Homework 04 Report

- B10609038 邱彥誠

建置環境

Visual Studio 2017, 使用 C++ 語言編譯.

Include Library: iostream; string; sstream;

專案內檔案(to compile): Main.cpp; RSA.h; RSA.cpp;

操作方式

1. 先輸入模式, 請輸入單個小寫英文字母 ‘k’, ‘e’, 或‘d’.
   k 代表輸出本程式使用的所有金鑰.
   e 代表加密一段原文.
   d 代表解密一段密文.
2. 當輸入 e 或 d 之後需要將原文或密文輸入進去.
3. 會以本程式的金鑰輸出加解密後的文字, 本程式的密文以整數數字輸出. 同時也須以整數數字輸入(同輸出即可).
4. 程式會不斷執行, 若要離開程式可在輸入 mode 時輸入其他文字即可跳出.

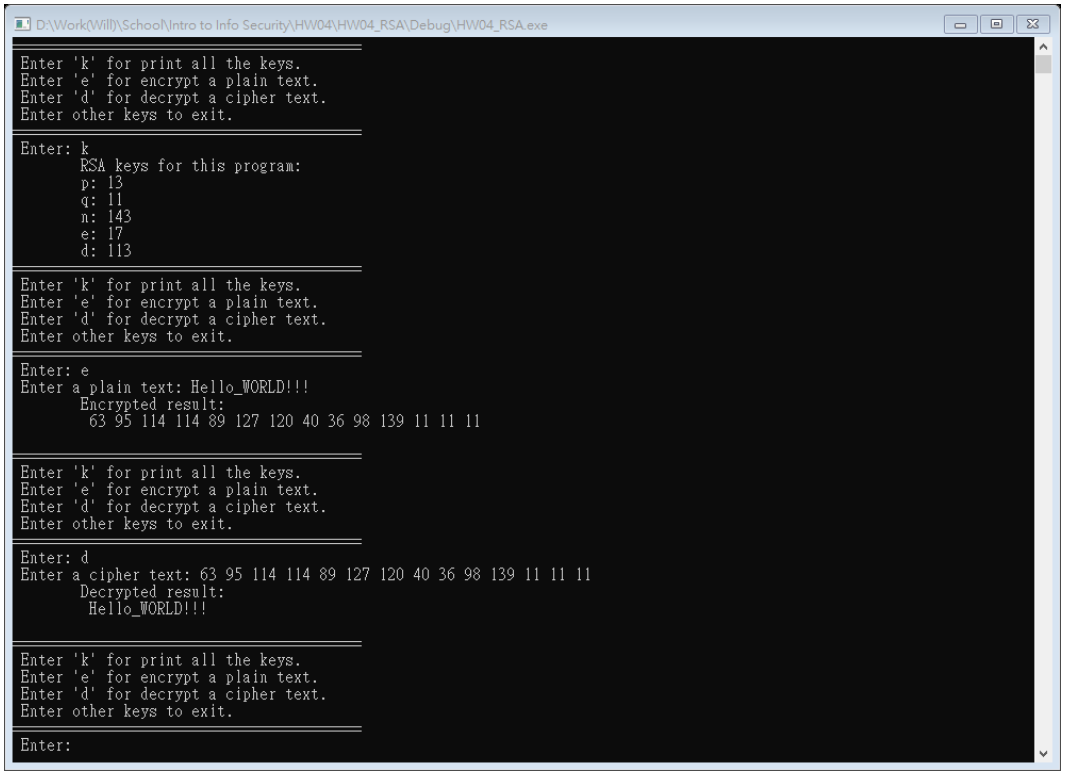
程式碼解說

- 程式起始點在 Main.cpp, 主要加解密程式碼在 RSA.cpp.
- 本程式僅使用小數字金鑰的加密方式, 金鑰於程式碼內 predefined.

  p:13, q:11, n = p*q = 143, e = 17, d = e^{-1} = 113 (mod 120)

  採用此金鑰僅是為了滿足輸入需求: (ascii 0x21 ~ 0x7A)

執行結果圖: (plain text: Hello_WORLD!!!)



遇到的困難與心得

這次僅做了小數字的加密, 所以比較簡單, 最麻煩的是其實 keys 都是自己找的, 因為要能夠滿足 ascii 0x21 ~ 0x7A 的輸入需求, 所以找了剛好能勉強符合範圍的數字.