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：林佳志

Instructor:Chia-Chih Lin

課程名稱：資訊安全導論

Course Title：Introduction to Information Security

2026/11/3

課程代號： CS4003701 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： W7(TR-409-1) W8(TR-409-1) W9(TR-409-1) Time/Location	
專業核心能力： Core Professional Competencies	
課程網址： Course Website	
課程宗旨： Course Objectives	1、網路安全威脅2、如何使網路更加安全？3、密碼理論4、傳統式和公開式密碼5、密碼應用技術和實例 6、公開金鑰基礎建設(PKI)7、IP Security (IPSec)8、虛擬私有網路(VPN)9、智慧卡(Smart Card)和資訊安全應用 1. Classical Encryption Techniques 2. Block Ciphers and the Data Encryption Standard 3. Basic Concepts in Number Theory and Finite Fields 4. Advanced Encryption Standard 5. Block Cipher and Stream Ciphers 6. Pseudorandom Number Generation 7. More Number Theory 8. Public-Key Cryptography and RSA 9. Other Public-Key Cryptosystems 10. Cryptographic Hash Functions 11. Message Authentication Codes 12. Digital Signatures 13. Key Management and Distribution
課程大綱： Outline of Lectures	1、網路安全威脅2、如何使網路更加安全？3、密碼理論4、傳統式和公開式密碼5、密碼應用技術和實例 6、公開金鑰基礎建設(PKI)7、IP Security (IPSec)8、虛擬私有網路(VPN)9、智慧卡(Smart Card)和資訊安全應用
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