COURSE SYLLABUS
CTT404 – Introduction to Cryptography

1. GENERAL INFORMATION

Course name: Introduction to Cryptography	

Course name (in Vietnamese): Nhập môn Mã hoá-Mật mã

Course ID: CTT404

Knowledge block: Professional Electives

Number of credits: 4

Credit hours for theory: 45

Credit hours for practice: 30

Credit hours for self-study: 90

Prerequisite: No

Prior-course: No

Instructors: Assoc. Prof. Nguyen Dinh Thuc Nguyen Van Quang Huy Ngo Dinh Hy	

2. COURSE DESCRIPTION

The course is designed to provide students an introduction to the basic theory of applied cryptography and to the mathematical ideas underlying that theory.

3. COURSE GOALS

At the end of the course, students are will not only be well prepared for further study in cryptography, bat will have acquired a real understanding of the underlying mathematical principles on which modern cryptography is based.

ID	Description	Program LOs
G1	Understanding fundamental knowledge in cryptography	1
G2	Ability to apply knowledge from multiple fields	1, 2
G3	Getting used to reading and understanding academic literature	1
G4	Applying cryptography to practical applications	2, 5, 6

4. COURSE OUTCOMES

CO	Description	I/T/U
G1.1	Understanding the most important symmetric primitives, such as block ciphers, hash functions, and message authentication functions	I, T
G1.2	Common cryptographic schemes	I, T
G1.3	Simple cryptanalysis techniques	I, T
G1.4	Standards of security	I, T
G2.1	Can apply basic mathematical results from algebra, number theory, discrete mathematics, and probability & statistics theory within the context of cryptography	I, T
G2.2	Applying from Computer Science: Algorithmic Complexity	I
G3.1	Reading academic books and papers in cryptography at a basic level	I
G4.1	Implementing learned cryptographic schemes	I, T, U
G4.2	Know how to perform basic attacks on cryptography	I, U
G4.3	Understanding how cryptographic libraries and frameworks works and using them correctly	I, U

5. TEACHING PLAN

ID	Topic	Course outcomes	Teaching/Learning Activities (samples)
1	Introduction to cryptosystems . Symmetric cryptosystems. . Asymmetric cryptosystems. . Cryptographic hash functions.	G1.1	Lecturing Group discussion on . Classical cryptosystems . Statistical analysis
2	RSA-cryptosystem: Ring Zn . Introduction to ring Zn . Basic algorithms	G2.1	Lecturing Group discussion on: . Group . Ring
3	RSA-cryptosystem: RSA theorem . RSA theorem . Proving the RSA theorem.	G1.2	Lecturing Demonstration, discussion: . Euler, Fermat theorems . Proving the CRT theorem

4	RSA-cryptosystem: RSA implementation. . Big integers . Primes . Security issues.	G1.3, G1.4, G2.1	Lecturing Demonstration, discussion: . Generating primes . Factorization.
5	DLP-based cryptosystem: Key exchange . Group-Ring-Field . Discrete Logarithm Problem – DLP. . Diffie-Hellman key exchange protocol . ElGamal cryptosystem	G1.2, G2.1	Lecturing Demonstration, discussion: . Field . Generators
6	DLP-based cryptosystem: implementation . Implementation . Security issues	G1.3, G1.4, G4.1	Lecturing Demonstration, discussion: . Seives methods . Index calculus method
7	Symmetric cryptosystems . Feistel network . Modes . Block and stream ciphers	G1.1, G1.2	Lecturing Demonstration, discussion: . Hill cipher . Matrix cipher
8	Applied crypt 1 . Cryptographic hash functions. . Messenger Authentication Code - MAC . Digital signature	G1.1	Lecturing Demonstration, discussion: . Hash function . Homomorphic hash function
9	Applied crypt 2 . Database security . Threshold scheme	G3.1, G4.1	Lecturing Demonstration, discussion . Lagrange polynomial
10	Advanced topic . ECC . Homomorphic cryptography	G2.2, G3.1	Lecturing Demonstration, discussion: . Homomorphic cryptography examples
11	Review		Lecturing Q&A, Discussion Project submitted

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	Homework: HW1-HW10	Home works to understand the topics discussed each week		30%
A2	**Projects**			**30%**
A21	Project			30%
A3	**Exams**			**40%**
A32	Midterm exam	Closed book exam. Describe the understanding of different topics, analyze & program to solve problems		20%
A33	Final exam	Closed book exam. Describe the understanding of different topics, analyze & program to solve problems		20%

7. RESOURCES

Textbooks

- Bui Doan Khanh - Nguyen Dinh Thuc, Mã hoá Thông tin: Lý thuyết và Ứng dụng, NXBLĐ-XH, 2004.

Others

- Jeffrey Hoffstein – Jill Pipher – Joseph H. Silverman, An Introduction to Mathematical Cryptographt, Springer 2008.

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.