香 港 資 優 教 育 學 苑
The Hong Kong Academy for Gifted Education

FROM NUMBER THEORY TO NETWORK COMMUNICATION SERIES:

INTRODUCTION TO CRYPTOGRAPHY (MATS3440)

Introduction

- How do QR codes work? Why are damaged QR codes still decodable?
- How does Bitcoin work? How to protect your Bitcoins against hackers?
- What is the theory behind e-signature? How to verify its authenticity? How to prevent the receiver from reusing it without the sender's authorisation?

With the rapid development of computers and the internet, there is a great demand on security and accuracy in electronic transmission of information, which has stimulated the great development of coding theory and cryptography over the past few decades. At heart, these theories rely heavily on number theory and abstract algebra, which are two important, classical branches of pure mathematics. In this series of courses, we will appreciate the interaction of pure and applied mathematics and explore some of their real-world applications.

The "From Number Theory to Network Communication Series" programmes offered by the **Department of Mathematics, The Chinese University of Hong Kong**, are designated for students to learn Cryptography progressively.

From Number Theory to Network Communication Series consists of the following programmes:

Programme	Code	Application	Programme held
Basic Number Theory	**MATS2440**	**Jul-19**	**Oct 2019**
Introduction to Abstract Algebra	**MATS3270**	**Oct-19**	**Dec 2019**
Foundations of Coding Theory	**MATS3430**	**Jan-20**	**Mar 2020**
Introduction to Cryptography	**MATS3440**	**Apr-20**	**Jun - Aug 2020**

Here comes the last programme in the series, Introduction to Cryptography.

Electronic banking, online shopping, social media have become part of our everyday live. Life becomes easier due to the advanced technology, but it also means it is easier for adversaries to access your private and sensitive information. Cryptography is the study of techniques for secure communication and information protection.

This course will discuss basic knowledge in cryptography including basic concepts and ideas, classical cryptosystems, RSA algorithm, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Discrete Logarithms, ElGamal public key cryptosystems, hash functions, digital signatures, digital cash, secret sharing schemes, games, zero-knowledge techniques, elliptic curves and Elliptic Curve Digital Signature Algorithm (ECDSA)

Programme Type / Level	Numbers and Arithmetic Course (Level 5) (Token-required)
Instructor(s)	Dr Chan Kai Leung
Pre-requisites	Student should have basic knowledge in: 1. Basic Number Theory

2. Vectors
3. Matrix Operations
4. Groups, Rings and Fields in Abstract Algebra

Target Participants

- S1 – S6 HKAGE student members
- Class size: 20

All applicants MUST submit the Screening Test answers **no later than 25 May 2020** (Mon) at **12 noon** except those who have

1) passed **BOTH** "Basic Number Theory" (MATS2440) and "Introduction to Abstract Algebra (MATS3270)"; OR
2) passed "Foundation of Coding Theory" (MATS3430)

Priority will be given to student members who have passed 1) **BOTH** MATS2440 & MATS3270 or 2) MATS3430. They could have direct admission to this programme when apply.

Medium of Instruction

Cantonese with English handouts

Certificate

E-Certificate will be awarded to participants who have:

- Attended **at least 6 sessions AND**
- Had satisfactory performance in all assignments and assessments

Intended Learning Outcomes

Upon completion of the programme, participants should be able to:

1. apply basic concepts and ideas of cryptography;
2. perform encryption and decryption procedures of various cryptosystems;
3. understand and appreciate the applications of mathematical theories via cryptography.

Application Deadline

18 May 2020
12:00 n.n.

Application Result Release Date

29 May 2020

If student members withdraw from the programme after the Application Deadline, the token will be deducted.

Schedule

Session	Date	Time	Venue	Content
Submission Deadline of Screening Test	**25 May**	**12:00 n.n.**	**---**	**Screening Test**
1	20 Jun	9:00 a.m. – 12:00 n.n.	Rm 505 Wu Ho Man Yuen Building	Concepts and Ideas of Cryptography Classical Cryptosystems
2	27 Jun			Brief Review of Number Theory RSA Cryptosystem
3	4 Jul			Data Encryption Standard (DES) Advanced Encryption Standard (AES)
4	11 Jul		~~Rm 505 Wu Ho Man Yuen Building~~	Discrete Logarithms and Its Applications ElGamal Public Key Cryptosystems Mid-term Quiz
5	18 Jul			Hash Functions Digital Signatures

6	25 Jul		**Online lecture: Platform to be used: Zoom Meeting**	Digital Cash Secret Sharing Schemes
7	1 Aug			Poker over Telephone Zero-Knowledge Techniques
8	8 Aug			Elliptic Curves Elliptic Curve Digital Signature Algorithm (ECDSA) Final Quiz

Remarks:

1. Screening Test paper will be sent to students concerned on 22 May (Fri) through email. Applicants should return their answers through email no later than 25 May (Mon) at 12 noon. Late submission will not be considered.
2. For any assessment to be held in the programme, no make-up will be arranged, including Screening Test.

Direction to Wu Ho Man Yuen Building from the University Station (Map)

Sample Examples for the Programme

1) Try to use frequency analysis attack to decrypt the ciphertext *lcllewljazlnnzmvyiylhrmhza* obtained by a shift cipher.
2) The ciphertext 5859 was obtained from the RSA algorithm using n = 11413 and e = 7467. Find the plaintext.
3) Suppose you have a secret which is represented by an integer, say 5. Design a system where four people are given shares of the secret in such a way that any two of them can determine the secret, but no one alone can determine it.

Enquiries

For enquiries, please contact us at 3940 0101 after language selection, press “1”.