龍 華 科 技 大 學

Lunghwa University of Science and Technology

課 程 簡 介

COURSE DESCRIPTION

部別 Daytime/Evening Session	日間部 Daytime	系別 Dept.	資網系 CIN	年制 Program	四技 Four-year	開課年級 Target Students	3下 3

科目編碼 Course Code	科目名稱（中文 Course Title (Chinese)	科目名稱（英文 Course Title (English)	學分數 Credit(s)	上課時數 Hour(s)
CN21083	密碼學	Cryptography	3	3

中文概述	本課程的目的將針對密碼學的基本觀念與保密、雜湊函數、數位簽章、網路安全的原理與實務部分提供詳細的介紹。我們會提供密碼學與網路安全技術的導覽，藉此說明網路安全功能的基本訴求。並且著重在網路安全的實務部分；介紹一些已經被實作出來可以提供網路安全的應用程式。我們將利用資訊理論與數論探討多種密碼系統的設計與攻擊，課程將涵蓋 DES、 AES、 RSA、 DSA、 ElGamal、Diffie-Hellman、SHA、ECC 等密碼學演算法及其應用。
English Description	It is the purpose of this course to provide a practical survey of both the principles and practice of cryptography and network security. In the first part, the basic issues to be addressed. By a network security capability are explored by providing a tutorial and survey of cryptography and network security technology. The latter part deals with the practice of network security: practical applications that have been implemented and are used to provide network security. Course includes introduction to the concepts of security, information theory, number theory, symmetric-key cryptographic algorithms, asymmetric-key cryptographic algorithms, public-key infrastructure, internet security protocols, user authentication mechanisms, practical implementations of cryptography.

系科名稱：資網系

科目名稱：密碼學

英文科目名稱: Cryptography

學年、學期、學分數：	第三學年、第二學期、3 學分

先修科目或先備能力:基礎數學、程式設計

教學目標：

一、知識：(一)基礎數學模數運算及矩陣
(二)傳統對稱式加密法
(三)代數結構
(四)現代對稱式加密法
(五)資料加密標準
(六)進階加密標準及運用
(七)質數及同餘方程式
(八)非對稱式加密法
(九)訊息完整性及確認性
(十)密碼雜湊及數位簽章
（知識 5/48=10.4%）

二、技能：(一)一般能力：1.數字邏輯及運算
2.使用電腦作業系統
3.邏輯思考、問題分析與解決
(二)專業能力：1.具備程式設計知識
2.具備數學基礎知識
（技能 42/48=87.5%）

三、態度：(一)謹守職業道德
(二)做事細心且有耐心
(三)具備主動積極的學習態度
(四)能夠迎接挑戰並學習解決問題
(五)負責任
（態度 1/48=2.1%）

四、其他：可以勝任資訊安全相關的工作

教材大綱：

單元主題	技能項目	相關知識	教學參考節數	備註
職場倫理個案及課程與教學計畫說明	職場倫理個案及課程與教學計畫說明	職場倫理個案及課程與教學計畫說明(A)	1	

密碼學簡介	熟悉資訊安全機制及攻擊	1.安全目標(K) 2.攻擊(K) 3.服務與機制(K)	2	
基礎數學模數運算及矩陣	熟悉基礎數學	1.整數算數(K) 2.模數算數(K) 3.矩陣及線性同餘(K)	3	
傳統對稱式加密法	熟悉傳統加密法	1.取代加密法(S) 2.換位加密法(S) 3.串流加密法與區塊加 密法(S)	3	
代數結構	熟悉代數運算	1.代數結構(S) 2.GF 體(S)	3	
現代對稱式加密法	熟悉現代對稱加密	1.現代區塊加密法(S) 2.現代串流加密法(S)	3	
資料加密標準	熟悉 DES	1.DES 結構分析(S) 2.多重 DES(S) 3.DES 安全性(S)	6	
進階加密標準及運用	熟悉 AES 及應用	1.AES 介紹(S) 2.加密法運用(S)	6	
質數及同餘方程式	熟悉質數運算	1.質數介紹(S) 2.指數運算與對數運算 (S)	3	
非對稱式加密法	熟悉 RSA 及 ELGamal	1.RSA 密碼系統(S) 2.ELGamal 密碼系統(S)	9	
訊息完整性及確認性	熟悉訊息完整相關作法	1.訊息完整性及確認性介紹(S)	3	
密碼雜湊及數位簽章	熟悉 SHA 與數位簽章機制	1.SHA 介紹(S) 2.數位簽章機制與應用 (S)	6	

1. 教學目標（歸納為四項）：分別為知識（Knowledge）、技能（Skills）、態度其他各一項。
2. 技能項目為表 A8 之任務項目。
3. 單元主題：為各項任務之彙整。
4. 技能項目及相關知識：各該科目應包括之任務及該任務相對應之相關知能，加上補充技能及相關知識（表 A8 中未列，但為達知識或技能的完整性且課程中需教授之能力），撰寫方式係以不含動詞的任務方式呈現。

※三者之關係：教學目標＞單元主題＞技能項目及相關知識。

※本課程將培養核心能力為: 1. 確認、分析和解決問題的能力 2. 具備問題分析與解決能力 3. 具備網路與資訊安全管理能力	
檢核項目	**是否符合**
1.是否將科目名稱、上課時數及學分數填入本 2.是否將教學目標、綱要名稱或單元名稱填入本 3.所填入的行業任務是否有考慮學生學習的順序性、邏輯性、連 貫性、完整 4.除了表 A7 所敘述的行業任務，是否有考慮到其他的任務，以成為一門完整	是回 否口 是回 否口 是回 否口 是回 否口

填表說明:

1.將實習、實驗科目名稱、上課時數及學分數填入本表。

2 依學生學習的順序性、邏輯性、連貫性、完整性等特性將表 A8 中的各該科目應包括之職責填入單元主題，並將該職責之任務及該任務相對應之相關知能分別填入表中的技能項目及相關知識欄中，並擬訂單元名稱並確立教學目標。

龍 華 科 技 大 學

Lunghwa University of Science and Technology

課 程 簡 介

COURSE DESCRIPTION

部別 Daytime/Evening Session	進修部 Training Department	系別 Dept.	資網系 CIN	年制 Program	四技 Four-year	開課年級 Target Students	3下 3

科目編碼 Course Code	科目名稱（中文 Course Title (Chinese)	科目名稱（英文 Course Title (English)	學分數 Credit(s)	上課時數 Hour(s)
CN21083	密碼學	Cryptography	3	3

中文概述	本課程的目的將針對密碼學的基本觀念與保密、雜湊函數、數位簽章、網路安全的原理與實務部分提供詳細的介紹。我們會提供密碼學與網路安全技術的導覽，藉此說明網路安全功能的基本訴求。並且著重在網路安全的實務部分；介紹一些已經被實作出來可以提供網路安全的應用程式。我們將利用資訊理論與數論探討多種密碼系統的設計與攻擊，課程將涵蓋 DES、 AES、 RSA、 DSA、 ElGamal、Diffie-Hellman、SHA、ECC 等密碼學演算法及其應用。
English Description	It is the purpose of this course to provide a practical survey of both the principles and practice of cryptography and network security. In the first part, the basic issues to be addressed. By a network security capability are explored by providing a tutorial and survey of cryptography and network security technology. The latter part deals with the practice of network security: practical applications that have been implemented and are used to provide network security. Course includes introduction to the concepts of security, information theory, number theory, symmetric-key cryptographic algorithms, asymmetric-key cryptographic algorithms, public-key infrastructure, internet security protocols, user authentication mechanisms, practical implementations of cryptography.

系科名稱：資網系

科目名稱：密碼學

英文科目名稱: Cryptography

學年、學期、學分數：	第三學年、第二學期、3 學分

先修科目或先備能力:基礎數學、程式設計

教學目標：

一、知識：(一)基礎數學模數運算及矩陣
(二)傳統對稱式加密法
(三)代數結構
(四)現代對稱式加密法
(五)資料加密標準
(六)進階加密標準及運用
(七)質數及同餘方程式
(八)非對稱式加密法
(九)訊息完整性及確認性
(十)密碼雜湊及數位簽章
（知識 5/48=10.4%）

二、技能：(一)一般能力：1.數字邏輯及運算
2.使用電腦作業系統
3.邏輯思考、問題分析與解決
(二)專業能力：1.具備程式設計知識
2.具備數學基礎知識
（技能 42/48=87.5%）

三、態度：(一)謹守職業道德
(二)做事細心且有耐心
(三)具備主動積極的學習態度
(四)能夠迎接挑戰並學習解決問題
(五)負責任
（態度 1/48=2.1%）

四、其他：可以勝任資訊安全相關的工作

教材大綱：

單元主題	技能項目	相關知識	教學參考節數	備註
職場倫理個案及課程與教學計畫說明	職場倫理個案及課程與教學計畫說明	職場倫理個案及課程與教學計畫說明(A)	1	

密碼學簡介	熟悉資訊安全機制及攻擊	1.安全目標(K) 2.攻擊(K) 3.服務與機制(K)	2	
基礎數學模數運算及矩陣	熟悉基礎數學	1.整數算數(K) 2.模數算數(K) 3.矩陣及線性同餘(K)	3	
傳統對稱式加密法	熟悉傳統加密法	1.取代加密法(S) 2.換位加密法(S) 3.串流加密法與區塊加 密法(S)	3	
代數結構	熟悉代數運算	1.代數結構(S) 2.GF 體(S)	3	
現代對稱式加密法	熟悉現代對稱加密	1.現代區塊加密法(S) 2.現代串流加密法(S)	3	
資料加密標準	熟悉 DES	1.DES 結構分析(S) 2.多重 DES(S) 3.DES 安全性(S)	6	
進階加密標準及運用	熟悉 AES 及應用	1.AES 介紹(S) 2.加密法運用(S)	6	
質數及同餘方程式	熟悉質數運算	1.質數介紹(S) 2.指數運算與對數運算 (S)	3	
非對稱式加密法	熟悉 RSA 及 ELGamal	1.RSA 密碼系統(S) 2.ELGamal 密碼系統(S)	9	
訊息完整性及確認性	熟悉訊息完整相關作法	1.訊息完整性及確認性介紹(S)	3	
密碼雜湊及數位簽章	熟悉 SHA 與數位簽章機制	1.SHA 介紹(S) 2.數位簽章機制與應用 (S)	6	

1. 教學目標（歸納為四項）：分別為知識（Knowledge）、技能（Skills）、態度其他各一項。
2. 技能項目為表 A8 之任務項目。
3. 單元主題：為各項任務之彙整。
4. 技能項目及相關知識：各該科目應包括之任務及該任務相對應之相關知能，加上補充技能及相關知識（表 A8 中未列，但為達知識或技能的完整性且課程中需教授之能力），撰寫方式係以不含動詞的任務方式呈現。

※三者之關係：教學目標＞單元主題＞技能項目及相關知識。

※本課程將培養核心能力為: 1. 確認、分析和解決問題的能力 2. 具備問題分析與解決能力 3. 具備網路與資訊安全管理能力	
檢核項目	**是否符合**
1.是否將科目名稱、上課時數及學分數填入本 2.是否將教學目標、綱要名稱或單元名稱填入本 3.所填入的行業任務是否有考慮學生學習的順序性、邏輯性、連 貫性、完整 4.除了表 A7 所敘述的行業任務，是否有考慮到其他的任務，以成為一門完整	是回 否口 是回 否口 是回 否口 是回 否口

填表說明:

1.將實習、實驗科目名稱、上課時數及學分數填入本表。

2 依學生學習的順序性、邏輯性、連貫性、完整性等特性將表 A8 中的各該科目應包括之職責填入單元主題，並將該職責之任務及該任務相對應之相關知能分別填入表中的技能項目及相關知識欄中，並擬訂單元名稱並確立教學目標。