FIN387 Financial Cryptography

Level: 3

Credit Units: 5 Credit Units

Language: ENGLISH

Presentation Pattern: EVERY JULY

Synopsis:

FIN387 Financial Cryptography aims to introduce information security and cryptographic techniques that are used to make blockchain work as a secure distributed ledger and to secure other FinTech applications. It examines fundamental security objectives, including data integrity protection, authentication, accountability, user privacy, and data confidentiality. Students will learn how different cryptographic techniques are used to achieve these objectives in both centralised and decentralised applications. In addition, students will learn how to distinguish security requirements and threat models of centralised applications from decentralised applications such as blockchain. From there, the course will examine cryptographic techniques that can be used to distribute trust and reduce risks. The topics include hash functions, digital signature and its variants, encryption, secure multi-party computing, secret-sharing, and zero-knowledge proofs. The course serves to prepare students to recognise existing information security and cryptographic techniques used in the blockchain and FinTech areas and prepare them for advanced courses on blockchain and financial technology as well as a career in this area. It will also expose the students to the use of software such as Cryptool and the Python cryptography library.

Topics:

- Security objectives, threats and defences
- Hash functions
- Digital signature and its variants
- Symmetric encryption
- Asymmetric encryption and its variants
- Cryptography and its application in blockchain
- Public-key infrastructure
- Peer-to-peer security
- Secure multi-party computing
- Secret-sharing
- Zero-knowledge proofs
- Privacy protection in blockchain

Textbooks:

William Stallings: Cryptography and Network Security: Principles and Practice 7 Pearson
ISBN-13: 9781292158594

Learning Outcome:

- Formulate security objectives, threat models and identify the defence mechanism
- Analyse data integrity protection in FinTech and blockchain applications
- Examine the usage of public key cryptography in centralised and decentralised settings
- Appraise security objectives and threat models of centralised and decentralised applications
- Contrast different privacy protection techniques and assess the need for user privacy in existing FinTech and blockchain applications
- Develop simple Python programs using the crypto library

Assessment Strategies (Evening Class):

Components	**Description**	**Weightage Allocation (%)**
Overall Continuous Assessment	TUTOR-MARKED ASSIGNMENT 1	15
	TUTOR-MARKED ASSIGNMENT 2	15
	PARTICIPATION 1	10
Overall Examinable Components	Written Exam	60
Total		**100**