

Pseudorandom Number

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

Pseudorandom number generator

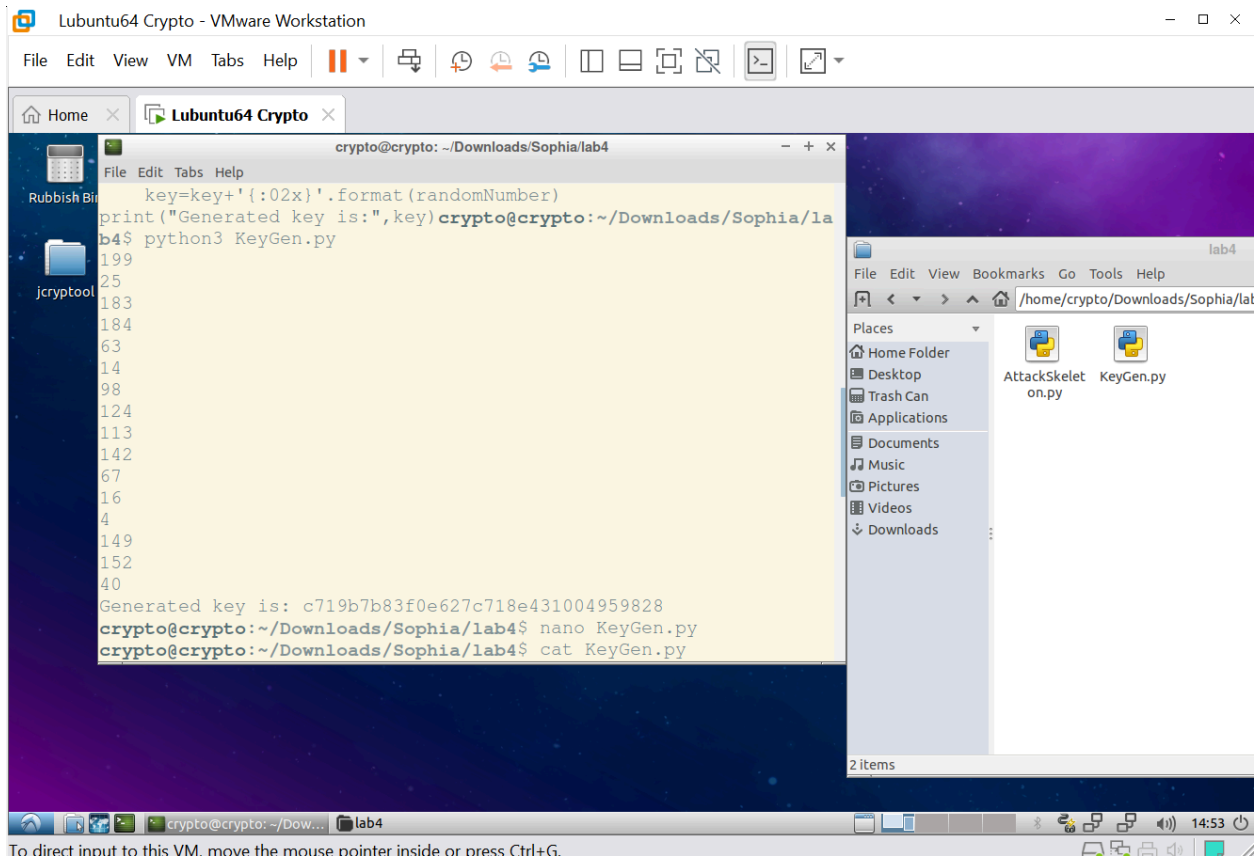
- Encryption keys sometimes generated inside the software
- More random = more effective encryption key
- Monte Carlo simulation (generating random numbers)
- But generate secure random numbers - or else there will be mistakes

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



```
crypto@crypto: ~/Downloads/Sophia/lab4
File Edit Tabs Help
key=key+'{:02x}'.format(randomNumber)
print("Generated key is:",key)
crypto@crypto:~/Downloads/Sophia/lab4$ python3 KeyGen.py
199
25
183
184
63
14
98
124
113
142
67
16
4
149
152
40
Generated key is: c719b7b83f0e627c718e431004959828
crypto@crypto:~/Downloads/Sophia/lab4$ nano KeyGen.py
crypto@crypto:~/Downloads/Sophia/lab4$ cat KeyGen.py
```

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

COMMAND: nano KeyGen.py

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

```
crypto@crypto: ~/Downloads/Sophia/lab4
File Edit Tabs Help
GNU nano 2.9.3 KeyGen.py

import random
import datetime

now=datetime.datetime.now()
timeStamp=datetime.datetime.timestamp(now)
random.seed(a=1)

keySize=16
key=""
for i in range(keySize):
    randomNumber=random.randint(0,255)
    print(randomNumber)
    key=key+'{:02x}'.format(randomNumber)
print("Generated key is:",key)
```

[Read 14 lines]

^G Get Help	^O Write Out	^W Where Is	^K Cut Text	^J Justify
^X Exit	^R Read File	^_\ Replace	^U Uncut Text	^T To Linter

crypto@crypt... [lab4] 20:56

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 X Lubuntu64 Crypto X

crypto@crypto: ~/Downloads/Sophia/lab4

File Edit Tabs Help

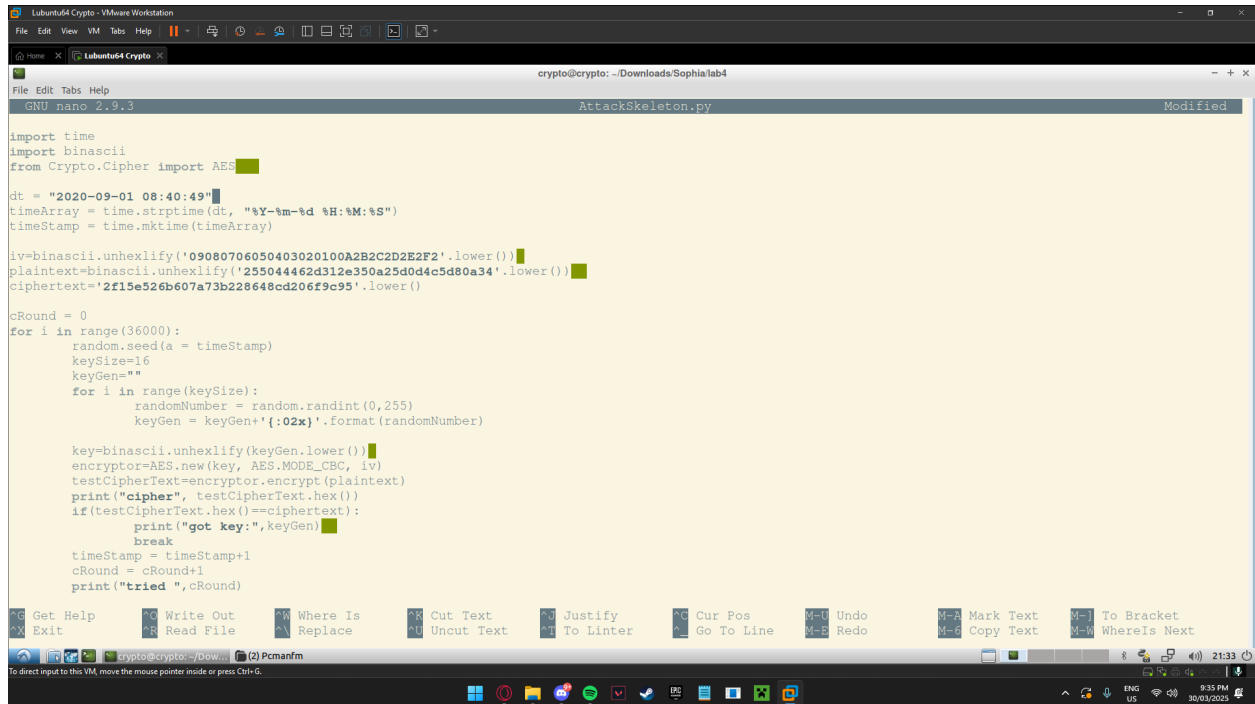
```
228
Generated key is: 4420823cfde6f1c26b30f90ec7dd01e4
crypto@crypto:~/Downloads/Sophia/lab4$ python3 KeyGen.py
68
32
130
60
253
230
241
194
107
48
249
14
199
221
1
228
Generated key is: 4420823cfde6f1c26b30f90ec7dd01e4
crypto@crypto:~/Downloads/Sophia/lab4$
```

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



The screenshot shows a virtual machine window titled "Lubuntu64 Crypto - VMware Workstation". Inside the VM, a terminal window is open with the command prompt "crypto@crypto: ~/Downloads/Sophia/tab4". The terminal displays the contents of a file named "AttackSkeleton.py", which is being edited with the nano text editor. The script is a Python program designed to brute-force an AES key. It starts by importing the 'time' module and the 'binascii' module from the 'Crypto.Cipher' module. It then defines a timestamp 'dt' as "2020-09-01 08:40:49", converts it to a time array, and then to a timestamp. The script defines a plaintext and a ciphertext, both in hexadecimal. It then enters a loop where it generates random keys of size 16, encrypts the plaintext using AES-CBC, and compares the resulting ciphertext with the target ciphertext. If a match is found, it prints the key and breaks the loop. The script also includes a counter for the number of rounds and a timestamp for each attempt.

```
import time
import binascii
from Crypto.Cipher import AES

dt = "2020-09-01 08:40:49"
timeArray = time.strptime(dt, "%Y-%m-%d %H:%M:%S")
timeStamp = time.mktime(timeArray)

iv=binascii.unhexlify('09080706050403020100A2B2C2D2E2F2'.lower())
plaintext=binascii.unhexlify('255044462d312e350a25d0d4c5d80a34'.lower())
ciphertext='2f15e526b607a73b228648cd206f9c95'.lower()

cRound = 0
for i in range(36000):
    random.seed(a = timeStamp)
    keySize=16
    keyGen=""
    for i in range(keySize):
        randomNumber = random.randint(0,255)
        keyGen = keyGen+'{:02x}'.format(randomNumber)

    key=binascii.unhexlify(keyGen.lower())
    encryptor=AES.new(key, AES.MODE_CBC, iv)
    testCipherText=encryptor.encrypt(plaintext)
    print("cipher", testCipherText.hex())
    if(testCipherText.hex()==ciphertext):
        print("got key:",keyGen)
        break
    timeStamp = timeStamp+1
    cRound = cRound+1
    print("tried ",cRound)
```

Lubuntu64 Crypto - VMware Workstation

File Edit View VM Tabs Help

Home x Lubuntu64 Crypto x

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

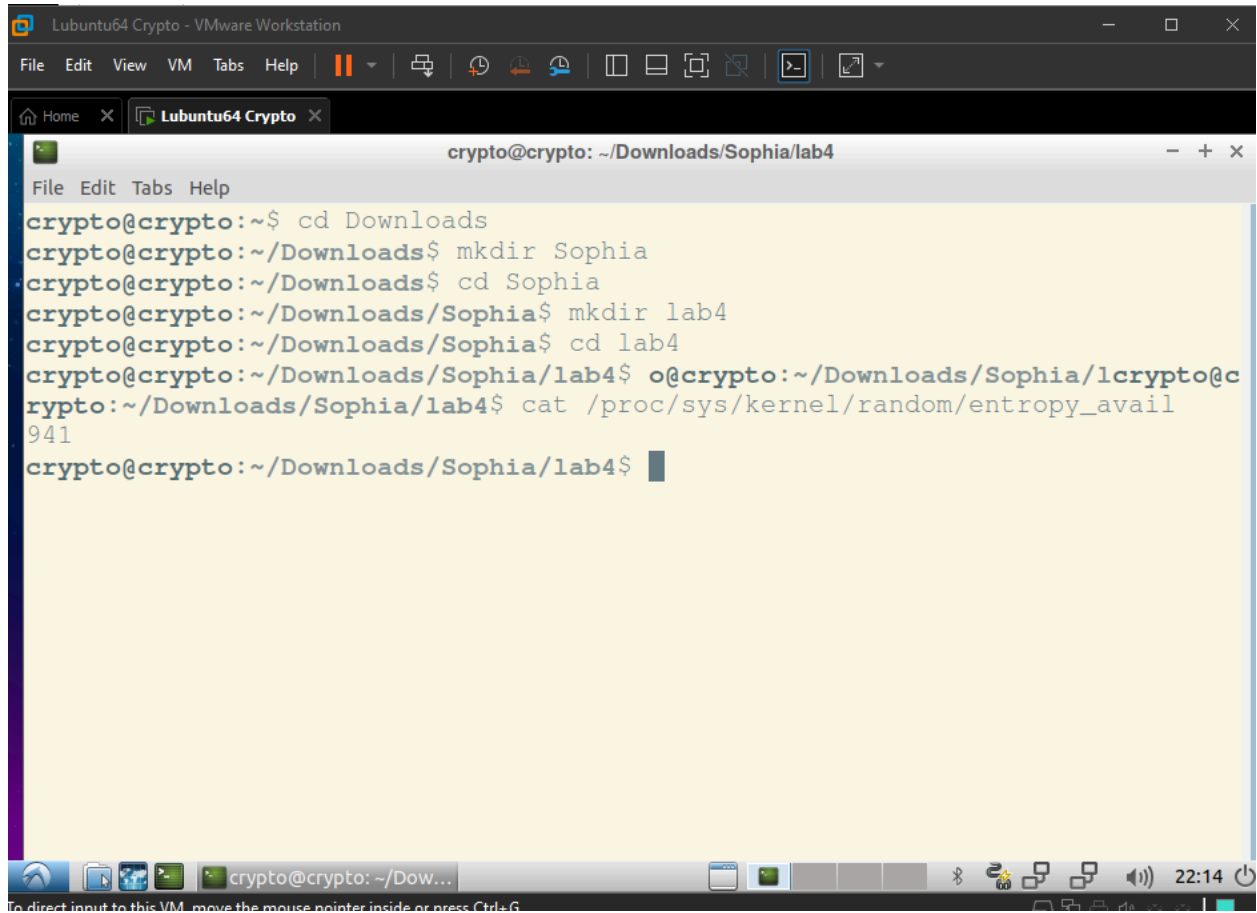
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

21:29

Task 3 - Measure the entropy of kernel

Describe observation in report

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

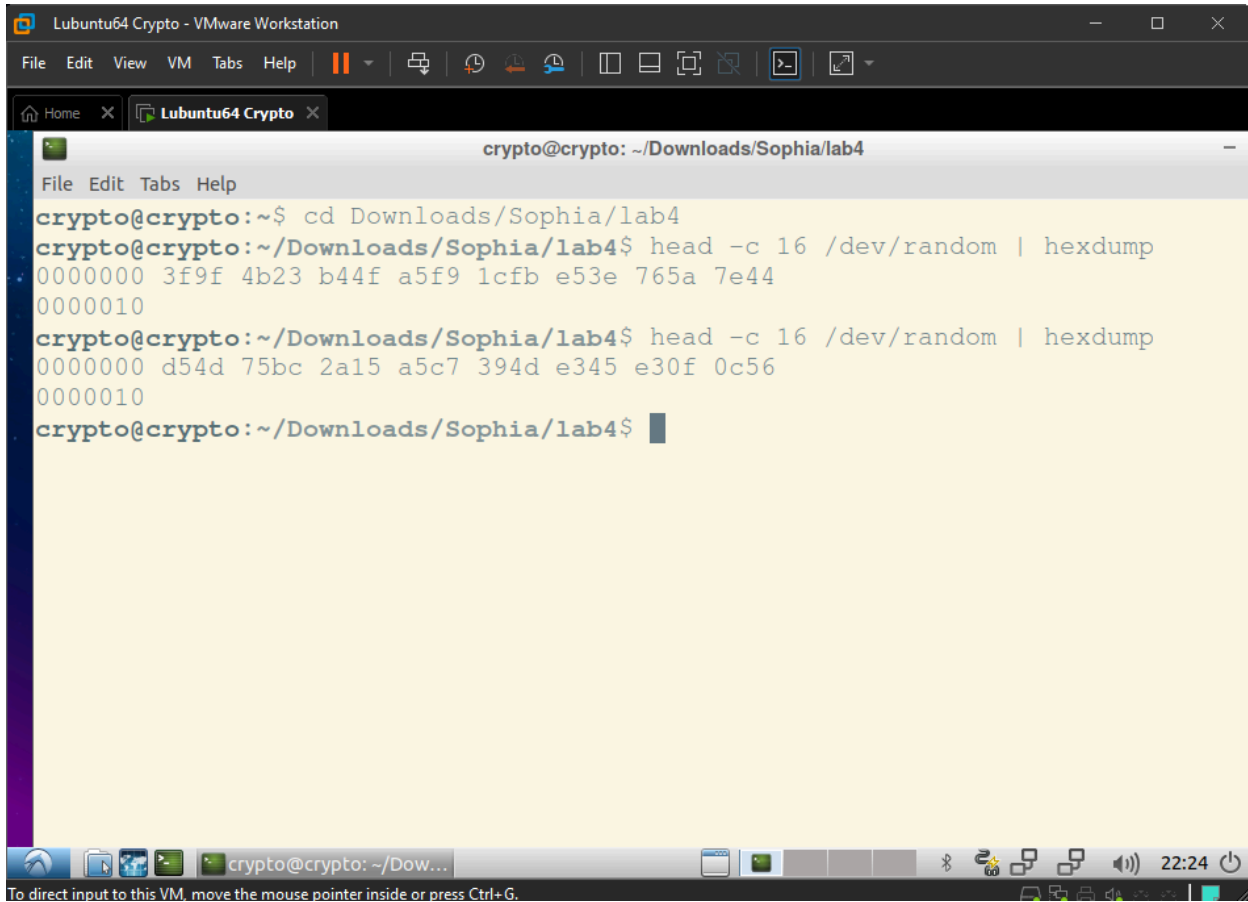


```
crypto@crypto: ~/Downloads/Sophia/lab4
File Edit Tabs Help
crypto@crypto:~$ cd Downloads
crypto@crypto:~/Downloads$ mkdir Sophia
crypto@crypto:~/Downloads$ cd Sophia
crypto@crypto:~/Downloads/Sophia$ mkdir lab4
crypto@crypto:~/Downloads/Sophia$ cd lab4
crypto@crypto:~/Downloads/Sophia/lab4$ cat /proc/sys/kernel/random/entropy_avail
941
crypto@crypto:~/Downloads/Sophia/lab4$
```

```
crypto@crypto: ~/Downloads/Sophia1ab4
File Edit Tabs Help
Every 0.1s: cat /proc/sys/kernel/random/entropy_avail
crypto: Sun Mar 30 22:17:17 2025
2384
```

Task 4 - Get random numbers from /dev/random

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



```
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
00000000 3f9f 4b23 b44f a5f9 1cfb e53e 765a 7e44
0000010
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 16 /dev/random | hexdump
00000000 d54d 75bc 2a15 a5c7 394d e345 e30f 0c56
0000010
crypto@crypto:~/Downloads/Sophia/lab4$
```

- 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 x Lubuntu64 Crypto x

crypto@crypto: ~/Downloads/Sophia/lab4

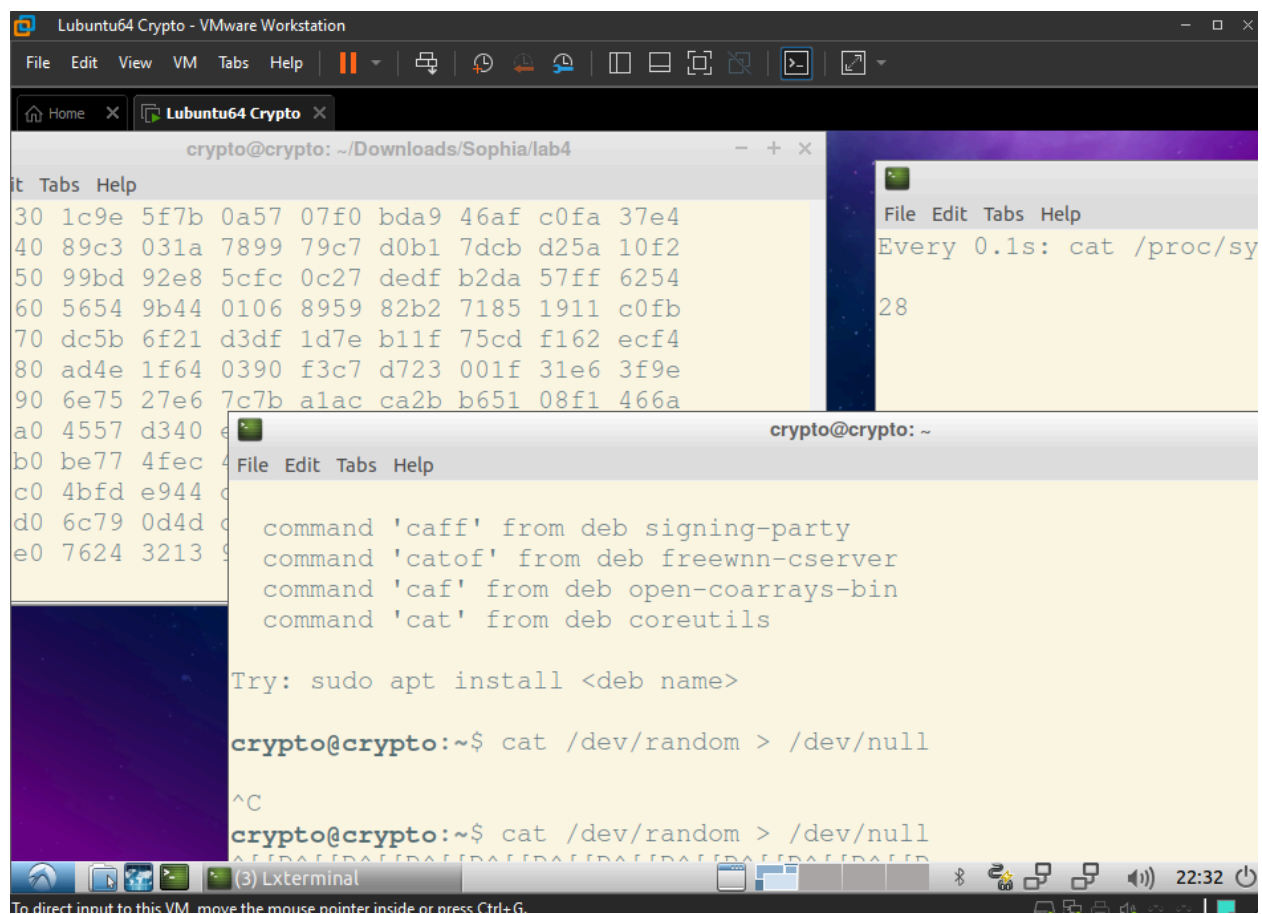
File Edit Tabs Help

```
crypto@crypto:~$ cd Downloads/Sophia/lab4
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 16 /dev/random | hexdump
00000000 3f9f 4b23 b44f a5f9 1cfb e53e 765a 7e44
00000010
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 16 /dev/random | hexdump
00000000 d54d 75bc 2a15 a5c7 394d e345 e30f 0c56
00000010
crypto@crypto:~/Downloads/Sophia/lab4$ cat /dev/random | hexdump
00000000 825f 70cf 1a37 1d6f 2f93 e201 6cc8 cd24
00000010 284f e1c4 f324 c372 9429 5e1f 2881 e147
00000020 9268 b90b 6378 4dfb 2c01 cf68 da82 e4ad
00000030 e6d0 3d1d 2824 0882 c56d 98dc 6c20 866f
00000040 e754 8056 1e60 26f6 58a6 9906 24de 1d79
00000050 2d13 01d0 b1fe 096c 3fda 72d8 f750 5ac5
00000060 bfc5 12b3 e92a 7a6e ebf3 c847 059c 2e78
00000070 0c65 d50e b629 b71a 364e ebca cabd 174b
00000080 a568 f067 f774 480b f831 0c0b 8644 44b2
00000090 036f 3a05 f94b dbe4 89ec 6f40 9987 c9ff
000000a0 8cd4 c6be 8eb7 cel f 8fd5 fbc0 c0f9 7fec
000000b0 ff85 feab 89ca 85d0 9911 d9da 3128 1b7e
000000c0 4887 7e76 0b25 dff0 2423 dedc 3463 7a26
000000d0 177 0126 100 66 7 01 6 0 51 6 1
```

crypto@crypto: ~/Dow...

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

22:26



Task 5 - Get random numbers from /dev/urandom

- Doesn't take entropy, uses the CPRNG pseudorandom 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

```
crypto@crypto: ~/Downloads/Sophia/lab4
File Edit Tabs Help
09fff60 dbd1 3b08 c68c c3ce 222b d475 f477 16c1
09fff70 975b 4bbf a92e a68e 63f9 edf9 6881 8b58
09fff80 8bd0 770b ca04 7c57 3f9d 4fef 9218 890d
09fff90 c445 121c ed46 226f fa9c f5ce 721c da95
09fffa0 bf7f 968a 47c1 d829 c2de eb03 b50a 1b94
09fffb0 1e59 1f7d 2b07 eebe cd38 e7e3 2f74 5d86
09fffc0 708c 1f26 79ed d3f6 e189 5579 598e f22f
09fffd0 6db6 5224 d463 cfae 1ba7 495e 5012 b578
09fffe0 d683 3a5b 4cfc ede7 2d29 ae56 9445 92ce
09ffff0 607a 4ee1 be1b 9104 27b7 b6b7 80f9 640c
0a00000
crypto@crypto:~/Downloads/Sophia/lab4$ head -c 10m /dev
/urandom | hexdump
```