

## 99-1 大葉大學 完整版課綱

### 基本資訊

課程名稱	密碼學	科目序號 / 代號	1182 / IFR5007
開課系所	資訊工程學系碩士班	學制 / 班級	研究所碩士班1年1班
任課教師	張世旭	專兼任別	專任
必選修 / 學分數	選修 / 3	畢業班 / 非畢業班	非畢業班
上課時段 / 地點	(二)567 / H713	授課語言別	中文

### 課程簡介

#### A、大葉大學資訊工程學系碩士班教育目標

- 1、教育學生在資訊工程領域的專業知能。
- 2、培養學生獨立發掘、分析暨解決問題之能力。
- 3、培養學生溝通協調及跨領域整合之能力。
- 4、培養學生領導、管理及規劃之能力。
- 5、培養學生宏觀的國際視野。
- 6、培養學生終身學習及生涯規劃能力。

#### B、大葉大學資訊工程學系碩士班培育之核心能力

- 1.1 具備軟硬體設計與系統整合之能力。
- 1.2 具備至少以下一種特定資訊工程領域之專業知識：(1) IC設計與自動化 (2) 網路多媒體 (3) 知識工程 (4) 行動通訊。
  - 2.1 具備應用相關數學、科學及工程原理解決工程技術或學術研究問題之能力。
  - 2.2 具備撰寫研究成果報告之能力。
    - 3.1 具備溝通與協調之能力。
    - 3.2 具有團隊合作之能力。
      - 4.1 具備專題策劃及專案執行之能力。
      - 4.2 具備專案領導之技巧與時程管理之能力。
        - 5.1 瞭解全球資訊研究及相關產業之發展現況與趨勢。
        - 5.2 具備應用外語之能力。
          - 6.1 瞭解終身學習的重要性及具備自我學習之能力。
          - 6.2 具備使用圖書資訊與網路資源之能力。

#### C、大葉大學資訊工程學系課程特色

- 1、結合理論與實務的教學。
- 2、推動證照考取。

#### 課程目標：

1. 本課程的主要內容是介紹加密和解密，包括傳統的密碼體制、公鑰密碼體制、數字簽名、識別和認證的基本方法。

讓學生了解密碼學的基本概念和基本理論。

2. 近代密碼學可為數論的應用，學習此課程可增進學生基本數學的能力，在各領域上均可應用密碼學的技術。(B1.2, B2.1)
3. 期末報告可使學生閱讀期刊論文具撰寫報告之能力。
4. 期末報告要求學生搜尋及閱讀近兩年內之期刊論文，在搜尋及閱讀的過程可瞭解目前密碼學的發展。(B5.1)
5. 學生研讀之期刊論文，皆以英文撰寫，學生修習此課程可熟悉此課程領域之英文關鍵字與表達方式，使學生具備此核心能力。(B5.2)
6. 期末報告要求學生搜尋及閱讀近兩年內之期刊論文，使學生主動使用圖書資訊與網路資源。(B6.2)

## 課程大綱

單元主題1：基礎介紹

單元主題2：數論

單元主題3：對稱式加密演算法

單元主題4：非對稱式加密演算法

單元主題5：Hash單向雜湊函數

單元主題6：簽章

單元主題7：網路安全應用實務: SET,PGP

## 基本能力或先修課程

演算法與基礎數學

## 課程與系所基本素養及核心能力之關連

- 1.1 具備軟硬體設計與系統整合之能力。
- 2.2 具備撰寫研究成果報告之能力。
- 3.1 具備溝通與協調之能力。
- 3.2 具有團隊合作的能力。
- 4.1 具備專題策劃及專案執行之能力。
- 4.2 具備專案領導之技巧與時程管理之能力。
- 6.1 瞭解終身學習的重要性及具備自我學習之能力。

## 成績稽核

教科書(尊重智慧財產權，請用正版教科書，勿非法影印他人著作)

書名	作者	譯者	出版社	出版年
無參考教科書				

參考教材及專業期刊導讀(尊重智慧財產權，請用正版教科書，勿非法影印他人著作)

書名	作者	譯者	出版社	出版年
無參考教材及專業期刊導讀				

上課進度		分配時數(%)				
週次	教學內容	講授	示範	習作	實驗	其他
1	Introduction	100	0	0		
2	Classical Encryption Techniques	70	20	10		
3	Block Ciphers: DES	70	20	10		
4	Block Ciphers: DES	70	20	10		
5	Introduction to Finite Fields	70	20	10		
6	Advanced Encryption Standard:AES	70	20	10		
7	Advanced Encryption Standard:AES	70	20	10		
8	Number Theory, greatest common divisor	70	20	10		
9	期中考	0	0	0		100
10	Integer factoring problem, discrete logarithm problem.	70	20	10		
11	Elliptic Curve Cryptography	70	20	10		
12	Public-Key Cryptography and RSA	70	20	10		
13	Hash Algorithms	70	20	10		
14	Digital Signatures	70	20	10		
15	Pseudo-random number generation	70	20	10		
16	Zero-knowledge proofs	70	20	10		
17	網路安全應用實務: SET, PGP	70	20	10		0
18	期末報告	0	0	0	0	100