Kingdom of Saudi Arabia

The National Commission for Academic Accreditation & Assessment

COURSE SPECIFICATION

Course Specification

Institution: Umm Al-Qura University
Department: Computer Engineering Department

A. Course Identification and General Information

1. Course title and code: Cryptography and Network Security – 14034108-3
2. Credit hours: 03
3. Program(s) in which the course is offered. (If general elective available in many programs indicate this rather than list programs) Computer Engineering
4. Name of faculty member responsible for the course Dr. Turki F. Al-Somani
5. Level/year at which this course is offered Level 9 or 10 (Elective)
6. Pre-requisites for this course (if any) Computer Networks
7. Co-requisites for this course (if any) N/A
8. Location if not on main campus

B Objectives

1. Summary of the main learning outcomes for students enrolled in the course.

Introduction to Security Threats, Services, and Mechanisms. Classical Encryption Techniques & Cryptanalysis. Modern Symmetric Encryption Techniques. Number Theory & Public Key Encryption. Hash Functions & Message Authentication. Authentication Protocols. Network and IP Security. Network Threats and Protection. Malicious Software. Firewalls

2. Briefly describe any plans for developing and improving the course that are being implemented. (eg increased use of IT or web based reference material, changes in content as a result of new research in the field)

N/A

C. Course Description (Note: General description in the form to be used for the Bulletin or Handbook should be attached)

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
• Introduction to Security Threats, Services, and Mechanisms	1,2	6
• Classical Encryption Techniques, Cryptanalysis	3,4,5	9
• Modern Symmetric Encryption Techniques	6,7	6
• Number Theory, Public Key Encryption	8,9	6
• Hash Functions, Message Authentication	10,11	6
• Authentication Protocols	12	3
• Network and IP Security	13	3
• Network Threats and Protection	14	3

• Malicious Software	15	3
• Firewall	16	3

2. Course components (total contact hours per semester):

Lecture: 48 contact Hrs	Tutorial: N/A	Laboratory: N/A	Practical/Field work/Internship: N/A	Other: N/A

3. Additional private study/learning hours expected for students per week. (This should be an average: for the semester not a specific requirement in each week)

An average student is expected to study 6 – 8 hours per week other than the class hours.

4. Development of Learning Outcomes in Domains of Learning

For each of the domains of learning shown below indicate:

- A brief summary of the knowledge or skill the course is intended to develop;
- A description of the teaching strategies to be used in the course to develop that knowledge or skill;
- The methods of student assessment to be used in the course to evaluate learning outcomes in the domain concerned.

a. Knowledge

(i) Description of the knowledge to be acquired

This course will provide students with an understanding of important concepts in network security and cryptography. A practical technological survey of cryptography and network security will be given. This includes conventional encryption algorithms such as DES and AES, public-key design and algorithms such as RSA and digital signatures and authentication protocols, key managements etc. Network security plans and procedures may be formulated at the end.

.

(ii) Teaching strategies to be used to develop that knowledge

Lecture presentation, Study of research papers

(iii) Methods of assessment of knowledge acquired

Quizzes, Home works, Presentation

b. Cognitive Skills

(i) Description of cognitive skills to be developed

1. Conduct a security risk analysis for simple cases
2. Identify and solve security breaches in a computer environment

(ii) Teaching strategies to be used to develop these cognitive skills

Lectures slides, case studies

(iii) Methods of assessment of students cognitive skills

Examination, Quizzes, Home works

c. Interpersonal Skills and Responsibility

(i) Description of the interpersonal skills and capacity to carry responsibility to be developed

Group projects to develop team work skills.

(ii) Teaching strategies to be used to develop these skills and abilities

Group assignments and projects.

(iii) Methods of assessment of students interpersonal skills and capacity to carry responsibility

Project reports and presentations.

d. Communication, Information Technology and Numerical Skills
(i) Description of the skills to be developed in this domain. To develop skills in this domain technical programming and training is given to the students.
(ii) Teaching strategies to be used to develop these skills Students' are advised to write assignments and project reports as per standard format to develop Writhing skills and presentations are arranged to give them chance to develop communication skills.
(iii) Methods of assessment of students numerical and communication skills To assess the students numerical and communication skills tests and conducted and presentations
e. Psychomotor Skills (if applicable)
(i) Description of the psychomotor skills to be developed and the level of performance required
(ii) Teaching strategies to be used to develop these skills
(iii) Methods of assessment of students psychomotor skills

5. Schedule of Assessment Tasks for Students During the Semester

Assessment	Assessment task (eg. essay, test, group project, examination etc.)	Week due	Proportion of Final Assessment
1	Bi-weekly quizzes	Every other week	15%
2	Mid Term	Mid of the semester	15%
3	Assignments	As and when needed	5%
4	Project	After the Mid term exam	25%
5	Final Exam	End of the classes	40%

D. Student Support

1. Arrangements for availability of teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

   4 hours per week by the course instructor as office hours

E. Learning Resources

1. Required Text(s)

   - William Stallings, *Cryptography and Network Security: Principles and Practice*, 5th Ed, 2010

2. Essential References

   N/A

3. Recommended Books and Reference Material (Journals, Reports, etc) (Attach List)
   - Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2/E, Wiley, 2008. https://www.cl.cam.ac.uk/~rja14/book.html
   - Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 3rd Edition, , Prentice Hall, 2002

4. Electronic Materials, Web Sites etc

   1. S. Goldwasser and M. Bellare: Lecture Notes on Cryptography. These are notes from a summer cryptography class given by Profs. Shafi Goldwasser and Mihir Bellare at MIT. The treatment here is focused on the theoretical foundations of cryptography.

   2. M. Bellare and P. Rogaway: Lecture Notes for a graduate cryptography course at UCSD. The approach here is still aimed towards precise definitions and provable security, although more emphasis is given to practical considerations.

   3. J. Katz lecture Notes for the Intro to Crypto class thought at University of Maryland.

5. Other learning material such as computer-based programs/CD, professional standards/regulations

   N/A

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (ie number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Lecture rooms, laboratories, etc.) Lecture room is required with multimedia projector.
2. Computing resources N/A
3. Other resources (specify e.g. If specific laboratory equipment is required, list requirements or attach list) N/A

G. Course Evaluation and Improvement Processes

1. Strategies for Obtaining Student Feedback on Effectiveness of Teaching There is a centralized system at the university level to get such feedbacks
2. Other Strategies for Evaluation of Teaching by the Instructor or by the Department None
3. Processes for Improvement of Teaching The process for improvement of teaching is based on results of student survey on course learning outcomes and the extent to which student outcomes (SOs) are achieved
4. Processes for Verifying Standards of Student Achievement (eg. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution) None
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement. The answer has been provided under item no. 3 above.