Annexe A: New/Revised Course Content in OBTL+ Format

Course Overview

The sections shown on this interface are based on the templates UG OBTL+ or PG OBTL+
If you are revising/duplicating an existing course and do not see the pre-filled contents you expect in the subsequent sections e.g. Course Aims, Intended Learning Outcomes etc. please refer to Data Transformation Status for more information.

Expected Implementation in Academic Year	AY2024-2025
Semester/Trimester/Others (specify approx. Start/End date)	Semester 1
Course Author * Faculty proposing/revising the course	Sim Siang Meng
Course Author Email	siangmeng.sim@ntu.edu.sg
Course Title	Modern Cryptography: Real-World Applications and Impact
Course Code	MH5301
Academic Units	3
Contact Hours	38
Research Experience Components	Not Applicable

Course Requisites (if applicable)

Pre-requisites	AO or H1 level Mathematics or equivalent
Co-requisites	
Pre-requisite to	
Mutually exclusive to	HG5012, HG8012
Replacement course to	
Remarks (if any)	

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.

Course's Intended Learning Outcomes (ILOs)

Upon the successful completion of this course, you (student) would be able to:

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

Course Content

Encryption algorithms, Hash functions, Message authentication codes, Authenticated encryptions, Public-key schemes, Random number generators, Digital signatures, Certificates, Protocols

Reading and References (if applicable)

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/)

NOTE: The above readings comprise the foundational readings for the course and more up-to-date relevant readings will be provided when they are available.

Planned Schedule

Week or Session	Topics or Themes	ILO	Readings	Delivery Mode	Activities
1	Introduction	1		In-person	lecture
2	Stream ciphers	2,10		In-person	lecture, tutorial
3	Block ciphers, Modes of operation	2,3,10		In-person	lecture, tutorial
4	Padding, Birthday paradox	2,3,10		In-person	lecture, tutorial
5	Hash function	9,10		In-person	lecture, tutorial
6	Message Authentication Codes, Authenticated Encryption	4,5,10		In-person	lecture, tutorial
7	Public-key encryption, RSA	6,10		In-person	lecture, tutorial
8	Diffie-Hellman Key Exchange, Elliptic curve cryptography	6,10		In-person	lecture, tutorial
9	Digital Signatures, Random number generators	7,8,9,10		In-person	lecture, tutorial
10	Certificates, Transport layer security	8,10		In-person	lecture, tutorial
11	Post quantum cryptography, lightweight cryptography	2,6		In-person	lecture, tutorial

Week or Session	Topics or Themes	ILO	Readings	Delivery Mode	Activities
12	Other applied crypto topics	1		In-person	lecture, tutorial
13	Case studies	10		In-person	lecture, tutorial

Learning and Teaching Approach

Approach	How does this approach support you in achieving the learning outcomes?
Lectures	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	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.

Assessment Structure

Assessment Components (includes both continuous and summative assessment)

No.	Component	ILO	Related PLO or Accreditation	Weightage	Team/Individual	Rubrics	Level of Understanding
1	Continuous Assessment (CA): Test/Quiz(Multiple Choice Questions)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	Not Applicable	15	Individual	Analytic	Not Applicable
2	Continuous Assessment (CA): Test/Quiz(Short Answer Questions)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	Not Applicable	15	Individual	Analytic	Not Applicable
3	Continuous Assessment (CA): Class Participation(Class participation)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	Not Applicable	10	Individual	Analytic	Not Applicable
4	Summative Assessment (EXAM): Final exam(Short Answer Questions)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	Not Applicable	15	Individual	Analytic	Not Applicable
5	Summative Assessment (EXAM): Final exam(Multiple Choice Questions)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	Not Applicable	45	Individual	Analytic	Not Applicable

Description of Assessment Components (if applicable)

The each of the 3 quizzes will consist of 5% MCQ and 5% SAQ, totally to 15% CA Quiz (MCQ) and 15% CA Quiz (SAQ).

CA class participation (10%) is awarded throughout the 13 weeks when students participate in class discussions or NTULearn discussion board discussions.

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.

NTU Graduate Attributes/Competency Mapping

This course intends to develop the following graduate attributes and competencies (maximum 5 most relevant)

Attributes/Competency	Level
Digital Fluency	Intermediate
Problem Solving	Basic
Sense Making	Basic
Transdisciplinarity	Basic

Course Policy

Policy (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. On the use of technological tools (such as Generative AI tools), different courses / assignments have different intended learning outcomes. Students should refer to the specific assignment instructions on their use and requirements and/or consult your instructors on how you can use these tools to help your learning. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Policy (General)

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

Policy (Absenteeism)

Absence from the quizzes 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.

Policy (Others, if applicable)

Diversity and inclusion policy

Integrating a diverse set of experiences is important for a more comprehensive understanding of science.

It is our goal to create an inclusive and collaborative learning environment that supports a diversity of perspectives and learning experiences, and that honours your identities; including ethnicity, gender, socioeconomic status, sexual orientation, religion or ability.

To help accomplish this:

If you are neuroatypical or neurodiverse, have dyslexia or ADHD (for example), or have a social anxiety disorder or social phobia;
If you feel like your performance in the class is being impacted by your experiences outside of class;
If something was said in class (by anyone, including the instructor) that made you feel uncomfortable;
Please speak to your teaching team, our school pastoral officer or a peer or senior (either in-person or via email) about how we can help facilitate your learning experience.

As a participant in course discussions, you should also strive to honour the diversity of your classmates. You can do this by: using preferred pronouns and names; being respectful of others opinions and actively making sure all voices are being heard; and refraining from the use of derogatory or demeaning speech or actions.

All members of the class are expected to adhere to the NTU anti-harassment policy. if you witness something that goes against this or have any other concerns, please speak to your instructors or a faculty member.