

# Final Project Requirement



Balance You  
2020/12/10

# IPR Notice

---

**All rights, titles and interests contained in this information, texts, images, figures, tables or other files herein, including, but not limited to, its ownership and the intellectual property rights, are reserved to PUFsecurity. This information may contain privileged and confidential information. Any and all information provided herein shall not be disclosed, copied, distributed, reproduced or used in whole or in part without prior written permission of PUFsecurity Corporation.**

**Date :  
1/7/2021**

**Report time:  
20-25 mins**

**1**

**Final Project Task**

**2**

**Project Content**

**3**

**Tips**

# Task – Pre-work

---

- Build an environment for NIST statistical test suite
  - Virtual machine with Ubuntu OS
- Download the test suite
  - [Test Suite](#)
  - Read README.md and Chapter 5 in [NIST SP800-22 document](#) to learn how to use the suite
- Study the document of NIST SP800-22 to know
  - Proper Input data size
  - Proper setting for parameters

# Task – Input Data Size and Parameters Setting

---

- Input data size
  - Check the Input Size Recommendation in each test in Chapter 2
  - Check Chapter 4.2.2
- Parameters Setting
  - Check the Input Size Recommendation in each test in Chapter 2
- Check Chapter 4.3 (d) and (f)

# Task – Analyze TRNG data with Test Suite

---

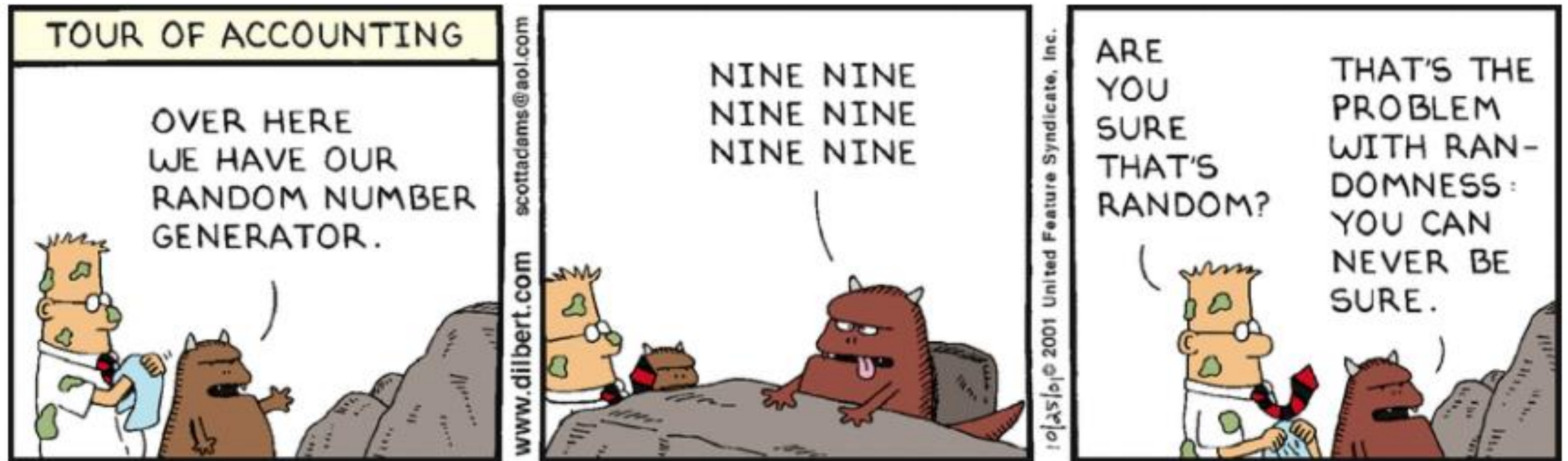
- Collect TRNG data with  $100 \cdot Y \cdot X$  bits
  - X: size of a bitstream(sequence)  
\*should satisfy the minimum size for all test
  - Y: number of bitstreams(sequences)
- You should at least get 100 files with  $Y \cdot X$  bits of random number in each file
- Analyze these files with test suite and check the pass rate
  - Compare your pass rate with the ideal one and the pass rate in Table III in the paper: <https://ieeexplore.ieee.org/document/7016926>

# Project content

---

- How do you choose your input data size and parameter setting?
- What is the pass rate of your 100 random number files?
- Observing “finalAnalysisReport.txt”, find which test fails mostly
  - Try to explain with the result of test and the paper below  
*“Study on the Pass Rate of NIST SP800-22 Statistical Test Suite”*
- How do you judge the TRNG you used in this course?
  - Under the knowledge of “null hypothesis” (NIST document Chapter 1) and the paper you studied

# Random?





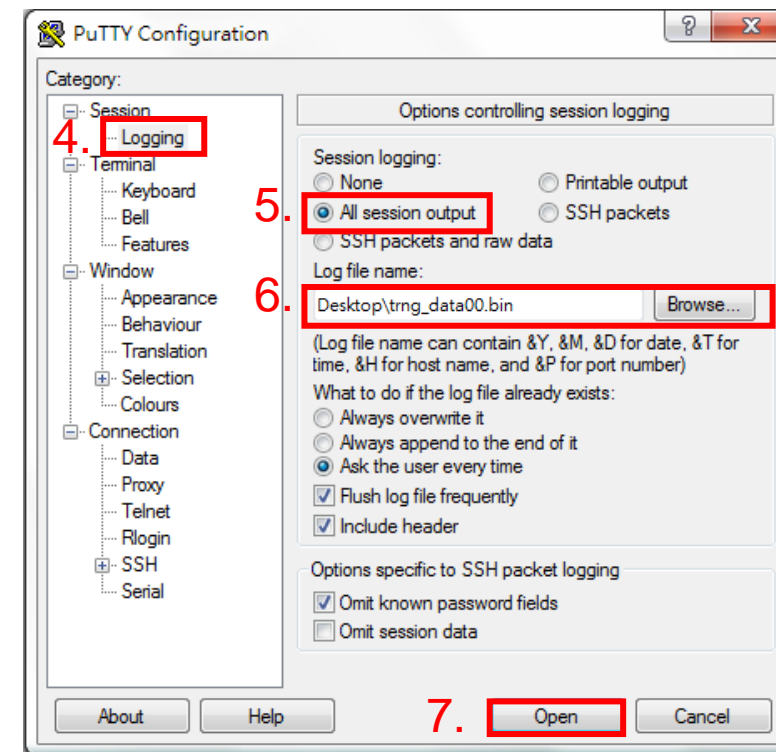
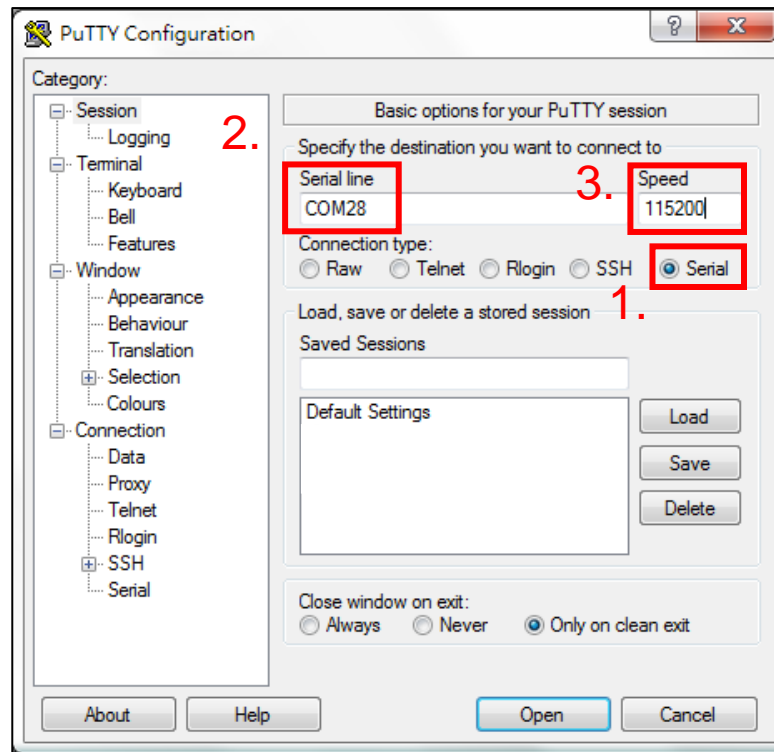
# Tips – Store data into file with PUTTY (1/3)

---

- To accelerate data collection, you can change the baud rate of DUE from “9600” to “115200”
- Output the 8-bit random number (outputdata) in binary format:
  - `Serial.write((outputdata&0xFF));`
- Program your code for RN collection into the DUE w/o testchip and open serial monitor to check the operation
- Keep pressing “Reset” button on **DUE** and setting PUTTY to store data into file
- PUTTY download:
  - <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

# Tips – Store data into file with PUTTY (2/3)

- Close serial monitor
- Set PUTTY with DUE port

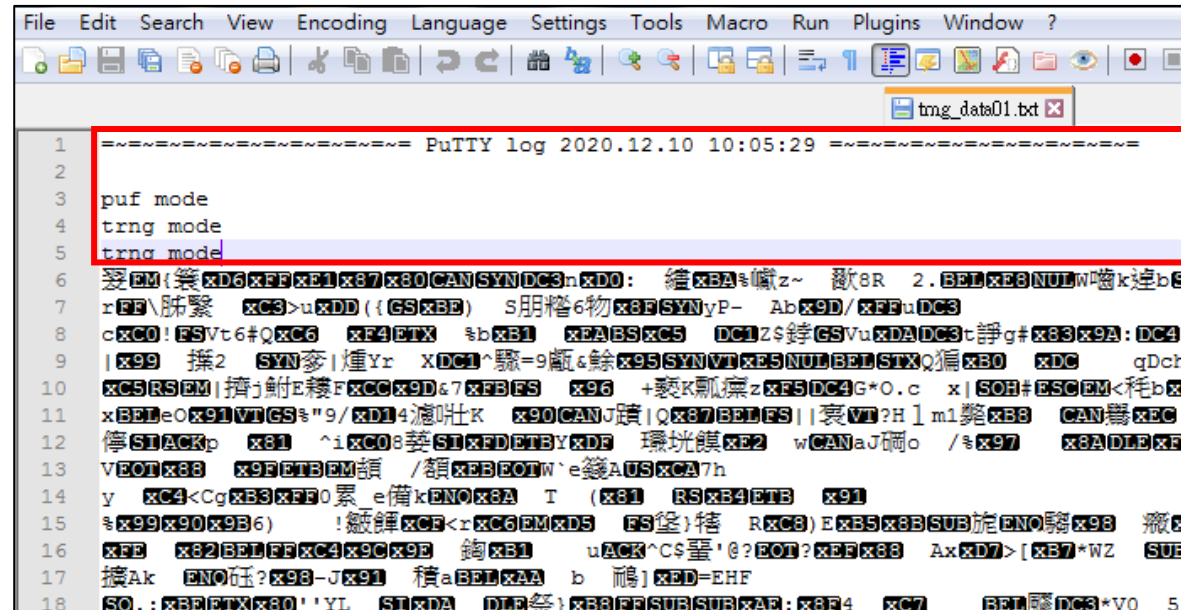


File name:  
XXX.bin

8. Release  
Reset button

# Tips – Store data into file with PUTTY (3/3)

- Delete the header and debug message from the data file



```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
tmng_data01.txt x
1 ===== PuTTY log 2020.12.10 10:05:29 =====
2
3 puf mode
4 trng mode
5 trng mode
6 娑EM{策XD6XFBXB1X87X80CANSYND3nXD0: 縉XBA%幟z~ 歡8R 2.BE1XEBNULW嚙k連bSI
7 rFE\肺繫 XC3>uXDD({GSXBE) S朋稽6物X8BSYNyP- AbX9D/XFBuDC3
8 cXC0!FSVt6#QXC6 XF4ETX %bXB1 XEABSC5 DC1Z$銑GSVuXDA DC3t諍g#X83X9A:DC4[
9 |X99 撰2 SYN麥|燿Yr XDC1^驟=9甌&餘X95SYNVTXESNULBELSTXQ編XB0 XDC qDch[
10 XC5RSEM|擠j鮒E縹FCCX9D&7XFBFS X96 +褻K瓢瘰zXESDC4G*O.c x|SOH#ESCEM<耗bXC
11 xBELeOx91VTGS%"9/XD14滄壯K X90CANJ讀|QX87BELFS||衰VT?H l m1癸XB3 CAN嚮XEC
12 停SIACKp X81 ^iXC08葵SIXFDETBXKDE 環坑縹XE2 wCANaJ礪o /%X97 X8ADLEXF0
13 VEOTX88 X9SETBEM讀 /縹XEBEOTW`e縹AUSXCA7h
14 y XC4<CgXB3XFF0累 e備kENOX8A T (X81 RSXB4ETB X91
15 %X99X90X9B6) !縹縹XCF<rXC6EMXD5 ES堡)縹 RXC8)EXB5X8BSUB旋ENO縹X98 癸XE
16 XFE X82BELFFXC4X9CX9E 鉤XB1 uACK^CS璽'@?EOT?XEFX88 AxXD7>[XB7*WZ SUB
17 縹Ak ENO旺?X98-JX91 縹aBELXAA b 鵠]XED=EHF
18 SO.:XBEITXIX80''YL SIXDA DLE縹;XB8FFSUBSUBXAE:X8F4 XC7 BEL縹DC3*V0 52
```

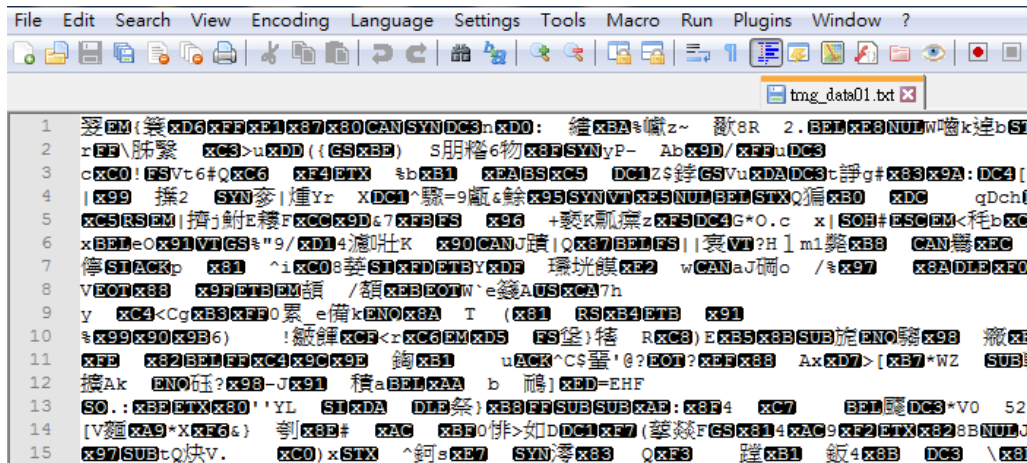
# Tips – Others (1/2)

---

- Virtual Machine with Ubuntu
  - Vmwave: <https://www.kjnotes.com/linux/18>
  - Virtualbox: <https://www.kjnotes.com/linux/29>
- You can transfer data files from your OS to virtual machine by:
  - Share folder ( google the key word with your virtual machine software)
  - Internet

# Tips – Others (2/2)

- Use “xxd” command on Ubuntu to check your data.bin file
  - xxd data.bin |less



```
1  00000000: 2020 0901 1807 40de fdad de35 4667 b4a5  ....@....5Fg..
2  00000010: 8d14 46ed 38e6 f0fb aee8 9184 e2dd 7b21  ..F.8.....{!
3  00000020: 48ab 9da9 d993 7680 ed91 feed 0182 cc7d  H.....v.....}
4  00000030: 7ae0 923e bf06 dd19 adfa 2383 59cc 1f79  z...>.....#.Y..y
5  00000040: d7a5 c81d b6ca 050d b0cd 22c4 4dbf ef99  .....".M...
6  00000050: a191 3f64 3740 0a6e 032d 521f 86fd 6fd4  ..?d7@.n.-R...o.
7  00000060: a5dd 5105 9032 e620 2865 1193 47f9 b4f8  ..Q..2. (e..G...
8  00000070: 4386 4d2d 0d6b acf6 7f7b 4156 cb6b 5c56  C.M-.k...{AV.k\V
9  00000080: 4f1a 4cf7 3135 284c 9490 6118 f97a 9b52  O.L.15(L..a..z.R
10 00000090: 4406 bcc4 b287 cb89 3475 9705 396e 98b4  D.....4u..9n..
11 000000a0: 1324 306a 7585 5c8d 4e37 0a1b eb0e 01c7  .$0ju.\.N7.....
12 000000b0: b894 8c8e 519c 0bd2 ec94 e30d 858c d08f  ....Q.....
13 000000c0: 7cc6 56d7 b584 f611 510f efaf cc46 68e1  |.V.....Q....Fh.
```

# THANK YOU



**PUF**security  
Secure the connected world