Subject Description Form

Subject Code	COMP5563
Subject Title	Applied Cryptography for Financial Applications
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil.
Objectives	The objectives of this subject are to equip students with foundational understandings of: 1. the main goals of cryptography and illustrate this with a number of examples of how cryptographic services are integrated in current applications; 2. goals and design principles for and common structures of secret key primitives such as block and stream ciphers and message authentication codes; 3. how basic public key primitives can be defined based on the difficulty of mathematical problems (e.g., discrete logarithm problem and factoring) and analyze variants of these mechanisms; 4. various notions of security, such as information-theoretic, computational, provable, and practical security as well as the security guarantees provided; 5. basic key management techniques in both secret key and public key cryptography; and 6. cryptography techniques used in different financial applications.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/academic knowledge and skills* 1. understand and apply fundamental cryptography concepts as well as advanced and specialized cryptographic knowledge for designing systems and solutions; 2. analyze and solve cryptographic problems through critical thinking, analytical thinking and creative thinking; 3. design and evaluate protocols/systems/applications to satisfy user needs and various requirements (e.g, analyze security, discover vulnerabilities and design countermeasures);

	Attributes for all-roundedness 4. deal with complex professional problems; 5. demonstrate leadership and qualities of reflective practitioners.
Subject Synopsis/ Indicative Syllabus	**Topics** **1. Overview** History, goals and services, types of cryptography, terminology. **2. Symmetric-key Encryption** One time pad, pseudo random generator, stream ciphers, block ciphers, DVD encryption system. **3. Message Integrity** Message authentication code (CBC-MAC and PMAC), collision resistant hashing (MACs from collision resistance), authenticated encryption (use KDC for a session setup), Merkle tree. **4. Public Key Cryptography** Arithmetic modulo primes, Diffie-Hellman key exchange, public key encryption (ElGamal), arithmetic modulo composites (RSA), RSA accumulator, Pederson commitment. **5. Digital Signatures** RSA signature, hash-based signatures, certificates (certificate transparency, certificate revocation), ring signature. **6. Protocols** Identification protocols (password protocols, salts; one-time passwords, challenge-response authentication), authenticated key exchange, zero-knowledge protocols, Zcash, RingCT.
Teaching/Learning Methodology	The course emphasizes on both the principles and practices of cryptographic concepts and methods. The principles will be covered mainly through the lectures, whereas the practice aspects will be achieved through the project integrate and apply what the students have learned.

Assessment Methods in Alignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed				
		a	b	c	d	e
Continuous Assessment	**50%**					
1. Assignments	25%	✓	✓	✓		✓
2. Project	25%				✓	✓
Examination	**50%**	✓	✓	✓		✓
Total	100 %					

The examination and assignments are designed to evaluate the students' understanding on the cryptographic concepts and applications. The group project, on the other hand, are designed to evaluate the students' practical skills on using cryptographic tools to solve real-world security problems.

Student Study Effort Expected

Class contact:	
▪ Lectures	39 Hrs.
▪ Tutorials/Workshops	0 Hrs.
Other student study effort:	
▪ Self-study (average 6 hours per week)	66 Hrs.
Total student study effort	105 Hrs.

Reading List and References

Textbooks:

1. Bellare Mihir, and Phillip Rogaway. *Introduction to modern cryptography*, 2nd Edition, 2005.

2. Boneh Dan, and Victor Shoup. *A graduate course in applied cryptography*, version 0.5, 2020.

Reference Books:

3. Koblitz Neal. *A course in number theory and cryptography,* vol. 114. Springer Science & Business Media, 1994.

4. Hoffstein Jeffrey, et al. *An introduction to mathematical cryptography,* vol. 1. New York: Springer, 2008.

5. Mollin Richard A. *An introduction to cryptography*. Chapman and Hall/CRC, 2006.

	6. Menezes Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography,* CRC press, 2018. 7. Guo Fuchun, Willy Susilo, and Yi Mu. Introduction to security reduction, Springer, 2018.