	**SULTAN QABOOS UNIVERSITY** **COLLEGE OF SCIENCE** **DEPARTMENT OF COMPUTER SCIENCE** **BACHELOR OF SCIENCE IN COMPUTER SCIENCE** **COURSE OUTLINE**

I. COURSE INFORMATION			
COURSE CODE	**COMP5507**		
COURSE TITLE	**Cryptography and Network Security**		
OMAN QUALIFICATION FRAMEWORK (OQF) LEVEL	**8**		
CREDIT HOURS	3		
CONTACT HOURS	4		
PRE-REQUISITES	**(COMP3502 OR COMP4502) AND COMP3203**		
CO-REQUISITES	-		
EQUIVALENT COURSES			
INCOMPATIBLE COURSES			
COURSE CATEGORY	☐ University Requirement	☐ University Elective	
	☐College Requirement	☐ College Elective	
	☐Department Requirement	☐ Department Elective	
	☐ Major Requirement	☐ Major Elective	
	☒ Specialization Requirement	☐ Specialization Elective	
	☐ Other (specify):		
COURSE OWNER	College: Science	Department: Computer Science	
	Center:	Unit:	
DELIVERY MODE	☒ Face to Face	☐ Blended	☐ Online

COURSE TYPE	☐ Lecture	☐ Lecture/Lab	
	☐ Lecture/Seminar	☐ Lecture/Studio	
	☒ Lecture/Tutorial	☐ Lecture/Lab/Tutorial or Seminar	
	☐Tutorial	☐ Laboratory (Practical)	
	☐ Field or Work Placement	☐ Studio	
	☐Seminar	☐ Internship	
	☐ Workshop	☐ Project	
	☐ Thesis	☐ Other (specify):	
LANGUAGE OF INSTRUCTION	English		
COURSE DESCRIPTION	This course focuses on the essentials of Network Security. Topics include Security Models and requirements, Symmetric Key and message confidentiality, Public Key Cryptography and Message Authentication, Key Managements, Electronic Mail Security such as PGP protocol, IP Security, Web and e-commerce Security, Firewalls, and Malicious Software.		
TEACHING AND LEARNING STRATEGIES	☐ Augmented Reality	☐ Flipped Classroom	
	☒ Blended Learning	☒ Problem-Based Learning	
	☐ Discovery-Based Learning	☐ Project-Based Learning	
	☐ Student-Led Learning	☐ Team-Based Learning	
	☐ Work-Based Learning	☐ Other (specify):	
ASSESSMENT COMPONENT AND WEIGHT	☒ In-term examination(s) (25 %)	☐ Quizzes	☒Other (specify):
	☒ Homework assignments (15 %)	☐Project (20 %)	
	☒ Final examination (40 %)	☐ Practical/ Lab	
TEXTBOOKS AND EDUCATIONAL MATERIAL	Cryptography and Network Security," Third Edition by William Stallings, Prentice-Hall, Third Edition.		
GRADING METHOD	☒ A-F Scale	☐ Pass/Not Pass	☐ Other (specify):

GRADING METHOD DESCRIPTION			
	Range	**Letter Grade**	**Description**
A-F GRADING SCALE:	90 – 100	A	**Exceptional performance:** All course objectives achieved and met in a consistently outstanding manner.
	86 – 89.9	A-	
	81– 85.9	B+	**Very Good Performance:** The majority of the course objectives achieved (majority being at least two-thirds) and met in a consistently thorough manner.
	77 – 80.9	B	
	73 – 76.9	B-	
	68 – 72.9	C+	**Satisfactory Performance:** At least most of course objectives have been achieved and met satisfactorily.
	64 – 67.9	C	
	60 – 63.9	C-	
	55 – 59.9	D+	**Minimally Acceptable Performance:** The course objectives met at a minimally acceptable level.
	50 – 54.9	D	
	0 – 49.9	F	**Unacceptable performance:** The course objectives not met at a minimally acceptable level.
PASS/NOT PASS:			
OTHER:			

II. SEMESTER INFORMATION			
SEMESTER/YEAR	Fall 2024	**SECTION(S)**	1
DAY AND TIME	Mon - WED	**VENUE(S)**	Theater 1
COURSE COORDINATOR	Prof. Abderezak Touzene	**COURSE TEAM**	
COORDINATOR OFFICE	0019	**OFFICE HOURS**	**SUN, TUS 10 – 11**
COORDINATOR EXTENSION	1482	**COORDINATOR EMAIL**	touzene@squ.edu.om

III. Alignment of Course Learning Outcomes (CLO), Program Learning Outcomes (PLO), Graduate Attributes (GA), and Oman Qualification Framework (OQF) Characteristics

CLO	PLO / SO	SQU Graduate Attributes	OQF Characteristics
1. Explain common attacks against network assets, the associated threats and vulnerabilities, and what network security do to secure assets	**SO1, SO2**	**A, B**	**1, 2**
2. Explain how to use symmetric key to help protect information and how to choose an appropriate encryption method.	**SO1, SO2**	**A, B**	**1, 2**
3. Discuss the concept of public key encryption and key distribution mechanisms	**SO1, SO2**	**A, B**	**1, 2**
4. Understand Message Authentication techniques	**SO1, SO2**	**A, B**	**1, 2**
5. Explain the network IP security protocol and its advantages	**SO1, SO2**	**A, B**	**1, 2**
6. Understand the Web Security protocols SSL and TLS.	**SO1, SO2**	**A, B**	**1, 2**
7. Discuss the principle of firewall, their configuration and access control.	**SO1, SO2**	**A, B**	**1, 2**
8. Distinguish between different malicious software and their different countermeasures	**SO1, SO2**	**A, B**	**1, 2**

IV. Course Learning Outcomes (CLOs) and Assessment Criteria and Methods (for each CLO)

CLO1: Explain common attacks against network assets, the associated threats and vulnerabilities, and what network security do to secure assets.

Assessment Criteria (to achieve this objective, the student must)		Assessment Methods
A)	Explain attacks and vulnerabilities at the physical layer	HM1, Midterm, Final Exam
B)	Explain attacks and vulnerabilities at the data layer and network level	
C)	Explain attacks and vulnerabilities at the transport layer and application level	

CLO2: Explain how to use symmetric key to help protect information and how to choose an appropriate encryption method.		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Explain the classical cryptography	HM2, Midterm, Final Exam
B)	Explain the basics of modern cryptography for block ciphers	
C)	Explain the principal and the use of stream ciphers	
CLO3: Discuss the concept of public key encryption and key distribution mechanisms		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Discuss the principals and different use of public key cryptography	HW2, Midterm, Final Exam
B)	Discuss RSA public key technique	
C)	Describe the different key exchange distribution mechanisms	
CLO4: Understand Message Authentication techniques		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Demonstrate an understanding of message authentication codes MAC	Midterm, Project , Final Exam
B)	Demonstrate an understanding of hash authentication method	
C)	Demonstrate an understanding and usages of digital signature	
CLO5: Explain the network IP security protocol and its advantages		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Demonstrate an understanding of IPSEC protocol	Final Exam
B)	Distinguish between the different security association modes	

CLO6: Understand the Web Security protocols SSL and TLS.		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Demonstrate an understanding web security SSL	Final Exam
B)	Demonstrate an understanding web security TLS	
CLO7: Discuss the principle of firewall, their configuration and access control.		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Demonstrate an understanding of access control using firewalls.	Final Exam
B)	Distinguish between the different firewall types	
CLO8: Distinguish between different malicious software and their different countermeasures		
ASSESSMENT CRITERIA (TO ACHIEVE THIS OBJECTIVE, THE STUDENT MUST)		**ASSESSMENT METHODS**
A)	Distinguish between viruses, worms, malware, adware, Trojan horses, etc.	Final Exam
B)	Demonstrate an understanding for the different antivirus generation for computer protection	

V. COURSE CONTENT AND SCHEDULE				
WEEK	**LECTURES #**	**TOPICS/ SUBJECTS**	**READINGS/ CHAPTERS**	**REMARKS (e.g., ASSESSMENTS)**
1	Lecture 1 Lecture 2	**Introduction**: OSI Security Architecture Network Security Models , Security services and type of attacks	Chapter 1	HW1, Midterm Exam, Final Exam
2	Lecture 3 Lecture 4	Network Protocols Vulnerability	Handout	HW1, Midterm Exam, Final Exam
3	Lecture 5 Lecture 6	Network Protocols Vulnerability (continues)	Handout	HW1, Midterm Exam, Final Exam
4	Lecture 7 Lecture 8	**Cryptography:** Symmetric Key, Basic Terminology, Cryptanalysis, Symmetric Block Encryption.	Chapter 2	HW2, Midterm Exam, Final Exam

5	Lecture 9 Lecture 10	Stream Cipher: RC4, Cipher Block chain	Chapter 2	HW2, Midterm Exam, Final Exam
6	Lecture 11 Lecture 12	**Confidentiality using Symmetric Encryption:** Placement of Encryption, Encryption vs Protocol Level, Traffic Analysis, Key Distribution	Chapter 3	HW2, Midterm Exam, Final Exam
7	Lecture 13 Lecture 14	**Public Key Cryptography and Message Authentication:** Message Authentication Approaches, Secure Hash Function	Chapter 3	Project, Midterm Exam, Final Exam
8	Lecture 15 Lab 7 Lecture 16	Public Key Cryptography and Message Authentication: Public Key Cryptography, Digital Signature, Key Management	Chapter 4	Project , Midterm Exam, Final Exam
9	Lecture 17 Lecture 18	Electronic Mail Security: Pretty Good Security (PGP)	Chapter 5	Project, Final Exam
10	Lecture 19 Lab 9 Lecture 20	**IP Security:** Overview, IP sec Architecture, AH, ESP	Chapter 5	Final Exam
11	Lecture 21	IP Sec continue: Combine Security association	Chapter 5	Final Exam
12	Lecture 22 Lecture 23	**SSH AND Web Security**: Web security requirements, Secure Socket Layer (SSL), Transport Layer Security (TLS)	Chapter 6	Final Exam
13	Lecture 24 Lab 11 Lecture 25	**Firewalls:** Introduction, Configuration, Access Control, Proxy, Personal firewall	Chapter 6	Final Exam
14	Lecture 26 Lecture 27	Malicious Software Intruders and Malicious Software: IDS, Virus and threats, Virus countermeasures	Chapter 7	Final Exam
15		Project Presentation		Report

VI. ADDITIONAL INFORMATION (e.g., RUBRICS, etc.)

Assessment Plan (*tentative*):

Item	Date In	Due Date	Weights
Homework 1	(W3) Mon	(W5) Wed	5%
Homework 2	(W5) Mon	(W7) Wed	5%
Midterm Exam	(W9) Wed		25%
Homework 3	(W10) Mon	(W12) Wed	5%
Project (2) / Coursera guided project (2) (Report & presentation)	(W7) Mon	(W15) Wed	20%
Final Exam	30/12/2024	11:00-14:30	40%

Department's Late Submission Policy:

(a) 1-24 hours: 25% of the mark will be deducted.
(b) > 24 hours: Not accepted.

Department's Policy for Dealing with Cheating:

It is essential that each student solves all programming assignments, lab tests and exams individually unless instructed otherwise, e.g., for group projects. Copying, plagiarism, collusion, switching, and falsification are violations of the university academic regulations. Students involved in such acts will be severely penalized. The department has adopted a firm policy on this issue. A zero mark will be assigned the first time a student is caught involved in copying and his/her name will be added to a watch list maintained by the Head of Department. Further repeated involvements in copying will cause the student to get an F grade in that course. This is in line with the university academic regulations.

VII. STUDENTS RESPONSIBILITIES	
It is the student's responsibility to know and comply with all University Academic Regulations relevant to participation in this course. These regulations specifically include attendance requirements and student academic code of conduct.	
ACADEMIC INTEGRITY	The University expects the students to approach their academic endeavors with the highest academic integrity. Please refer to the **Undergraduate Academic Regulations**.
ADD AND DROP	Students who wish to drop or add the course should review the **Undergraduate Academic Regulations**.
ATTENDANCE	Sultan Qaboos University has a clear requirement for students to attend courses, detailed in the **Undergraduate Academic Regulations**.
ASSESSMENT AND GRADING	To ensure the provision of a sound and fair assessment and grading, please review the **Undergraduate Academic Regulations**.
GRADE APPEAL	Students who wish to appeal their grades should review the **Undergraduate Academic Regulations**.
CLASSROOM POLICIES	Students are expected to dress professionally during class time as required by the University. Use of phones or any other electronic devices in the classroom during class time is strictly prohibited. Unauthorized use may lead to faculty member confiscation of the device for the remainder of the class. Behavior that persistently or grossly interferes with classroom activities is considered disruptive behavior and may be subject to disciplinary action. A student responsible for disruptive behavior may be required to leave the class.
LATE AND MAKE-UP WORK	Students are required to meet the course objectives by submitting coursework no later than the assigned due date. Students may be allowed to submit late work if approved by the course coordinator. Assignments submitted after the due date may be penalized.
MISSED EVALUATIONS	All quizzes, tests, clinical evaluations, and exams must be completed by the date they are assigned. If a quiz, test, or exam is missed due to a documented emergency situation (e.g., medical emergency, death in the immediate family), it is the student's responsibility to contact the instructor.
OTHER	

Course Outline Appendix

A. PROGRAM LEARNING OUTCOMES

SO1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

SO2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program discipline.SO3. Communicate effectively in a variety of professional contexts.

SO4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

SO5. Function effectively as a member or leader of a team engaged in activities appropriate to the program discipline.

SO6. Apply computer science theory, software development fundamentals to produce computing-based solutions.

B. SQU Graduate Attributes and Competencies for Undergraduate Studies

GRADUATE ATTRIBUTES	GRADUATE COMPETENCIES FOR UNDERGRADUATE STUDIES
A. Cognitive Capabilities: The graduate has sufficient general and specialized theoretical knowledge that enables him/her to deal well with his/her specialty and other related fields.	1. Demonstrates familiarity and works with advanced specialized knowledge in the area of specialization.
	2. Demonstrates a general understanding of the relationship of advanced specialized knowledge with knowledge in other relevant professional fields and aspects.
	3. Demonstrates a comprehensive understanding of the theories, principles, and methods used in his/her specialty, and how to create and apply new knowledge.
	4. Demonstrates general knowledge of the legal environment and necessary relevant regulatory frameworks.
	5. Shows awareness of contemporary literature and research.

B. Skill and Professional Capability: The graduate has sufficient skill and practical experience that enables him/her to perform all tasks related to the specialization and other related fields.	1. Applies concepts, theories, and investigative methods to synthesize and interpret information to evaluate conclusions.
	2. Applies appropriate research methods and techniques and employs digital knowledge
	3. Evaluates and critiques information independently
	4. Uses cognitive and technical skills to analyze complex issues and develop appropriate solutions.
	5. Initiates new ideas or processes in the professional, educational or research context.
C. Effective Communication: The graduate has the ability to communicate effectively with others to achieve the desired results	1. Explains, presents, and adapts information to suit the recipients.
	2. Employs appropriate information and communication technology to collect and analyze information.
D. Autonomy and Leadership: The graduate has the ability to lead, make decisions and take responsibility for decisions.	1. Performs advanced professional activities independently.
	2. Demonstrates leadership skills.
	3. Takes professional responsibility.
	4. Assumes full accountability for the tasks and their output.
E. Responsibility and Commitment: The graduate appreciates the importance of available resources and deals with them effectively and is committed to the ethics of the profession and society.	1. Manages time and other resources assigned to accomplishing tasks effectively and responsibly.
	2. Demonstrates effective practices when working in teams.
	3. Demonstrates advanced levels of understanding of values and ethics relevant to the specialization, profession and local and international society and promotes them among others.
	4. Works within the professional, institutional, and specialization guiding frameworks and strategic plans.
	5. Interacts with community affairs positively and preserves national identity.

F. Development and Innovation: The graduate has a passion for development and innovation in the field of specialization.	1. Demonstrates the ability to independently manage learning tasks, with an awareness of how to develop and apply new knowledge.
	2. Utilizes specialized knowledge and skills for entrepreneurship.
	3. Utilizes creative and innovative skills in the field of specialization.

C. OQF CHARACTERISTICS

1. Knowledge
2. Skills
3. Communication, Numeracy, and Information and Communication Technology Skills.
4. Autonomy and Responsibility
5. Employability and Values
6. Learning to learn