**ATTACHMENT 2 (g)**

**Course Report**

**Kingdom of Saudi Arabia**

**The National Commission for Academic Accreditation & Assessment**

# Course REPORT
# (CR)
# Cryptography and Information Security
# CIS 446-Z

**Dr. Hassan Aly**

A separate Course Report (CR) should be submitted for every course and for each section or campus location where the course is taught, even if the course is taught by the same person. Each CR is to be completed by the course instructor at the end of each course and given to the program coordinator

A combined, comprehensive CR should be prepared by the course coordinator and the separate location reports are to be attached.

# Course Report

**For guidance on the completion of this template refer to the NCAAA handbooks or the NCAAA Accreditation System help buttons.**

| | |
|---|---|
| Institution: Majmaah university | Date of Course Report 1436 |
| College/ Department: College of Science / Department of Computer Science and Information | |

## A. Course Identification and General Information

| | | | |
|---|---|---|---|
| 1. Course title | Cryptography and Information Security | Code # CIS 446-Z | Section 122 |
| 2. Name of course instructor | Dr. Hassan Aly | Location College of Science at AzZulfi | |
| 3. Year and semester to which this report applies. First Semester 1436/1436 | | | |
| 4. Number of students starting the course? | 11 | Students completing the course? | 11 |

5. Course components (actual total contact hours and credits per semester):

| | Lecture | Tutorial | Laboratory | Practical | Other: | Total |
|---|---|---|---|---|---|---|
| Contact Hours | 45 | | | | | 45 |
| Credit Hours | 45 | | | | | 45 |

## B. - Course Delivery

1. Coverage of Planned Program

| Topics Covered | Planned Contact Hours | Actual Contact Hours | Reason for Variations if there is a difference of more than 25% of the hours planned |
|---|---|---|---|
| 1. Overview: computer security concepts, the OSI security Architecture, Security attacks, Security mechanisms, Model of network security. | 3 | 3 | |
| 2. Classical Encryption Techniques: Symmetric cipher model, substitution techniques, Transposition techniques, Rotor machines. | 6 | 6 | |

| | | | |
|---|---|---|---|
| 3. Block ciphers and DES: Block cipher principles, DES, the strength of DES, Differential and linear cryptanalysis, Block cipher design principles. | 6 | 3 | Teaching the DES cipher needs time which is not available. |
| 4. Review of Mathematical concepts: Divisibility, Division algorithm, the Euclidean algorithm, Modular arithmetic, Groups, rings, fields. Finite Fields. | 3 | 3 | |
| 5. Advanced Encryption Standard: Finite Field Arithmetic, AES structures, AES transformation, AES key expansion. | 6 | 6 | |
| 6. Block cipher operation: Multiple and triple DES, ECB, CBC, CFB, OFB, Counter, and XTS mode of encryptions. | 3 | 3 | |
| 7. Review of Number theory concepts: prime numbers, Fermat's and Euler's theorem, testing primality, Chinese remainder theorem, Discrete logarithms. | 3 | - | This topic is concealed since there is no enough time. |
| 8. Public key Cryptography and RSA: principles of public key cryptosystems, The RSA algorithm. | 3 | 3 | |
| 9. Other public key cryptosystem: DH scheme, ElGamal cryptosystem. | 3 | 3 | |
| 10. Cryptographic Hash functions: Applications of Cryptographic hash functions, simple hash functions, SHA-3, Digital signatures. Applications in authentication. | 9 | 6 | No enough time. |

| 2. Consequences of Non Coverage of Topics<br>For any topics where the topic was not taught or practically delivered, comment on how significant you believe the lack of coverage is for the course learning outcomes or for later courses in the program. Suggest possible compensating action. | | |
|---|---|---|
| Topics (if any) not Fully Covered | Effected Learning Outcomes | Possible Compensating Action |
| Review of Number theory concepts: prime numbers, Fermat's and Euler's theorem, testing primality, Chinese remainder theorem, Discrete logarithms. | No effect | The topics have been covered in other courses. |
| DES Cipher | No effect | We have examined the AES instead. |

**3. Course learning outcome assessment.**

| | List course learning outcomes | List methods of assessment | Summary analysis of assessment results |
|---|---|---|---|
| 1 | Assess the implications of cryptography in terms of privacy, security, and ethical issues. | Written Exam<br>Homework assignments<br>Lab assignments<br>Class Activities<br>Quizzes<br>Observations<br>Presentations<br>Group Discussion | The average of the final results is 3.44 (C+) of a total of 18 students. |
| 2 | Evaluate and compare encryption standards and techniques. | | |
| 3 | define the basic terminology , notation, and concepts of computer security. | | |
| 4 | Compile, integrate and appraise various methods of encryption information. | | |
| 5 | Measure and determine appropriate encryption standards and techniques to suite specific business and technological needs. | | |
| 6 | Analyze strengths and weaknesses in different systems. | | |
| 7 | Design security protocols and methods to solve specified security problem. | | |
| 8 | work cooperatively in a small group environment. | | |

| | | | |
|---|---|---|---|
| 9 | keep your computer safe from different threats. | | |

Summarize any actions you recommend for improving teaching strategies as a result of evaluations in table 3 above.

- Individual presentations
- Brainstorming
- Improving programming tools.

4. Effectiveness of Planned Teaching Strategies for Intended Learning Outcomes set out in the Course Specification. (Refer to planned teaching strategies in Course Specification and description of Domains of Learning Outcomes in the National Qualifications Framework)

| List Teaching Methods set out in Course Specification | Were these Effective? | | Difficulties Experienced (if any) in Using the Strategy and Suggested Action to Deal with Those Difficulties. |
|---|---|---|---|
| | No | Yes | |
| • Lectures<br>• Homework<br>• Conversation with instructors | | √ | |
| • Conversation with other students.<br>• Indirect questions.<br>• Working groups for course activities | | √ | |

**Note:** In order to analyze the assessment of student achievement for each course learning outcome, student performance results can be measured and assessed using a KPI, a rubric, or some grading system that aligns student work, exam scores, or other demonstration of successful learning.

## C. Results

1. Distribution of Grades

| Letter Grade | Number of Students | Student Percentage | Explanation of Distribution of Grades |
|---|---|---|---|
| A | 0 | 0% | |
| B | 1 | 9.09% | |
| C | 4 | 36.36% | |
| D | 5 | 45.45% | |
| F | 1 | 9.10% | |
| Denied Entry | 0 | 0 | |
| In Progress | 0 | 0% | |
| Incomplete | 0 | 0 | |
| Pass | 10 | 90.91% | |
| Fail | 1 | 9.09% | |
| Withdrawn | 0 | 0 | |

2. Analyze special factors (if any) affecting the results

The results are normal since this course is the last level of the student progress.

3. Variations from planned student assessment processes (if any) (see Course Specifications).

We have use the same assessment processes as in the course specifications.

a. Variations (if any) from planned assessment schedule (see Course Specification)

| Variation | Reason |
|---|---|
| | |
| | |
| | |

| b. Variations (if any) from planned assessment processes in Domains of Learning (see Course Specification) | |
|---|---|
| Variation | Reason |
| | |
| | |
| | |

| 4. Student Grade Achievement Verification (eg. cross-check of grade validity by independent evaluator). | |
|---|---|
| Method(s) of Verification | Conclusion |
| Interview students, including answers and model answer sheet and learning resources for decision | Good result |
| | |

**D. Resources and Facilities**

| 1. Difficulties in access to resources or facilities (if any) | 2. Consequences of any difficulties experienced for student learning in the course. |
|---|---|
| | |

**E. Administrative Issues**

| 1 Organizational or administrative difficulties encountered (if any) | 2. Consequences of any difficulties experienced for student learning in the course. |
|---|---|
| | |

**F Course Evaluation**

| 1 Student evaluation of the course (Attach survey results report)<br>Attached kindly find the survey report of the student evaluation of the course. |
|---|
| a. List the most important recommendations for improvement and strengths |
| |

| |
|---|
| b. Response of instructor or course team to this evaluation |
| 2. Other Evaluation (e.g. by head of department, peer observations, accreditation review, other stakeholders) |
| a. List the most important recommendations for improvement and strengths |
| b. Response of instructor or course team to this evaluation |

**G. Planning for Improvement**

| 1. Progress on actions proposed for improving the course in previous course reports (if any). | | | |
|---|---|---|---|
| Actions recommended from the most recent course report(s) | Actions Taken | Results | Analysis |
| a. increasing efforts for lab assignments to help students implement the ciphers. | Choose a teaching assistant for the lab course. | | |
| b. increasing efforts to clarify the mathematics underline the subject. | Increase the assignments of the mathematics part of the subject. | | |
| c. | | | |
| d. | | | |

2. List what actions have been taken to improve the course (based on previous CR, surveys, independent opinion, or course evaluation).

1. Assign a teaching assistant to help students to do lab assignments.
2. Solve more assignments of the mathematics part of the subject.

3. Action Plan for Improvement for Next Semester/Year

| Actions Recommended | Intended Action Points and Process | Start Date | Completion Date | Person Responsible |
|---|---|---|---|---|
| a. | | | | |
| b. | | | | |
| c. | | | | |
| d. | | | | |
| e. | | | | |

**Name of Course Instructor: Hassan Aly**

**Signature: _____ Date Report Completed:** 20.3.1436

**Program Coordinator: Yosry Azzam**

**Signature: _____ Date Received:** 20.3.1436