傳統密碼系統的基本原理

- 現代密碼學(下一章介紹)
- 傳統密碼學的基本原理
  - 字元加密/解密技巧：
    - 換位加密法 (Transposition Cipher)
      - 將原明文(以字元為單位)位置重新排列成密文。
      - 解密時，再依相關位置回復原狀。
      - 關鍵(key)：需要一套換位規則。
    - 取代加密法 (Substitution Cipher)
      - 將原明文(以字元為單位)，由另一個字元取代。
      - 關鍵(key)：需要一只取代表。