浙江大學

MATH519

Number Theory with Cryptographic Applications

MATH519
Number Theory with Cryptographic Applications

Instructor Contact Details

Lecturer-in-charge: Yifeng LIU

Email: wlwyxy_29@zju.edu.cn
Office location: Huajiachi Campus, Zhejiang University, Hangzhou, China
Consultation Time: Book appointment by sending email to: wlwyxy_29@zju.edu.cn

Teaching Times, Modes and Locations

Course Duration: 28 Jun 2026 to 17 Jul 2026
Modes: Face-to-face
Location: Huajiachi Campus, Zhejiang University via face-to-face

Academic Level

Undergraduate

Credit Points:

The course is worth 6 units of credit point.

Credit Hours

The number of credit hours of this course equals to the credits of a standard semester- long course.

Contact Hours

The course contains a total of 53 contact hours, which consists of orientation, lectures, seminars, quiz, discussion, research, case study, small tests, assignments, on-site field trip(s), in-class and after-class activities, revision, self-study, and final exam. Students will receive an official transcript which is issued by Zhejiang University when completing this course.

Enrolment Requirements

Eligibility requires enrollment in an overseas university as an undergraduate or postgraduate student, proficiency in English, and pre-approval from the student's home institution.

Course Description:

This course offers a concise yet rigorous exploration of the mathematical foundations behind modern cryptography. Blending classical number theory with real-world security applications, it provides students with essential tools to understand and evaluate cryptographic systems. Through both theoretical insights and practical examples, the course demystifies how mathematical principles ensure secure communication in the digital age.

.

Prerequisite:

N/A

Learning Resources

- R. Howlett, Number Theory and Cryptography, School of Mathematics and Statistics, University of Sydney, 2019.

Learning Objectives

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

- Grasp key concepts in elementary number theory and modular arithmetic.
- Apply mathematical reasoning to analyze cryptographic protocols.
- Understand the mechanics behind major public key systems such as RSA, Elgamal, and Diffie-Hellman.
- Assess the computational complexity and security assumptions of cryptographic methods.

Course Delivery:

- Face-to-face Lecture mode includes lectures, seminars, quiz, discussion, research, case study, small tests, assignments, on-site field trip(s), in-class and after-class activities, revision, and final exam.

The following course will be taught in English. There will also be guest speakers and optional field trips available for students who would like to enhance their learning experience. All courses and other sessions will be run during weekdays.

Topics and Course Schedule:

WK	Topic	Activities
1	Introduction to number theory and cryptography; mathematical reasoning and proof techniques	Lecture; Tutorial
1	Divisibility, primes, and the Euclidean algorithm	Lecture; Tutorial
1	Extended Euclidean algorithm; applications in solving linear congruences	Lecture; Tutorial
1	The Fundamental Theorem of Arithmetic; integer factorisation methods	Lecture; Tutorial
1	Modular arithmetic basics: congruences, residue systems, inverses	Lecture; Tutorial
2	Modular powers and orders; Fermat's Little Theorem and Euler's Theorem	Lecture; Tutorial
2	Introduction to classical ciphers and basic cryptanalysis	Closed book
2	RSA algorithm: theory, encryption/decryption, and key generation	Lecture; Tutorial
2	Chinese Remainder Theorem and efficient modular computation	Lecture; Tutorial
2	Euler's totient function, multiplicative functions, and Mobius inversion	Lecture; Tutorial
3	Fast modular exponentiation and integer multiplication techniques	Lecture; Tutorial
3	Discrete logarithms; primitive roots and their use in cryptography	Lecture; Tutorial
3	Diffie–Hellman key exchange and the Elgamal encryption scheme	Lecture; Tutorial
3	Advanced topics: quadratic residues, square roots mod p, and Rabin cryptosystem	Lecture; Tutorial
3	Revision	Tutorial
	Final exam	Closed book

Assessments:

Class participation	15%
In-class Test	15%
Assignments	20%
Final exam	50%

Pass Requirement (Double Pass Rule)

To pass this course, students are required to achieve:

- an overall mark of 50% or above, and
- a pass mark (50% or above) in the Final Examination.

Students who achieve an overall mark of 50% or above but do not achieve a pass in the Final Examination will receive a fail grade for the course.

Grade Descriptors:

HD	High Distinction	85-100
D	Distinction	75-84
Cr	Credit	65-74
P	Pass	50-64
F	Fail	0-49

High Distinction 85-100

- Treatment of material evidences an advanced synthesis of ideas Demonstration of initiative, complex understanding, and analysis.
- Work is well-written and stylistically sophisticated, including appropriate referencing, clarity, and some creativity where appropriate.
- All criteria addressed to a high level.

Distinction 75-84

- Treatment of material evidences an advanced understanding of ideas Demonstration of initiative, complex understanding and analysis Work is well-written and stylistically strong.
- All criteria addressed strongly.

Credit 65-74

- Treatment of material displays a good understanding of ideas
- Work is well-written and stylistically sound, with a minimum of syntactical errors.
- All criteria addressed clearly.

Pass 50-64

- Treatment of material indicates a satisfactory understanding of ideas Work is adequately written, with some syntactical errors.
- Most criteria addressed adequately.

Fail 0-49

- Treatment of ideas indicates an inadequate understanding of ideas Written style inappropriate to task, major problems with expression.
- Most criteria not clearly or adequately addressed.

Academic Integrity

Students are expected to uphold the university's academic honesty principles which are an integral part of the university's core values and principles. If a student fails to observe the acceptable standards of academic honesty, they could attract penalties and even disqualification from the course in more serious circumstances. Students are responsible for knowing and observing accepted principles of research, writing and any other task which they are required to complete.

Academic dishonesty or cheating includes acts of plagiarism, misrepresentation, fabrication, failure to reference materials used properly and forgery. These may include, but are not limited to: claiming the work of others as your own, deliberately applying false and inaccurate information, copying the work of others in part or whole, allowing others in the course to copy your work in part or whole, failing to appropriately acknowledge the work of other scholars/authors through acceptable referencing standards, purchasing papers or writing papers for other students and submitting the same paper twice for the same subject.

This Academic Integrity policy applies to all students of the Zhejiang University in all programs of study, including non-graduating students. It is to reinforce the University's commitment to maintain integrity and honesty in all academic activities of the University community.

Policy

The foundation of good academic work is honesty. Maintaining academic integrity upholds the standards of the University. The responsibility for maintaining integrity in all the activities of the academic community lies with the students as well as the faculty and the University. Everyone in this community must work together to ensure that the values of truth, trust and justice are upheld.

Academic dishonesty affects the University's reputation and devalues the degrees offered. The University will impose serious penalties on students who are found to have violated this policy. The following penalties may be imposed:

- ✓ Expulsion
- ✓ Suspension
- ✓ Zero mark /fail grade
- ✓ Marking down
- ✓ Re-doing/re-submitting of assignments or reports, and
- ✓ Verbal or written warning