# Course Description Form

- Course Name:

Cryptanalysis

- Course Code:

CSCS4220

- Semester / Year:

Second Semester/2025-2024

- Description Preparation Date:

28/1/2025

- Available Attendance Forms:

In classroom

- Number of Credit Hours (Total) / Number of Units (Total)

30 hours/3 units

- Course administrator's name (mention all, if more than one name)

Name: Hala Bahjat Abdul Wahab
Email: Hala.B.AbdulWahab@uotechnology.edu.iq

- **Course Objectives**

| | |
|---|---|
| **Course Objectives** | 1. Providing an advanced basis for the cryptanalysis<br>2. Identify methods of cryptanalysis applied in computer security<br>3. Deepening mathematical methods and algorithms developing cryptanalysis techniques |

- **Teaching and Learning Strategies**

| | |
|---|---|
| **Strategy** | -Theoretical lectures - practical laboratories – methodological books - resources (Internet)<br>-Using modern devices to deliver the material to students using data show in addition to the smart board. |

- **Course Structure**

| Week | Hours | Required Learning Outcomes | Unit or subject name | Learning method | Evaluation method |
|---|---|---|---|---|---|
| 1 | 2 theoretical | 1, 6,7 | Introduction for cryptanalysis, cryptanalysis requirements. | Theoretical lecture | Attendance - Discussions Tests |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 2 theoretical | 1, 6,7 | Transposition cryptanalysis, Scrytal, Keyword columm transposition Double transposition | Theoretical lecture | Attendance - Discussions Tests |
| 3 | 2 theoretical | 1, 6,7 | Substution cryptanalysis, additive,multiplication, affine, keyword. | Theoretical lectures | Attendance - Discussions Tests |
| 4 | 2 theoretical | 1, 6,7 | Statistical cryptanalysis , unilateral frequency distribution | Theoretical lectures | Attendance - Discussions Tests |
| 5 | 2 theoretical | 1, 6,7 | Letter frequency in cryptogram, roughness. | Theoretical lectures | Attendance - Discussions Tests |
| 6 | 2 theoretical | 1,6,7 | Coincidence tests, index of coincidence. | Theoretical lectures | Attendance - Discussions Tests |
| 7 | 2 theoretical | 1,6,7 | Cryptanalysis for the affine using statistical cryptanalysis'. | Theoretical lectures | Attendance - Discussions Tests |
| 8 | 2 theoretical | 1,6,7 | Solve different problems, affine, transposition,….etc | Theoretical lectures | Attendance - Discussions Tests |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| 9 | 2 theoretical | 1,6,7 | Polyalabetic analysis, vigin method, computing k length. | Theoretical lectures | Attendance - Discussions Tests |
| 10 | 2 theoretical | 1, 6,7 | Kasiski test, Shift itself, Percentage of coincidence, comple examples. | Theoretical lectures | Quiz<br>Homework<br>Attendance Exam<br>Project assessme |
| 11 | 2 theoretical | 1, 6,7 | Stream cipher cryptanalysis : introduction of stream cipher, LFBSR, primitive polynomials | Theoretical lectures | Attendance - Discussions Tests |
| 12 | 2 theoretical | 1,6,7 | Cryptanalysis for LFBSR , using Massy algorithm , examples, solve problems | Theoretical lectures | Attendance - Discussions Tests |
| 13 | 2 theoretical | 1,3,5,6,7 | Differential Cryptanalysis, An Attack on a 3-round DES | Theoretical lectures | Attendance - Discussions Tests |
| 14 | 2 theoretical | 1,,6,7 | Public Key Attacks, Introduction, Factoring Algorithms , Trial Division | Theoretical lectures | Attendance - Discussions Tests |

| | | | | | |
|---|---|---|---|---|---|
| 15 | 2 theoretical | 1, 6,7 | Final Exam | Theoretical lectures | Exam |

## • Course Evaluation

Distributing the score out of 100 according to the tasks assigned to the student such as daily preparation, daily oral, monthly, or written exams, reports .... etc

5 marks of attendance
5 marks Assignments and reports
15 marks for mid-course exam (mid)
15 marks for the laboratory exam. Implementing programs for algorithms and file management
60 marks for the end-of-course exam (first semester)

## • Learning and Teaching Resources

| | |
|---|---|
| **Required textbooks (curricular books, if any)** | Not required |
| **Main references (sources)** | Operating System Concepts – $9^{th}$ Edition |
| **Recommended books and references (scientific journals, reports…)** | Operating System Concepts – $10^{th}$ Edition<br>Operating System Concepts – $11^{th}$ Edition |
| **Electronic References, Websites** | power point for Operating System Concepts – $9^{th}$ Editi |