Pseudorandom Number

- Process used to generate pseudorandom numbers used to create encryption keys

Pseudorandom number generator

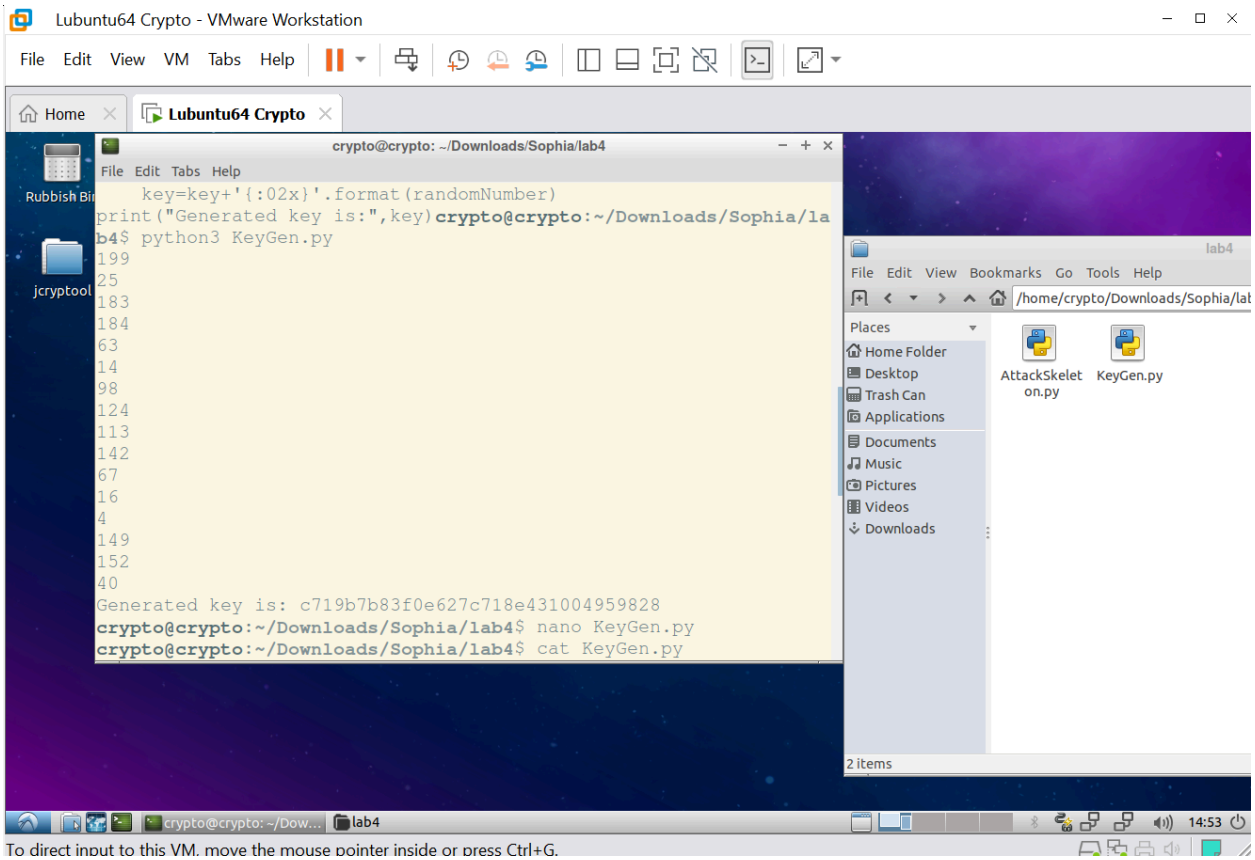
- Encryption keys sometimes generated inside the software
- More random = more effective encryption key
- Monte Carlo simulation (generating random numbers)
- But generate secure random numbers - or else there will be mistakes

Task 1 - generating random numbers in a wrong way

- Generate good pseudorandom numbers by starting with something random

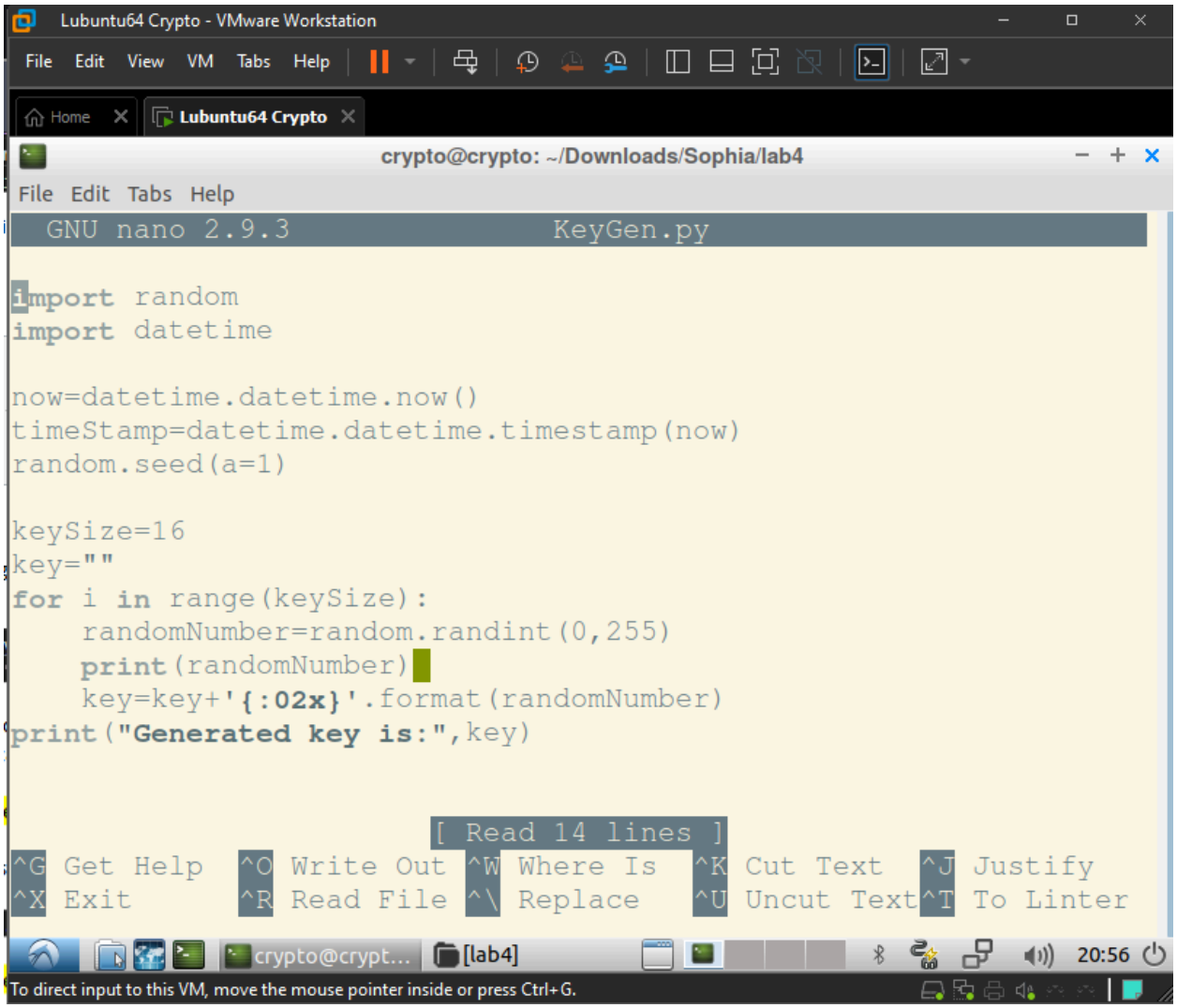
COMMAND: python3 KeyGen.py

- Code generates 16 random numbers as the key
    - Obtains system timestamp, uses timestamp as seed of the random module



COMMAND: nano KeyGen.py

- Setting seed to be a constant: a=1
    - same seed=same outcome



Lubuntu64 Crypto - VMware Workstation

File Edit View VM Tabs Help

Home | Lubuntu64 Crypto

crypto@crypto: ~/Downloads/Sophia/lab4

File Edit Tabs Help

```
228
Generated key is: 4420823cfde6f1c26b30f90ec7dd01e4
crypto@crypto:~/Downloads/Sophia/lab4$ python3 KeyGen.py
68
32
130
60
253
230
241
194
107
48
249
14
199
221
1
228
Generated key is: 4420823cfde6f1c26b30f90ec7dd01e4
crypto@crypto:~/Downloads/Sophia/lab4$
```

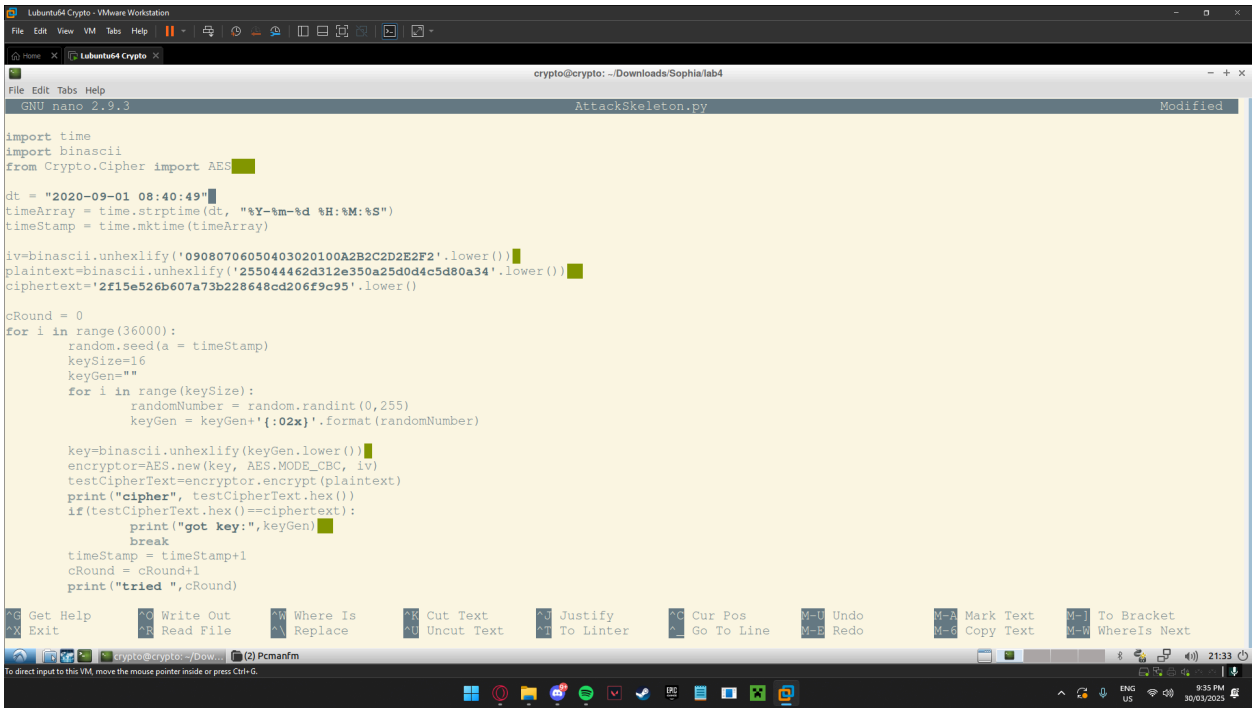
crypto@crypt... [lab4] 20:55

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Task 2 - guessing the key

- Describe your idea to find out the key
    - Using the timestamp of the encrypted file: "2020-09-01 10:40:49" - generate key
    - Decrypt by reversing the AES-CBC encryption

- Code used - Find out the key
    - Loop continuously runs combinations of characters until key is correct - brute forcing



Lubuntu64 Crypto - VMware Workstation

File Edit View VM Tabs Help

Home | Lubuntu64 Crypto

crypto@crypto: ~/Downloads/Sophia/lab4

File Edit Tabs Help

```
cipher 7ac6b5d9f66dd49f710a9edf083d87d8
tried  7143
cipher 809013d2099cdf415ff5ab449ddc6074
tried  7144
cipher 69a6cc9ef0852114c3b8b42e7e1a3c74
tried  7145
cipher a5f8792bc79ef65701788f03c1374650
tried  7146
cipher 8db1e056f8f3c5d83156637c10c19b01
tried  7147
cipher c1ed9837ed2ab092507136aaf2d53d46
tried  7148
cipher cb8fd499765a41128a6752d7dbb0e6e9
tried  7149
cipher 222d9c76d412614e2b192939328d58ff
tried  7150
cipher 75bc4c5df1d5af1a57decae6a7238977
tried  7151
cipher 2f15e526b607a73b228648cd206f9c95
got key: f22a5ca541af283c48c5d53e530e0abb
crypto@crypto:~/Downloads/Sophia/lab4$
```

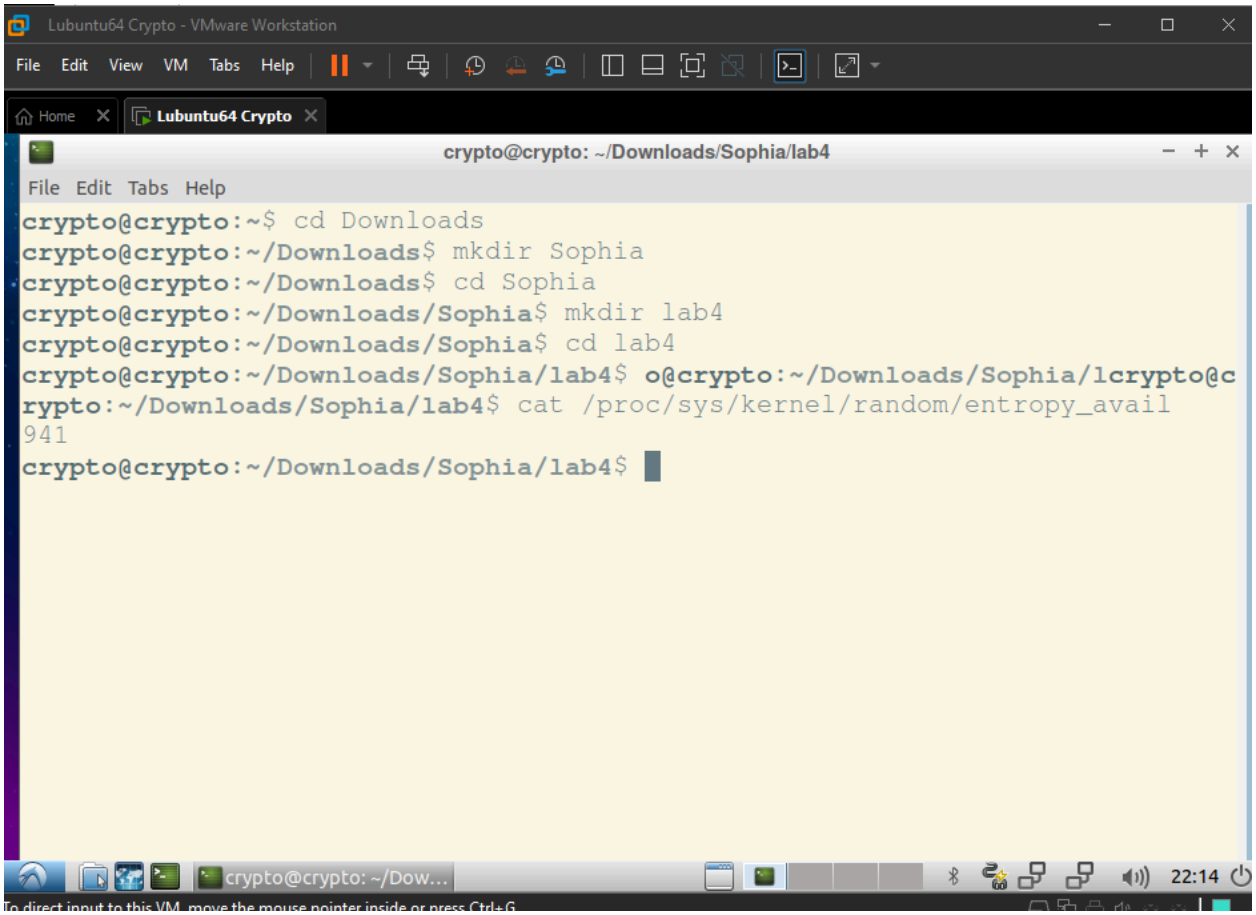
crypto@crypto: ~/Dow... | (2) Pcmanfm | 21:29

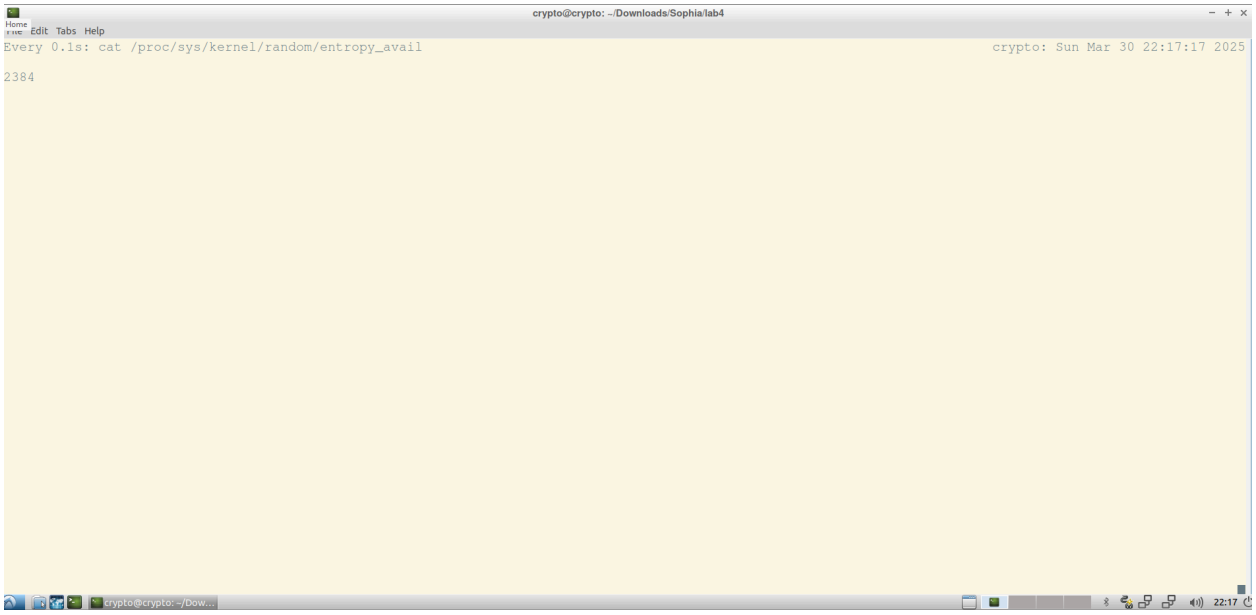
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Task 3 - Measure the entropy of kernel

Describe observation in report

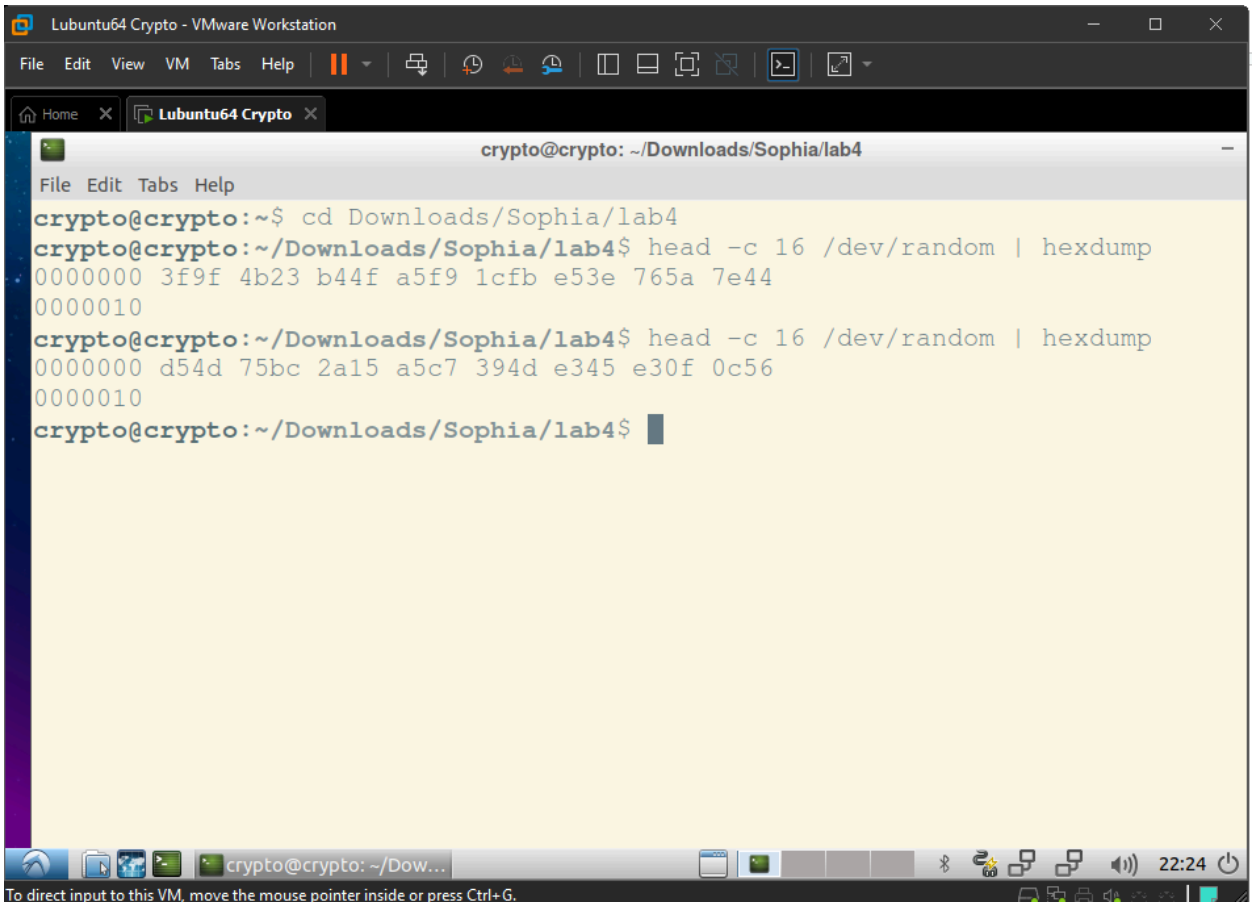
- Moving mouse, entropy level increases (more of it is generated)




crypto@crypto: ~/Downloads/Sophia/lab4
File Edit Tabs Help
Home
Every 0.1s: cat /proc/sys/kernel/random/entropy_avail
crypto: Sun Mar 30 22:17:17 2025
2384
crypto@crypto: ~/Dow...
22:17

Task 4 - Get random numbers from /dev/random

- Run the command a few times and check the randomness of the printed values



- Entropy should be stuck at 0
  - Cat /dev/random > /dev/null
  - Keep on spamming it
  - Not stuck - system keeps on generating entropy
- Numbers and letters being generated consecutively
- Randomness being generated by entropy levels - random

Lubuntu64 Crypto - VMware Workstation

File Edit View VM Tabs Help

Home | Lubuntu64 Crypto

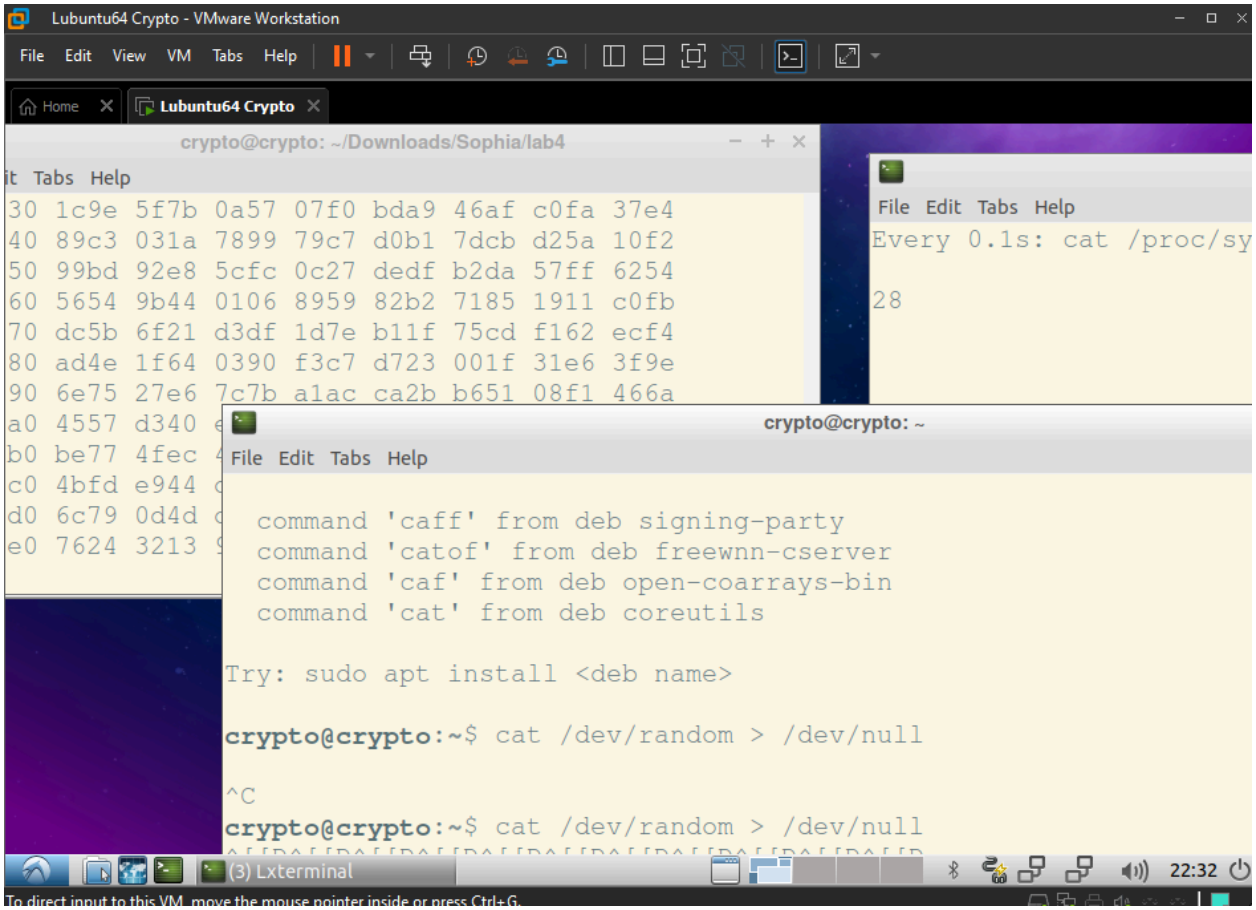
crypto@crypto: ~/Downloads/Sophia/lab4

File Edit Tabs Help

```
crypto@crypto:~$ cd Downloads/Sophia/lab4
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 16 /dev/random | hexdump
0000000 3f9f 4b23 b44f a5f9 1cfb e53e 765a 7e44
0000010
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 16 /dev/random | hexdump
0000000 d54d 75bc 2a15 a5c7 394d e345 e30f 0c56
0000010
crypto@crypto:~/Downloads/Sophia/lab4$ cat /dev/random | hexdump
0000000 825f 70cf 1a37 1d6f 2f93 e201 6cc8 cd24
0000010 284f e1c4 f324 c372 9429 5e1f 2881 e147
0000020 9268 b90b 6378 4dfb 2c01 cf68 da82 e4ad
0000030 e6d0 3d1d 2824 0882 c56d 98dc 6c20 866f
0000040 e754 8056 1e60 26f6 58a6 9906 24de 1d79
0000050 2d13 01d0 b1fe 096c 3fda 72d8 f750 5ac5
0000060 bfc5 12b3 e92a 7a6e ebf3 c847 059c 2e78
0000070 0c65 d50e b629 b71a 364e ebca cabd 174b
0000080 a568 f067 f774 480b f831 0c0b 8644 44b2
0000090 036f 3a05 f94b dbe4 89ec 6f40 9987 c9ff
00000a0 8cd4 c6be 8eb7 ce1f 8fd5 fbc0 c0f9 7fec
00000b0 ff85 feab 89ca 85d0 9911 d9da 3128 1b7e
00000c0 4887 7e76 0b25 dff0 2423 dedc 3463 7a26
```

crypto@crypto: ~/Dow... 22:26

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Lubuntu64 Crypto - VMware Workstation
File Edit View VM Tabs Help
Home
Lubuntu64 Crypto
crypto@crypto: ~/Downloads/Sophia/lab4
Tabs Help
30 1c9e 5f7b 0a57 07f0 bda9 46af c0fa 37e4
40 89c3 031a 7899 79c7 d0b1 7dcb d25a 10f2
50 99bd 92e8 5cfc 0c27 dedf b2da 57ff 6254
60 5654 9b44 0106 8959 82b2 7185 1911 c0fb
70 dc5b 6f21 d3df 1d7e b11f 75cd f162 ecf4
80 ad4e 1f64 0390 f3c7 d723 001f 31e6 3f9e
90 6e75 27e6 7c7b a1ac ca2b b651 08f1 466a
File Edit Tabs Help
Every 0.1s: cat /proc/sy
28
crypto@crypto: ~
File Edit Tabs Help
command 'caff' from deb signing-party
command 'catof' from deb freewnn-cserver
command 'caf' from deb open-coarrays-bin
command 'cat' from deb coreutils
Try: sudo apt install <deb name>
crypto@crypto:~$ cat /dev/random > /dev/null
^C
crypto@crypto:~$ cat /dev/random > /dev/null
(3) Lxterminal
22:32
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Task 5 - Get random numbers from /dev/urandom

- Doesn't take entropy, uses the CPRNG pseudornaom number generator algorithm

- Describe your outcome and analyse whether the quality of the random numbers is good or not
    - Very close to = quality of randomness is very high