COURSE OUTLINE: MH4311

Course Title	**Cryptography**		
Course Code	**MH4311**		
Offered	Study Year 4, Semester 1		
Course Coordinator	Wu Hongjun (Assoc Prof)	wuhj@ntu.edu.sg	6513 7192
Pre-requisites	MH1301 and MH2200		
AU	4		
Contact hours	Lectures: 39, Tutorials: 12		
Approved for delivery from	AY 2021/22 semester 1		
Last revised	7 Dec 2020, 10:13		

Course Aims

This course will introduce cryptography and cryptanalysis. Cryptography is applied to protect data confidentiality and to authenticate data. Cryptanalysis is to analyze the security of cryptosystems. The course will cover five types of cryptosystems: symmetric key encryption, symmetric key authentication (message authentication code), hash function, public key encryption and public key authentication (digital signature). The applications of cryptography will be covered, especially the TLS which is widely used to protect the Internet traffic.

Intended Learning Outcomes

Upon successfully completing this course, you should be able to:

1. Define the specifications of the commonly used cryptography algorithms
2. Analyze the security of the commonly used cryptography algorithms
3. Apply the cryptography algorithms to solve security problems in applications
4. Implement cryptography algorithms in a secure way

Course Content

Classical ciphers - Caesar cipher, Substitution cipher, frequency cryptanalysis, Vigenere cipher, Playfair cipher and Transposition (permutation) cipher

Symmetric key encryption - One time pad, Shannon's information theory, Block ciphers, Data Encryption Standard (DES), Double DES, Triple DES, Advanced Encryption Standard (AES), Modes of operation, Attacks on block ciphers, Stream ciphers, Block cipher based stream ciphers, LFSR based stream ciphers, NLFSR based stream ciphers

Hash function and Message Authentication Code, Birthday paradox, birthday attack, Cryptographic hash function, Hash function structures, Secure Hash Algorithm (SHA-1, SHA-2, SHA-3), Message Authentication Code, CMAC, HMAC

Public key encryption, RSA encryption, RSA algorithm, Implementation of RSA: primality testing; fast modular exponential computation, Security of RSA: integer factorization; other attacks on RSA, ElGamal encryption, ElGamal algorithm, Algorithms for the discrete logarithm problem, Message padding: Optimal asymmetric encryption padding (OAEP)

Digital Signature, RSA signature scheme, ElGamal signature scheme, Digital Signature Standard (DSS), Digital Signature Algorithm (DSA), RSA Digital Signature Algorithm, Elliptic Curve Digital Signature Algorithm (ECDSA)

Key establishment and management, Key generation, Key establishment & management with symmetric key cryptography, Key establishment & management with public key cryptography,

Public key infrastructure (PKI), Applications: SSL/TLS, electronic passport, Secret Sharing, Shamir's Threshold Scheme

Elliptic Curve Cryptography

Post-Quantum Cryptography

Introduction to other topics, Quantum cryptography, Side-channel attacks

Assessment

Component	Course ILOs tested	SPMS-MAS Graduate Attributes tested	Weighting	Team / Individual	Assessment Rubrics
Continuous Assessment					
Tutorials					
Assignment	1, 2, 3, 4	**1.** a, b, c **2.** b	10	individual	See Appendix for rubric
Mid-semester Quiz					
Mid-term test	1, 2, 3, 4	**1.** a, b, c **2.** b	30	individual	See Appendix for rubric
Examination (2 hours)					
Final Examination	1, 2, 3, 4	**1.** a, b, c **2.** b	60	individual	See Appendix for rubric
		Total	**100%**		

These are the relevant SPMS-MAS Graduate Attributes.

1. Competence

a. Independently process and interpret mathematical theories and methodologies, and apply them to solve problems

b. Formulate mathematical statements precisely using rigorous mathematical language

c. Discover patterns by abstraction from examples

2. Creativity

b. Build on the connection between subfields of mathematics to tackle new problems

Formative Feedback

Feedback on common mistakes and the level of difficulty of the problems is given.

Students will receive individual feedback on their performance in the test and assignments.

Learning and Teaching Approach

Lectures (39 hours)	Most of the content will be taught in the lectures. We will practice solving the problem in tutorials and assignments. Some new knowledge will be learned in tutorials and assignments through self-study.
Tutorials (12 hours)	In tutorials, we expect you to: Explain the motivation behind mathematical concepts. Present systematic ways to solve problems related to the concepts developed. Derive important formulas and theorem that are fundamental in the study of Calculus. Develop competence in solving a variety of problems related to rates of change and optimization.

Reading and References

Cryptography Theory and Practice (Third Edition)
Author: Doug Stinson
Publisher: Chapman & Hall; 3rd edition (November 1, 2005)
ISBN-10: 1584885084 ISBN-13: 978-1584885085

Handbook of Applied Cryptography
Authors: Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
Publisher: CRC-Press; 1 edition (Dec 16 1996)
ISBN-10: 0849385237 ISBN-13: 978-0849385230
Free online version available at: http://www.cacr.math.uwaterloo.ca/hac/

Course Policies and Student Responsibilities

Absence Due to Medical or Other Reasons

If you are sick and not able to attend a quiz or midterm, you have to submit the original Medical Certificate (or another relevant document) to the administration to obtain official leave. In this case, the missed assessment component will not be counted towards the final grade.

Academic Integrity

Good academic work depends on honesty and ethical behaviour. The quality of your work as a student relies on adhering to the principles of academic integrity and to the NTU Honour Code, a set of values shared by the whole university community. Truth, Trust and Justice are at the core of NTU's shared values.

As a student, it is important that you recognize your responsibilities in understanding and applying the principles of academic integrity in all the work you do at NTU. Not knowing what is involved in maintaining academic integrity does not excuse academic dishonesty. You need to actively equip yourself with strategies to avoid all forms of academic dishonesty, including plagiarism, academic fraud, collusion and cheating. If you are uncertain of the definitions of any of these terms, you should go to the Academic Integrity website for more information. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Course Instructors

Instructor	Office Location	Phone	Email
Wu Hongjun (Assoc Prof)	SPMS-MAS-05-47	6513 7192	wuhj@ntu.edu.sg

Planned Weekly Schedule

Week	Topic	Course ILO	Readings/ Activities
1	Classical Ciphers	1, 2	Study lecture notes
2	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes
3	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes
4	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes
5	Hash function and Message Authentication code	1, 2, 3	Study lecture notes
6	Hash function and Message Authentication code	1, 2, 3	Study lecture notes
7	Public key Encryption (RSA, integer factorization, ElGamal and discrete logarithm algorithms)	1, 2, 3, 4	Study lecture notes
8	Public key Encryption (RSA, integer factorization, ElGamal and discrete logarithm algorithms)	1, 2, 3, 4	Study lecture notes
9	Public key Encryption (RSA, integer factorization, ElGamal and discrete logarithm algorithms)	1, 2, 3, 4	Study lecture notes
10	Digital Signature	1, 2, 3, 4	Study lecture notes
11	Key generation and Establishment	1, 2, 3	Study lecture notes
12	Elliptic curve cryptography	1, 2, 3	Study lecture notes
13	Post-quantum cryptography and introduction to side-channel attacks	1, 2, 3, 4	Study lecture notes

Appendix 1: Assessment Rubrics

Rubric for Tutorials: Assignment (10%)
Point-based marking (not rubrics based)

Rubric for Mid-semester Quiz: Mid-term test (30%)
Point-based marking (not rubrics based)

Rubric for Examination: Final Examination (60%)
Point-based marking (not rubrics based)