密碼系統的安全性

- 密碼系統的真實情況
  - 密碼演算法必須是公開的
  - 明文格式是無法隱藏的
  - 密文是唾手可得的
- 密碼系統的觀念
  - 鑰匙功能：『印章』
  - 鑰匙是可破解的
  - 鑰匙的曝光率

密碼的破解技巧

- 密碼的破解技巧一：統計分析技巧
  - 只知密文破解
  - 已知明文破解
  - 選擇明文破解
  - 選擇密文破解
- 技巧二：暴力攻擊法 **(Brute-Force Attack)**
  - 嘗試各種可能出現的鑰匙

密碼破解因素

- 『計算上的安全』(Computationally Secure)
  - 破解密碼所需的成本是否合乎該訊息的價值
  - 破解密碼所需的時間是否超過該鑰匙的壽命
- 演算法的複雜度
  - 混淆：密文與鑰匙之間的複雜度。
    - 同一把鑰匙，加密不同明文，之間的密文相似度越低越好。
  - 擴散：明文與密文間的複雜度。
    - 同一筆明文，被不同鑰匙加密後，之間的密文相似度越低越好。