

# 真理大學 108 學年度第 1 學期教學計劃表

科目名稱：(中) 電影中的密碼學      (英) Cryptography in the Movies

授課教師：林熙中

系別：資訊工程學系

專任     兼任

|         |   |  |
|---------|---|--|
| 開課班級    | <input type="checkbox"/> 校訂共同必修 <input type="checkbox"/> 通識核心必修 <input checked="" type="checkbox"/> 通識分類選修  |  |
| 學分數     | 2 學分 2 小時      預備知識：無   |  |
| 授課方式    | <input checked="" type="checkbox"/> 口頭講授 <input checked="" type="checkbox"/> 分組討論 <input checked="" type="checkbox"/> 媒體教學 <input type="checkbox"/> 上機實習 <input type="checkbox"/> 其他（請詳述於後）   |  |
| 教學目標    | 中文  | <p>隨著電腦科技與網路應用的普及與發展，資訊安全已是全民皆應具備的基本素養。其中，電腦密碼學雖然是眾多資安技術背後的基礎，但往往被歸類為理工科專屬的艱澀數學課程。</p> <p>本課程將藉由電影情節的介紹與討論，帶領非資訊相關科系學生，在不涉及複雜數學的前提下，循著密碼技術發展的歷史脈絡，一步步了解密碼學。內容包含古代加密技術、對稱式加密器、公開金鑰密碼學、網路安全、電子商務應用等主題。</p>   |
|         | 英文  | <p>As the growth and popularization of computer technologies and network applications, the basic ability of information security became a required general capacity of everyone. Cryptography is the basis behind many information security techniques, but usually it is considered as a difficult math course only for students major in science and engineering.</p> <p>In this course, through the plot of movies and history of cryptosystems, students will learn the basics of cryptography. Content of this course includes but not limited to the following topics: classic encryption techniques, symmetric-key cryptosystems, public-key cryptography, network security, and e-commerce applications.</p> |
| 教材課本    | 自編教材  |  |
| 參考書籍    | <ol style="list-style-type: none"> <li>1. Cryptography and Network Security: Principles and Practice (6th Edition), William Stallings, Pearson, 2013.</li> <li>2. 資訊安全與智慧、行動網路安全應用實務，王旭正、李榮三、許富皓，博碩，2015。</li> <li>3. 認識密碼學的第一本書，王旭正著，究竟，2015。</li> <li>4. 密碼大揭密：法老王時代到量子世界的密碼全紀錄，Stephen Pincock 著，林潔盈翻議，好讀出版，2011。</li> <li>5. 世界第一簡單密碼學，三谷政昭、佐藤伸一合著，林羿奴翻譯，世茂，2009。</li> <li>6. 密碼傳奇：從軍事隱語到電子晶片，Rudolf Kippenhahn 著，鄧白樺、姚文俊、滕峻輝翻譯，世茂，2003。</li> </ol> |  |
| 教學進度及內容 | 授課進度表   |  |
|         | 週次  | 單元主題      內容   |
|         | 1   | 課程介紹      認識密碼學：「新世紀福爾摩斯：不識貨的行員」   |
| 2       | 古代密碼技術（一）      解謎與尋寶：柯南·道爾「福爾摩斯探案集-跳舞的小人」中的替換法則與「國家寶藏：古籍秘辛」中的 Playfair 培菲加密器  |  |

|  |   |            |  |
|--|---|------------|--|
|  | 3   | 古代密碼技術（二）  | 戰爭中的密碼：「模仿遊戲」、「攔截密碼戰」、「獵殺 U-571」中的 Enigma 奇迷機<br>*實作專題一：用洋芋片紙筒製作奇迷機* |
|  | 4   | 古代密碼技術（三）  | 戰爭中的密碼：從「獵風行動」中的方言密碼到「接觸未來」  |
|  | 5   | 古代密碼技術（四）  | 戰爭中的密碼：從麥家小說「解密」與「暗算」，到電影「風聲」與「聽風者」                                  |
|  | 6   | 近代密碼技術（一）  | 對稱式加密器：「終極密碼戰」與「神鬼尖兵」  |
|  | 7   | 近代密碼技術（二）  | 對稱式加密器：認識 DES 區塊加密器  |
|  | 8   | 近代密碼技術（三）  | 密碼與數學：「美麗境界」與「X+Y 愛的方程式」   |
|  | 9   | 期中考試       |  |
|  | 10  | 近代密碼技術（四）  | 密碼與數學：認識公開金鑰密碼系統<br>*實作專題二：數論的循環群與秘密金鑰交換*                            |
|  | 11  | 資訊安全（一）    | 國家安全與個人隱私：從「全民公敵」、「竊聽風暴」到「隱藏攝影機」                                     |
|  | 12  | 資訊安全（二）    | 駭客攻擊：從「終極警探 4.0」、「黑帽駭客」到「千禧年三部曲」                                     |
|  | 13  | 資訊安全（三）    | 網路犯罪：從「CSI 犯罪現場：網路犯罪」到「我是誰：沒有絕對安全的系統」                                |
|  | 14  | 資訊安全（四）    | 電子商務：「比特幣的崛起」  |
|  | 15  | 未來的資安挑戰（一） | 資安白皮書：「2020 網路危機」  |
|  | 16  | 未來的資安挑戰（二） | 虛擬世界的資訊安全：「夏日大作戰」  |
|  | 17  | 未來的資安挑戰（三） | 世界大戰 3.0：「Zero Days 零日網路戰」   |
|  | 18  | 期末報告       |  |
| 本課程能達成通識之教育目標<br>*請老師勾選(複選)              | <ul style="list-style-type: none"> <li>■培養學生成為一個具品德及人文教養的人。</li> <li>■培養學生成為一個具獨立思考和批判能力的人。</li> <li>■培養學生成為一個具自我學習的人。</li> <li>■培養學生成為一個具國際視野的人。</li> <li><input type="checkbox"/>培養學生成為一個懂得愛護地球環境與保育生命的人。</li> </ul>  |            |  |
| 學生基本素養<br>*請老師勾選(複選，並填寫權重。權重總分需為 100 分。) | <ul style="list-style-type: none"> <li>■人文反省素養。權重 15 %</li> <li>■溝通表達素養。權重 15 %</li> <li>■社會實踐素養。權重 0 %</li> <li>■多元文化素養。權重 20 %</li> <li><input type="checkbox"/>自然與健康素養。權重 0 %</li> <li>■資訊素養。權重 50 %</li> <li><input type="checkbox"/>體育素養。權重 0 %</li> </ul> |            |  |
| 成績考核方式                                   | 期中考：30 %<br>期末報告：30 %<br>平時成績（含課堂參與及隨堂作業等項目）：40 %   |            |  |
| 老師基本資料                                   | E-mail: hclin@mail.au.edu.tw  |            |  |

|    |   |
|----|---|
|    | 教學網站: <a href="http://ilms.au.edu.tw">ilms.au.edu.tw</a><br>電話(公): 分機3210<br>地點: 5 棟 5907 |
| 備註 | 為鼓勵評分方式之多元化，避免僅以期中及期末考為評分依據，請詳述成績考核方式，並於開學時宣佈，以強化學習效果。                                    |