

通訊所專業必修/必選修課程綱要表

課程名稱：(中文) 通訊系統特論-有限體之工程應用		開課學程	通訊所
(英文) Tentative course in Communication Systems - Applications of Finite Fields in Engineering		課程代碼	COM5990
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：包含有限個元素的體被稱為有限體。它在諸多通訊、資訊工程學門裡中有著重要的應用。如密碼學等。本課程的目標是以教授通訊電路設計中的 m-sequence 以及其相關的數列 Gold sequence、Kasami sequence 的理論為主。另外會包括有限體的其它應用: AES, Elliptic Curve Cryptosystem。主要用的數學工具以抽象代數為主，但本課程是為工程背景的同儕設計，所以除離散數學外不需要其它的數學背景。			
教科書 ¹	Robert J. McEliece: Finite Fields for Computer Scientists and Engineers		
參考書目	n/a		
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)
Introduction	1. 序、抽象代數簡介：群、環、體 2. 輾轉相除法 3. 有限體的建構 4. 有限體的性質		1- <input type="checkbox"/> A <input checked="" type="checkbox"/> B <input checked="" type="checkbox"/> C <input type="checkbox"/> D 2- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 3- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 4- <input type="checkbox"/> A <input type="checkbox"/> B 5- <input type="checkbox"/> A <input type="checkbox"/> B

Some applications	1. AES 加密系統 2. 橢圓函數加密系統 3. 有限體內的因式分解 4. 有限體的線性遞迴	1- <input type="checkbox"/> A <input checked="" type="checkbox"/> B <input checked="" type="checkbox"/> C <input type="checkbox"/> D 2- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 3- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 4- <input type="checkbox"/> A <input type="checkbox"/> B 5- <input type="checkbox"/> A <input type="checkbox"/> B
Other Selected Topics	1. m-sequence 2. m-sequence 的交互相關(crosscorrelation)性質 3. Gold sequence 4. Kasami sequence	1- <input type="checkbox"/> A <input checked="" type="checkbox"/> B <input checked="" type="checkbox"/> C <input type="checkbox"/> D 2- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 3- <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> B 4- <input type="checkbox"/> A <input type="checkbox"/> B 5- <input type="checkbox"/> A <input type="checkbox"/> 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, and final exam 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。