112 學年下學期 資訊安全與密碼學第三次作業

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：「HW03_學號_姓名」。
繳交時間：4/24 下午 5:00 前。遲交一周內 7 折，逾一周不計分。

1. (30%) 請求出所有 G 的循環子群
   (1) $G = \langle Z_{6^*}, \times \rangle$
   (2) $G = \langle Z_{12^*}, \times \rangle$
   (3) $G = \langle Z_{14^*}, \times \rangle$

2. (30%) Which of the following is a ring and which is a field? Please explain your answer.
   (1) $\langle \mathbb{Z}, +, \times \rangle$
   (2) $\langle \mathbb{R}, +, \times \rangle$
   (3) $\langle \{e, g, g^2, \ldots, g^{n-1}\}, +, \times \rangle$ where $g^n = e$

3. (18%) 請求出在 $GF(2^8)$ 下，$a(x) = x^7 + x + 1$ 在模 $m(x)$ 下的乘法反元素，其中不可分解多項式 $m(x) = x^8 + x^7 + x^3 + x + 1$。

4. (12%) 請計算在 $GF(2^5)$ 下，$(x^3 + x + 1) \otimes (x^4 + x^2)$ 的結果，其中不可分解多項式為 $x^5 + x^2 + 1$。

5. (10%) 請找出多項式 $x^6 + x^3 + 1$ 所代表的 7 位元字組。