IT4015 NHẬP MÔN AN TOÀN THÔNG TIN

Introduction to Information Security

Phiên bản: 2021.3.9

1. THÔNG TIN CHUNG

Tên học phần:	Nhập môn an toàn thông tin
Course name	*Introduction to Information Security*
Mã số học phần:	IT4015
Code:	IT4015E
Khối lượng:	3(3-1-0-6)
Credit	- Lý thuyết - Lecture: 45 hours - Bài tập – Exercise: 15 hours - Thí nghiệm - Experiments: 0 hours
Học phần tiên quyết: **Prerequisite**	NA
Học phần học trước:	- IT3020: Toán rời rạc - Discrete Math - IT3070: Hệ điều hành - Operating Systems
Học phần song hành:	- IT3080: Mạng máy tính – Computer Networks

2. MÔ TẢ HỌC PHẦN

Trang bị cho sinh viên các kiến thức cơ sở về an toàn thông tin dưới góc độ nhà kỹ thuật và phát triển hệ thống tin học. Sinh viên nắm được bức tranh toàn cảnh về an toàn thông tin nhìn từ 2 chiều: từ cơ sở lý thuyết và từ thực tiễn. Các kiến thức kỹ thuật cần thiết về cơ sở: cơ sở lý thuyết mật mã, bài toán xác thực, bài toán quản lý điều khiển truy nhập, tấn công mạng.

Tổng quan: các khái niệm cơ bản xung quanh tài sản thông tin, các mối đe dọa & tấn công; các mục tiêu cơ bản của ATTT. Mối quan hệ giữa cơ sở lý thuyết và các giải pháp thực tiễn. Cơ sở lý thuyết mật mã và các công cụ bảo mật cơ bản. Bài toán xác thực và các giải pháp phổ biến. Bài toán quản lý điều khiển truy nhập và các cơ chế tiếp cận phổ biến. Tổng quan về an toàn mạng và các tấn công mạng phổ biến. Học phần này tạo nền tảng cơ sở vững chắc cho các môn học nâng cao tiếp theo về ATTT cũng như hỗ trợ cơ sở cho quá trình tự học, tự đào tạo sau này (nếu sinh viên không lấy thêm các học phân nâng cao về ATTT).

Equip students with the basic knowledge of information security from the technical perspective of information system developers. Students grasp the overall picture of information security from two dimensions: from theoretical basis and from practice. Necessary technical knowledge about the basis: elementary cryptology, authentication problems, access control problems, network attacks.

Overview: the basic concepts surrounding information assets, threats & attacks; the general goals of the security system; reflecting on relationship between theoretical basis and practical solutions. Fundamentals of cryptography and basic security tools. Authentication problem and popular solutions. Access control problems and common access mechanisms. Overview of network security and common network attacks. This module provides a solid foundation for the next advanced courses on information security (IS) as well as supports the basis for self-study and self-training later (if students do not take more advanced courses on IS)

3. MỤC TIÊU VÀ CHUẨN ĐẦU RA CỦA HỌC PHẦN

Sinh viên hoàn thành học phần này có khả năng:

After this course the student will obtain the followings:

Mục tiêu/CĐR	Mô tả mục tiêu/Chuẩn đầu ra của học phần	CĐR được phân bổ cho HP/ Mức độ (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 Grasp the meaning, importance and specific purpose of information security in life	1.2.4, 1.3.1
M1.1	Nắm vững các mục tiêu cơ bản của ATTT Master the basic goals of information security	1.2.4(TU) 1.3.1 (I)
M1.2	Nhận diện, so sánh và phân loại được các dạng yêu cầu ATTT cụ thể trong đời sống Identify, compare and classify specific types of information security requirements in 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 basic steps in building information security solutions in practice	1.2.4,1.3.1, 2.1.1-4, 2.5.3-4
M2.1	Hiểu biết cơ bản về phân tích yêu cầu ATTT trong một môi trường thực tế cụ thể sinh động: hiểu biết về phân tích yêu cầu (phân tích đe dọa) từ đó xây dựng chính sách phù hợp. Basic understanding of IS requirements analysis in specific, vivid scenarios in real world: understanding requirements analysis (threat analysis) from which to develop appropriate policies.	1.2.4(TU) 1.3.1 (I) [2.1.1,2.1.2](T) [2.1.3,2.1.4](I)
M2.2	Hiểu biết qui trình từ xây dựng chính sách đến tìm giải pháp kỹ thuật cụ thể Understand the process from policy formulation to finding 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) 2.5.3-4 (I)
M3	Nắm vững các nền tảng kỹ thuật cơ bản trong ATBM như mật mã, xác thực, điều khiển truy nhập Mastering the basic technical foundations in security such as encryption, authentication, and access control	1.1.2,1.1.4,1.2.1,1.2.2 1.2.4,1.3.1, 2.1.1-4, 2.4.2-4, 3.3.3
M3.1	Nắm vững các công cụ mật mã cơ sở, có khả năng vận dụng tương đối linh hoạt trong thực tế Mastering the basic cryptographic tools, capable of	1.1.2 (IU);1.1.4(U); 1.2.1(IU);1.2.4(TU) 3.3.3 (U)

	applying relatively flexibly in practice	
M3.2	Nắm vững các giải pháp và mô hình cơ sở của bài toán xác thực và bài toán điều khiển truy nhập. Có khả năng phân tích và tìm ra điểu yếu đối với một giải pháp thực tiễn liên quan. Master the solutions and basic models of the authentication problem and the access control problem. Ability to analyze and find the essentials of a relevant practical solution	1.2.2(IU), 1.2.4(TU), 1.3.1(I) [2.1.1,2.1.2](T) [2.1.3,2.1.4](I), 3.3.3 (U)

4. TÀI LIỆU HỌC TẬP

Giáo trình

Textbook (Vietnamese)

[1] TS. Nguyễn Khanh Văn (2015). *Giáo trình Cơ Sở An Toàn Thông Tin*. Nhà xuất bản Bách Khoa Hà nội.

Sách tham khảo

Reference books

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

[2] Charles P.Pfleeger (2006). *Security in Computing*. Prentice Hall.

[3] William Stallings (2005). Cryptography And Network Security: Principles and Practices. Prentice Hall.

[4] Bruce Schneier (1996). Applied Cryptography. Wiley.

[5]

5. CÁCH ĐÁNH GIÁ HỌC PHẦN

Điểm thành phần	Phương pháp đánh giá cụ thể	Mô tả	CĐR được đánh giá	Tỷ trọng
[1]	[2]	[3]	[4]	[5]
A1. Điểm quá trình (*) Midterm	**Đánh giá quá trình Progress eval**			**40%**
	A1.1. Thi giữa kỳ Midterm exam	Tự luận Written	M1.1; M2; M3.1;	30%
	A1.2. Kiểm tra ngắn Several Quizs	Tự luận Written	M3.2;	10%
A2. Điểm cuối kỳ	**A2.1. Thi cuối kỳ Final Exam**	Thi viết Written exam	M1; M2; 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

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
1	A.Mục đích môn học Phương pháp tiếp cận môn học - Nêu các phương pháp phổ biến - Giới thiệu tiếp cận sử dụng, yêu cầu cụ thể với SV Chương Mở đầu (CMĐ): B.Định nghĩa và minh họa về khái niệm chung "An toàn thông tin": - Tầm quan trọng - Toàn cảnh lĩnh vực: khái quát về xây dựng giải pháp an toàn thông tin C.Khái quát về nền tảng kiến thức kỹ thuật cần có của một KS ATTT - Các khái niệm cơ bản xung quanh tài sản thông tin và các mối đe dọa, tấn công; các mục tiêu cơ bản của ATTT. Sơ lược về đạo đức trong ATTT. - Ba mục tiêu cơ bản (Confidentiality-Intergrity-Availability) - Các khái niệm cơ bản; từ khóa: đe dọa, điểm yếu (lỗ hổng), tấn công, chính sách, kiểm soát, cơ chế, các vấn đề nhân sự A.Purpose of the course Course approach - Outline the common methods - Introduce the approach used in course requirements to students Opening Chapter (CMD): B. Definition and illustration of the general concept "Information security": - Importance	M1	Giới thiệu tài liệu, sách giáo trình và trang Web môn học Tài liệu: Chương Mở đầu – GT [1]-Ch. 1 [2]- Ch. 1 Giảng bài; Ví dụ & bài tập liên hệ thực tế : GV tự đưa ra các ví dụ thực tế có phân tích tình huống minh họa. Phân tích tình huống minh họa (đe dọa vs. "lỗ hổng", chính sách vs. cơ chế, biện pháp kiểm soát, các ví dụ tấn công phổ biến …) Introducing course materials, textbooks and course Website Ref. Textbook – Opening chap. Teaching; Examples & exercises related to the practice Teachers give their own real-world examples with case analysis with illustration (threats vs. vulnerab., policies vs. mechanisms, control measures, common attack examples ...)	A1.1

	- Field overview: an overview of information security solution development C.An overview of the required technical knowledge base of an security engineer - The basic concepts surrounding information assets and threats and attacks; the basic goals of the security system. Outline of ethics in IS. - Three basic goals (Confidentiality-Intergrity-Availability) - Basic key concepts: threat, vulnerabilities, attacks, policies, assurance, mechanisms, human issues			
2	CMĐ - tiếp về tổng quan ATTT - Giới thiệu các công cụ nền tảng (cryptography, access control, authentication, ...) - Giới thiệu các nội dung kỹ thuật chính sẽ trình bày:lý thuyết mật mã và ứng dụng, các công cụ nền tảng khác Chương 1: Giới thiệu về Lý thuyết Mật mã - Các khái niệm cơ bản trong LTMM - Mô hình truyền tin bảo mật và các dạng tấn công cơ bản Continuing on IS - the general picture - Introduce fundamental tools (cryptography, access control, authentication, ...) - Introduction to the main technical contents that will be discussed in course: cryptographic theory and applications, other background tools Chapter 1: Introduction to Cryptography Theory - Basic concepts - Fundamental model for secure communication and basic attacks	M1 M2	Tài liệu: Chương Mở đầu & Chương 1 [1]-Ch. 1 [2]- Ch. 1 Giảng bài Lấy ví dụ. Câu hỏi và bài tập. Using opening Chap & first chap. Teaching. Giving examples Giving in-class exercise & quiz	A1.1 A2.1
3	Chương 1: Mật mã cổ điển và các nguyên lý cở sở của mật mã - Các hệ mã cộng tính, một-bảng thế, đa-bảng-thế	M1.1; M3.1;	Đọc trước tài liệu: GT-Ch1 [1]-8.2 [3]-Ch. 2	A1.1 A1.2

	- Phương pháp phân tích phá mã dựa tần xuất - Mật mã Vigenere và ý tưởng phá mã thông qua biết độ dài từ khóa Chapter 1: Classical cryptography and its fundamentals - Additive, mono-alphabetic substitution, - poly-alphabetic substitution ciphers - Frequency-based cryptanalysis of mono-alphabetic cipher - Vigenere cipher and the idea of breaking code through knowing the keyword length		Giảng bài; Bài tập minh họa: - phân tích phá mã theo tần xuất - Vigenere và độ dài từ khóa Teaching Illustrative exercises: code-breaking analysis according to frequency - Vigenere & keyword length	
4	Ch1: Mật mã cổ điển (tiếp) - Mật mã Vigenère: Khái niệm độ đo trùng khớp (IC) và cách tìm độ dài từ khóa dựa vào IC - Hệ mã One-time-pad - Giới thiệu khái quát: khái niệm bí mật tuyệt đối (định nghĩa Shannon), khoảng cách duy nhất, độ dư thừa Chap1 - Classic cipher (continued) - Vigenère cipher: The concept of the measure of the match (IC) and how to find the keyword length based on IC - One-time-pad Cipher - General introduction: perfect secret (Shannon definition), unique distance, redundance rate	M1.1; M3.1;	Đọc trước tài liệu: GT-Ch1, [1]-8.2,[3]-Ch. 2; Giảng bài; Bài tập minh họa: - So sánh Vigenere và One-time-pad - VD về Unicity distance Reading: TB-Ch1, [1] - 8.2, [3] -Ch. 2; Teaching; Illustrative exercise: - Compare Vigenere & One-time-pad - Example of Unicity distance	A1.1 A2.1
5	Chương 2: Mật mã khối và chế độ sử dụng - Khái niệm & nguyên lý xây dựng hệ mật mã khối - Sơ đồ cấu trúc vòng lặp Feistel - Nguyên lý, sơ đồ chi tiết của hệ mã DES và phân tích - S-box và tranh luận xung quanh - Tấn công vét cạn; phê bình DES; Chapter 2: Block ciphers and usage modes - Conceptual principles of building block ciphers - Feistel loop structure diagram	M1.1; M3.1;	Đọc trước tài liệu: GT-Ch2 [3]-Ch. 3 [2]-2.6; Giảng bài; Bài tập minh họa (phân tích thêm về thiết kế của DES và các vấn đề gây tranh cãi lúc ra đời) Reading: TB-Ch2 [3]-Ch. 3 [2]-2.6;	A1.1 A1.2 A2.1

	- Principles, detailed diagram of the DES cipher and analysis - S-box and critic arguments (history) -DES analysis: Exhautive Key Search attack & others		Teaching; Illustrative exercise: further analysis of the design of DES and controversial issues at birth	
6	Chương 2 - tiếp - Sơ đồ 2-DES, 3-DES - Giới thiệu hệ mã AES Các chế độ mật mã thông dụng và phân tích: ECB, CBC, CFB, OFB, CTR; phân tích & so sánh để thấy khác biệt & ưu nhược điểm Chapter 2 - continued - Diagrams of 2-DES, 3-DES - Brief review of AES cipher Common cryptographic modes: ECB, CBC, CFB, OFB, CTR; analyze & compare: the differences, advantages and disadvantages & suitable application scenarios.	M1.1; M3.1;	Đọc trước tài liệu:-nt; Giảng bài; Bài tập trên lớp về 2-DES - có gợi ý Phân tích & so sánh 5 chế độ để thấy rõ sự khác biệt, ưu nhược điểm & các tình huống ứng dụng phù hợp. Teaching; Guided solving a problem on 2-DES	A1.1 A1.2 A2.1
7	Chương 3: Mật mã khóa công khai - Nguyên lý xây dựng (ý tưởng Diffie-Hellman) và ứng dụng - Hệ mã dựa Knapsack (bài toán cái túi) - Thuật toán GCD mở rộng - Hệ mã RSA: ý tưởng thiết kế Chapter 3: Public key cryptography - Principle of construction (Diffie-Hellman idea) and application - Knapsack-based construction (bag problem) - Extended GCD algorithm - RSA cipher: conceptual design	M1.1; M3.1;	Đọc trước tài liệu GT-Ch3 Giảng bài Bài tập ví dụ & và câu hỏi mở rộng Reading TB- Chap 3 Teaching Examples, exercise & open questions	A1.1, A2.1
8	Chương 3 - tiếp - Hệ mã RSA: mô tả đầy đủ và phân tích - Các chủ đề xung quanh RSA: số nguyên tố lớn, bài toán phân tích TSNT, tính hàm mũ nhanh ...	M1.1; M3.1;	Đọc trước tài liệu: GT-Ch3&4; Giảng bài; Bài tập minh họa: k/n CKĐT yếu; bài tập về nguyên lý Thỏ-chuồng;	A1.1 A2.1

	Chương 4: Chữ kỹ điện tử và hàm băm - Sơ đồ chữ ký đơn giản và điểm yếu - Hàm băm và ứng dụng - Nguyên lý Dirichle (thỏ-chuồng); vấn đề đụng độ băm; và nghịch lý ngày sinh nhật Kiểm tra giữa kỳ Chapter 3 - continued - RSA cipher: fully described and analyzed - Related Issues on RSA: generation of large primes, factorization problem, fast exponential algo ... Chapter 4: Digital signature and hash functions - Simple digital signature (DS) scheme and weaknesses - Hash functions and application in secure DS - Dirichlet principle (rabbit-barn); hash collision problem; and the birthday paradox Mid-term Test		khảo sát nghịch lý Ngày Sinh Nhật (NSN) Minh họa về việc giả mạo chữ ký nhờ tấn công NSN Reading TB- Chap 3&4 Teaching: Illustrative Examples; Disscuss weak DS scheme; Exercises on Dirichlet principle, Birthday attack; Illustration of forging signature thanks to birthday attack	
9	Chương 5: Phân phối và quản lý khóa - Khái niệm khóa phiên - Khái niệm giao thức an toàn (mật mã) và ký pháp - Thiết lập khóa phiên: Giao thức Needham-Schoeder và các mở rộng Hệ Kerberos: Khái niệm và ứng dụng. Mở rộng (nếu thời gian cho phép): Ứng dụng của hệ Kerberos trong việc thiết kế các hệ thống đa máy chủ như các MXH (Google, Facebook ...), cho phép đăng nhập chỉ 1 lần nhưng có thể kết nối nhiều lần đến nhiều máy chủ dịch vụ phía trong bằng các kênh bảo mật riêng (khóa phiên riêng). Chapter 5: Key distribution & management - Session key concept - Security (cryptographic) protocol: basic concepts and common notation - Key agreement protocols: Needham-Schoeder and extensions	M1.2 M1.1; M3.1;	Đọc trước tài liệu: GT-Ch5, [1]-9.1-4, [3]-Ch.10; Giảng bài; Bài tập minh họa: Needham-Schroeder (NS); Ý nghĩa R1,R2 … Bài tập: Áp dụng cơ chế xác thực của NS trong đăng nhập mật khẩu. Bài tập: Áp dụng của NS trong thiết kế Kerberos Reading TB- Ch5, [1]-9.1-4, [3]-Ch.10; Teaching: Illustrative Exercises on Needham-Schroeder protocol: understanding randoms R1, R2; Application of NS protocol in password-based authentication and	A1.1 A2.1

	Kerberos System: Concepts and Applications. Extensions (if time allows): Application of Kerberos system in designing multi-service systems (Google, Facebook as typical), allowing Single Sign-on but Multiple Serives (with private, secret session key).		in Kerberos design	
10	Chương 5 -tiếp Quản lý khóa công khai: - Trao chuyển khóa sử dụng Hệ khóa công khai - Tấn công Kẻ ngồi giữa và vấn đề xác thực khóa - Hạ tầng chứng chỉ khóa Chương 6: Xác thực danh tính - Nguyên lý xác thực - Xác thực dùng mật khẩu: mô hình khái quát, các tấn công phổ biến, kỹ thuật an toàn mật khẩu Chapter 5 - next Public key management: - Key transfer using PK encryption - The man-in-the-middle attack and the issue of key authentication - Key certificate infrastructure Chapter 6: Identity authentication - The principles of authentication - Password authentication: basic concepts, dictionary attacks, password security techniques	M1.1; M2.2; M3.1; M3.2	Đọc trước: GT-Ch5&6 Giảng bài; Bài tập minh họa: mô hình CA phân cấp & cấp phát chứng chỉ chéo Reading TB- Ch5&6 Teaching: Illustrative Exercises: Multiple CA models & Cross Certifying; Certificate Authority Hierarchy	A1.2 A2.1
11	Chương 6 – tiếp - Cơ chế thách thức-đáp ứng và mật khẩu dùng một lần; quản lý mật khẩu trong hệ điều hành Unix - Hệ Kerberos (tiếp): sơ đồ chi tiết và ứng dụng về xác thực đa máy chủ - Xác thực thông qua các phương pháp khác (sinh trắc học, token, dựa vị trí …) Chapter 6 - continued - Challenge-response techniques; one-time	M1.1; M2.1 -2; M3.1; M3.2	Đọc trước: GT-Ch6 [1]-Ch.11 Giảng bài BT về tấn công mật khẩu: khảo sát terminal attack; Liên hệ Needham-Schroeder; Keberos và xác thực trong hệ đa máy chủ (vd: mạng XH) Reading TB- Ch6, [1]-	A1.2 A2.1

	passwords; password management in Unix - Kerberos system (cont.): Detailed diagram and application of multi-server authentication - Other authentication methods (biometric, token, location based ...)		Ch.11 Teaching: Exercises on password attacks, challenge-response scheme & comparison to Using Needham-Schroeder	
12	Chương 7: Điều khiển truy nhập - Nguyên lý cơ bản và ma trân điều khiển truy nhập - Mô hình DAC (Discretionay Access Control) - Mô hình MAC (Mandatory Access Control) Chapter 7: Access Control - Basic principles and access control matrix - Discretionary Access Control method - Mandatory Access Control method	M1.1; M2.1 -2; M3.2	Đọc trước TL: GT-Ch6 [1]-Ch.2,14; Giảng bài; Bài tập tình huống: BT-CH cuối chương (GT) Reading TB- Ch6, [1]-Ch.2,14; Teaching In-class exercises, related to practical scenarios	A1.2 A2.1
13	Chương 7 – tiếp - Mô hình RBAC (Role-based Access Control) - Case Study (đọc thêm): Điều khiển truy nhập trong hệ điều hành Unix Tổng quan an toàn mạng máy tính - Các giao thức mạng và mối đe dọa phổ biến Chapter 7 - continued - Role-based Access Control method - Case Study: Access control in Unix Overview of computer network safety Common network protocols and threats	M1.1; M2.1 -2; M3.2	Đọc trước: GT-Ch7, [2]-Ch.7 [3]-Ch.16,17 Giảng bài; Bài tập liên hệ thực tế; Reading TB- Ch7, [2]-Ch.7 [3]-Ch.16,17 Teaching In-class exercises, related to practical scenarios	A1.2 A2.1
14	Tổng quan an toàn mạng máy tính - Nhìn lại mô hình mạng OSI và liên hệ tổng quan đến các vấn đề an toàn của các tầng giao thức - Các tấn công phổ biến - Tấn công DoS: tấn công SYN flood đối với giao thức TCP	M1.1; M3.2	Đọc trước: GT- Ch8; Bài tập phân tích tình huống Reading TB- Ch8	A2.1

	Overview of computer network safety - Review the OSI network model and relate it to the security issues of the protocol layers in general - Common attacks DoS attack: SYN flood attack against TCP protocol		Teaching In-class exercises: with practical scenarios	
15	*Tổng kết môn học -- Review of Course major contents*			

7. QUY ĐỊNH CỦA HỌC PHẦN

(Các quy định của học phần nếu có)

8. NGÀY PHÊ DUYỆT: ……..

Chủ tịch Hội đồng **Nhóm xây dựng đề cương**

9. QUÁ TRÌNH CẬP NHẬT

Lần cập nhật	Nội dung điều chỉnh	Ngày tháng được phê duyệt	Áp dụng từ kỳ/khóa	Ghi chú
1	Bổ sung CĐR và hoàn thiện đề cương chi tiết theo yêu cầu của Viện (TS. Phạm Đăng Hải)	19.5.2019		
2	Hoàn thiện bản Song-Ngữ (Bổ sung phần tiếng Anh, ghép nối - chỉnh sửa)	9.3.2021		