# 100-1 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 | 1152 / 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)678 / 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。
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。
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。
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。

## 教學計畫表

| 系所核心能力 | 權重(%)【A】 | 檢核能力指標(績效指標) | 教學策略 | 評量方法及配分權重 | 核心能力學習成績【B】 | 期末學習成績【C=B*A】 |
|---|---|---|---|---|---|---|
| 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。 | 75% | 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。 | | 期中考: 20%<br>期末考: 30%<br>課程參與度: 50% | 加總: 100 | 75 |
| 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。 | 10% | 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。 | | 作業: 100% | 加總: 100 | 10 |
| 5.1 瞭解全球資訊研究及相關產業之發展現況與趨勢。 | 5% | 瞭解全球資訊研究及相關產業之發展現況與趨勢。 | | 口頭報告: 100% | 加總: 100 | 5 |
| 5.2 具備應用外語之能力。 | 5% | 具備應用外語之能力。 | | 作業: 100% | 加總: 100 | 5 |
| 6.2 具備使用圖書資訊與網路資源之能力。 | 5% | 具備使用圖書資訊與網路資源之能力。 | | 書面報告: 100% | 加總: 100 | 5 |

## 成績稽核

課程參與度: 37.5%
期末考: 22.5%
作業: 15%
期中考: 15%
口頭報告: 5%
書面報告: 5%

| 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 |
| Cryptography and Network Security | William Stallings | 巫坤品/曾志光 | Pearson Education(?峰中譯版) | 2005 |

| 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 |
| 近代密碼學及其應用 | 賴溪松,韓亮,張真誠 | | 旗標, 松崗 | 2000 |
| Applied Cryptography | Bruce Schneier | http://www.schneier.com/book-applied.html | John Wiley & Sons | 1996 |
| Handbook of applied cryptography | Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone | | CRC Press | 1996 |

| 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 | | | | |
| 2 | Introduction | 100 | | | | |
| 3 | Symmetric Ciphers | 100 | | | | |
| 4 | Symmetric Ciphers | 100 | | | | |
| 5 | Block Ciphers and the Data Encryption Standard | 100 | | | | |
| 6 | Block Ciphers and the Data Encryption Standard | 100 | | | | |
| 7 | Finite Fields | 100 | | | | |
| 8 | Finite Fields | 100 | | | | |
| 9 | 期中考 | | | | | 100 |
| 10 | Advanced Encryption Standard | 100 | | | | |
| 11 | Advanced Encryption Standard | 100 | | | | |
| 12 | More on Symmetric Ciphers | 100 | | | | |
| 13 | More on Symmetric Ciphers | 100 | | | | |
| 14 | Public-Key Encryption and Hash Functions | 100 | | | | |
| 15 | RSA | 100 | | | | |
| 16 | Digital Signatures and Authentication Protocols | 100 | | | | |
| 17 | Applications:  SET | 100 | | | | |
| 18 | 期末考 | | | | | 100 |