VIETNAM NATIONAL UNIVERSITY – HO CHI MINH CITY

UNIVERSITY OF INFORMATION TECHNOLOGY

SYLLABUS

<NT219 – Cryptography>

1. GENERAL INFORMATION

Course name (Vietnamese):	**Mật mã học** .....
Course name (English):	**Cryptography** .....
Code:	**NT219** .....
Type of course:	Compulsory .....
Deparment:	Faculty of Computer Network and Communications .....
Instructor:	Nguyen Ngoc Tu .....
	Email:tunn@uit.edu.vn
Number of credits:	3 credits
Theory:	2 credits (30 credit hours) .....
Lab:	1 credits (20 credit hours) .....
Self-study:	2 credits (30 credit hours) .....
Prerequisite course(s):	.....
Pre-course(s):	.....

2. COURSE DESCRIPTION

This course provides students with the fundamental theory of cryptography and its applications. The foundation knowledge, including classical cryptographic algorithms, symmetric-key cryptography, and the current standard of symmetric cipher algorithms, is fully presented. The modern public-key cryptography based on the factorization problem (RSA, RSADSS), and discrete logarithm problem(DH, ECDH, DSA, ECDSA, ElGamal cipher, ECIES), are also considered in detail. The application is discussed in the computer network context, including authentication; key agreement; and specific secure protocols such as TLS, SSH, IPSec, and Kerberos. Other application topics as consensus-based security, blockchain, and some candidate for post-quantum public-key cryptography are also introduced.

3. COURSE GOALS

Goal No.	Goal description	Program learning outcomes (LOs)	Contribute level
G1	Comparing between all cryptographic algorithms and applying cryptographic knowledge using in secure network protocols	LO2 (2.7.2)	Knowledge - 3
G2	Collecting related documents, proposing solutions to real-world problems to ensure integrity, confidentiality, and availability	LO3 (3.1, 3.3)	Skill - 3
G3	Forming attack hypotheses to multi-application scenarios and proposing the corresponding solution. Demonstrating the testes and verifying the soundness of the solutions	LO4 (4.1)	Skill - 3

4. COURSE LEARNING OUTCOMES

Table 2.

Course outcomes	Descriptions	Level of teaching
G1.1	Understand and compare between all cryptographic algorithms	T,U
G1.2	Apply cryptographic knowledge using in secure network protocols	T,U
G2.1	Collecting related documents from several sources to survey a specific topic.	I,U
G2.2	Proposing solutions to real-world problems to ensure integrity, confidentiality, and availability.	T,U
G3.1	Forming attack hypotheses to multi-application scenarios, including networks, data and data centers, operating systems, and hardware.	I,T,U
G3.2	Proposing solutions to attack hypothesis including security models and required input resources.	T,U
G3.3	Demonstrating the testes and verifying the soundness of the solutions	I,U

5. COURSE CONTENT, LESSON PLAN

a. Theory

Table 3.

Week (3 class hours per week)	Contents	Course learning outcomes	Activities	Assessment element
1	**Introduction to the course** • Course syllabus and policy; • Reading guides for textbooks and references; • Guides for required tools and libraries; • Guides for searching and managing documents.	G1.1, G2.1	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
2	**Introduction to cryptography** • Introduction to cryptography: motivations and overview; • Common terminologies; • Classical cryptography algorithms.	G1.1, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
3	**Symmetric cryptography** • Overview; • Stream ciphers • Block ciphers:DES and triple DES;	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
4	**Symmetric cryptography(cont.)** • Block ciphers AES; • Modes of operations in block cipher	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related	A1,A4

			issues, problems. **Work at home**: assignment, project	
5	**Mid-term project presentation:** Group presentation (10 minutes each): • Project topics • Scenario • Related entities and security requirements • References • Literature survey sketch • Goals of the projects • Demonstration proposal	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2, G3.3	**Teaching:** gives questions and instructions; **Study in class:** present their project. **Work at home**: do project research	A1,A4
6	**Asymmetric cryptography: Cryptosystems based on the factoring problem** • Motivations and Overview; • RSA cipher, RSA-based signature	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
7	**Asymmetric cryptography: Cryptosystems based on the discrete logarithm problem** • Motivations; • Diffie–Hellman key exchange • Elgamal cipher; • DSA signature,	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
8	**Asymmetric cryptography: Elliptic curve cryptosystems** • Motivations; • ECC Diffie–Hellman key exchange • ECC ciphers • ECDSA	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4

9	**Hash function and data authentication (P1)** • Motivations • Hash functions: • Secure Hash Algorithms SHA2;	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
10	**Hash function and data authentication (P2)** • Motivations • Secure Hash Algorithms SHA3; • Data integrity verifying: MAC • HMAC;	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
11	**Digital Signature** • Motivations • Elgamal digital signature scheme • Schnorr digital signature scheme • NIST digital signature schemes -RSASSA-PKCS -RSASSA-PSS -DSA, ECDSA • Public key distribution (X.509 digital certificates)	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
12	**Applied cryptography: Network security** • Authentication; • Sesion key agreement; • Deployment secure protocols; • SSH, TLS, IPSec	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
13	**Applied cryptography: Consensus mechanism and blockchain-base security** • Motivations	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question;	A1,A4

	• Consensus-based security (majority-rule security) • Integrity verification: Hash-based and signature-based • Blockchain: a case study • Transaction protocol (smart contract) • Implementation and application sectors		**Study in class:** exchange related issues, problems. **Work at home**: assignment, project	
14	**Applied cryptography: Candidates for post-quantum cryptography** • Motivations • Candidates for post-quantum public-key cryptography • Computational hardness assumptions on lattice; • Lattice-based cryptography; • NTRU-based cryptography	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2	**Teaching:** lecturer gives instructions, demo, question; **Study in class:** exchange related issues, problems. **Work at home**: assignment, project	A1,A4
15	**Final project presentation** • Scenario and security requirements; • Literature survey; • Research project results; • Demonstration results;	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** gives questions and assessment **Study in class:** present their project.	A1,A4

b. Labs

Table 4.

Week (5 class hours per week)	Contents	Course learning outcomes	Activities	Assessment element
1	**Implement block ciphers (P1)** • cryptopp library: compile and integrate to C++ projects • Coding DES, AES using cryptopp library; • Compile demo codes on both Window and Linux OSs;	G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** Instructors explain the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	A3,A4

2	**Implement block ciphers (P2)** • Implement DES, AES with different mode of operations; • Compile demo codes on both Window and Linux OSs; • Execute the codes and analyze the computational performances; • Coding DES, AES without using external cryptographic library;	G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** Instructors explain the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	A3,A4
3	**Implement asymmetric ciphers** • Perform computation on large numbers using cryptopp library; • Implement RSA, Elgamar ECC ciphers using cryptopp library; • Execute the codes and analyze the computational performances;	G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** Instructors explain the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	A3,A4
4	**Implement DHE and signatute** • Implement DHE, ECDHE using cryptopp library; • Demontrate man-in-the-midle attacks • Implement RSASSA, ECDSA, • Execute the codes and analyze the computational performances;	G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** Instructors explain the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	A3,A4
5	**Implement hash funtions and HMAC** • Implement SHA2, SHA3; • Implement digital certificate (X509); • Execute the codes and analyze the computational performances;	G2.1, G2.2, G3.1, G3.2 G3.3	**Teaching:** Instructors explain the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	A3,A4
6	**Cryptanalysis Hash funtions** • Compute MD5, SHA1 collision using hashclash;	G2.1, G2.2, G3.1, G3.2	**Teaching:** Instructors explain	A3,A4

	• Do length extension attacks SHA1, SHA2 using HashPump • Implement codes to perform length extension attacks on SHA2;	G3.3	the objective, scenario and the content of the lab. **Learning:** Students do the lab, verify the results and write the lab report.	

6. COURSE ASSESSMENT

Table 5.

Assessment element	Course learning outcomes	Percentage (%)
A1. Project	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2, G3.3	*30%*
A2. Mid-term exam		*0*
A3. Labs	G2.1, G2.2, G3.1, G3.2 G3.3	*20%*
A4. Final exam	G1.1, G1.2, G2.1, G2.2, G3.1, G3.2,	*50%*

a. Project assessment rubric (A1)

- Each group (at most 3 students) has to select a topic for their project based on course description, course syllabus, and keywords introduced in the first week;
- Each group has to select (at least 1) new articles that proposed solution for topics;
- Each group has to study the articles, survey the related knowledge and propose demo applications;

	Distinction	Merit	Pass	Fail
The first presentation (33%)	- Topic is related to the course - Good References -Excellent presentation skills: Context, related entities, security requirement, proposed project solution -Well proposed	- Topic is related to the course - Good References - Good presentation skills: Context, related entities, security requirement, proposed	- Topic is related to the course - References are related to the topic - Presentation is acceptable: Understand the context and related entities, list some security requirements but does not completeness, do	-Topic is not really related to the course; - References does not relate to the topic; - Poor presentation skills - Poor demo application

	demo application	project solution -Good proposed demo application	some literature surveys and project solution Promote dome idea for demo but not fully understand the context	
The Final presentation (33%)	-Good updated references; - Excellent presentation: Context, related entities, security requirement, well literature surveys, project solution - Good demo application	- Good updated references; - Good presentation: Context, related entities, and security requirement; good literature surveys, project solution - Good demo application but not fully related to the topic	- references does not update; - Presentation is acceptable: Understand the context, related entities and security requirement, do some literature surveys buts not fully understand, project solution - Do some demo application but does not apply the topic knowledge	-Poorly understanding the topics; -Poor Presentation - Cannot deploy any demo applications
Final report(33%)	-Fully understand the related knowledge - Clear and coherent writing; - Fully present the demo application - Code can run well	-Mostly understand the related knowledge - Clearly in writing; - well present the demo application - Code can compile and run	-Somewhat understand the related knowledge - Clearly in writing; - present the demo application but does not thoroughly; - Do some coding but does not compile and run;	-Does not understand the related knowledge - Poorly in writing; -Poorly presented demo application; - Do some coding but does not compile and run;

b. Lab assessment rubric (A3)

Students have to complete the 6 labs and do the experiment on both Window and Linux operating systems.

	Distinction	**Merit**	**Pass**	**Fail**
Labs 1,2, 3,4,5,6	- Complete the tasks - The code can compile and run well; - Full comments for code lines - Do experiments fully	- Mostly complete the tasks - The code can compile and run well; -Make some	- Compete for at least half of the tasks - The code can compile and run;	-Compete at less than half of the tasks - Does not do

	on both Windows and Linux; -Fully present the running performances	comments for code lines but does not fully; - Do experiments on Windows or Linux; - Present some running performance	- Do experiments on Windows or Linux but does not fully;	experiments on both OSs

c. Final assessment rubric (A4)

	Contents	Distinction	Merit	Pass	Fail
Fundamental knowledge questions (40%)	- Ciphers: Symmetric (DES, AES), asymmetric (RSA, Elgamar, ECC) - Hash and HMAC - Digital Signatures (discrete logarithm-based, ECC-based, lattice-based) -Digital certificate	- Fully understand the knowledge - Analyse the algorithms and do some comparison; - Analyse the security of the algorithms	- Mostly understand the knowledge - Can do some analyse the algorithms; - Can Make some comments on the security of the algorithms	- Mostly understand the knowledge; - Present primarily security property of the algorithms	- Does not understand the knowledge; - Does not fully remember the security property of the algorithms
Cryptoanalysis questions (30%)	Cryptoanalysis - Public key cryptosystem: RSA, DHE - Hash functions -Analize the robustness of knowing cryptographic algorithms	- Analyse the algorithms and do comparison; - Analyse the security of the algorithms; - Completely demonstrating attack examples;	- Analyse the algorithms and do partly comparison; - Analyse the security of the algorithms; - Can propose some demonstrating attack examples;	- Describe security of the algorithms buts does not do comparison; - Can do some cryptoanalysis and give correctly attack examples	- Does not understand the security property of the algorithms; - Does not give correctly demonstrating attack examples;
Applying questions (30%)	- Authentication - Network communication - Storage on distributed systems	- Propose some demo applications -Fully analyse the security and efficiency; - Comment the applications on some contexts;	- Propose some demo applications -Understand the security properties;	- Propose some demo applications - Detail some security properties but doest not fully understand;	Do not detail application given contexts

7. COURSE REQUIREMENTS AND EXPECTATIONS

- **Laboratory**: they can be done in the forms of assignments, or those in laboratories, depending on lecturers. Students must fulfill all lecturer's requirements. Late submission is not accepted;
- **Projects:** lecturers hand out team-work projects for the students;
- **Class attendance:** Students are checked their attendance in class. Failing to show up by the time of checking is considered to be absent;
- **Midterm and Final examination:** Students that fail to show up on the examination day without acceptable reasons will get 0.

8. COURSE MATERIALS

❖ **Textbooks**

[1] Stallings, W. (2019). *Cryptography and network security : principles and practice (8th):* Pearson Education.

[2] Yan, S. Y.(2019). *Cybercryptography: Applicable Cryptography for Cyberspace Security*: Springer.

❖ **Labs**

[3] Mihailescu, M. I., & Nita, S. L. (2021). *Pro cryptography and cryptanalysis with C++20: creating and programming advanced algorithms:* Apress.

❖ **References**

[4] Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd): CRC press.

9. SOFTWARE, TOOLS

[1]. CrypTool 2: https://www.cryptool.org/en/ct2/
[2]. Cryptopp Library version 8.6: https://www.cryptopp.com/
[3]. C++ code editing, *Visual Studio Code*, https://code.visualstudio.com/
[4]. C++ library, *MSYS2 with mingw64 packages*, https://www.msys2.org/;
[5]. Operating systems, *Windows 7, 10; Ubuntu 20 or Kali Linux* https://www.kali.org/; https://releases.ubuntu.com/20.04/
[6]. Openssl library version 3.03, https://github.com/openssl/openssl

Date: June 01, 2022

Department Head **Instructor**

Nguyen Ngoc Tu