

The Hong Kong University of Science and Technology

UG Course Syllabus

[Course Title] Cryptography

[Course Code] COMP3631

[No. of Credits] 3

[Prerequisite] COMP2711 or COMP2711H

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 and a prerequisite of the popular course COMP4634 Cybersecurity.

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.

Assessments

Assessment Task	Contribution to Overall Course grade (%)
Lecture attendance	2%
Four assignments	48%
Final examination	50%

Recommended textbook

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