112 學年下學期 資訊安全與密碼學第五次作業

繳交方式：紙本及電子檔都要。作業的手寫題請附過程，上傳的電子檔請依以下方式命名：「HW05_學號_姓名」。
繳交時間：6/12 下午 5:00 前，遲交一周內 7 折，逾一周不計分。
繳交地點：紙本請至理學大樓 922B 繳交。

1. (12%) (二次剩餘) 請找出下列二次剩餘方程式的解，若無解請說明理由。
   (1) $x^2 \equiv 4 \pmod 7$
   (2) $x^2 \equiv 12 \pmod{17}$

2. (16%) (公鑰系統) 請試著描述機率式公鑰密碼系統 ElGamal 整個演算法的架構，並分析其加解密效能、密文長度與安全性。

3. (24%) (公鑰系統) RSA 與 Rabin 安全性差別為何？(請試著解說詳細一點)
   若欲證明某 A 機制難度等於分解因數，必須讓下列兩點成立：
   (1) 若能分解因數，則某 A 機制可破。
   (2) 若某 A 機制可破，則可分解因數。
   可根據(1)(2)來試著說明 RSA 和 Rabin 安全性的差別。

4. (30%) (數位簽章) 試比較「RSA」、「ElGamal」與「Schnorr」三種數位簽章方法的相異處與相同處？

5. (18%) (數位簽章) 請就「ElGamal」、「Schnorr」與「DSA」三種數位簽章方法的驗證部份證明其正確性。