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 cryptography techniques that are used as the underlying technology for blockchain and cyber security for FinTech. It examines different security concepts and how cryptographic techniques are used to realise different security objectives. Students will learn how the properties of a secure cryptographic function can be used to protect data integrity and user privacy in blockchain and FinTech applications and evaluate the feasibility of the protocol design. Topics include data integrity and confidentiality protection techniques, public-key infrastructure, peer-to-peer security, access control models and advanced cryptographic techniques to provide user privacy. The course serves to prepare students to recognise existing information security and cryptography techniques used in the blockchain and FinTech areas, and prepare them for courses related to blockchain programming and financial technology. It will also expose the students to the use of existing open source security software such as Cryptool, GNU Privacy Guard, and the Python cryptography library.

Topics:

- Security objectives, threats and defenses
- Pseudorandom functions
- Symmetric encryption
- Block ciphers
- Asymmetric encryption
- Hash function
- Digital signature
- Public-key infrastructure
- Peer-to-peer security
- Access control
- User privacy
- Zero-knowledge proofs

Textbooks:

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

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

Learning Outcome:

- Define security objectives, threat models and identify the defense mechanisms
- Explain the concepts of data integrity protection techniques
- Describe different state-of-the-art encryption algorithms
- Illustrate how cryptographic techniques are used to make blockchain works as a secure distributed ledger technology
- Appraise peer-to-peer security and relate it to blockchain applications
- Evaluate the need of user privacy and critique how user privacy is provided in existing blockchain and FinTech applications
- Identify design flaw(s) in cryptographic protocols and propose solutions
- Recognise existing public-key infrastructure in web applications
- Demonstrate proficiency in writing
- Practice the use of digital signature and encryption in email systems
- Develop simple Python programs using the crypto library

Assessment Strategies:

Continuous Assessment Component	**Weightage (%)**
PRE-COURSE QUIZ	2
PRE-CLASS QUIZ	2
PRE-CLASS QUIZ	2
GROUP BASED ASSIGNMENT	38
PARTICIPATION	6
Sub-Total	**50**

Examinable Component	**Weightage (%)**
Written Exam	50
Sub-Total	**50**

Weightage Total	**100**