113-1 科技新知講座心得

日期: 113/12/10

系所: 電子工程系

學號: B11013039

姓名: 柯龍宇

主題: 資訊安全

摘要（至少 100 字）:
此次演講主題為「資訊安全」，涵蓋了對稱與非對稱加密的基礎知識，包括古典密碼學如凱撒密碼、維吉尼亞密碼，以及現代加密技術如AES和DES。並介紹了流加密、分組加密模式及其應用。此外，還討論了加密技術在數據隱私保護中的重要性。

心得（至少 300 字）:
此次演講深入淺出地介紹了密碼學的核心概念與應用，讓我對數據安全有了更全面的理解。首先，通過古典密碼學的介紹，我深刻體會到加密技術從簡單規則到複雜算法的進化歷程。凱撒密碼與維吉尼亞密碼展示了早期如何透過字母位移和密碼表實現基本的信息隱藏。接下來，現代密碼學的部分尤其令人印象深刻，例如AES加密的五大核心組件（Key Expansion、Add Round Key、Sub Bytes等），不僅展示了數據分組加密的複雜性，還揭示了其在現代信息安全中的應用價值。講者還提到了CTR等分組加密模式，讓我更了解實際加密技術如何應對不同場景需求。此外，對流加密算法如RC4及eSTREAM的討論顯示出其在實時數據加密中的效率。最後，演講也強調了數據隱私的重要性。