Department of Mathematics

College of Science

Salahaddin University-Erbil

Subject: Introduction to Cryptography

Course Book: Fourth Stage-Second Semester

Lecturer's Name: Dr. Andam Ali Mustafa

Academic Year: 2022-2023

Course Book

1. Course name	Cryptography
2. Lecturer in charge	Andam Ali Mustafa
3. Department / College	Mathematics / Science
4. Contact	**E-mail:** andam.mustafa@su.edu.krd **Tel:** +9647504302367
5. Time (in hours) per week	2 hours
6. Office hours	Sunday 8:30-10:30 Or Thursday 8:30-10:30
7. Course code	
8. Teacher's academic profile	❖ **25/8/2022** PhD in University Roma Tre in Rome, Italy. ❖ **3/3/2015** M.Sc. in the Department of Mathematics, College of Science, Salahaddin University-Erbil, Iraq. ❖ **31/3/2015** Assistant lecturer in the Department of Mathematics, College of Science, Salahaddin University-Erbil, Iraq. ❖ **2/7/2009** B.Sc. in the Department of Mathematics, College of Science, Salahaddin University-Erbil, Iraq. ❖ **2004-2005** Awarded a baccalaureate from the Kurdistan High School, Erbil, Iraq.
9. Keywords	sender, receiver, opponent ciphertext, cryptogram, decryption, encryption, cryptanalysis, classical encryption methods, RSA system and ECC.

10. Course overview:

Cryptology is the study of codes and ciphers. It deals with the study of making and breaking secret codes. In this introductory undergraduate course, we will be studying situations that are often framed as a game between three parties: a sender (e.g., an embassy), a receiver (the government office) and an opponent (a spy). We assume that the sender needs to get an urgent message to the receiver through communication channels which are vulnerable to the opponent.

To do this communication, the sender and receiver agree in advance to use some sort of code which is unlocked by a keyword or phrase. The opponent will be able to intercept the message. Is he/she able to unlock the message without knowing the key?

11. Course objective:

To give the students an operational understanding of basic cryptography including some basics of Elliptic Curve.

12. Student's obligation

- Students reign a commitment to come on time and remain in the classroom for the duration of scheduled classes.
- Nothingness speaks students with each other during lecture.
- All devices must be turned off.
- When teacher ask question, Students will be to raise your hand before answer his question.
- Students own an obligation to write tests and final examinations at the times scheduled by the teacher or the College.

13. Forms of teaching

I give hard copy of My lecture notes to students before coming lecturer time. first, I remember students about previous lecture, and then I start new lecture. At the end of the lecture give a homework for the next lecture. During this proses I use presentation and whiteboard.

14. Assessment scheme

1. Exam: 20% marks **2. Quiz:** 10% marks **3. Homework:** 5% marks

4. Assignments and other activities: %5 marks **5. Final exam:** 60 % marks

15. Student learning outcome:

- Explain some of the concepts of number theory, a primary area of mathematics, using examples.
- Apply mathematical ideas and concepts within the context of number theory.
- Solve a range of problems in number theory.
- Recognize the appropriate use of the division algorithm, the divides relation and congruences in problem solving.

16. Course Reading List and References:

- Bruce Schneier, **Applied cryptography** (Second Edition), 1996.
- Joseph H. Silverman, **a Friendly introduction to Number Theory,** (Fourth Edition), 2012.
- Titu Andreescu, Dorin Andrica, **Number Theory, Structures, Examples, and Problems** (2009).
- Craig P. Bauer, **Secret History, The Story of Cryptography**, CRC (2013).

- Washington, Lawrence C. **Elliptic curves: number theory and cryptography,** Chapman and Hall/CRC, (2008).

17. The Topics:	**Lecturer's name**
Chapter One: Classical Cipher Systems. (5 Weeks) Introduction, Definitions and Terminology, what is Cryptography Used for? Methods for Utilizing Keys and Encryption, Classical Encryption Methods: Greek Ciphers (Scytale Cipher, Polybius Cipher, Bifid Cipher, Trifid cipher), Permutation Cipher, Rail-Fence Transposition, Pigpen cipher, Francis Bacon's Cipher, Caesar Cipher, Vigenère Cipher, Playfair Cipher. Modulo Operation, Affine Cipher, Letter Frequency Analysis, Other Ciphers and Codes (Morse code, ASCII Codes), The Hill Cipher. **Chapter Two: Public Key Cryptography. (5 Weeks)** Introduction, Knapsack system, RSA System, fast exponential procedure; Modifications of RSA type will be chosen from: Lu-Lee system, William’s System, Rabin System. Discrete Logarithms. **Chapter Three: Elliptic Curve Cryptography. (3 Weeks)** Introduction, Weierstrass Equations, Elliptic Curve, Group Law, Elliptic Curves Over Finite Fields, Use of Elliptic Curves in Cryptography.	**Dr. Andam Ali Mustafa**
18. Practical Topics (If there is any)	

19. Examinations:

Questions in the examination will be arranged the matching mode by way of the examples and exercises that I give delivered in the lecture notes.
Sometimes will be have extra mark in examination for worthy students.
Many of the questions will take from those books that I mentioned in the References part.

20. Extra notes:

Answers of examination will find in the board’s declaration physics department after every examination.

21. Peer review

.