1.

(1). 檢查所有可能的 x 值 {0,1,2,3,4,5,6}

$0^2 \equiv 0 \pmod 7$

$1^2 \equiv 1 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$4^2 \equiv 2 \pmod 7$

$5^2 \equiv 4 \pmod 7$

$6^2 \equiv 1 \pmod 7$

⇨ x = 2 & x =5

(p-1) / 2 = 3 個

$a^{(p-1)/2} = 4^3 = 64 \pmod 7 \equiv 1$ => 有解

4 在 Z_7 is QR

(2). 檢查所有可能的 x 值 {0,1,…,16}

$0^2 \equiv 0 \pmod{17}$

$1^2 \equiv 1 \pmod{17}$

$2^2 \equiv 4 \pmod{17}$

$3^2 \equiv 9 \pmod{17}$

$4^2 \equiv 16 \pmod{17}$

$5^2 \equiv 8 \pmod{17}$

$6^2 \equiv 2 \pmod{17}$

$7^2 \equiv 15 \pmod{17}$

$8^2 \equiv 13 \pmod{17}$

$9^2 \equiv 13 \pmod{17}$

$10^2 \equiv 15 \pmod{17}$

$11^2 \equiv 2 \pmod{17}$

$12^2 \equiv 8 \pmod{17}$

$13^2 \equiv 16 \pmod{17}$

$14^2 \equiv 9 \pmod{17}$

$15^2 \equiv 4 \pmod{17}$

$16^2 \equiv 1 \pmod{17}$

⇨ 無解，因為上述可以看到無人 mod 結果為 12

$a^{(p-1)/2} = 12^8 = 16 \pmod 7$ => 無解

2.

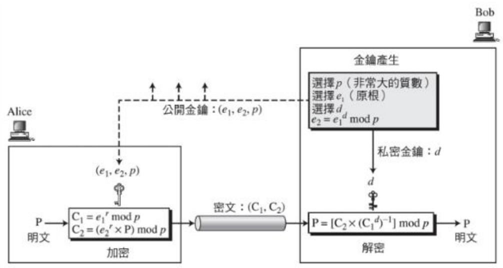
大致架構:

在 ElGamal 密碼系統中的加密或解密位元運算複雜度是多項式型態的。

1.密鑰生成

2.加密

3.解密



效能：加密和解密的主要計算是模指數運算，其計算量與模 p 的大小成對數關係。

密文長度：每個消息 mmm 加密後的密文為(c1,c2)，即兩個元素，每個元素的長度與模數的長度相同。

安全性：若希望 ElGamal 密碼系統是安全的，p必須至少 300 位數字，而且對每一次加密，r都必須採用一個全新的數值。

3.

安全性比較

RSA:

安全性基於大數分解問題。要破解 RSA，必須能有效分解 n=pq

分解的關係：

➔ 如果能分解 n，則可以計算出私鑰，從而破解 RSA

➔ 如果可以破解 RSA，即可以找到私鑰，那麼也就可以分解 n

Rabin:

安全性基於平方剩餘問題。Rabin 加密系統是基於 x^2 mod n 的困難性

分解的關係：

➔ 如果能分解 n，則可以解平方剩餘問題，從而破解 Rabin 加密系統

➔ 如果可以破解 Rabin 加密系統，可解平方剩餘問題，那麼也就可以分解 n

主要差別:

Rabin 加密系統的安全性等同於大數分解問題，他在理論上比 RSA 更安全，因為破解 Rabin 加密系統直接意味著可以分解大數

RSA 的安全性依賴於選擇的指數，並不直接等同於大數分解問題，這使得其安全性更難以形式化

4.

相同:

基於數學難題：

這三種數位簽章方法都依賴於數學難題來保證安全性。RSA 依賴於大數因數分解的難題，ElGamal 和 Schnorr 則依賴於離散對數問題的難解性。

用於認證：

這三種方法都用於數位簽章，主要目的是認證數位訊息的真實性和完整性。

公私鑰體系：

所有這些方法都使用公私鑰體系。簽章者使用私鑰生成簽名，驗證者使用公鑰驗證簽名。

相異:

設計原理：

RSA：基於大數因數分解問題。

ElGamal：基於離散對數問題。ElGamal 簽名方案是一種隨機化的簽名算法。

Schnorr：基於離散對數問題。

簽章&驗證流程：

RSA：簽名過程是使用私鑰對消息的 hash 進行加密。

ElGamal：簽名過程涉及計算多個值並使用隨機數來生成簽名，驗證過程則涉及到原消息與簽名值的計算結果比對。

Schnorr：簽名過程包括生成隨機值並計算簽名值，驗證過程則需要驗證方對簽名和消息進行一些模運算和比對。

效率：

RSA：涉及大數的模指數運算。

ElGamal：簽名過程涉及多個模運算，但簽名結果較長。驗證過程也比較複雜。

Schnorr：通常效率較高，計算量相對較小。

安全性：

RSA：安全性依賴於大數因數分解的難度。

ElGamal：若隨機數不夠隨機，可能導致安全性問題。

Schnorr：在抵禦某些攻擊例如選擇消息攻擊有較強的安全性。

5.

ElGamal

- **驗證：**
  - 假設 Bob 欲驗證 Alice 的簽章是否有效
  - Bob 透過明文 m 與數位簽章 (r,s) 檢查 $e_1^m \mathrel{?}\equiv e_2^r r^s \pmod p$

Schnorr

- **驗證：**
  - 假設 Bob 欲驗證 Alice 的簽章是否有效
  - 步驟一：Bob 求出 $t' = g^s y^r \bmod p$
  - 步驟二：Bob 檢查 $H(t', m) \mathrel{?}= r$
  - 如果該式滿足，則 (r,s) 為 m 的合法數位簽章

DSA

- **驗證：**
  - 假設 Bob 欲驗證 Alice 的簽章是否有效
  - 步驟一：Bob 檢查 r 和 s 是否均屬於 $[0,(q-1)]$，如果不是，則表示 (r,s) 非簽章
  - 步驟二：Bob 計算 $t = s^{-1} \bmod q$
  - 步驟三：Bob 計算 $r' = \left[\left(g^{H(m)t}\right) y^{rt} \bmod p\right] \bmod q$
  - 如果 $r' = r$，則 (r,s) 為 m 的合法數位簽章