Syllabus(2025-2nd semester)

Course	Fundamentals of Modern Cryptography	Department	Cyber Security	Office Hours	매주 월요일 14:00 ~ 16:00
Course No. and Class	38475-01	Hours	3.0	Academic Credit	3.0
Professor	Jongkil Kim		Office	Jinseonmi-gwan 225	
Telephone	4253		E-MAIL	jongkil@ewha.ac.kr	
Value of competence	Pursuit of Knowledge(50), Creative Convergence(40), Global Citizenship(10)		Keyword	Cryptography, Cryptographic Algorithms, Cryptographic Protocols	

1. Course Description

In this course, we study fundamental notions of cryptography, including pseudorandomness and computational indistinguishability, and we also study basic concepts, security definitions, and fundamental algorithms from various cryptographic services, including block ciphers, stream ciphers, hash functions, public-key and symmetric-key encryption, and digital signatures.

2. Prerequisites

This course will be mostly self-contained, so there are no particular prerequisites.
But, it would be best if you already took the following: Discrete mathematics and Number theory

3. Course Format

Lecture	Discussion/Presentation	Experiment/Practicum	Field Study	Other
80%	0%	20%	0%	0%

- explanation of course format :

The subject consists of lectures and tutorials. It may require the implementation of simple cryptographic algorithms.

4. Course Objectives

- Students will understand exactly what kind of security guarantee each cryptographic scheme gives.
- Students will be able to apply cryptographic tools for solving security-related problems.
- Students will be able to understand basic methodologies of modern cryptography.

5. Evaluation System

* Absolute evaluation

Midterm Exam	Final Exam	Quizzes	Presentation	Projects	Assignments	Participation	Other
40%	40%	0%	0%	0%	15%	5%	0%

* Evaluation of group projects may include peer evaluations.

- explanation of evaluation system

There will be no make-up exams, except in some very exceptional circumstances.
Students cannot get passing grades (A–D) unless they take the final exam.
Due to the university policy (and the policy of the Ministry of Education), if a student is absent for more than 1/3 of the class, she will get an F.
For detailed information, please do check the university policy.
Quizzes in the lectures are online assessments designed to verify that you have completed the online lectures before attending the offline classes.

6. Required Materials

I will provide lecture notes for this course.

7. Supplementary Materials

N/A

8. Optional Additional Readings

N/A

9. Course contents

Week	Date	Topics, Materials, Assignments	Form of Class
Week 1	2025/09/02(TUE)	Introduction & overview	Off-Line
	2025/09/05(FRI)	Randomness and pseudorandomness	On-Line
Week 2	2025/09/09(TUE)	Randomness and pseudorandomness – Quiz and Tutorial	Off-Line
	2025/09/12(FRI)	Classical Cryptography	On-Line
Week 3	2025/09/16(TUE)	Classical Cryptography – Quiz and Tutorial	Off-Line
	2025/09/19(FRI)	Block ciphers (1)	On-Line
Week 4	2025/09/23(TUE)	Block ciphers (1) – Quiz and Tutorial	Off-Line
	2025/09/26(FRI)	Block ciphers (2)	On-Line
Week 5	2025/09/30(TUE)	Block ciphers (2) – Quiz and Tutorial	Off-Line
	2025/10/03(FRI)	National Foundation Day	
Week 6	2025/10/07(TUE)	Chuseok (Korean Thanksgiving Day)	
	2025/10/10(FRI)	Block ciphers (3)	On-Line
Week 7	2025/10/14(TUE)	Block ciphers (3) – Quiz and Tutorial	Off-Line
	2025/10/17(FRI)	Hash functions	On-Line
Week 8	2025/10/21(TUE)	Hash functions – Quiz and Tutorial	Off-Line
	2025/10/24(FRI)	PRFs and MACs (1)	On-Line
Week 9	2025/10/28(TUE)	Mid-term Exam	Off-Line
	2025/10/31(FRI)	Mode of Operation (1) - Quiz and tutorial	Off-Line
Week 10	2025/11/04(TUE)	PRFs and MACs (1,2) - Quiz and Tutorial	Off-Line
	2025/11/07(FRI)	PRFs and MACs (2)	On-Line
Week 11	2025/11/11(TUE)	PRFs and MACs (2) - Quiz and Tutorial	Off-Line
	2025/11/14(FRI)	Cryptographic Hard Problem	On-Line
Week 12	2025/11/18(TUE)	Cryptographic Hard Problem - Quiz and Tutorial	Off-Line
	2025/11/21(FRI)	RSA	On-Line
Week 13	2025/11/25(TUE)	RSA - Quiz and Tutorial	Off-Line
	2025/11/28(FRI)	Diffie-Hellman Problem	On-Line
Week 14	2025/12/02(TUE)	Diffie-Hellman Problem- Quiz and Tutorial	Off-Line
	2025/12/05(FRI)	PKI (Public Key Infrastructure)	On-Line
Week 15	2025/12/09(TUE)	PKI (Public Key Infrastructure) - Quiz, Tutorial	Off-Line
	2025/12/12(FRI)	FInal Exam	Off-Line
Makeup Classes 1	2025/10/10(FRI)	Mode of Operation (1)	On-Line
Makeup Classes 2	2025/10/14(TUE)	Mode of Operation (2)	On-Line

10. Course Policies

* For laboratory courses, all students are required to complete lab safety training.

11. Special Accommodations

* According to the University regulation #57, students with disabilities can request special accommodation related to attendance, lectures, assignments, and/or tests by contacting the course professor at the beginning of semester. Based on the nature of the students' requests, students can receive support for such accommodations from the course professor and/or from the Support Center for Students with Disabilities (SCSD).

***** The contents of this syllabus are not final—they may be updated.