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

數論到網絡通訊漫談：密碼學初探(MATS3440)

簡介

- QR 碼如何運作？為何損壞了的 QR 碼仍然可以解碼？
- 比特幣如何運作？如何保護你的比特幣免受黑客入侵？
- 電子簽名背後的理論是甚麼？如何驗證其真實性？如何阻止接收者未經發送人授權重複使用電子簽名？

由於電腦和互聯網快速發展，人們對電子傳信的安全性和準確度要求甚高，因而引發了過去幾十年來編碼理論和密碼學方面的重大發展。這些理論很大程度上建基於數論和抽象代數這兩門在純數學上重要而又經典的分支。在這系列課程中，我們將欣賞純數學和應用數學的相互作用，並探索兩者的一些實際應用。

「數論到網絡通訊漫談」系列由**香港中文大學數學系**提供，讓學生逐步學習密碼學。

這系列課程包括：

課程	編號	申請日期	上課日期
基礎數論	MATS2440	2019 年 7 月	2019 年 10 月
抽象代數初探	MATS3270	2019 年 10 月	2019 年 12 月
基礎編碼理論	MATS3430	2020 年 1 月	2020 年 3 月
密碼學初探	MATS3440	2020 年 4 月	2020 年 6 至 8 月

這系列最後一項課程是：密碼學入門。

電子銀行、網上購物和社交媒體已成為我們日常生活的一部分。先進的科技令我們的生活變得更輕鬆，但也讓對手更容易取得你的私人及敏感資訊。密碼學就是研究安全通信和信息保護的技術。

本課程會討論密碼學的基本知識，包括相關的基本概念和構想、經典密碼系統、RSA 算法、數據加密標準（DES）、高級加密標準（AES）、離散對數、ElGamal 公鑰密碼系統、雜湊函數、數碼簽署、數碼現金、秘密共享方案、遊戲、零知識技術、橢圓曲線和橢圓曲線數字簽名算法（ECDSA）。

活動種類/程度

數與算術課程（程度五）（代幣課程）

導師

陳啟良博士

修讀條件

學員須具備以下基本知識：

1. 基礎數論
2. 向量
3. 矩陣運算
4. 抽象代數中的群，環和域

對象

- 中一至中六香港資優教育學苑學員
- 名額：20

除了以合格成績完成
1) 「基礎數論（MATS2440）」及「抽象代數初探（MATS3270）」**兩個**課程　或
2) 「基礎編碼理論（MATS3430）」課程
的學員外，所有報名之學員必須於 **2020 年 5 月 25 日（星期一）正午 12 時前**提交甄選測驗的答案。

以及格成績完成 1) MATS2440 及 MATS3270 **兩個**課程 或 2) MATS3430 課程的學員可優先報讀本課程，並可獲直接取錄。

授課語言

粵語授課與英文筆記

證書

學員必須達到以下要求方能完成此課程，並獲發**電子證書**：

- 出席**最少六節課堂** 及
- 於課堂作業及課程評估中表現良好

預期學習成果

完成本課程後，學員應能：

1. 應用密碼學的基本概念和構想；
2. 執行各種密碼系統的加密和解密程序；及
3. 透過認識密碼學，了解並欣賞數學理論的應用。

截止報名日期

2020 年 5 月 18 日
正午 12 時

報名結果發佈日期

2020 年 5 月 29 日

如學員於截止報名日期後取消報名，其代幣將不獲退還。

日程表

課節	日期	時間	地點	內容
提交甄選測驗的截止日期	**5 月 25 日**	**正午 12:00**	**---**	**甄選測驗**
1	6 月 20 日	上午 9:00 – 正午 12:00	香港中文大學 伍何曼原樓 505 室	Concepts and Ideas of Cryptography Classical Cryptosystems
2	6 月 27 日			Brief Review of Number Theory RSA Cryptosystem
3	7 月 4 日			Data Encryption Standard (DES) Advanced Encryption Standard (AES)
4	7 月 11 日		~~香港中文大學 伍何曼原樓 505 室~~ 網上授課:	Discrete Logarithms and Its Applications ElGamal Public Key Cryptosystems Mid-term Quiz
5	7 月 18 日			Hash Functions Digital Signatures
6	7 月 25 日			Digital Cash Secret Sharing Schemes

7	8 月 1 日		使用平台： Zoom 會議	Poker over Telephone Zero-Knowledge Techniques
8	8 月 8 日			Elliptic Curves Elliptic Curve Digital Signature Algorithm (ECDSA) Final Quiz

注意事項：

1. 甄選測驗卷將於 5 月 22 日（星期五）以電郵發送給相關考生，考生必須於 5 月 25 日（星期一）正午 12 時前提交甄選測驗的答案，逾時作廢。
2. 課程中任何評估，包括評核試，均不設補考。

往伍何曼原樓指示圖（地圖）

課程例子

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.

查詢

如有查詢，請致電 3940 0101 選擇語言後，按「1」字與我們聯絡。