【密碼學】課程綱要

課程名稱	(中文) 密碼學	開課單位	通訊工程研究所
	(英文) Cryptography	課號	COM5336
學分數	3	必/選修	專業選修
開課頻率	每學年	建議修課年級	四年級
先修課程或先備能力：C/C++程式設計			
隸屬學程：	☐ 電力工程學程 ☐ 計算機工程學程 ☐ 電子電路設計學程	☐ 數位訊號處理學程 ☐ 電子工程學程 ☒ 通訊工程學程	☐ 光電工程學程 ☐ 生物醫學電子學程 ☐ 基礎課程
課程類型：	☒ 講授	☐ 實驗	☐ 演講 ☐ 其他：

課程目標：本課程前半部涵蓋當代主要密碼系統基本原理及常見應用，如加解密、金鑰交換、數位簽名等。後半部主要是介紹與實作目前最先進的橢圓曲線以及 XTR 及密碼系統，並以實作為主要重點。透過本課程，學生可以學習到目前最常見的密碼技術內部的運作原理並具備實作的能力和經驗。

培養之核心能力：

☐	一、豐富的數學、物理、科學與工程知識，以及實際運用的能力。
☐	二、設計實驗、執行實驗、分析數據及歸納結果的能力。
☒	三、執行電機工程實務所需理論、方法、技術及使用相關軟硬體工具之能力。
☐	四、電機工程系統、模組、元件或製程之設計能力。
☒	五、團隊合作所需之組織、溝通及協調的能力。
☐	六、發掘問題、分析問題及處理問題的能力。
☐	七、掌握科技趨勢，並了解科技對人類、環境、社會及全球的影響。
☐	八、理解專業倫理及社會責任。
☒	九、專業的外語能力及與國際社群互動的能力。

教學內容與課程大綱：

1. 對稱式密碼系統基本觀念
2. DES 及 RC4 密碼系統
3. 不對稱式密碼系統基本觀念
4. RSA, ElGamal, 以及 Rabin 密碼系統
5. 數位簽名: RSA, Rabin, ElGamal, DSA, Nyberg-Rueppel 簽名
6. 有限體
7. 有限體實作
8. AES 密碼系統
9. 橢圓曲線密碼系統
10. XTR 密碼系統
11. 橢圓曲線及 XTR 密碼系統實作