1.

(1). 檢查所有可能的 x 值 {0,1,2,3,4,5,6}

02 ≡ 0 (mod 7) (p-1) / 2 = 3個

12 ≡ 1 (mod 7) a(p-1)/2 = 43 = 64 (mod 7) ≡ 1 => 有解

22 ≡ 4 (mod 7) 4在Z7 is QR

32 ≡ 2 (mod 7)

42 ≡ 2 (mod 7)

52 ≡ 4 (mod 7)

62 ≡ 1 (mod 7)

* x = 2 & x =5

(2). 檢查所有可能的 x 值 {0,1,…,16}

02 ≡ 0 (mod 17)

12 ≡ 1 (mod 17) a(p-1)/2 = 128 = 16 (mod 7) => 無解

22 ≡ 4 (mod 17)

32 ≡ 9 (mod 17)

42 ≡ 16 (mod 17)

52 ≡ 8 (mod 17)

62 ≡ 2 (mod 17)

72 ≡ 15 (mod 17)

82 ≡ 13 (mod 17)

92 ≡ 13 (mod 17)

102 ≡ 15 (mod 17)

112 ≡ 2 (mod 17)

122 ≡ 8 (mod 17)

132 ≡ 16 (mod 17)

142 ≡ 9 (mod 17)

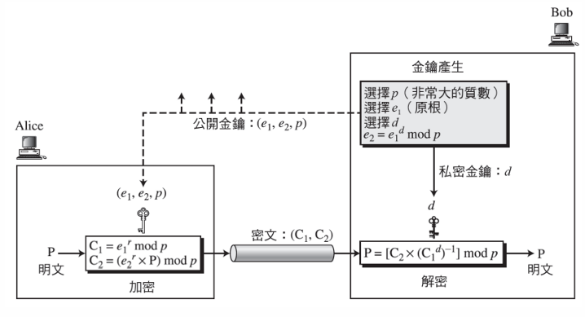
152 ≡ 4 (mod 17)

162 ≡ 1 (mod 17)

* 無解，因為上述可以看到無人mod結果為12

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 x2 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：

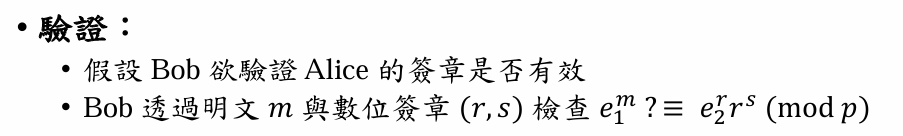
RSA：安全性依賴於大數因數分解的難度。

ElGamal：若隨機數不夠隨機，可能導致安全性問題。

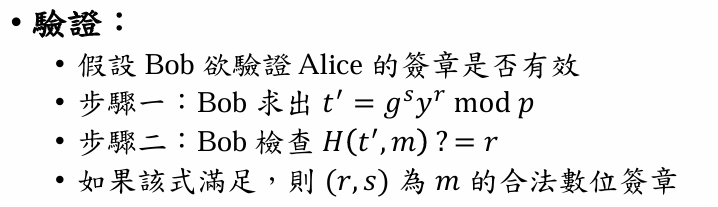
Schnorr：在抵禦某些攻擊例如選擇消息攻擊有較強的安全性。

5.

ElGamal



Schnorr



DSA

