通訊所專業必修/必選修課程綱要表

課程名稱：（中文）密碼學				開課學程	通訊所
（英文）Cryptography				課程代碼	COM5336
授課教師：黃之浩					
學分數	3	必/選修	選修	開課年級	碩士班、博士班
先修科目或先備能力：					
課程概述與目標：This course provides an in-depth study of cryptographic techniques and their role in practical computer systems and applications. The first part of this course covers the algorithms for basic symmetric as well as asymmetric encryption/decryption algorithms, and the protocols to achieve practical security objectives such as confidentiality, authentication, data integrity, non-repudiation. In the second part, our focus will be on two asymmetric cryptosystems: Elliptic Curve and XTR. To facilitate deep understanding of Elliptic Curve and XTR cryptosystems, some basic material on finite fields will be taught prior to them. The main focus of this course is to develop necessary skills and hands-on experience for implementing cryptographic algorithms/protocol on hardware efficiently.					
教科書 [1]	1. Menzes, van Oorschot, Vanstone, Handbook of Applied Cryptography, CRC 2. W. Stallings, Cryptography and Network Security – Principles and Practices, 4e, Pearson Education.				
參考書目	R. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers				

對應之學生核心能力	核心能力達成指標	比例
1. 發掘、分析、解決問題與獨立研究之能力	A.具備發掘問題之能力 B.具備分析問題之能力 C.具備解決問題之能力 D.具備獨立研究之能力	30%
2.通訊科技整合與創新之能力	A.具備整合通訊知識之能力 B.具備創新通訊科技知識之能力	25%
3.學習新知識與技術之能力	A. 具備主動學習新知識之能力 B. 具備學習新技術之能力	20%
4.良好溝通、表達與外語能力	A. 具備與通訊專業人員溝通與表達專業知識之能力 B. 具備外語專業能力用以溝通通訊專業知識	10%
5.具團隊精神及遵守專業倫理	A.具備團隊合作之能力與精神 B.能遵守專業倫理	15%

課程綱要	內容綱要	核心能力達成指標（請勾選）

Symmetric Cryptography	1. Block cipher 2. Stream cipher	1-□A■B■C□D 2-■A■B 3-■A■B 4-□A□B 5-□A□B
Basic Asymmetric Cryptosystems	1. Encyrption/Decryption 2. Digital signatures and key exchange protocols	1-□A■B■C□D 2-■A■B 3-■A■B 4-□A□B 5-□A□B
Finite fields	1. Introduction to finite fields 2. Implementation of finite fields	1-■A■B■C■D 2-■A■B 3-■A■B 4-□A□B 5-□A□B
Elliptic Curve Cryptography	Elliptic Curve Cryptography	1-□A■B■C□D 2-■A■B 3-■A■B 4-□A□B 5-□A□B
XTR Cryptosystem	XTR Cryptosystem	1-□A■B■C□D 2-■A■B 3-■A■B 4-□A□B 5-■A■B
教學要點概述[2]： 1. 教材編選：教科書及參考書如上述 2. 教學方法：上課講解、演算法實作(使用 C/C++程式) 3. 評量方法：assignments, 1 final project 4. 教學資源：		

註：1. 教科書請註明書名、作者、出版社、出版年等資訊。

2. 教學要點概述請填寫教材編選、教學方法、評量方法、教學資源、教學相關配合事項等。

3. 研究所所有開設之課程皆須填寫此表格或提供原有格式之課程綱要表，並呈現於實地訪評現場。