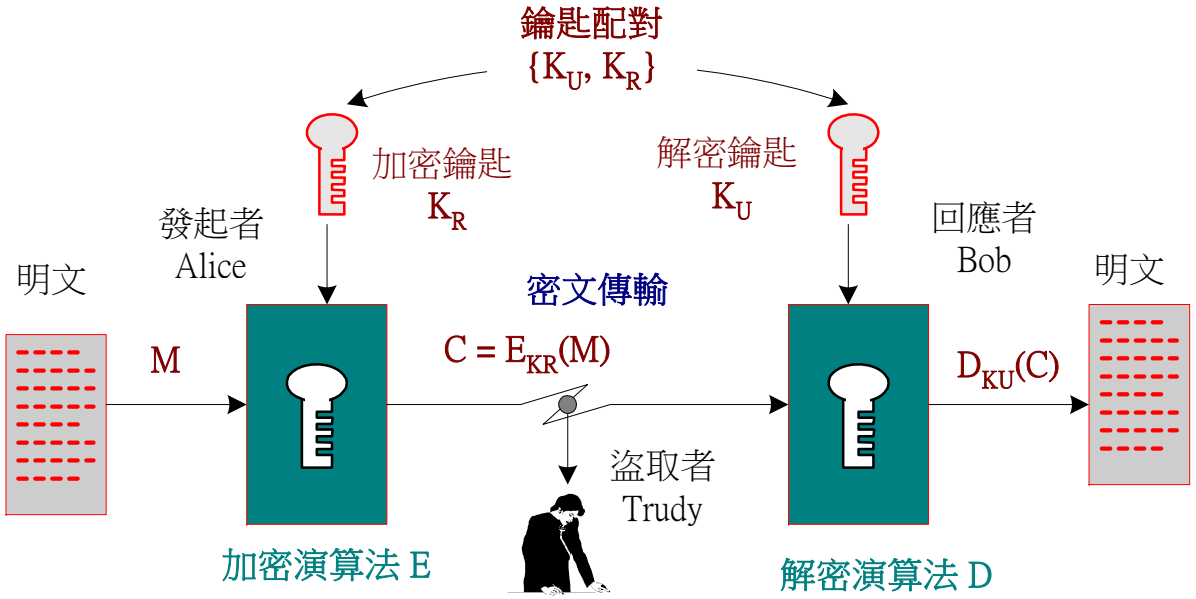
公開鑰匙系統簡介

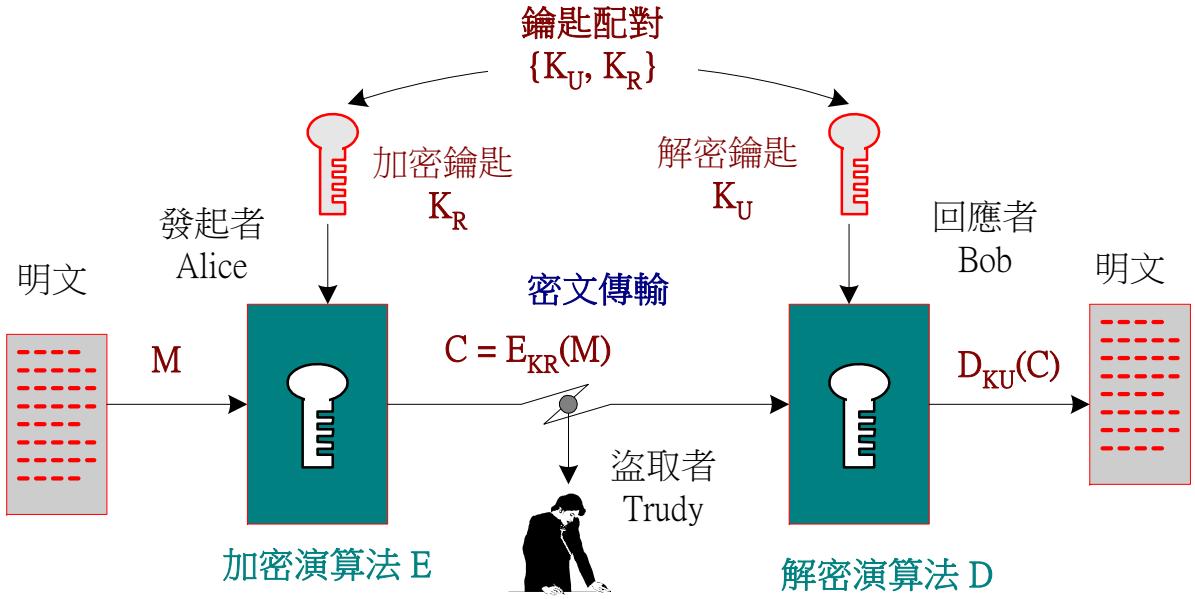
公鑰系統架構 (Public-key Cryptosystem)

- 1976 年 Diffie-Hellman 暗門函數觀念
- E：加密演算法、D：解密演算法、P：明文
  1. D(E(P)) = P
  2. 由 E 很難推演出 D
  3. E 不會被選定明文攻擊法破解



公開鑰匙系統簡介

- **1978 年 Rivest 、Shamir 與 Adleman (RSA) 提出公開鑰匙架構**
  - 每一使用者都有兩把鑰匙，一把加密，另一把則解密。
  - 兩把鑰匙：
    - **公開鑰匙 (Public Key)**
    - **私有鑰匙 (Private Key)**
  - 通訊雙方至少持有對方的一把鑰匙。



公開鑰匙系統的演算法

- 『數論』(Number Theory) 推導出來
  - RSA 演算法 (本章介紹)
  - 橢圓曲線密碼學 (Elliptic Curve Cryptographic, ECC) (本書未介紹)
  - Diffie-Hellman 演算法 (本章介紹)
  - 數位簽章標準 (Digital Signature Standard, DSS) (第七章介紹)
  - ElGamal 演算法 (本書未介紹)