**Cryptography**

**2021-2022 –Second Semester**

**Dr. Banar Fareed**

**Academic Year: 2021-2022**

**Course Book**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Information** | **Details** |
|  | **Course Name** | Cryptography |
|  | **Course Code** | 401RM |
|  | **Lecturer In-charge** | Banar Fareed |
|  | **College/Department** | IT |
|  | **Contact Information** | 07504812594 |
|  | **Time (in hours) per Week** | From 9:00AM up to 2:30AM from Sunday to Thursday |
|  | **Office Hours** |  |
|  | **Teacher’s Academic Profile** | Education:  B.Sc. In computer science  M. Sc. In computer science  PhD. in Computer Engineering at Cyprus International University.  Lectures of :  Cryptography, information Security, Computer Architecture . Advanced IT, Research Method |
|  | **Academic Title** | Asst. Lecturer |
|  | **Keywords** |  |
|  | **Course Overview:**  The objective of the course is to cover the fundamental issues of information system security and assurance. | |

|  |  |
| --- | --- |
| **12.** | **Aims & Objective:** The objective of the course is to cover the fundamental issues of information system security and assurance, the algorithms of Cryptography. |
| **13.** | **Course Requirement:**  Attendance and completion of all tests, exams, reports, presentations. |
| **14.** | **Teaching and Learning Method:**   * Book, Data Show and PowerPoint, whiteboard, Lectures, homework, and assignments. |
| **15.** | **Assessment Scheme:**   * 25 % Mid-term Examination * 15 % Assignments and Quizzes * 60 % Final Examination |
| **16.** | **Students Learning Outcome:**  The lecture slides will be provided in the class and will be the core of the course, however additional reference pages will advise reading. Moreover to slides the whiteboard and pen are used to explain some complex ideas. |
| **17.** | **Course Reading List and References**   * The InfoSec HandBook / An Introduction to Information Security * The Complete Reference Information Security * Principles of Cryptography * The Basics of Cryptography * Internet |
| **18.** | **Course Content** |

**Course Content**

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Lecture Date** | **No. of Hours** | **Topics** |
| 1. | 25/1/2022 | 3 | Introduction to cryptography |
| 2. | 1/2/2022 | 3 | Encryption Algorithms, Square cipher, Transposition cipher |
| 3. | 8/2/2022 | 3 | Vignar Cipher ,Keyword Cipher |
| 4. | 15/2/2022 | 3 | Playfair cipher, |

|  |  |  |  |
| --- | --- | --- | --- |
| 5. | 22/2/2022 | 3 | Atbash Cipher, Affine Cipher |
| 6. | 29/2/2022 | 3 | Hill cipher |
| 7. | 8/3/2022 | 3 | Mathematics of Cryptography |
| 8. | 29/3/2022 | 3 | Euclidean algorithm |
| 9. | 5/4/2022 | 3 | RSA cipher |
| 10. | 12/4/2022 | 3 | Midterm exams |
| 11. | 19/4/2022 | 3 | Examples of RSA cipher |
| 12. | 26/4/2022 | 3 | DES cipher |
| 13. | 3/5/2022 | 3 | Examples of DES Cipher |
| 14. | 10/5/2022 | 3 | Review for Final Examination |
| 15. | 17/5/2022 | Final Examination | |

|  |  |
| --- | --- |
| **19.** | **Examinations:**  **-Compositional:**   * Compositional:   In this type of exam the questions usually starts with explain (How…? / What …? /Why…?) With their typical answers. (see example below) How can I avoid computer viruses?  Ans: Most viruses travel through email or internet downloads. Never open attachment from unknown senders and be very cautious when downloading software from Internet sources.   * Multiple Choices:   In this type of exam there will be a number of phrases next or below a statement, students will match the correct phrase. (see example below) In a typical information security program, what is the primary responsibility of information (data) owner?  A. Ensure the validity and accuracy of data  B. Determine the information sensitivity or classification level. C. Monitor and audit system users.  D. Ensure availability of data.  Ans: B |
| **20.** | **Notes: :**  I kept the topics general so that I can give updated lecture every time depending on every day new technology. |