COURSE OUTLINE: MH5301

Course Title	**Modern Cryptography: Real-World Applications and Impact**		
Course Code	**MH5301**		
Offered	Study Year X, Semester 1		
Course Coordinator	Sim Siang Meng (Adjunct Asst Prof)	siangmeng.sim@ntu.edu.sg	6796 8197
Pre-requisites	AO or H1 level Mathematics or equivalent		
Mutually exclusive	HG5012, HG8012		
AU	3		
Contact hours	Lectures: 26, Tutorials: 13		
Approved for delivery from	AY 2022/23 semester 1		
Last revised	6 May 2022, 13:24		

Course Aims

This course aims to introduce you to the world of modern cryptography. To let you better understand and appreciate how modern cryptography is used in daily life to safeguard our digital information, we look at how modern cryptography is used in real-world applications and case studies of flawed cryptosystem. This course is suitable for students of various disciplines, including but not limited to mathematics, computer science and engineer, electronic engineering.

Intended Learning Outcomes

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

1. Recognize the high-level description of how various cryptographic components play a part in the entire architecture of cryptosystem
2. Identify the basic functionalities and determine the use-case of encryption ciphers
3. Identify the basic functionalities and determine the use-case of modes of operation
4. Identify the basic functionalities and determine the use-case of message authentication codes
5. Identify the basic functionalities and determine the use-case of authenticated encryption schemes
6. Identify the basic functionalities and recall the underlying hard problems of public-key schemes
7. Identify the basic functionalities and determine the use-case of random number generators
8. Identify the basic functionalities and determine the use-case of digital signatures and certificates
9. Identify the basic functionalities and determine the use-case of hash functions
10. Interpret the situation when primitives or cryptosystems are not used in their intended way and identify the potential issues

Course Content

Encryption algorithms

Message authentication codes

Authenticated encryptions

Public-key schemes

Random number generators

Digital signatures

Hash functions

Assessment

Component	Course ILOs tested	SPMS-MAS Graduate Attributes tested	Weighting	Team / Individual	Assessment Rubrics
Continuous Assessment					
Technology-enhanced Learning					
Multiple Choice Questions	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	**1.** a, b, c, d **2.** a, b, c, d **3.** a	15	both	
Participation	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	**1.** a, c, d **2.** d **3.** a	10	both	See Appendix for rubric
Mid-semester Quiz					
Multiple Choice Questions	1, 2, 3, 9, 10	**1.** a, b, c, d **2.** a, b, c, d **3.** a	15	individual	
Short Answer Questions	1, 2, 3, 9, 10	**1.** a, b, c, d **2.** a, b, c, d **3.** a	10	individual	See Appendix for rubric
Examination (2.0 hours)					
Multiple Choice Questions	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	**1.** a, b, c, d **2.** a, b, c, d **3.** a	40	individual	
Short Answer Questions	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	**1.** a, b, c, d **2.** a, b, c, d **3.** a	10	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

d. Use computer technology to solve problems, and to communicate mathematical ideas

2. Creativity

a. Critically assess the applicability of mathematical tools in the workplace

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

c. Develop new applications of existing techniques

d. Critically analyse data from a multitude of sources

3. Communication

a. Present mathematics ideas logically and coherently at the appropriate level for the intended audience

Formative Feedback

For the CAs and final exams, feedback on the common mistakes are given on NTULearn after the grades are announced. Common mistakes are often repeated and addressing this will be important for achieving the learning outcomes. For the tutorial problems, tutors will discuss and answer any questions about mistakes, and give feedback.

Learning and Teaching Approach

Lectures (26 hours)	Motivates the concepts in the learning objectives through examples. The general theory and principles are then explained. This also introduces more abstract mathematical reasoning. Develops competence in solving a variety of problems.
Tutorials (13 hours)	Motivates the concepts in the learning objectives through examples. The general theory and principles are then explained. This also introduces more abstract mathematical reasoning. Develops competence in solving a variety of problems. You will work together to gain experience in explaining concepts to others and presenting solutions.

Reading and References

Main teaching material
- Understanding Cryptography. Christof Paar & Jan Pelzl (Chapter 1-12)
(ISBN10: 3642041000, ISBN13: 9783642041006)

Additional reference material
- Cryptography: Theory and Practice. Douglas R. Stinson
(ISBN10: 1138197017, ISBN13: 9781138197015)
- A Graduate Course in Applied Cryptography. Dan Boneh & Victor Shoup
(ISBN not available, free book available on https://toc.cryptobook.us/)

Course Policies and Student Responsibilities

(1) General
You are expected to complete all assigned pre-class readings and activities, attend all tutorial classes punctually and take all scheduled assignments and tests by due dates. You are expected to participate in all tutorial discussions and activities.

(2) Absenteeism
Absence from the midterm without a valid reason will affect your overall course grade. Valid reasons include falling sick supported by a medical certificate and participation in NTU's approved activities supported by an excuse letter from the relevant bodies. There will be no make-up opportunities for CA components.

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
Sim Siang Meng (Adjunct Asst Prof)	DSO National Laboratories	6796 8197	siangmeng.sim@ntu.edu.sg

Planned Weekly Schedule

Week	Topic	Course ILO	Readings/ Activities
1	Course information, Introduction to modern crypto	1	tutorial on basic math for crypto
2	Stream ciphers	2, 10	tut for wk1 lect
3	Block ciphers, Modes of operation	2, 3, 10	tut for wk2 lect
4	Padding, Birthday paradox	2, 3, 10	tut for wk3 lect
5	Hash functions	9, 10	tut for wk4 lect
6	Message Authentication Codes, Authenticated Encryption	4, 5, 10	tut for wk5 lect
7	Other applied cryptography topics	1	Midterm: wk1-5
8	Public-key encryption, RSA	6, 10	Midterm feedback tut for wk6 lect
9	Diffie-Hellman Key Exchange, Elliptic curve cryptography	6, 10	tut for wk8 lect
10	Digital Signatures, Random number generators	7, 8, 9, 10	tut for wk9 lect
11	Certificates, Transport layer security	8, 10	tut for wk10 lect
12	Post Quantum Cryptography	6	tut for wk11 lect
13	Revision: wk1-12	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	revision

Appendix 1: Assessment Rubrics

Rubric for Technology-enhanced Learning: Participation (10%)

Point based marking

Rubric for Mid-semester Quiz: Short Answer Questions (10%)

Point-based marking (not rubrics based)

Rubric for Examination: Short Answer Questions (10%)

Point-based marking (not rubrics based)