理 學 院
107學 年 度 第 一 學 期 模 組 化 課 程

現代密碼數學基礎
Mathematics in modern cryptography

授課教師：

黃柏嶧
國立成功大學數學系

課程類別	學分數	選必修	開課人數	開課日期及上課時間	上課地點
講義+演習	1	選修	30	2018/08/20(一)-2018/08/24(五) 下午 14:00-17:30	待確認

先修課程或先備能力：

高中數學

建議修課年級：

不設限

建議修課學生背景：

適合各領域學生修習

教學方法：

講授 85%、報告/討論/測驗 15%

評量方式：

問題考試 60%、出席率 40 %

學習規範：

上課關閉手機

課程概述：

1.密碼學歷史悠久而應用廣泛，本課程將簡單介紹其理論及應用。
2.本課程會學習一些其背後的數學，主要是 residue class ring, prime number generation。
3.現代密碼學包含對稱式密碼、公開金鑰密碼數位簽章等，課程將一一介紹。
4.密碼學主要牽涉數學和計算機科學，本課程目標是沒有這些背景的同學也能修習，認識此學門；有數學或資訊背景的同學能開啟興趣，或許能進一步更深入學習研究。
5.星期一二四有四十分鐘演習課，由助教帶領。星期三五有四十分的考試。

理 學 院
107學 年 度 第 一 學 期 模 組 化 課 程

課程進度：

堂次	時數(小時)	進 度 說 明
1	3 hours	Introduction to cryptography history, Euclidean algorithm, complexity theory, congruence,
2	3 hours	Introduction to modern cryptography, residue class ring, Fermat's little theorem, Chinese remainder theorem.
3	3 hours	Finite fields, symmetric cryptosystem, AES.
4	3 hours	Prime number generation, public-key cryptosystem, RSA, Diffle-Hellman.
5	3 hours	Hash-function, birthday paradox, digital signatures, public-key infrastructures, application

課程學習目標：

1.認識現代密碼學

2.認識對稱式密碼及公開金鑰密碼

3.認識數位簽章等應用

課程的重要性、跨域性與時代性：

1.本課程所需預備知識只有中學數學及基礎的計算機理論，會在一週課程教完密碼學重要基本概念，課程有其完整性。

2.聚焦於現代密碼學，包含密碼理論，牽涉到的數學，現實生活應用。

3.跨域性: 密碼學主要涉及數學和計算機科學，原理包含數論、資訊理論、複雜度理論等等。

4.當代性: 密碼學是歷史悠久的學門，電腦發明以後理論、應用皆突飛猛進，最近的例子是進來火熱的比特幣(Bitcoin)。

其他備註:

參考書目:

Introduction to Cryptography, Johannes A. Buchmann, Springer.