

## 112 學年下學期 資訊安全與密碼學第一次作業

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：「HW01\_學號\_姓名」。

繳交時間：3/27 下午 5:00 前。遲交一週內 7 折，逾一週不計分。

1. Let  $\gcd(a, b) = s \times a + t \times b$ . Please find  $(s, t)$ ? (6% each)
  - (1)  $\gcd(179, 17)$
  - (2)  $\gcd(229, 119)$
  - (3)  $\gcd(359, 78)$
  - (4)  $\gcd(487, 157)$
  
2. Find the following multiplicative inverse of  $\alpha$  in  $Z_n$ . If there is no solution found, please explain why. (6% each)
  - (1)  $\alpha = 7, n = 31$
  - (2)  $\alpha = 11, n = 29$
  - (3)  $\alpha = 31, n = 199$
  - (4)  $\alpha = 27, n = 666$
  
3. Find the solutions for the following remainder equations. If there is no solution found, please explain why. (10% each)
  - (1)  $4x - 19 \equiv 6 \pmod{29}$
  - (2)  $8x + 7 \equiv 4 \pmod{17}$
  - (3)  $10x - 1 \equiv 4 \pmod{23}$
  - (4)  $7x \equiv 2 \pmod{31}$
  - (5) 
$$\begin{cases} 2x \equiv 4 \pmod{7} \\ 9x \equiv 5 \pmod{8} \end{cases}$$