Problem 1

(a)
直接執行RNG.py即可，程式主要用Python內建的secrets函式庫的token_bytes()函式提供1M bytes(1024^2 bytes)長度的cryptographically secure random numbers，並將其存至random.bin

RNG.py > ...

```python
import secrets

random_bytes = secrets.token_bytes(1024*1024)

with open("random.bin", "wb") as f:
    f.write(random_bytes)
```

(b)
在Ubuntu環境中下載並架好NIST SP 800-22 statistical test後，輸入 ./assess 8388608
這裡的8388608是指一個序列有多少bit(1M bytes = 1024 * 1024 * 8 bits = 8388608 bits)

```
sky@ubuntu20:~/sts-2.1.2$ ./assess 8388608
          G E N E R A T O R    S E L E C T I O N
          ---------------------------------------

     [0] Input File                 [1] Linear Congruential
     [2] Quadratic Congruential I   [3] Quadratic Congruential II
     [4] Cubic Congruential         [5] XOR
     [6] Modular Exponentiation     [7] Blum-Blum-Shub
     [8] Micali-Schnorr             [9] G Using SHA-1

    Enter Choice:
```

接下來就是將輸入指定random.bit並調設定，基本上參考助教範例

```
            User Prescribed Input File: random.bin

            S T A T I S T I C A L   T E S T S
            _________________________________

 [01] Frequency                       [02] Block Frequency
 [03] Cumulative Sums                 [04] Runs
 [05] Longest Run of Ones             [06] Rank
 [07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
 [09] Overlapping Template Matchings  [10] Universal Statistical
 [11] Approximate Entropy             [12] Random Excursions
 [13] Random Excursions Variant       [14] Serial
 [15] Linear Complexity

      INSTRUCTIONS
         Enter 0 if you DO NOT want to apply all of the
         statistical tests to each sequence and 1 if you DO.

Enter Choice: 1
```

```
      P a r a m e t e r   A d j u s t m e n t s
      -----------------------------------------
  [1] Block Frequency Test - block length(M):         128
  [2] NonOverlapping Template Test - block length(m): 9
  [3] Overlapping Template Test - block length(m):    9
  [4] Approximate Entropy Test - block length(m):     10
  [5] Serial Test - block length(m):                  16
  [6] Linear Complexity Test - block length(M):       500

 Select Test (0 to continue): 1

 Enter Block Frequency Test block length: 65536

      P a r a m e t e r   A d j u s t m e n t s
      -----------------------------------------
  [1] Block Frequency Test - block length(M):         65536
  [2] NonOverlapping Template Test - block length(m): 9
  [3] Overlapping Template Test - block length(m):    9
  [4] Approximate Entropy Test - block length(m):     10
  [5] Serial Test - block length(m):                  16
  [6] Linear Complexity Test - block length(M):       500

 Select Test (0 to continue): 0

 How many bitstreams? 1
```

等待Testing跑完後就會生成finalAnalysisReport.txt

```
  Enter Block Frequency Test block length: 65536

       P a r a m e t e r   A d j u s t m e n t s
       ----------------------------------------
    [1] Block Frequency Test - block length(M):         65536
    [2] NonOverlapping Template Test - block length(m): 9
    [3] Overlapping Template Test - block length(m):    9
    [4] Approximate Entropy Test - block length(m):     10
    [5] Serial Test - block length(m):                  16
    [6] Linear Complexity Test - block length(M):       500

  Select Test (0 to continue): 0

  How many bitstreams? 1

  Input File Format:
    [0] ASCII - A sequence of ASCII 0's and 1's
    [1] Binary - Each byte in data file contains 8 bits of data

  Select input mode:  1

     Statistical Testing In Progress.........

     Statistical Testing Complete!!!!!!!!!!!!
```

打開來看一下，應該沒什麼問題

```
sky@ubuntu20:~/sts-2.1.2$ cat experiments/AlgorithmTesting/finalAnalysisReport.t
xt
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <random.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
  0   0   0   0   0   1   0   0   0   0     ----       1/1       Frequency
  0   0   0   1   0   0   0   0   0   0     ----       1/1       BlockFrequency
  0   0   0   0   1   0   0   0   0   0     ----       1/1       CumulativeSums
  0   1   0   0   0   0   0   0   0   0     ----       1/1       CumulativeSums
  0   0   0   0   1   0   0   0   0   0     ----       1/1       Runs
  0   0   0   0   0   0   0   0   1   0     ----       1/1       LongestRun
  0   0   0   1   0   0   0   0   0   0     ----       1/1       Rank
  0   0   0   1   0   0   0   0   0   0     ----       1/1       FFT
  0   0   0   0   0   0   1   0   0   0     ----       1/1       NonOverlappingT
emplate
```

```
  0   0   0   0   1   0   0   0   0   0     ----      1/1       RandomExcursion
sVariant
  0   0   0   0   0   0   0   0   0   1     ----      1/1       RandomExcursion
sVariant
  0   0   0   0   0   0   0   1   0   0     ----      1/1       RandomExcursion
sVariant
  0   0   0   0   1   0   0   0   0   0     ----      1/1       RandomExcursion
sVariant
  0   0   1   0   0   0   0   0   0   0     ----      1/1       Serial
  0   1   0   0   0   0   0   0   0   0     ----      1/1       Serial
  0   0   1   0   0   0   0   0   0   0     ----      1/1       LinearComplexit
y


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0 for a
sample size = 1 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately = 0 for a sample size = 1 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
```