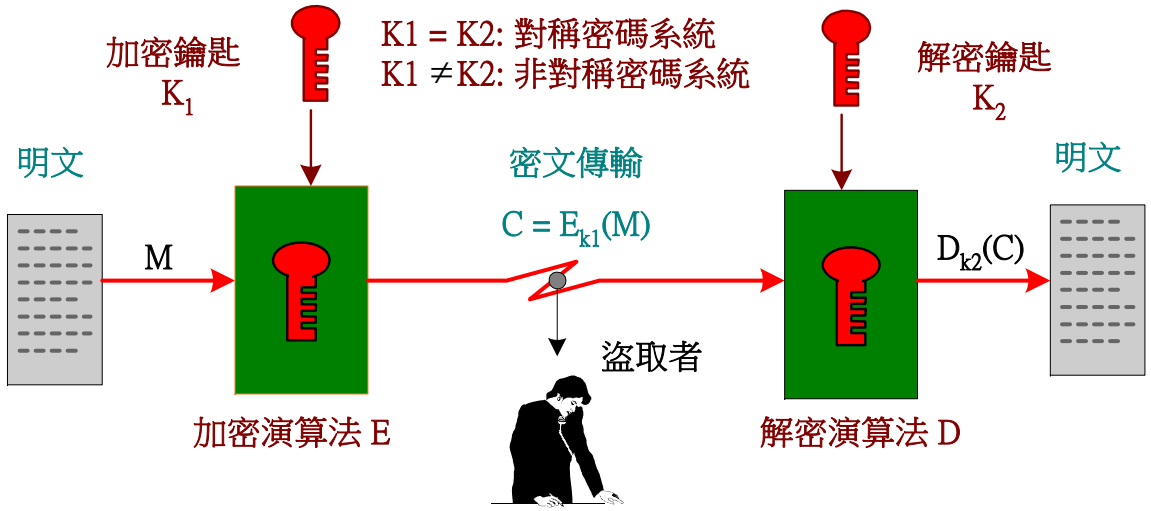
密碼系統概論(1)

- **Cryptography, 密碼學定義：**
  - **"kryptos" 與 "grphein" 為『位置混排處理』**
  - 加密動作 **(Enciphering)**
  - 解密動作 **(Deciphering)**
  - 密碼系統 **(Cryptosystem)**



密碼系統概論(2)

- 加密與解密的運作程序：
- 變數定義：
  - M = 明文 、C = 密文 、K_1 = 加密鑰匙，K_2 = 解密鑰匙
  - E = 加密演算法 、D = 解密演算法
- 運作程序：
  - 加密運作：$C = EK_1(M)$ 、解密運作：$M = DK_2(C) = DK_2(EK_1(M))$