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

Secret Codes –

How to make them and how to break them (MATP2721)

Introduction	Cryptography is about the story of code making as well as the story of code breaking. Codes are part of our world and have been silently integrated into everyone's daily life. Credit card number and Hong Kong Identity Card number are two well-known examples. Codes are also part of our history. Many people remember that the course of World War II was changed by the achievements of cryptographers in breaking German and Japanese ciphers. – In this course we will show how to make and how to break several traditional encryption ciphers. We aim to provide students with the understanding of basic algorithms for some elementary ciphers as well as their mathematical principles. In fact, modern cryptography algorithms utilise prime numbers and modular arithmetic extensively; which are actually a field that draws heavily upon Mathematics. Data Encryption Standard (DES) was considered unbreakable private key cryptography in the 1970s. However, by the late 1990s, it was possible to break it in a matter of several days aided by computational power. Besides, how do you know the message comes from where it says and the person who has apparently sent the message really did so are two essential aspects of secure communication. Public key cryptography plays an important role in this area. Simplified versions of DES and RSA, examples of public key cryptography used on the Internet today, will also be introduced in the course.
Programme Type / Level	Numbers and Arithmetic Course (Level 1) (Token-required)
Instructor(s)	Mr. Li Kwok Kwan（Former Vice-Principal of TWGHs Sun Hoi Directors' College, Senior Secondary School Mathematics and Computer Teacher）
Pre-requisite	Students should have basic knowledge of Number Theory.
Target Participants	➢ P4 to P6 HKAGE student members ➢ Class size: 30
Medium of Instruction	Cantonese with English/ Chinese handouts
Certificate	**E-Certificate** will be awarded to participants who have: 1. Attended **AT LEAST 3** sessions AND 2. Completed all the assessments with satisfactory performance

Intended Learning Outcomes

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

1. Understand basic concepts and algorithms of cryptography;
2. Understand the application of modular arithmetic in cryptography;
3. Recognize different coding systems;
4. Recognize various attacks in cryptography;
5. Understand the confidentiality, integrity, authenticity issues of data transmission.

Screening

Please answer the screening question in the online application form.
*The screening question is designed to help the applicant understands the course level and the course content. The question must be answered by the student applicant and it can only be attempted once. The answer cannot be changed once the application is submitted. Selection is based on students' performance in answering the question. Only students who can demonstrate motivation and knowledge of number theory in the screening question can be enrolled in the programme.

Application Deadline

12 Nov, 2018

Application Result Release Date

21 Nov, 2018

Student members may withdraw from the programme on or before the deadline. Otherwise, the token will be deducted.

Schedule

Session	Date	Time	Venue (HKAGE)
1	5 Jan 2019	2:00 p.m.- 5:00 p.m.	Room 303
2	12 Jan 2019	9:30 a.m.-12:30 p.m.	
3	19 Jan 2019	9:30 a.m.- 12:30 p.m.	
4	26 Jan 2019	2:00 p.m.- 5:00 p.m.	

Sample Example for the Programme

Enquiries

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