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	Wu Hongjun (Assoc Prof)
Course Author Email	wuhj@ntu.edu.sg
Course Title	Cryptography
Course Code	MH4311
Academic Units	4
Contact Hours	51
Research Experience Components	Not Applicable

Course Requisites (if applicable)

Pre-requisites	MH1301
Co-requisites	
Pre-requisite to	
Mutually exclusive to	
Replacement course to	
Remarks (if any)	

Course Aims

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

Course's Intended Learning Outcomes (ILOs)

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

ILO 1	Define the specifications of the commonly used cryptography algorithms
ILO 2	Analyze the security of the commonly used cryptography algorithms
ILO 3	Apply the cryptography algorithms to solve security problems in applications.
ILO 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, DataEncryption Standard (DES), Double DES, Triple DES, Advanced Encryption Standard (AES),Modes of operation, Attacks on block ciphers, Stream ciphers, Block cipher based streamciphers, 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: primalitytesting; fast modular exponential computation, Security of RSA: integer factorization; otherattacks on RSA, ElGamal encryption, ElGamal algorithm, Algorithms for the discrete logarithmproblem, Message padding: Optimal asymmetric encryption padding (OAEP)

Digital Signature, RSA signature scheme, ElGamal signature scheme, Digital SignatureStandard (DSS), Digital Signature Algorithm (DSA), RSA Digital Signature Algorithm, EllipticCurve Digital Signature Algorithm (ECDSA)

Key establishment and management, Key generation, Key establishment & management withsymmetric 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

Reading and References (if applicable)

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

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

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	Classical Ciphers	1, 2	Study lecture notes	In-person	Learn the history and applications of cryptography . Learn classical ciphers.
2	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes	In-person	Learn one-time pad, introduction to block cipher. Practice tutorial on classical cipher.
3	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes	In-person	Learn DES, AES. Practice tutorial on one time pad and information theory.
4	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3, 4	Study lecture notes	In-person	Learn AES. Practice tutorial on DES.
5	Symmetric key ciphers (block cipher and stream cipher)	1, 2, 3	Study lecture notes	In-person	Learn block cipher modes, attacks and stream cipher. Practice tutorial on AES.

Week or Session	Topics or Themes	ILO	Readings	Delivery Mode	Activities
6	Hash function	1, 2, 3	Study lecture notes	In-person	Learn hash function. Practice tutorial on block cipher modes and attacks.
7	Message Authentication Code	1, 2, 3, 4	Study lecture notes	In-person	Learn message authentication codes. Practice tutorial on hash function.
8	Public key Encryption (RSA, integer factorization, ElGamal and discrete logarithm algorithms)	1, 2, 3, 4	Study lecture notes	In-person	Learn RSA. Practice tutorial on message authentication code.
9	Midterm Exam, Public key Encryption (RSA, integer factorization, ElGamal and discrete logarithm algorithms)	1, 2, 3, 4	Study lecture notes	In-person	Midterm Exam. Learn RSA and ElGamal Encryption. Practice tutorial on RSA.
10	Digital Signature	1, 2, 3, 4	Study lecture notes	In-person	Learn Digital Signature. Practice another tutorial on RSA.

Week or Session	Topics or Themes	ILO	Readings	Delivery Mode	Activities
11	Key generation and Establishment	1, 2, 3	Study lecture notes	In-person	Learn key generation and establishment. Practice tutorial on digital signature.
12	Elliptic curve cryptography	1, 2, 3	Study lecture notes	In-person	Learn elliptic curve cryptography. Practice tutorial on key generation and establishment.
13	Post-quantum cryptography and introduction to side-channel attacks	1, 2, 3, 4	Study lecture notes	In-person	Learn post-quantum cryptography and side-channel attacks. Practice tutorial on elliptic curve cryptography.

Learning and Teaching Approach

Approach	How does this approach support you in achieving the learning outcomes?
Lectures	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	In tutorials, we expect you to: Present systematic ways to solve problems related to the design and security analysis in cryptography.
Assignments	To self learning material related to the applications of cryptography, and work on the assignments.

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): Assignment(Tutorial - Assignment)	1, 2, 3, 4	Not Applicable	10	Individual	Analytic	Relational
2	Continuous Assessment (CA): Test/Quiz(Mid-semester Quiz - Mid-Term test)	1, 2, 3, 4	Not Applicable	30	Individual	Analytic	Relational
3	Summative Assessment (EXAM): Final exam()	1, 2, 3, 4	Not Applicable	60	Individual	Analytic	Relational

Description of Assessment Components (if applicable)

The CA includes two assignments and one midterm test. The students need to work on the assignments independently. The midterm test is open-book.

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.

NTU Graduate Attributes/Competency Mapping

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

Attributes/Competency	Level
Creative Thinking	Advanced
Curiosity	Intermediate

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 attend all lectures punctually and take all scheduled assignments by due dates. You are expected to take responsibility to follow up with course notes, assignments and course related announcements for lectures you have missed. You are expected to participate in all tutorial sessions.

Policy (Absenteeism)

If you are sick and unable to attend your class, you have to:

1. Send an email to the instructor regarding the absence.
2. Submit the Medical Certificate* or official letter of excuse to your Home school.

* The medical certificate mentioned above should be issued in Singapore by a medical practitioner registered with the Singapore Medical Association.

In this case, the missed assessment component will not be counted towards the final grade.

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.

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)