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

密碼–創造與拆解 (E1MAT016C)

簡介	密碼學是由編碼和解碼交織出來的故事。密碼是我們生活的一部分，並已無聲無息地融入每個人的日常生活中，信用卡號碼和香港身份證號碼就是其中兩個眾所周知的例子。密碼亦是我們歷史的一部分，相信不少人仍記起在第二次世界大戰，由於德國和日本的密碼被密碼學家所破解，從而改寫了大戰的歷史。在本課程中，我們將會介紹如何製作和破解多種傳統的加密法，讓學員了解密碼的基本演算法及其數學原理。事實上，現代密碼演算法是一門運用了大量數學知識的學科，更廣泛地應用了質數和模算數。 資料加密標準（DES）在二十世紀七十年代被視為牢不可破的私鑰加密術。然而，到了二十世紀九十年代末，在電子計算機輔助之下，可能在數天內便能破解。此外，如何確認資料的來源及資料發放人的身份是安全通訊協定的兩個基本問題，公開金鑰加密法在這方面發揮了重要的作用。 本課程亦會為學員介紹簡化版的 DES 和公開金鑰加密法 RSA 的演算法。
活動種類/程度	數與算術課程（程度一）（代幣課程）
導師	李國坤先生（東華三院辛亥年總理中學前副校長， 資深中學數學及電腦科老師）
先備知識	學員應具備數論的基本知識。
對象	➢ 小四至小六香港資優教育學苑學員 ➢ 名額：24
授課語言	粵語授課及中文筆記
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 **最少四節** 課堂；及 ❖ 於課程習作中表現良好
預期學習成果	完成本課程後，學員應能： 1. 了解密碼學的基本概念和演算法,包括加密和解密； 2. 識別不同的編碼系統； 3. 識別密碼學中的各種「攻擊」； 4. 了解數據傳輸上的機密性，完整性和真實性的問題； 5. 培養使用資訊科技的責任和正面態度。
甄選	請作答於網上報名表格的甄選題目 * 甄選題目旨在讓學員對所報讀的課程內容及程度有更深的了解。題目必須由學員作答。學員只可作答一次，報名表格一經提交，學員不得更改答案。學苑將根據學員的答題表現甄選同學。只有於作答甄選問題中，能夠證明其學習動機和具備的數論知識的學員方可參加此課程。

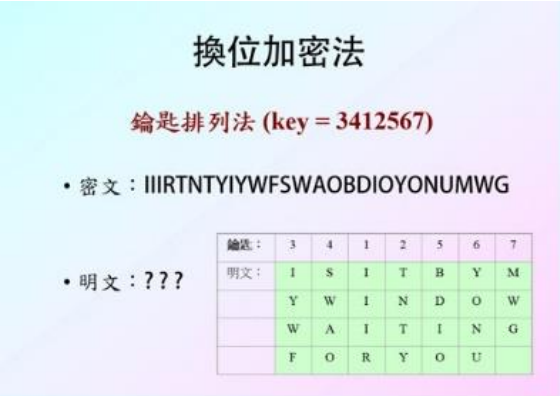
截止報名日期 **2021 年 8 月 16 日 正午 12 時**　　報名結果發佈日期 **2021 年 8 月 27 日**

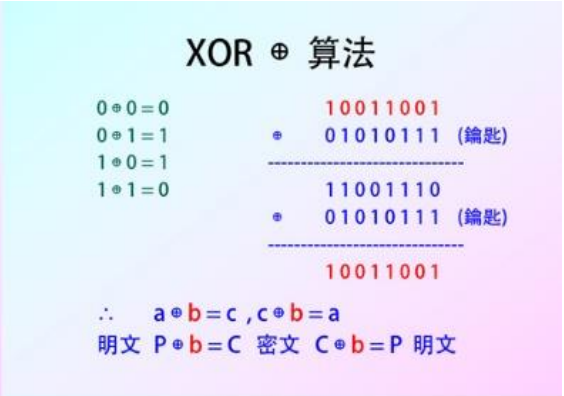
學員可於此日期前取消報名。否則，代幣將不獲退還。

日程表

課節	日期	時間	地點（香港資優教育學苑）
1	~~2021 年 10 月 9 日~~ 10 月 16 日	上午 9:00 – 正午 12:00	303 室
2	~~10 月 16 日~~ 10 月 23 日		
3	~~10 月 23 日~~ 10 月 30 日		
4	~~10 月 30 日~~ 11 月 6 日		203 室

課程例子





參考資料：

[1] 三谷政昭、佐藤伸一合著 / 林羿妏譯 (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)
Introducation to Cryptography with Coding Theory Prentice-Hall

[7] John E. Hershey (2003)
Cryptography Demystified McGraw-Hill

查詢 如有查詢，請致電 3940 0101 選擇語言後，按「1」字與我們聯絡。