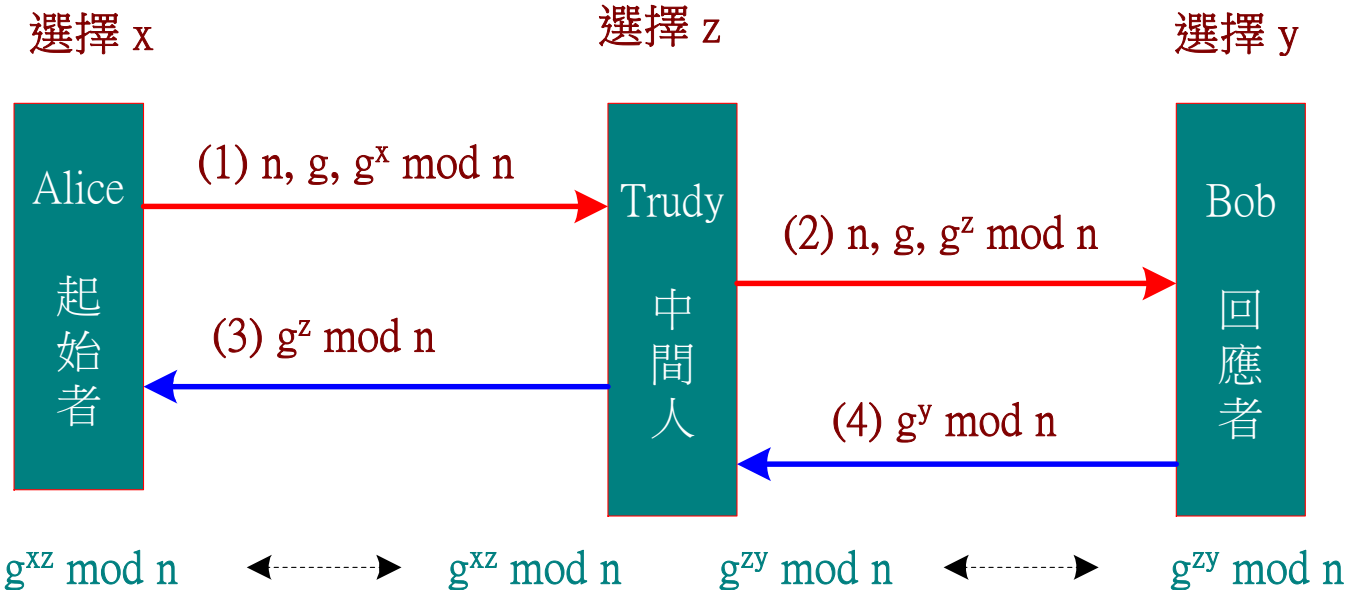
DH 中間人攻擊

- 中間人攻擊 (Man-in-the-middle Attack)
  - Trudy 為中間人
- 防禦中間人攻擊
  - 公開 Diffie-Hellman 參數
  - 認證的 Diffie-Hellman 參數