

CCY4005 Advanced Cryptography**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY3002	4	7/8	2	2	--	3

COURSE AIM

To get the students to:

- Develop an advanced understanding of cryptography, covering topics such as interactive proofs, secure protocols, and zero-knowledge proofs.
- Gain expertise in advanced cryptographic techniques, including non-interactive zero-knowledge proofs, two-party secure computation, homomorphic encryption, multiparty secure computation, key ratcheting, and quantum cryptography.
- Explore additional cryptography-related subjects, including fingerprinting, steganography, and digital watermarking.
- Be equipped with the knowledge and skills necessary to address complex cryptographic challenges and develop secure communication and data protection solutions.
- Prepare for advanced research or practical applications in the field of cryptography.
-

COURSE WEEKLY CONTENTS

- 1 Introduction to Advanced Cryptography
- 2 Interactive Proofs and Their Applications
- 3 Secure Protocols in Cryptography
- 4 Zero-Knowledge Proofs
- 5 Non-Interactive Zero-Knowledge Proofs
- 6 Two-Party Secure Computation
- 7 7th week Assessment
- 8 Homomorphic Encryption
- 9 Multiparty Secure Computation
- 10 Key Ratcheting and Its Importance
- 11 12th week Assessment
- 12 Quantum Cryptography Principles
- 13 Fingerprinting in Cryptography
- 14 Steganography: Hiding Data within Data
- 15 Digital Watermarking for Data Protection

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17	Final Exam						40

REFERENCES

Textbook William Stallings, Cryptography and Network Security: Principles and Practice, Pearson
 Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography, <https://toc.cryptobook.us/>