國立成功大學跨領域模組化課程

開課學年度/學期：113 學年度第 1 學期 **領域：自然與工程科學**

現代密碼數學基礎
Mathematics in modern cryptography

授課教師	任職單位	畢業學校
黃柏嶧	成功大學數學系	國立台灣大學

課程類別	學分數	選必修	開課人數	其他注意事項
Lecture + Recitation	1	選修	35	

先修課程或先備能力

無

課程難易度

□難■中偏難 □中偏易 □易

建議修課學生背景

全校各院

教學方法

講授 85 %，討論/測驗 15 %

評量方式

問題考試 60 %
作業 30 %：演習課由助教帶學生做作業
出席率 10 %：含課堂出席及演習課出席

學習規範

上課時請關閉手機

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需要的數學，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. 本課程將簡單介紹比特幣(此為學術課程，介紹其數學原理運作，並非投資課程)。

星期一、二、四有四十分鐘演習課，由助教帶領。星期三、五有四十分鐘的考試。

關鍵字：密碼學，質數，公開金鑰密碼

課程概述(英文)

Cryptography is a key technology in electronic key systems, we will study cryptography theory and its application. In this course, we will study symmetric cryptosystem, public-key cryptosystem, digital signatures; And using some mathematics, for example: residue class ring, prime number generation.

Keywords：Cryptography, prime number, public-key cryptosystem

國立成功大學跨領域模組化課程

開課學年度/學期：113 學年度第 1 學期 **領域：自然與工程科學**

課程進度

日期	時間	進度說明
	14:00-17:00	Introduction to cryptography history, Euclidean algorithm, complexity theory, congruence,
	17:00-17:40	演習課
	14:00-17:00	Introduction to modern cryptography, residue class ring, Fermat's little theorem, Chinese remainder theorem.
	17:00-17:40	演習課
	14:00-17:00	Finite fields, symmetric cryptosystem, AES.
	17:00-17:40	Exam：17:00-17:40
	14:00-17:00	Prime number generation, public-key cryptosystem, RSA, Diffle-Hellman.
	17:00-17:40	演習課
	14:00-17:00	Hash-function, birthday paradox, digital signatures, introduction to bitcoin
	17:00-17:40	Exam：17:00-17:40

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. 重要性：密碼學是歷史悠久的學門，電腦時代起理論、應用皆突飛猛進。網路傳輸、手機通訊、信用卡交易等，皆有用到現代密碼學。
2. 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。
3. 時代性：這幾年來極受矚目的區塊鏈、比特幣(Bitcoin)，用到大量的密碼學。

其他備註

參考書目：

Introduction to Cryptography, Johannes A. Buchmann, Springer.

本課程若因天災等不可抗力之因素或中央、地方政府公告停課，授課教師需依情況依建議補課方式調整課程進度與補課；若需使用假日、國定假日補課，則需與所有修課學生達成共識方能用例假日補課。

建議補課方式：

1. 線上授課方式補課；
2. 當預期可能會因天災(颱風、超大豪雨...等)宣佈停課時，建議老師先行調整加快課程進度或預先增加可能天氣預警之前幾次課程時數；
3. 停課後隔天起延後下課，補足停課延誤的進度；若停課超過 1 天，則在開始上課後延後下課補課，或當週星期六、日補課；
4. 更改課程授課方式，例如：DEMO 改以考試、報告、作業取代。