IT4010E NHẬP MÔN AN TOÀN THÔNG TIN

INTRODUCTION TO CRYPTOGRAPHY AND SECURITY

Version: 2019.05.13

1. THÔNG TIN CHUNG
GENERAL INFORMATION

Tên học phần	Nhập môn An toàn Thông tin
Course name:	Introduction to Cryptography and Security
Mã học phần	IT4010E
Code:	
Khối lượng	3(3-1-0-6)
Credit:	- Lý thuyết - Lecture: 45 hours - Bài tập - Exercise: 15 hours (If capstone project is used, please indicate clearly) - Thí nghiệm - Experiments: 0 hours
Học phần tiên quyết	No
Prerequisite:	
Học phần học trước	- IT3020E: Toán rời rạc
Prior course:	- IT3020E: Discrete Mathematics
Học phần song hành	No
Paralell course:	

2. MÔ TẢ HỌC PHẦN - COURSE DESCRIPTION

Học phần nhằm cung cấp cho sinh viên các kiến thức cơ sở về an toàn thông tin dưới góc độ nhà kỹ thuật và phát triển hệ thống. Sau môn học, sinh viên sẽ nắm được bức tranh toàn cảnh về an toàn thông tin nhìn từ hai chiều: từ thực tiễn và từ cơ sở lý thuyết; hiểu các thành phần và giao thức mật mã, bài toán xác thực, bài toán quản lý điều khiển truy nhập, kỹ thuật tấn công mạng; và có thể sử dụng các công cụ mật mã một cách đúng đắn để bảo vệ an toàn các hệ thống máy tính.

The course provides students with the basic concepts of information security; principles and basic construction techniques of cryptosystems; cryptographic applications. Students will learn the process of developing information security systems, be able to design and apply common cryptographic protocols to create security solutions for information systems.

3. MỤC TIÊU VÀ CHUẨN ĐẦU RA CỦA HỌC PHẦN

GOAL AND OUTPUT REQUIREMENT

Sinh viên hoàn thành học phần này có khả năng

After this course the student will obtain the followings:

Mục tiêu/CĐR Goal	Mô tả mục tiêu/Chuẩn đầu ra của học phần Description of the goal or output requirement	CĐR được phân bổ cho HP/ Mức độ (I/T/U) Output division/ Level (I/T/U)
[1]	[2]	[3]
M1	**Nắm vững ý nghĩa, tầm quan trọng và mục đích cụ thể của an toàn bảo mật thông tin trong đời sống** **Understand the meaning, importance and specific purpose of information security in real life.**	1.2.4 (TU), 1.3.1 (I)
M2	**Hiểu biết các bước cơ bản trong xây dựng giải pháp ATBM trong thực tế** **Understand the required processes in creating information security solutions in real life, from requirement analysis, policy development to find specific technical solutions**	1.2.4(TU) 1.3.1 (I) [2.1.1,2.1.2](T) [2.1.3,2.1.4](I) [2.5.3, 2.5.4](I)
M3	**Nắm vững các nền tảng kỹ thuật cơ bản trong ATTT như mật mã, xác thực, điều khiển truy nhập** **Understand the basic technical backgrounds in information security such as encryption, authentication, access control**	1.1.2 (IU); 1.1.4(U); 1.2.1(IU); 1.2.4(TU) 3.3.3 (U) [1.3.1, 1.4.1](I) [2.1.1, 2.1.2](T) [2.1.3, 2.1.4](I), 3.3.3 (U)

4. TÀI LIỆU HỌC TẬP

Reference

Textbook

[1] Nguyễn Khanh Văn (2015). *Giáo trình Cơ sở An toàn Thông tin*. NXB. Bách Khoa – Hà Nội.

[2] Christof Paar and Jan Pelzl (2009). *Understanding Cryptography: A Textbook for Students and Practitioners* (1st ed.). Springer Publishing Company, Incorporated. Website: http://www.crypto-textbook.com/

Reference book

[1] Matt Bishop (2004). *Introduction to Computer Security*. Addison-Wesley.

[2] Charles P. Pfleeger et al. (2015). *Security in Computing* (5th Ed.) Pearson Education.

[3] William Stallings (2017). *Cryptography And Network Security: Principles and Practices* (7th Ed.) Pearson Education.

[4] Bruce Schneier (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd Ed.) John Wiley & Sons, Inc., New York, USA.

5. CÁCH ĐÁNH GIÁ HỌC PHẦN - EVALUATION

Điểm thành phần Module	Phương pháp đánh giá cụ thể Evaluation method	Mô tả Detail	CĐR được đánh giá Output	Tỷ trọng Percent
[1]	[2]	[3]	[4]	[5]
A1. Điểm quá trình **Mid-term (*)**	**Đánh giá quá trình** **Progress**			**40%**
	A1.1. Thi giữa kỳ Midterm Exam	Tự luận Written	M1-M3	20%
	A1.2. Bài tập về nhà Homework	Tự luận Written	M1 – M3	20%
A2. Điểm cuối kỳ **Final term**	**A2.1. Thi cuối kỳ** **Final exam**	Thi viết Written exam	M1-M3	**60%**

** Điểm quá trình sẽ được điều chỉnh bằng cách cộng thêm điểm chuyên cần. Điểm chuyên cần có giá trị từ –2 đến +1, theo Quy chế Đào tạo đại học hệ chính quy của Trường ĐH Bách khoa Hà Nội.*

The evaluation about the progress can be adjusted with some bonus. The bonus should belong to [-2, +1], according to the policy of Hanoi University of Science and Technology.

6. KẾ HOẠCH GIẢNG DẠY - SCHEDULE

Tuần Week	Nội dung Content	CĐR học phần Output	Hoạt động dạy và học Teaching activities	Bài đánh giá Evaluated in
[1]	[2]	[3]	[4]	[5]
1	**Chương 1. Giới thiệu về An toàn Thông Tin** **Chapter 1: Introduction to Information Security** 1.1.What is information security? 1.2.Threats 1.3.Harm 1.4.Vulnerabilies 1.5.Controls	M1, M2	Note reading; Teaching;	A1 A2
2	**Chương 2. Giới thiệu về Mật mã** **Chapter 2. Introduction to Cryptography** 2.1. Overview of Cryptology 2.2. Symmetric Cryptography 2.3. Cryptanalysis	M2, M3	Note reading; Teaching;	A1 A2

Tuần Week	Nội dung Content	CĐR học phần Output	Hoạt động dạy và học Teaching activities	Bài đánh giá Evaluated in
[1]	[2]	[3]	[4]	[5]
	2.4. Modular Arithmetic and More Historical Ciphers **Chương 3. Mã dòng** **Chapter 3. Stream Ciphers** 3.1. Introduction (Stream cipher vs block cipher, Encryption and Decryption with Stream ciphers) 3.2. Random Numbers and an Unbreakable Stream Cipher			
3	**Chương 4. Chuẩn mã hóa nâng cao (AES)** **Chapter 4. The Advanced Encryption Standard (AES)** 4.1. Overview of the AES Algorithm 4.2. Some Mathematics: A Brief Introduction to Galois Fields 4.3. Internal Structure of AES 4.4. Decryption 4.5. Implementation in Software and Hardware	M2, M3	Note reading; Teaching;	A1 A2
4	**Chương 5. Sử dụng mã khối** **Chapter 5. More About Block Ciphers** 5.1.Encryption with Block Ciphers: Modes of Operation 5.2.Exhaustive Key Search Revisited 5.3.Increasing the Security of Block Ciphers	M3	Note reading; Teaching;	A1 A2
5	**Chương 6. Giới thiệu về Mật mã Khóa công khai** **Chapter 6. Introduction to Public-Key Cryptography** 6.1. Symmetric vs. Asymmetric Cryptography 6.2. Practical Aspects of Public-Key Cryptography 6.3. Essential Number Theory for Public-Key Algorithms	M1, M2, M3	Note reading; Teaching;	A1 A2
6	**Chương 7. Hệ mật RSA** **Chapter 7. The RSA Cryptosystem** 7.1. Encryption and Decryption	M2, M3	Note reading; Teaching;	A1 A2

Tuần Week	Nội dung Content	CĐR học phần Output	Hoạt động dạy và học Teaching activities	Bài đánh giá Evaluated in
[1]	[2]	[3]	[4]	[5]
	7.2. Key Generation and Proof of Correctness 7.3. Encryption and Decryption: Fast Exponentiation 7.4. Finding Large Primes 7.5. RSA in Practice: Padding 7.6. Attacks			
7	**Chương 8. Hệ mật khóa công khai dựa trên bài toán Logrit rời rạc** **Chapter 8. Public-Key Cryptosystems Based on the Discrete Logarithm Problem** 8.1. Diffie–Hellman Key Exchange 8.2. Some Algebra 8.3. The Discrete Logarithm Problem 8.4. Security of the Diffie–Hellman Key Exchange 8.5. The Elgamal Encryption Scheme	M2, M3	Note reading; Teaching;	A1 A2
8	**Chương 9. Chữ ký số** **Chapter 9. Digital Signatures** 9.1. Introduction 9.2. The RSA Signature Scheme 9.3. The Elgamal Digital Signature Scheme 9.4. The Digital Signature Algorithm (DSA)	M2, M3	Note reading; Teaching;	A1 A2
9	**Chương 10. Hàm băm** **Chapter 10. Hash Functions** 10.1. Motivation: Signing Long Messages 10.2. Security Requirements of Hash Functions 10.3. Overview of Hash Algorithms 10.4. The Secure Hash Algorithm SHA2 10.5. Case study: Ecash and Bitcoin	M2, M3	Note reading; Teaching;	A1 A2
10	**Chương 11. Mã xác thực thông điệp** **Chapter 11. Message Authentication Codes (MACs)** 11.1.Principles of Message Authentication Codes	M2, M3		A1 A2

Tuần Week	Nội dung Content	CĐR học phần Output	Hoạt động dạy và học Teaching activities	Bài đánh giá Evaluated in
[1]	[2]	[3]	[4]	[5]
	11.2.MACs from Hash Functions: HMAC 11.3.MACs from Block Ciphers: CBC-MAC 11.4.Galois Counter Message Authentication Code (GMAC)			
11	**Chương 12. Thiết lập khóa** **Chapter 12. Key Establishment** 12.1.Key Establishment Using Symmetric-Key Techniques 12.2.Key Establishment Using Asymmetric Techniques 12.3.Public-Key Infrastructures (PKI) and CAs	M1, M2, M3	Note reading; Teaching;	A1 A2
12	**Chương 13. Xác thực** **Chapter 13. Authentication** 13.1.Authentication basics 13.2. Password authentication: overview, common attacks, password security technique, challenge-response and one-time password, password management in Unix 13.3. Other authentication methods (biometric, token, location-based)	M1, M2, M3		A1 A2
13	**Chương 14. Điều khiển truy nhập** **Chapter 14. Access control** 14.1. Basic principles and access control matrix 14.2. Discretionay Access Control) 14.3. Mandatory Access Control 14.4. Role-based Access Control 14.5.Case Study: access control in Unix	M1, M2, M3	Note reading; Teaching;	A1 A2
14	**Chương 15. Sơ lược về an toàn mạng máy tính** **Chapter 15. Computer network security** 15.1 Network protocols and common threats 15.2. Common attacks (DoS attack in TCP)	M1, M2, M3	Note reading; Teaching;	A1 A2

Tuần Week	Nội dung Content	CĐR học phần Output	Hoạt động dạy và học Teaching activities	Bài đánh giá Evaluated in
[1]	[2]	[3]	[4]	[5]
	15.3. Common solutions, security protocols: IP-SEC, SSL/TSL			
15	***Ôn tập*** ***Summary***			

15. QUY ĐỊNH CỦA HỌC PHẦN - COURSE REQUIREMENT

(The specific requirements if any)

16. NGÀY PHÊ DUYỆT - DATE: …….

Chủ tịch hội đồng **Committee chair**	**Nhóm xây dựng đề cương** **Course preparation group**

17. QUÁ TRÌNH CẬP NHẬT - UPDATE INFORMATION

STT No	Nội dung điều chỉnh Content of the update	Ngày tháng được phê duyệt Date accepted	Áp dụng từ kỳ/ khóa Applicable from	Ghi chú Note
1	……			
2	……			