國 立 高 雄 師 範 大 學 教 學 綱 要 (105 學 年 度)

科目名稱：密碼學研究　　□必修 ■選修　　教師：楊中皇
任課班級：軟體工程與管理學系碩士班
每學期開課學分數：上學期____學分　　下學期__3__學分
總學分數：__3__學分　每週上課時數：__3__小時
連繫電話：　1703　　辦公地點：　電算中心二樓　辦公時間（Office hour）：TBA

※※請遵守智慧財產權觀念、不得非法影印※※

一、教學目標：密碼學(Cryptography)技術為現代電子商務、行動安全等必備之工具。本課程將介紹密碼學的基本觀念與國際標準保密、單向雜湊函數、及數位簽章等密碼學演算法。我們將探討密碼學技術於 Android 手機的應用。本課程冀以循序漸進的教學方式，引發學生對密碼學的興趣。

二、課程核心能力及其配分：本課程內容包含：

1. 密碼學技術介紹
2. 密碼學技術基本術語。
3. 橢圓曲線密碼學演算法介紹。
4. 橢圓曲線密碼學演算法的實現技巧。
5. 橢圓曲線密碼學技術使用個案。
6. Android 手機安全。

三、教材內容：課本與講義(參見 http:/security.nknu.edu.tw/crypto/)。

四、實施方法：

1. 講授：依據教學進度講授教學單元之各項內容。
2. 提問與討論：每週課程前提出問題引導學生學習，另外也鼓勵學生針對授課內容提出問題進行討論。
3. 文獻研讀：配合教授單元，透過文獻(應用實例)之研討，加強學生對網際網路技術應用之能力。每位同學需各別針對密碼學軟體應用實例或論文探討進行期中與期末報告。

五、評量方式：

1. 期中報告：佔總成績 60%
2. 期末報告：佔總成績 30%
3. 課堂參與：佔總成績 10%

六、主要讀本及參考書目：

（1）主要讀本：.

- Nikolay Elenkov, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2015. (Chapter 5)
- 楊中皇，網路安全理論與實務，學貫行銷股份有限公司，2008 年 9 月出版。(第六章)

（2）參考書目：

- D. R. Hankerson, S. A. Vanstone, A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, 2004.
- A.J. Menezes, et al, *Handbook of Applied Cryptography* (CRC Press Series on Discrete Mathematics and Its Applications), 1996. 參閱 http://www.cacr.math.uwaterloo.ca/hac/有 PDF 電子檔

七、教學進度：

週	別	內　　容	作　　業	參　考　資　料
（上學期或下學期）	1	課程說明		
	2	密碼學演算法簡介		
	3	Android/iPhone 手機安全與加解密軟體		
	4	Android 設備 Cryptographic Primitives		
	5	Elliptic-Curve Cryptography - 1		
	6	Elliptic-Curve Cryptography - 2		
	7	Efficient Implementations		
	8	Cryptographic Providers		
	9	期中報告		
	10	SM2 橢圓曲線公鑰密碼算法		
	11	SM3 密碼雜湊算法		
	12	SM4 分組密碼算法		
	13	FIPS Library and Android		
	14	Full-Disk Encryption		
	15	File-Based Encryption		
	16	Android/iPhone Security Discussions - 1		
	17	Android/iPhone Security Discussions - 2		
	18	期末報告		