The Hong Kong University of Science and Technology

UG Course Syllabus (Fall 2025-26

[Course Title] Cryptography

[Course Code] COMP3631

[No. of Credits] 3

[Prerequisite] COMP2711 or COMP2711H (Discrete Mathematics) or a similar course

Name: [Instructor(s) Name] Cunsheng Ding

Email: [Your Email Address] cding@ust.hk

Course Description

This course is a foundation of cybersecurity and computer security. It covers the following topics: mathematical foundations of cryptography, private-key and public-key ciphers, public key infrastructures, key management, digital signature schemes, authentication protocols, hash functions, keyed hash functions, security services, security tools, cryptographic protocols, cryptographic primitives, secret sharing. After finishing this course, students will learn certain basic security tools and will be able to use these security tools to build real-world security systems.
Any year-2 or year-3 or year-4 student from any program or joint program offered by all schools of HKUST can take this course as long as the student has taken a course on discrete mathematics (COMP2711 or COMP2711H) or a similar mathematics course and has a reasonable mathematical capability.

Intended Learning Outcomes (ILOs)

By the end of this course, students should be able to:

1. evaluate certain potential vulnerabilities and attacks on computer and communication systems;

2. learn certain basic security tools; and

3. select and apply basic security tools to build security systems.

Assessment and Grading

Each assignment has about five questions and carries 100 marks. The criteria used for evaluation depends on the specific questions in each assignment. Since the questions in each assignment vary from year to year and are unknown in advance, it is impossible to specify a set of specific grading criteria. This course will be assessed using criterion-referencing and grades will not be assigned using a curve.

Assessments

Assessment Task	Contribution to Overall Course grade (%)
Lecture attendance	4%
Four assignments	56%
Final examination	40%

Mapping of Course ILOs to Assessment Tasks

Assessed Task	Mapped ILOs	Explanation
Assignments	ILO1, ILO2, ILO3	The four assignments assess students' ability to evaluate certain vulnerabilities and attacks on computer and communication systems. They also assess if students have mastered the basic security tools and if they can use the tools.
Final exam	ILO1, ILO2, ILO3	The final exam assesses students' ability to evaluate certain vulnerabilities and attacks on computer and communication systems. It also assesses if students have mastered the basic security tools and if they can use the tools.

Grading Rubrics

Each assignment has five questions and carries 100 marks. The criteria used for evaluation depends on the specific questions in each assignment. Since the questions in each assignment vary from year to year and are unknown in advance, it is impossible to specify a set of specific grading criteria.

Final Grade Descriptors:

Grades	Short Description	Elaboration on subject grading description
A	Excellent Performance	Demonstrates a comprehensive grasp of subject matter, expertise in problem-solving, and significant creativity in thinking. Exhibits a high capacity for scholarship and collaboration, going beyond core requirements to achieve learning goals.
B	Good Performance	Shows good knowledge and understanding of the main subject matter, competence in problem-solving, and the ability to analyze and evaluate issues. Displays high motivation to learn and the ability to work effectively with others.
C	Satisfactory Performance	Possesses adequate knowledge of core subject matter, competence in dealing with familiar problems, and some capacity for analysis and critical thinking. Shows persistence and effort to achieve broadly defined learning goals.
D	Marginal Pass	Has threshold knowledge of core subject matter, potential to achieve key professional skills, and the ability to make basic judgments. Benefits from the course and has the potential to develop in the discipline.
F	Fail	Demonstrates insufficient understanding of the subject matter and lacks the necessary problem-solving skills. Shows limited ability to think critically or analytically and exhibits minimal effort towards achieving learning goals. Does not meet the threshold

		requirements for professional practice or development in the discipline.

Course AI Policy

The use of generative artificial intelligence tools to complete assessment tasks is not allowed, as it will destroy the learning process.

Communication and Feedback

Assessment marks for individual assessed tasks will be communicated via Canvas within two weeks of submission. Students who have further questions about the grading of their assignment papers should consult the teaching assistant within five working days after their assignment grades are posted on Canvas.

Resubmission Policy

Each assignment has a submission deadline specified in the assignment paper. Students are allowed to resubmit their solution papers within the deadline **only**.

Required Texts and Materials

W. Stallings, Cryptography and Network Security, Seventh Edition, Pearson, 2017.

Academic Integrity

Students are expected to adhere to the university's academic integrity policy. Students are expected to uphold HKUST's Academic Honor Code and to maintain the highest standards of academic integrity. The University has zero tolerance of academic misconduct. Please refer to Academic Integrity | HKUST – Academic Registry for the University's definition of plagiarism and ways to avoid cheating and plagiarism.