Subject Description Form

Subject Code	COMP3311
Subject Title	Applied Cryptography
Credit Value	3
Level	3
Pre-requisite/	COMP2012 Discrete Mathematics
Objectives	To equip students with a foundational understanding of cryptography. Students will be equipped to: 1. understand the main goals of cryptography and illustrate this with a number of examples of how cryptographic services are integrated into current applications; 2. understand goals and design principles for and common structures of secret key primitives such as block and stream ciphers and message authentication codes; 3. understand how basic public key primitives can be defined based on the difficulty of mathematical problems (e.g., discrete logarithm problems and factoring) and analyze variants of these mechanisms; 4. understand various notions of security, such as information-theoretic, computational, provable, and practical security, as well as the security guarantees provided; and 5. understand basic key management techniques in both secret key and public key cryptography.
Intended Learning Outcomes *(Note 1)*	Upon completion of the subject, students will be able to: <u>*Professional/academic knowledge and skills*</u> a) get an overview of basic cryptographic concepts and methods; b) understand some commonly used cryptographic primitives and protocols; c) acquire practical skills in analyzing the security of different cryptography mechanisms; and d) acquire practical skills and knowledge to employ cryptographic tools to build secure systems. <u>*Attributes for all-roundedness*</u>

	e) acquire the skills to reducing problems to some existing (security) problems; and f) solve complex problems in team and function effectively in a team environment to achieve a common goal.
Subject Synopsis/ Indicative Syllabus *(Note 2)*	**Topic** **1. Overview** History, goals and services, types of cryptography, terminology **2. Symmetric-key Encryption** One time pad, pseudo random generator, stream ciphers, block ciphers **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) **4. Public Key Cryptography** Arithmetic modulo primes, Diffie-Hellman key exchange, public key encryption (ElGamal), arithmetic modulo composites (RSA) **5. Digital Signatures** RSA signature, hash-based signatures, certificates (certificate transparency, certificate revocation). **6. Protocols** Identification protocols (password protocols, salts; one-time passwords, challenge-response authentication), authenticated key exchange, zero-knowledge protocols.
Teaching/Learning Methodology *(Note 3)*	The course emphasizes 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 learnt.

Assessment Methods in Alignment with Intended Learning Outcomes

(Note 4)

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

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

The examination and assignments are designed to evaluate the students' understanding of cryptographic concepts and applications. The project, on the other hand, is 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.
▪	Hrs.
Other student study effort:	
▪ Self-study (average 6 hours per week)	66 Hrs.
▪	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.