



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: 24

Medium of Instruction



Cantonese with Chinese handouts

Certificate



E-Certificate will be awarded to participants who have:

1. Attended **AT LEAST FOUR** sessions AND
2. Completed all the assessments with satisfactory performance

Intended Learning Outcomes



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

1. Understand the basic concepts and algorithms of cryptography, including

- encryption and decryption;
- 2. Recognise different coding systems;
- 3. Recognise various attacks in cryptography;
- 4. Understand the confidentiality, integrity and authenticity issues of data transmission;
- 5. Develop responsible and positive attitudes towards the use of I.T. technologies.

Screening



Please answer the screening question in the online application form.
 *The screening question is designed to help the applicant understand 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

5 Aug, 2019
12:00 n.n

Application Result Release Date

16 Aug, 2019

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	30 Nov	9:30 a.m. - 12:30 p.m.	Room 303
2	7 Dec		Room 403
3	14 Dec		Room 303
4	21 Dec		Room 303
5	23 Dec		Room 403

Sample Example for the Programme

換位加密法

鑰匙排列法 (key = 3412567)

• 密文: IIIRTNTYIYWFSWAOBIDIOYONUMWG

• 明文: ???

鑰匙:	3	4	1	2	5	6	7
明文:	I	S	I	T	B	Y	M
	Y	W	I	N	D	O	W
	W	A	I	T	I	N	G
	F	O	R	Y	O	U	

XOR ⊕ 算法

$$\begin{array}{r}
 0 \oplus 0 = 0 \quad \quad \quad 10011001 \\
 0 \oplus 1 = 1 \quad \quad \oplus 01010111 \text{ (鑰匙)} \\
 1 \oplus 0 = 1 \quad \quad \quad \text{-----} \\
 1 \oplus 1 = 0 \quad \quad \quad 11001110 \\
 \quad \quad \quad \oplus 01010111 \text{ (鑰匙)} \\
 \quad \quad \quad \text{-----} \\
 \quad \quad \quad 10011001
 \end{array}$$

∴ $a \oplus b = c, c \oplus b = a$
 明文 $P \oplus b = C$ 密文 $C \oplus b = P$ 明文

模算數

0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

明文 (Plaintext) — 原資料

密文 (Ciphertext) — 加密後的內容

例: $C \equiv 5P \pmod{26}$
 $P \equiv 5^{-1}C \pmod{26} \therefore 55^{-1} \equiv 1 \pmod{26},$
 $5^{-1} = ??, P \equiv ??C \pmod{26}$

RSA 範例 - 產生金鑰

- 選擇質數: $p = 17$ & $q = 11$
- 計算 $n = pq = 17 \times 11 = 187$
- 計算 $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
- 計算 $L = \text{LCM}(16, 10) = 80$
- 選擇 $e: \text{gcd}(e, 80) = 1$
- 算出 $d: de \equiv 1 \pmod{160}$ 且 $d < 80$

公開金鑰 $PU = \{ e, pq \}$
 私密金鑰 $PR = \{ d, pq \}$

Reference:

- [1] 三谷政昭、佐藤伸一合著 / 林羿玟譯 (2011)
世界第一簡單密碼學 世茂出版集團
- [2] 王旭正 (2015)
認識密碼學的第一本書 究竟出版社股份有限公司
- [3] Stephen Pincock / 林潔盈譯 (2011)
密碼大揭秘 Codebreaker 好讀出版有限公司
- [4] 霍安琪 (2003)
密碼學 九章出版社
- [5] Sean Callery (2006)
Codes and Ciphers Collins
- [6] Wade Trappe, Lawrence C. Washington (2002)
Introduction to Cryptography with Coding Theory Prentice-Hall
- [7] John E. Hershey (2003)
Cryptography Demystified McGraw-Hill

Enquiries



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