MẬT MÃ HỌC CƠ SỞ (INTRODUCTION TO CRYPTOGRAPHY)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: Mật mã học cơ sở (Introduction to Cryptography)

Course code: SEC1403_CLC

Course type: Compulsory

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with the basic knowledge about cryptography and some cryptanalytic techniques.

Skills:

After completing the course, students will:

- Have the skills to select and apply encryption algorithms in ensuring information security.
- Know how to test and evaluate the weaknesses and vulnerabilities of some encryption algorithms.

Attitude:

Students are required to attend classes and complete assignments/projects.

3. Abstracts

The course provides students with basic knowledge of cryptography including: the role and importance of cryptography; some basic mathematical issues applied in cryptography; common symmetric and asymmetric encryption algorithms; popular hash functions; cryptography problems such as: symmetric encryption and asymmetric encryption; some practical applications of encryption algorithms; key management and distribution techniques.

4. Teaching and learning methods

Lectures:	24 hours
Exercises:	5 hours
Projects :	8 hours
Labs:	8 hours
Individual reading:	0 hours

5. Prerequisites: SEC1401_CLC

6. Learning outcomes

After completing this course, students is able to:

[CLO1]: Explains methods or algorithms for encryption, decryption and key distribution and agreement techniques.
[CLO2]: Select and deploy a number of encryption, key distribution and agreement algorithms to solve basic problems in information security.

7. Assignment criteria

Learning outcomes	Assignment criteria
[CLO1]: Explains methods or algorithms for encryption, decryption and key distribution and agreement techniques	Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5
[CLO2]: Select and deploy a number of encryption, key distribution and agreement algorithms to solve basic problems in information security	Chapter 2, Chapter 3, Chapter 4, Chapter 5

8. Outlines

CHAPTER 1: OVERVIEW OF CRYPTOGRAPHY

1.1. Basic terms and concepts
1.2. Development history
1.3. Classify
1.4. Role
1.5. Applications of cryptography
1.6. Mathematical concepts in cryptography

CHAPTER 2. SYMMETRIC ENCRYPTION

2.1. Introduction to Symmetric encryption
2.2. Classical symmetric encryption techniques
    2.2.1. Alternative method
    2.2.2. Permutation encryption method
    2.2.3. XOR encryption method
    2.2.4. Running key cipher method
2.3. Symmetric block encryption techniques
    2.3.1. Overview of block ciphers
    2.3.2. DES/3DES encryption algorithm
    2.3.3. AES encryption algorithm
2.4. Stream encoding techniques
    2.4.1. Overview of stream encoding
    2.4.2. A51 encryption algorithm
    2.4.3. RC4 encryption algorithm
2.5. Advantages and disadvantages of symmetric encryption

CHAPTER 3. ASYMMETRIC ENCRYPTION

3.1. Introduction to asymmetric encryption

3.2. RSA encryption algorithm

3.3. Advantages and disadvantages of asymmetric encryption

3.4. Applications of asymmetric key encryption

CHAPTER 4. HASH FUNCTION

4.1. General introduction to hash functions.

4.1.1. Define

4.1.2. Basic properties

4.1.3. Classify

4.1.4. Role

4.2. Common hash functions

4.2.1. MD family hash function

4.2.2. SHA family hash function

CHAPTER 5. KEY MANAGEMENT AND DISTRIBUTION

5.1. General overview of key management and distribution

5.2. Management and distribution of private keys

5.3. Public key management and distribution

9. Required Textbooks

[1] Jonathan Katz; Yehuda Lindell, Introduction to Modern Cryptography 2nd Edition, Chapman & Hall/ CRC, 2017.

10. Suggested Textbooks

[2] William Stallings, *Cryptography and Network Security 7th Edition*, Prentice Hall, 2021.

[3] Đỗ Xuân Chợ. Bài giảng Mật mã học cơ sở. Học viện công nghệ bưu chính viễn thông. 2021.

[4] Nguyễn Bình, Ngô Đức Thiện. Cơ sở mật mã học. Học Viện Công Nghệ Bưu Chính Viễn Thông, 2013. 237 trang.

11. Schedule

Main contents	Duration	Specific contents

Chapter 1. Overview of cryptography	4h lecture	1.1.Basic terms and concepts 1.2.Development history 1.3.Classify 1.4.Role 1.5.Applications of cryptography 1.6.Mathematical concepts in cryptography
Chapter 2. Symmetric encryption	6 hours lecture 1h exercise 2h lab 2h project	2.1. Introduction to symmetric key encryption 2.2. Classical symmetric encryption techniques 2.3. Symmetric block encryption techniques 2.4. Stream encoding techniques 2.5. Advantages and disadvantages of symmetric encryption
Chapter 3. Asymmetric encryption	4h lecture 1h exercise 2h project 2h lab	3.1. Introduction to asymmetric encryption 3.2. RSA encryption algorithm 3.3. Advantages and disadvantages of asymmetric encryption 3.4. Applications of asymmetric key encryption
Chapter 4. Hash functions	4h lecture 2h project 2h lab 1h exercise	4.1. General Introduction to hash function 4.2. Common hash functions
Chapter 5. Key management and distribution	6 hours reading 2h exercise 2h project 2h lab	5.1. General overview of key management and distribution 5.2. Management and distribution of private keys 5.3. Public key management and distribution

12. Grading Policy

Attendance: 10%
Mid-term exam/exercises: 10%
Course projects: 30%
Final examination: 50%