國立台灣科技大學 114學年 第2學期　課程大綱

Spring 2026 NTUST Course Outline

授課教師：黃政嘉

Instructor:JHENG-JIA HUANG

課程名稱：可證明安全導論

Course Title：An Introduction to Theory of Provable Security

2026/11/3

課程代號： MI5128701 Course Code 學分數： 3 Credits	必選修：選修/半學年 Required/Electve:Elective/Half Yr. 先修課程： Prerequisites
節次教室： Time/Location	W6(TR-516) W7(TR-516) W8(TR-516)
專業核心能力： Core Professional Competencies	具備解決問題的能力 培養創新與創業的行動力
課程網址： Course Website	
課程宗旨： Course Objectives	將對可證明安全理論進行介紹，在安全協定的設計中可透過可證明安全理論針對所設計之機制進行理論上的安全證明，並將針對不同的證明模型進行介紹，其中包含但不限於RO(random oracle)模型及標準模型。
課程大綱： Outline of Lectures	1. 可證明安全理論簡介 2. 安全協定簡介 3. RO(random oracle)模型方法論與其應用 4. 標準模型的應用 5. 相互認證的可證明安全理論
授課方式： Method of Instruction	講授 Lecture：% 分組討論 Group discussion：% 案例研討 Case study：% 操做練習 Practical exercises：% 講授 Lecture：%
教科書： Textbooks	
參考書目： References	
修課須知： Notice	
評量方式： Grading	
備註說明： Notes	