理　學　院

111 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	任職單位	畢業學校
黃柏嶧	國立成功大學數學系	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	無

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

適合各領域學生修習

教學方法

講授 85%，討論/測驗 15%

評量方式

問題考試 60%，出席率 40%

補充說明：

出席率 40 %(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)。
6. 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。

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.

~ 接下頁 ~

理　學　院

111 學年度第一學期模組化課程

課程進度

日期	時間	進 度 說 明
8/1(一)	14:00-17:00 17:00-17:40	Introduction to cryptography history, Euclidean algorithm, complexity theory, congruence, 演習課
8/2(二)	14:00-17:00 17:00-17:40	Introduction to modern cryptography, residue class ring, Fermat's little theorem, Chinese remainder theorem. 演習課
8/3(三)	14:00-17:00 17:00-17:40	Finite fields, symmetric cryptosystem, AES. Exam：17:00-17:40
8/4(四)	14:00-17:00 17:00-17:40	Prime number generation, public-key cryptosystem, RSA, Diffle-Hellman. 演習課
8/5(五)	14:00-17:00 17:00-17:40	Hash-function, birthday paradox, digital signatures, introduction to bitcoin Exam：17:00-17:40

課程學習目標

1. 認識現代密碼學
2. 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.