هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T4
2020

# Course Specifications

| | |
|---|---|
| **Course Title:** | **Cryptography and Information Security** |
| **Course Code:** | **CSI 423** |
| **Program:** | **Computer Science and Information Technology** |
| **Department:** | **Computer Science and Information** |
| **College:** | **College of Science** |
| **Institution:** | **Majmaah University** |

## Table of Contents

## A. Course Identification

| | |
|---|---|
| **1. Credit hours:** | **3 ( 3 Lec. + 1 Lab )** |
| **2. Course type** | |
| **a.** | University □ College □ Department ☑ Others □ |
| **b.** | Required ☑ Elective □ |
| **3. Level/year at which this course is offered:** | 7 /3 |
| **4. Pre-requisites for this course** (if any)**:** | Design and Analysis of Algorithms (CSI 321) |
| **5. Co-requisites for this course** (if any)**:** | **N/A** |

**6. Mode of Instruction** (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1 | **Traditional classroom** | 48 | 80% |
| 2 | **Blended** | 6 | 10% |
| 3 | **E-learning** | 6 | 10% |
| 4 | **Distance learning** | 0 | 0 |
| 5 | **Other** | 0 | 0 |

**7. Contact Hours** (based on academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1 | **Lecture** | 30 |
| 2 | **Laboratory/Studio** | 15 |
| 3 | **Tutorial** | 15 |
| 4 | **Others** (specify) | 0 |
| | **Total** | 60 |

## B. Course Objectives and Learning Outcomes

### 1. Course Description

The aim of this course is to facilitate understanding of the inherent strengths and limitations of cryptography, especially when used as a tool for information security. Armed with this knowledge, student should be able to make more informed decisions when building secure systems.

The course covers various aspects of symmetric and asymmetric cryptography. While some topics will be dealt with in more detail, the course will attempt to provide a broad coverage of possibly all the core areas of cryptography. The students will be expected to implement and analyze some simple cryptographic schemes and read various articles. To understand the principles of encryption algorithms; conventional and public key cryptography. To have a detailed knowledge about authentication, hash functions and application level security mechanisms.

## 2. Course Main Objective

The main course objectives can be outlined in the following points:

1. Develop an understanding of information assurance as practiced in computer systems and network applications.
2. Gain familiarity with prevalent network and distributed system attacks and defenses against them.
3. Develop an understanding of cryptography, how it has evolved, and some key encryption techniques used today.
4. Develop an understanding of security polices (such as authentication, integrity, and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

## 3. Course Learning Outcomes

| | CLOs | Aligned PLOs |
|---|---|---|
| 1 | **Knowledge and Understanding** | |
| 1.1 | Assess the implications of cryptography in terms of privacy, security, and ethical issues. | |
| 1.2 | Evaluate and compare encryption standards and techniques. | |
| 1.3 | Define the basic terminology, notation, and concepts of computer security. | |
| **2** | **Skills :** | |
| 2.1 | Compile, integrate and appraise various methods of encryption information. | |
| 2.2 | Measure and determine appropriate encryption standards and techniques to suite specific business and technological needs. | |
| 2.3 | Analyze strengths and weaknesses in different systems. | |
| 2.4 | Design security protocols and methods to solve specified security problem. | |
| **3** | **Values:** | |
| 3.1 | Work cooperatively in a small group environment. | |
| 3.2 | Keep your computer safe from different threats. | |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1 | Overview: computer security concepts, the OSI security Architecture, Security attacks, Security mechanisms, Model of network security. | 4 |
| 2 | Classical Encryption Techniques: Symmetric cipher model, substitution techniques, Transposition techniques, Rotor machines. | 8 |
| 3 | Block ciphers and DES: Block cipher principles, DES, the strength of DES, Differential and linear cryptanalysis, Block cipher design principles. | 8 |
| 4 | Review of Mathematical concepts: Divisibility, Division algorithm, the Euclidean algorithm, Modular arithmetic, Groups, rings, fields. Finite Fields. | 4 |
| 5 | Advanced Encryption Standard: Finite Field Arithmetic, AES structures, AES transformation, AES key expansion. | 8 |
| 6 | Block cipher operation: Multiple and triple DES, ECB, CBC, CFB, OFB, Counter, and XTS mode of encryptions. | 4 |
| 7 | Review of Number theory concepts: prime numbers, Fermat's and Euler's theorem, testing primality, Chinese remainder theorem, Discrete logarithms. | 4 |

|  |  |  |
|---|---|---|
| 8 | Public key Cryptography and RSA: principles of public key cryptosystems, The RSA algorithm. | 4 |
| 9 | Other public key cryptosystem: DH scheme, ElGamal cryptosystem | 4 |
| 10 | Cryptographic Hash functions: Applications of Cryptographic hash functions, simple hash functions, SHA-3, Digital signatures. Applications in authentication. | 12 |
| **Total** |  | 60 |

## D. Teaching and Assessment

### 1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Teaching Strategies | Assessment Methods |
|---|---|---|---|
| **1.0** | **Knowledge and Understanding** |  |  |
| 1.1 | Assess the implications of cryptography in terms of privacy, security, and ethical issues. | Lectures<br>Lab demonstrations<br>Case studies<br>Individual presentations | Written Exam<br>Homework assignments<br>Lab assignments<br>Class Activities<br>Quizzes |
| 1.2 | Evaluate and compare encryption standards and techniques. |  |  |
| 1.3 | Define the basic terminology, notation, and concepts of computer security. |  |  |
| **2.0** | **Skills** |  |  |
| 2.1 | Compile, integrate and appraise various methods of encryption information. | Lectures<br>Lab demonstrations<br>Case studies<br>Individual presentations<br>Brainstorming | Written Exam<br>Homework assignments<br>Lab assignments<br>Class Activities<br>Quizzes<br>Observations |
| 2.2 | Measure and determine appropriate encryption standards and techniques to suite specific business and technological needs. |  |  |
| 2.3 | Analyze strengths and weaknesses in different systems. |  |  |
| 2.4 | Design security protocols and methods to solve specified security problem. |  |  |
| **3.0** | **Values** |  |  |
| 3.1 | Work cooperatively in a small group environment. | Small group discussion<br>Whole group discussion<br>Brainstorming<br>Presentation | Observations<br>Homework assignments<br>Lab assignments<br>Class |
| 3.2 | Keep your computer safe from different threats. |  |  |

### 2. Assessment Tasks for Students

| # | Assessment task* | Week Due | Percentage of Total Assessment Score |
|---|---|---|---|
| **1** | First written mid-term exam | 6 | 15% |
| **2** | Second written mid-term exam | 12 | 15% |
| **3** | Presentation, class activities, and group discussion | Every week | 10% |
| **4** | Homework assignments | After each chapter | 10% |

| # | Assessment task* | Week Due | Percentage of Total Assessment Score |
|---|---|---|---|
| 5 | Implementation of presented protocols | Every two weeks | 10% |
| 6 | Final written exam | 16 | 40% |
|  | Total |  | 100% |

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

## E. Student Academic Counseling and Support

**Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :**

Office hours: Sun: 10-12, Mon. 10-12, Thru. 8-10
Office call: Sun. 12-1 and Wed 12-1
Email: h.haly@mu.edu.sa
Mobile: 0538231332

## F. Learning Resources and Facilities

### 1.Learning Resources

|  |  |
|---|---|
| **Required Textbooks** | W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013. |
| **Essential References Materials** | C. Kaufman, Radia Perlman, Mike Speciner, Network Security, Private Communication in a PublicWorld, Prentice Hall, 2002 |
| **Electronic Materials** | www.iacr.org |
| **Other Learning Materials** | Video and presentation are available with me |

### 2. Facilities Required

| Item | Resources |
|---|---|
| **Accommodation**<br>(Classrooms, laboratories, demonstration rooms/labs, etc.) | Classroom and Labe available at College of science in Zulfi. |
| **Technology Resources**<br>(AV, data show, Smart Board, software, etc.) | All resource are available in the halls |
| **Other Resources**<br>(Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list) | N/A |

## G. Course Quality Evaluation

| Evaluation Areas/Issues | Evaluators | Evaluation Methods |
|---|---|---|
| Effectiveness of teaching and assessment | Students<br>Reviewers | Questionnaires (course evaluation) filled by the students and electronically organized by the university.<br>Student-faculty and management meetings. |

**Evaluation areas** (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
**Evaluators** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
**Assessment Methods** (Direct, Indirect)

## H. Specification Approval Data

| | |
|---|---|
| **Council / Committee** | **Dr. Abdelall Alourini**<br>**Dr. Hassan Aly** |
| **Reference No.** | 3441 |
| **Date** | 27.09.2021 |

جامعة المجمعة
Majmaah University
كلية العلوم بالزلفي
قسم الحاسب الآلي والمعلومات