Course Specification

(Postgraduate Programs)

Course Title:	**Cryptography**
Course Code:	**MSCS 622**
Program:	**Master Programme in Computer Science**
Department:	**Computer Science**
College:	**Computer Science and Information Technology**
Institution:	**King Faisal University**
Version:	*Course Specification Version Number*
Last Revision Date:	*Pick Revision Date.*

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: 3 (3-0-6)				
2. Course type				
A.	☐University	☒ College	☐Department	☐Track
B.	☐ Required		☒ Elective	
3. Level/year at which this course is offered: : Level 2 , 3 or 4				
4. Course General Description:				
Basic concepts in Number Theory, e.g., Euclidean algorithm, Euler's functions. Fermat's theorem and Euler's generalization, Chinese remainder theorem, primitive roots and discrete logarithms, quadratic residues, Legendre and Jacobi Symbols. And familiarity with various basic cryptographic concepts, tools and algorithms including DES and differential and linear cryptanalysis, AES, RSA system. Digital signatures, El Gamal signature, digital signature standard, one time undeniable and fail stop signature. Hash functions, and coding and information theory. Probability Review, Entropy, Huffman Codes & Perfect Secrecy, The course also covers Error Correcting Codes, Bounds on General Codes, Linear Codes, Hamming Codes, Golay and Cyclic Codes, BCH Codes, Reed-Solomon Codes and Quantum Techniques in Cryptography.				
5. Pre-requirements for this course (if any)**:**				
NA				
6. Pre-requirements for this course (if any)**:**				
NA				
7. Course Main Objective(s):				
The objective of this course is to develop a foundational understanding of cryptography as used in the real world. .				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom		
2	E-learning		
3	Hybrid • Traditional classroom	45	100%

No	Mode of Instruction	Contact Hours	Percentage
	• E-learning		
4	Distance learning		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
2.	**Laboratory/Studio**	-
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify)……**	-
	Total	45

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

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Describe digital signature techniques and algorithms.	K1	Lectures	- Quizzes - Exams - Assignments
1.2	Describe various error correcting codes and information theory	K1	Lectures	- Quizzes - Exams - Assignments
2.0	**Skills**			
2.1	**Analyze** encryption, decryption, security and efficiency of various cryptographic techniques and.	S2	- Lectures	- Quizzes - Exams - Assignments
2.2	Analyze different algorithms, number theoretic concepts required for cryptosystems	S1	- Lectures	- Quizzes - Exams - Assignments

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
...				
3.0	**Values, autonomy, and responsibility**			
3.1	Demonstrate team work by applying Cryptographic skills in projects using cutting edge techniques, technologies and recent research.	V1	- Lectures - Case studies -Research assignment	Project Report and Presentation
...				

C. Course Content:

No	List of Topics	Contact Hours
1. 1	Introduction to Information Security and Cryptography	3
2. 2	Block ciphers and DES	4.5
3	Basic Concepts in Number Theory and Finite Field	4.5
4	Advanced Encryption Standards	3
5	Block cipher Operations	3
6	Pseudorandom Number Generation and Stream ciphers	4.5
7	Public Key cryptography and RSA	4.5
8	Cryptographic Hash functions : Message authentication codes	3
9	Digital Signatures	3
10	Key Management and Distribution	3
Total		**45**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	Continuous	10%
2.	Quiz	Continuous	10%
3.	Mid Term	8^{th}- 9^{th}	25%
4	Capstone Project	15^{th}	15%
5	Final Exam	16^{th}- 17^{th}	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:

Required Textbook	1. Cryptography and Network Security: Principles and Practice by William Stallings, 7th Edition, Prentice Hall, 2017. ISBN: 978-0134444284. 2. Introduction to Cryptography with Coding Theory by Wade Trappe and Lawrence Washington, 2nd Edition, Prentice Hall, 2002. ISBN: 0131862391. .
Essential References	1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, Wiley Publications, 1996. ISBN-13: 978-0471117094 2. Joshua Holden, "The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption", 1st Edition, Princeton University Press, 2017. ISBN-13: 978-0691141756
Supportive References	
Electronic Materials	https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines https://www.rsa.com/ https://www.ietf.org/
Other Learning Materials	Research Papers in the field of cryptography and information security published in international conferences and journals

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Sufficient seats (typically 20) as per student registration required in the lecture
Technology equipment (Projector, smart board, software)	Sufficient computer terminals with required setup having the necessary software installed and configured for the students to complete assignments and projects. Data show is needed to demonstrate in the class
Other equipment (Depending on the nature of the specialty)	Not Required

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect Assessment Teaching through Evaluation

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of students' assessment	Faculty	Indirect assessment through Course Evaluation Survey
Quality of learning resources	Students	Indirect Assessment through Learning Resources Survey
The extent to which CLOs have been achieved	**Faculty**	Direct assessment through Rubrics analyses
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	