VNUHCM-UNIVERSITY OF SCIENCE
FACULTY OF INFORMATION TECHNOLOGY

COURSE SYLLABUS

CSC15003 - Mã hóa ứng dụng

1. GENERAL INFORMATION

Course name:	Applied Cryptography
Course name (in Vietnamese):	Mã hóa ứng dụng
Course ID:	CSC15003
Knowledge block:	
Number of credits:	4
Credit hours for theory:	45
Credit hours for practice:	30
Credit hours for self-study:	90
Prerequisite:	
Prior-course:	
Instructors:	Truong Toan Thinh, Tran Minh Triet

2. COURSE DESCRIPTION

The course is designed to provide students a broad introduction to cryptography and communication security mechanisms based on cryptography. The course covers fundamental aspects such as security evaluation criteria and the mathematical constructs underlying cryptographic primitives as well as applied aspects like the design of major encryption and hashing algorithms, details of security mechanisms relying on cryptography such as data encryption, integrity, digital signature, authentication, key management, and public-key infrastructures.

3. COURSE GOALS

At the end of the course, students are able to

ID	Description	Program LOs
G1	Work on a personal and team level to learn the basic concepts of applied cryptography	LO9
G2	Know and explain English terminology in the field of Cryptography	LO10
G3	Understand the basic concepts, terms, responsibility and fundamental principles in the field of Cryptography	LO1, LO11, LO12
G4	Identify and categorize Cryptography algorithms for real world application.	LO1, LO2, LO5
G5	Understand and apply techniques in the field of applying Cryptography.	LO2, LO4, LO5, LO6
G6	Understand the methods to attack Cryptography algorithms.	LO3, LO5, LO7

4. COURSE OUTCOMES

CO	Description	I/T/U
G1.1	Establishment, organization, operation, and management of the computer security team	I
G1.2	Participate in discussions and group discussions on course topics	U
G1.3	Analyze, synthesize, and write technical documentation according to a given model individually or in a team collaboration	I, T
G2.1	Know and understand English terminology of the subject	I
G2.2	Reading comprehension of English documents related to lectures	I

G3.1	Explain the basic concepts in Information Security: security requirements, services and mechanisms, security layers, etc.	I, T
G3.2	Know the role, responsibility and professional ethics when working in the field of Cryptography	I
G3.3	Know how to update new knowledge, self-study, self-development, and adaptation	I
G3.4	Know how to start a career	I
G4.1	Distinguish between cryptographic algorithms such as: Symmetric and Asymmetric Cryptography, Hashing, Digital Signature, etc.	I, T, U
G4.2	Know how to apply Cryptography in every specific real-world problem.	I, T, U
G5.1	Identify security services required by a computing system	I, T
G5.2	Design a secure communication system using cryptographic mechanisms	I, T, U
G5.3	Analyze the security of an existing communication system	I, T, U
G5.4	Know how to implement the cryptographic algorithms	I, T, U
G6.1	Understand the security problems in some cryptographic algorithms, how to attack them and the basic countermeasures.	I, T, U
G6.2	Identify the mistakes when implementing of cryptographic algorithms and how to fix them	I, T, U

5. TEACHING PLAN

ID	Topic	Course outcomes	Teaching/Learning Activities (samples)
1	Introduction to Security Requirements, Services and Mechanisms of Security. Introduction to Cryptography: • Classical Cipher • Classification • Security Evaluation • Perfect Secrecy.	G1.1, G1.2, G1.3, G2.1, G2.2, G3.1, G3.2, G3.3	Lecturing Q&A, Group discussion
2	Symmetric Cryptography: • Block Ciphers • Feistel Cipher • DES • Number Theory Refresher • IDEA, AES • Cascade of ciphers • Stream Ciphers, RC4	G4.1, G4.2, G5.1, G5.2	Lecturing Q&A QZ1: Quiz 1
3	Asymmetric Cryptography: • Number theory • One-way functions • Diffie-Hellman • RSA • El Gamal • Elliptic Curve Cryptography	G4.1, G4.2, G5.1, G5.2	Lecturing Q&A QZ2: Quiz 2 In-class exercise.

4	Data Encryption Mechanism: • Statistical Attacks • Chaining Modes (CBC, CFB, OFB, CTR, XTS)	G5.1, G5.2, G5.3	Lecturing Case study and discussion Q&A QZ3: Quiz 3
5	Hash Functions and Integrity • Hash Functions • MAC, MDC • Security Properties • Alternatives for MAC	G4.1, G4.2, G5.1, G5.2	Lecturing Q&A QZ4: Quiz 4
6	Digital Signatures and Non-Repudiation • El Gamal Signature Algorithm • Digital Signature Standard • Non-repudiation of receipt	G4.1, G4.2, G5.1, G5.2	Lecturing Q&A, QZ5: Quiz 5 In-class exercise.
7	Authentication • Classification • Authentication Protocols • Passwords • Smartcards	G4.2, G5.1, G5.2, G5.3	Lecturing Q&A, QZ6: Quiz 6 In-class exercise.
8	Key Management • Key Generation • Symmetric Key Distribution ◦ Kerberos ◦ Public-key Certification and PKI systems • Law Enforcement	G4.2, G5.1, G5.2, G5.3	Lecturing Q&A, QZ7: Quiz 7 In-class exercise.

9	Optional topics: • Security for Database. • Authorization/Access Control	G4.2, G5.1, G5.2, G5.3	Lecturing Q&A, QZ8: Quiz 8 In-class exercise.
10	Advanced topics: • Searchable Encryption. • Blockchain. • Quantum Cryptography • Securing Microservice with mTLS, JWT and gRPC. • Applied Cryptography. • …	G4.2, G5.1, G5.2, G5.3	Lecturing QZ9: Quiz 9 Q&A, In-class exercise.
11	Review	G5.1, G5.2, G5.3, G3.4	Discussion

For the practical laboratory work, there are 10 weeks which cover similar topics as it goes in the theory class. Each week, teaching assistants will explain and demonstrate key ideas on the corresponding topic and ask students to do their lab exercises either on computer in the lab or at home. All the lab work submitted will be graded. There would be a final exam for lab work.

6. ASSESSMENTS

ID	Topic	Description	Course outcomes	Ratio (%)
A1	**Assignments**			**30%**
A11	Quizzes: QZ1, QZ2, QZ3, QZ4, QZ5, QZ6, QZ7, QZ8 and QZ9	Small quizzes in class for each topic	G1.1, G1.2, G1.3, G2.1, G2.2, G3.1, G3.2, G3.3	15%

A13	Weekly CTF Challenges	Solve the security challenges on the CTF Wargame CryptoHack	G5.4, G6.1, G6.2	15%
A2	**Labs**			**30%**
A21	Lab 01: Implementing CRT, Euler Totient, Inverse Modulo, and Extended GCD.	Group of 2 students work on the lab.	G5.4	10%
A22	Lab 02: Implementing RSA, EC, and attacking RSA.	Group of 2 students work on the lab.	G5.4, G6.1, G6.2	10%
A23	Lab 03: Implement PKI	Group of 2 students work on the lab.	G5.4	10%
A3	**Exams**			**40%**
A31	Final exam	Closed book exam. Describe the understanding of different topics, analyze & program to solve problems	G5.1, G5.2, G5.3, G6.1, G6.2	40%

7. RESOURCES

Textbooks

- **Cryptography Theory and Practice** 4th Edition, *Douglas Robert Stinson, Maura Paterson*, 2017.
- **Serious Cryptography: A Practical Introduction to Modern Encryption**, *Jean-Philippe Aumasson*, 2017.

- **Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographe**, *Jean-Philippe Aumasson*, 2021.
- **Real-World Cryptography**, *David Wong*, 2021.
- **Quantum Cryptography: From Key Distribution to Conference Key Agreement**, *Federico Grasselli*, 2021.

Others

- CryptoHack: https://cryptohack.org/
- Root-me: https://www.root-me.org/?lang=en
- id0-rsa: https://id0-rsa.pub/

8. GENERAL REGULATIONS & POLICIES

- All students are responsible for reading and following strictly the regulations and policies of the school and university.
- Students who are absent for more than 3 theory sessions are not allowed to take the exams.
- For any kind of cheating and plagiarism, students will be graded 0 for the course. The incident is then submitted to the school and university for further review.
- Students are encouraged to form study groups to discuss on the topics. However, individual work must be done and submitted on your own.