

學程描述：

「密碼學」在於概述密碼學及其相關應用的基礎知識。課程內容含蓋數論原理以及相關密碼學相關演算法，包括了：隱藏術、區塊/串流加密、對稱式加密、質數、亂數、因數分解、離散對數、公開金鑰加密、金鑰管理、雜湊函數、數位簽章、以及憑證與相關認證協定。

「資訊與網路安全」課程將介紹網路安全基本觀念及相關技術，並設計相關的實習課程，其課程內容包含網路與資訊安全簡介、電子郵件之安全性、網路基礎知識與防火牆、IP安全機制、無線網路安全機制、Web安全性、入侵偵測與惡意軟體。本課程介紹資訊安全的管理標準、資訊與其風險、資訊安全管理系統的開發與維護、資產和風險管理、人力資源管理、實體環境安全管理、通訊與作業管理、資訊安全事故管理、營運持續管理、內部稽核與管理審查。

課程組合：

必選修	課程編碼	科目名稱	學分	課程群/分類
必修	IEE1005	線性代數	3	1.基礎
必修	IECS3052	密碼學	3	2.進階
必修	IECS4052	資訊與網路安全	3	2.進階
選修	IECS2007	離散數學	3	1.基礎
選修	IECS4075	資安韌性與社會實踐	3	3.應用

取得資格總學分： 9

必修學分數： 9

選修學分數： 0

對應產業類別：

J62	電腦程式設計、諮詢及相關服務業
J63	資訊服務業

學程修課規則：

一、修讀對象/先備知識

本校學士班、進修學士班學生，不開放碩士班以上學生申請。

二、取得微學程的修業規定

(一)取得微學程之最低學分數：9學分，

(二)承認微學程之科目學分

1. 科目名稱或內容相同者，承認學分數不得重複計算。

2. 修習之科目實際學分數超過微學程承認學分數，則以承認學分數計算。如實際學分數低於微學程承認學分數，則以實際學分數計算。

(三)學生修滿規定之科目學分者，得依逢甲大學跨領域學程設置要點第7點規定，經本微學程審查修畢學分確認後，由學校發給微學程證明書。

三、對接專長/能力：資訊科技

四、對接產業類別：電腦程式設計業/入口網站經營業/資料處理、主機及網站代管服務業/其他資訊服務業

職業名稱：資安工程師

可取得證照：CompTIA Security+、EC-Council CEH (Ethical Hacker)、iPAS 資訊安全工程師

五、微學程設置理由

1. 國家需求：建構數位韌性，捍衛國家級資通安全戰略

隨著5G、AI及智慧物聯網的普及，資安威脅已從個人層級演變為影響國家安全與關鍵基礎設施穩定的重大課題。本微學程之設置，旨在響應國家「資安即國安」之戰略方針。完成本微學程的畢業生，不僅具備扎實的密碼學理論，亦掌握網路防禦技術與安全認證協定，未來進入職場能直接為政府機關、國防、金融與能源等關鍵基礎設施建構更具韌性的防禦體系，對提升我國整體資通安全實力與社會經濟發展做出關鍵貢獻。

2. 市場需求：對接企業合規浪潮，填補高階資安人才缺口

隨著全球供應鏈對資訊安全的嚴格要求，國內外法規（如個人資料保護法、上市櫃公司資安主管設置新規、ISO 27001 國際標準等）對企業資安合規的要求達到前所未有的高度。人力市場對於兼具「底層技術防禦（如密碼應用、惡意軟體分析）」與「高層治理合規（如風險管理、ISMS 稽核）」的複合型資安人才求才若渴。本微學程對接科技產業、金融機構、資安顧問公司與政府部門，畢業生具備系統整合與風險審查的即戰力，能有效協助企業跨越合規門檻，解決資安人才嚴重短缺的產業議題。

3. 學術需求：整合技術與管理雙軌，建構跨域新型態資安議題

在傳統大學教育中，資安學科常面臨「技術研發（資工/電子）」與「合規管理（資管/商管）」兩條平行線的斷層，導致學生缺乏全面性的全局思維。本微學程之設置，有效補充並深化了學校現有的資通訊學術學門。我們透過橫向的微學程架構，將偏向數學與底層演算法的「密碼學」，與偏向網路工程、實習防禦及 ISO 管理標準的「資訊與網路安全」有機串聯，打破學科壁壘。從數論基礎、技術攻防到合規稽核，建立起漸進式且知行合一的新型態教學範式，健全校內資訊安全教育架構。

管理單位：資訊電機學院 / 資訊工程學系