INTRODUCTION TO CRYPTOGRAPHY

1.Thông tin về học phần (General Information)

Tên học phần (Course name): Introduction to Cryptography

Mã học phần (Course code): INT1344

Số tín chỉ (Number of credits): 3

Loại học phần (Course type): Compulsory

Học phần tiên quyết (Prerequisites):

Học phần trước (Previous courses):

Học phần song hành (Parallel courses):

Các yêu cầu đối với học phần (Course requirements):

- Lecture room: Projector, microphone and speaker.
- Laboratory: Projector, microphone and speaker, programming support tools.

Giờ tín chỉ đối với các hoạt động (Teaching and Learning hours):

- Lý thuyết (Lectures): 30h
- Bài tập (Exercises): 0h
- Bài tập lớn (Projects): 8h
- Thực hành (Labs): 7h
- Tự học (Individual reading): 0h

Địa chỉ Khoa/Bộ môn phụ trách học phần (Address of the Faculty/Department in charge of the course):

- Address: Faculty of Information Technology 1 - Posts and Telecommunications Institute of Technology, Km10, Nguyen Trai Street, Ha Dong District, Hanoi.
- Phone number: (024) 33510432

2. Mục tiêu học phần (Objectives)

Về kiến thức (Knowledge):

The aim of this course is to provide students with background information and knowledge of cryptography, including:

- mathematical concepts in cryptography;
- commonly-used encryption algorithms;
- hash functions
- key management and distribution issues;
- applications of cryptography in practice.

Kỹ năng (Skills):

The aim of this course is to equip students with skills in:

- analyzing and selecting appropriate cryptographic algorithms for real problems;
- applying suitable cryptographic techniques for information security problems in practice.

Thái độ, Chuyên cần (Attitude):

Students must ensure the required class attendance, assigned projects & labs and self-studying hours.

3. Tóm tắt nội dung học phần (Description)

This course provides students with basic knowledge of cryptography, including: the roles and the importance of cryptography, basics of applied mathematics in cryptography, common symmetric and asymmetric encryption algorithms, hash functions, issues on management, agreements and distribution of the keys in cryptography, and some practical applications of encryption algorithms.

4. Nội dung chi tiết học phần (Outlines)

Chapter 1 Introduction of cryptography

1.1. Basic terminology and concepts
1.2. History of cryptography
1.3. Classification of cryptography
1.4. The role of cryptography

Chapter 2 Symmetric – key encryption

2.1. Introduction
2.2. Mathematical aspects of symmetric – key encryption
2.3. Classical symmetric – encryption techniques
2.4. Modern symmetric – encryption techniques
    2.4.1. Data Encryption Standard (DES)
    2.4.2. Advanced encryption standard (AES)
    2.4.3. Stream ciphers
2.5. Evaluation of symmetric – encryption algorithms
2.6. Some applications of symmetric key encryption

Chapter 3 Asymmetric – key encryption

3.1. Introduction
3.2. Mathematical aspects of asymmetric – key encryption
3.3. Some asymmetric – key encryption algorithms
3.4. Evaluation of asymmetric – encryption algorithms
3.5. Some applications of asymmetric – key encryption

Chapter 4 Hash Functions

4.1. Introduction
4.2. Unkeyed hash functions (MDCs)
4.3. Keyed hash functions (MACs)
4.4. Some common hash functions
    4.4.1. MD5
    4.4.2. SHA1
4.5. Hash Function Applications

Chapter 5 Key Management and Distribution

5.1. Introduction
5.2. Background and basic concepts
5.3. Techniques for distributing confidential keys
5.4. Techniques for distributing public keys
5.5. Key agreement
    5.5.1. Key agreement based on symmetric techniques
    5.5.2. Key agreement based on asymmetric techniques
5.6. Real applications of key management and distribution.

5. Học liệu (Textbooks)

5.1. Học liệu bắt buộc (Required Textbooks)

[1] William Stallings. Cryptography and Network Security. Prentice Hall. 6th Edition. 2013.

5.2. Học liệu tham khảo (Optional Textbooks)

[2] Đỗ Xuân Chợ. Bài giảng Mật mã học cơ sở, Học viện Công nghệ Bưu chính viễn thông. 2016.

[3] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. 1996.

[4] Behrouz A. Forouzan. Introduction to cryptography and network security. McGraw-Hill Higher Education. 2008.

[5] Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography. Chapman & Hall/ CRC. 2007.

6. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập học phần (Grading Policy)

Grading method	Percentage	Group/Individual
- Attendance	10%	Individual
- Mid-term exams	10%	Individual
- Projects	20%	Group or individual
- Final examination	60%	Individual

Trưởng Bộ môn **(Head of Department)**	**Giảng viên biên soạn** **(Lecturer)**
Hoàng Xuân Dậu	**Đỗ Xuân Chợ**