attack on Encrypted Messages, Encryption Scheme Security: unconditionally secure, computationally secure, Substitution techniques: Caesar cipher, Monoalphabetic ciphers, frequency analysis, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, Vigenère Cipher, Vernam Cipher, One-Time Pad, Difficulties with One-Time Pad, Transposition cipher, Rail fence cipher, Steganography	4T + 4P

2.	Block Cipher Stream cipher, Block cipher, Feistel cipher, Diffusion and Confusion, Feistel Cipher Design Features, Data Encryption Standard (DES), Strength of DES, Advanced Encryption Standard (AES), AES Encryption Process, AES S-Box structure, AES Implementation, Implementation Aspects, Meet-in-the-Middle Attack, Triple DES with Three Keys, Block cipher operation mode: Multiple and triple DES, Electronic Code Book (ECB), Cipher Block Chaining Mode (CBC), Cipher Feedback Mode(CFB), Output Feedback Mode (OFB), Counter (CTR) Mode	4T + 4P
3.	Pseudorandom Number Generation and Stream Cipher Random Numbers, Randomness, Criteria for Randomness, Unpredictability, Pseudorandom Numbers, random number generators, True Random Number Generator (TRNG), Pseudorandom Number Generator (PRNG), PRNG Requirements, Randomness Test, Blum Blum Shub (BBS) Generator, Blum Blum Shub (BBS) block diagram, Generic structure of typical Stream Cipher, Stream Cipher Design Considerations, RC4 stream cipher, Strength of RC4, Entropy Sources, Possible Sources of Randomness, Comparison of PRNGs and TRNGs, Conditioning	4T + 4P
4.	Public key Cryptography Terminology related to Asymmetric encryption, Misconceptions Concerning Public-Key Encryption, Principles of Public-Key Cryptosystems, Public-Key Cryptosystems scheme, Conventional vs Public-Key Encryption, Authentication and Secrecy using Public-Key Cryptosystem, Applications for Public-Key Cryptosystems, Public-Key Requirements, Public-Key Cryptanalysis, Rivest-Shamir-Adleman (RSA) Algorithm, Key Generation, Timing Attacks, Countermeasures, Fault-Based Attack, Chosen Ciphertext Attack (CCA), Diffie-Hellman Key Exchange, ElGamal Cryptography, Elliptic Curve Cryptography (ECC), Security of Elliptic Curve Cryptography, Comparison of Different public key algorithms, Exponentiation in Modular Arithmetic, Factoring Problem, Elliptic Curve Arithmetic	4T + 4P
5.	Lightweight and Post-Quantum Cryptography Lightweight Cryptography Concepts, Embedded Systems, Microcontrollers, Deeply Embedded Systems, Constrained Devices, Categories of Constraints for Lightweight Cryptography, Radio Frequency Identification (RFID), Profiles of Lightweight cryptography, Post-quantum Cryptography, Grover's Algorithm, Crypto-period, Impact of Quantum computing on Common cryptographic algorithms, Vulnerable Categories, Alternatives, Side-Channel Attack	4T + 4P
6.	Cryptocurrency and Blockchain Technologies Blockchain, Shortcomings of current transaction systems, Emergence of Bitcoin, Advantages of Bitcoin, Bitcoin and Blockchain, Blockchain	4T + 4P

	characteristics, Blockchain Model, Blockchain transaction, Blockchain Working, Types of Blockchain, Building trust with Blockchain, Blockchain Key Business Benefits, Key Concepts of blockchain for Business, Consensus Mechanism, Smart contracts, Blockchain Applications	
Total		26T+26P

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm Exam	7th-8th week	15%
2.	Assignment I	9th week	10%
3.	Assignment II (Case Study/ Group assignment)	12th week	15%
4.	Lab Exam	14th Week	20%
5.	Final Theory Exam	15th Week	40%

*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	Stallings, William. Cryptography and network security: Principles and practice. Pearson, 8th Edition, 2020. ISBN-13: 978-0135764213
Supportive References	• Understanding Cryptography, Paar, Christof, Pelzl, Jan, 2nd Edition, Springer, 2010, ISBN-13: 978-3642041006. • Handbook of Applied Cryptography: Menezes, van Oorschot and Vanstone, 5th Edition, CRC Press, 2001, ISBN-13: 978-0849385230. • Blockchain For Dummies®, IBM Limited Edition Published by John Wiley & Sons, Inc., 2018 ISBN: 978-1-119-37139-7
Electronic Materials	• https://learncryptography.com/ • https://www.garykessler.net/library/crypto.html • https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography • https://www.khanacademy.org/computing/computer-science/cryptography • www.iacr.org • https://blackarch.org/crypto.html • https://www.tutorialspoint.com/cryptography/index.htm • https://en.wikipedia.org/wiki/Blockchain • https://www.blockchain-council.org/blockchain/top-10-real-world-applications-of-blockchain-technology/
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• Classroom equipped with projector, whiteboard, and sufficient seating arrangements. • Lab with software installed and an individual computer terminal for each student.
Technology equipment (projector, smart board, software)	• Whiteboards and projectors for classroom and labs Following software for lab work: • Cryptool • Java Compiler
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	Indirect (Course evaluation survey form)
Effectiveness of Students' assessment	CRC / QAU / HoD	Direct (Course reports/result analysis)
Quality of learning resources	Track leaders / CRC	Indirect (Review, meetings, and star rating with suggestions for further modification and improvements)
The extent to which CLOs have been achieved	CRC / QAU	Direct (CLO assessment template further verified at course coordinator, Track leader and QAU level)
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	DEPARTMENT COUNCIL
REFERENCE NO.	
DATE	15/10/2022