**Applied Cryptography (UE20CS314)**

**Lab 3**

**Name: Vishwa Mehul Mehta**

**SRN: PES2UG20CS389**

**Section: F**

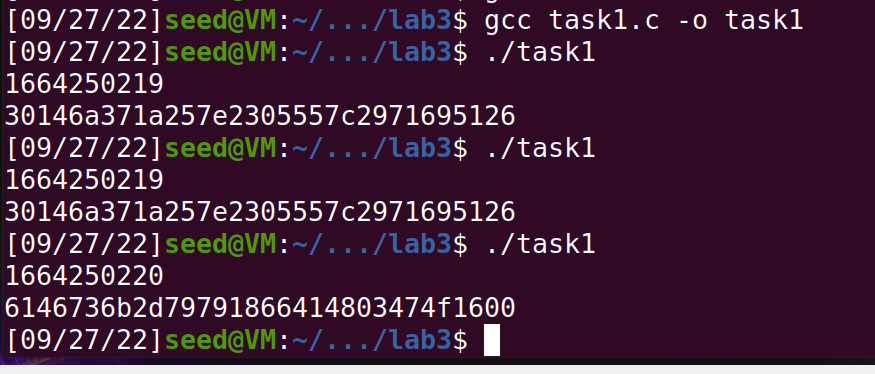
**Task 1: Generate Encryption Key in a Wrong Way**

Step 1:-

**Code:**



**Output:**



**Observation:**

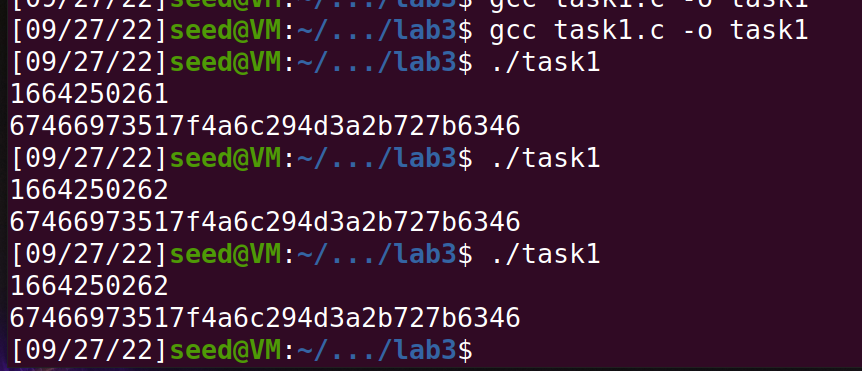
A new key is generated every second as the seed value we pass is the time elapsed in seconds till that point.

Step 2:-

**Code:**



**Output:**



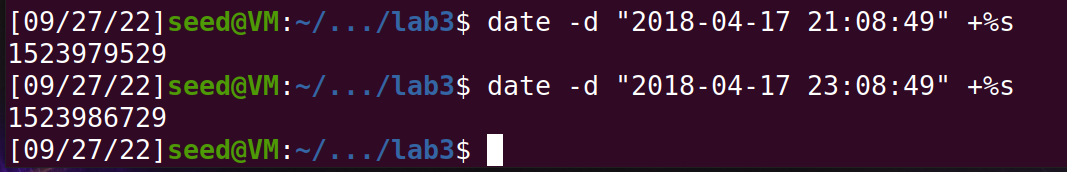
**Observation:**

Here the same key is generated as there’s no new seed value being passed to the rand function.

**Task2: Guessing the key**

Step 1:-

**Output:**

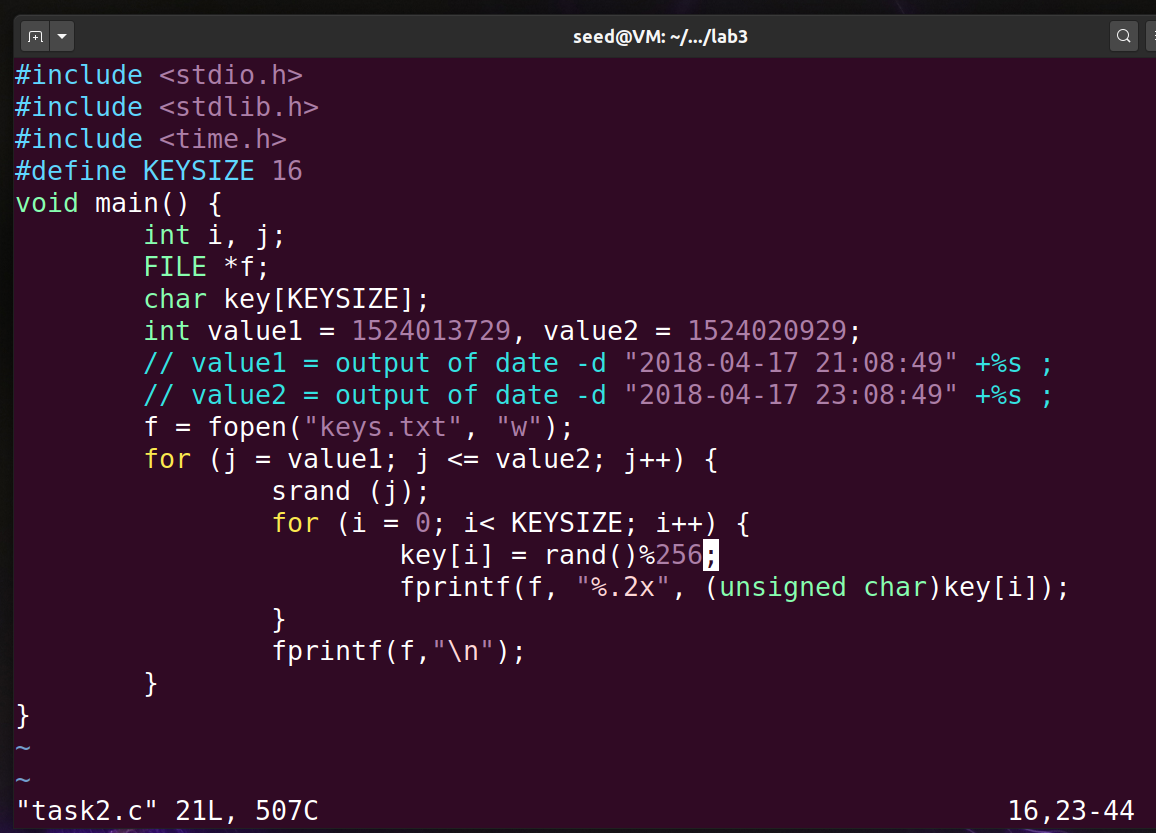


**Observation:**

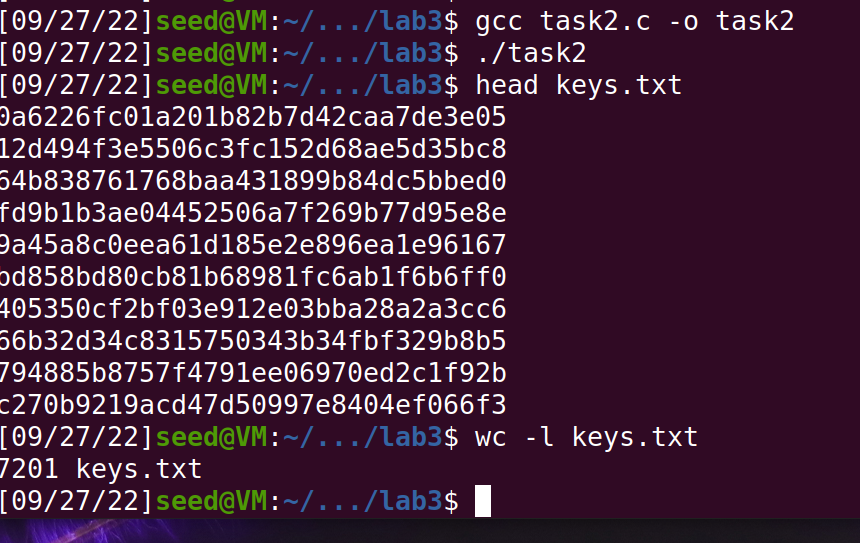
The output is the time elapsed in seconds between the current time and the time specified in the argument.

Step 2:-

**Code:**



**Output:**

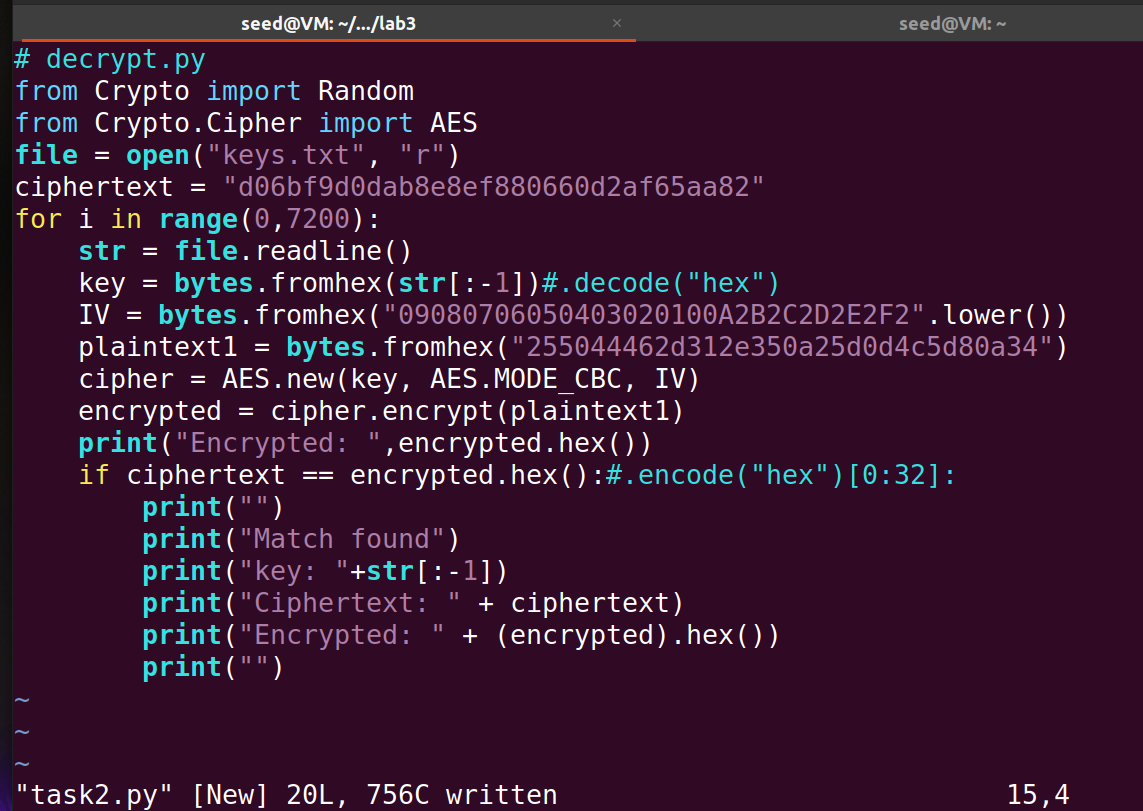


**Observation:**

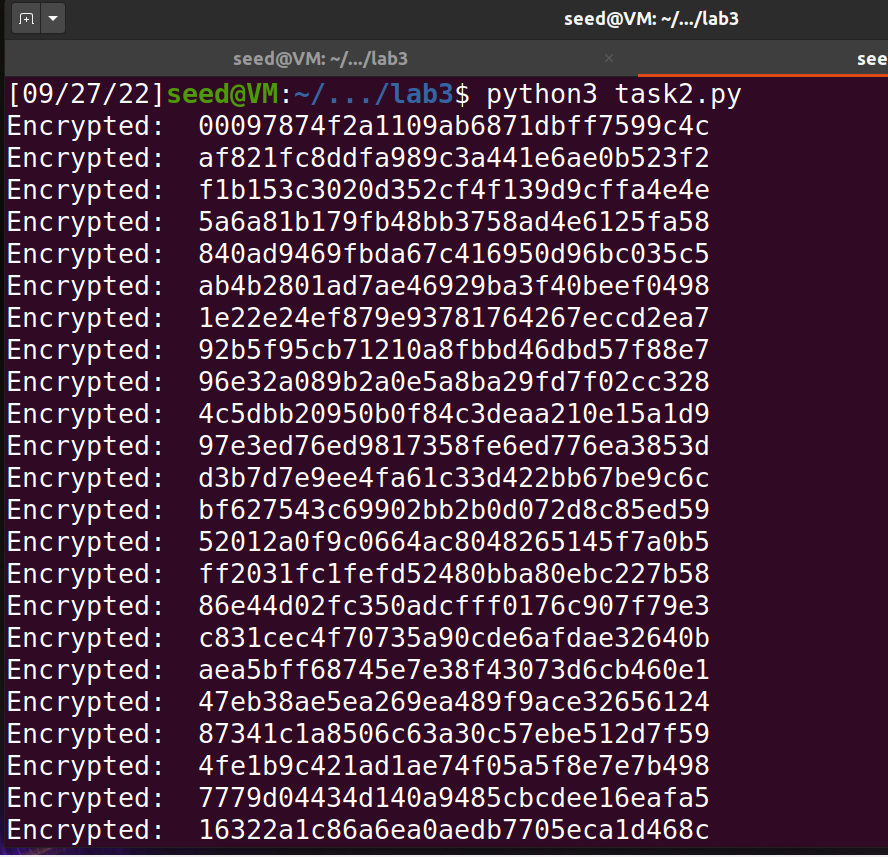
The output is all the possible keys that could have been generated between the time of value1 and value2.

Step 3:-

**Code:**



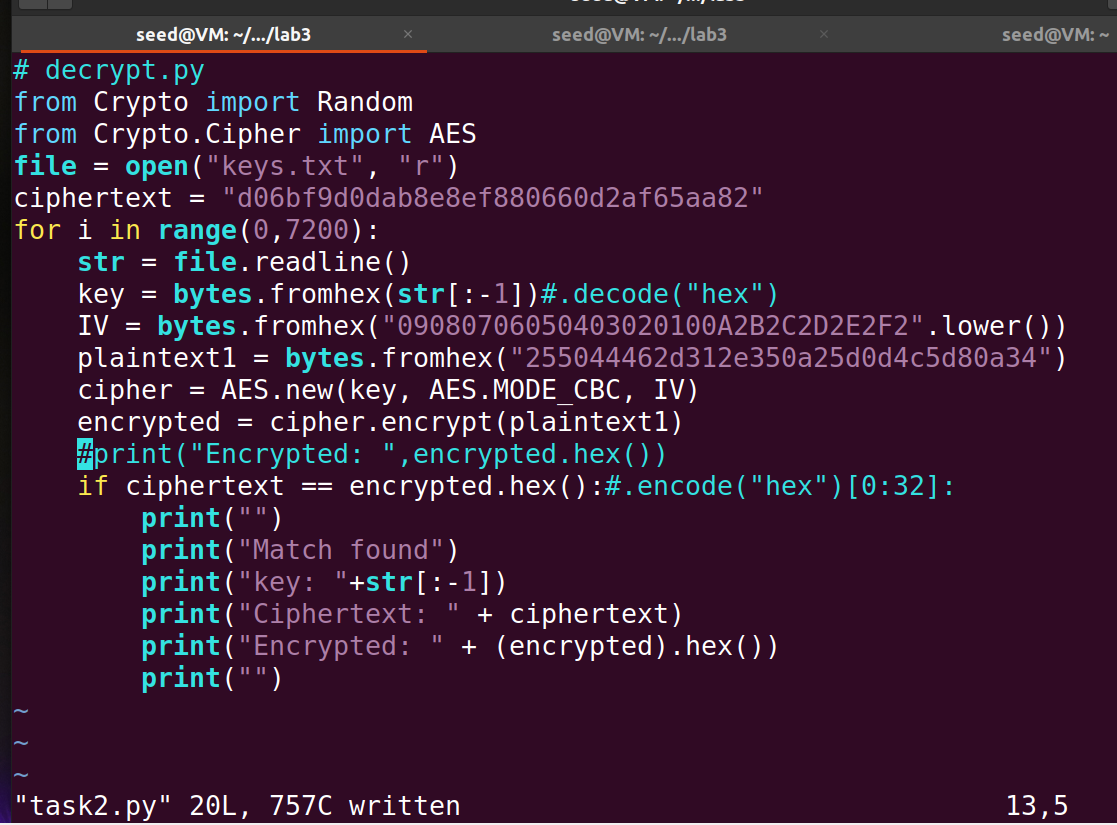
**Output:**



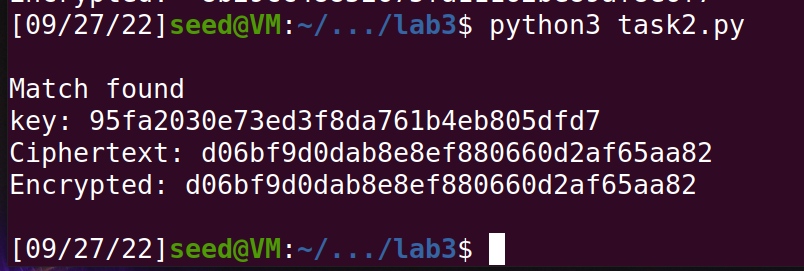
**Observation:**

Gives the output of encrypted plaint text over all the stored keys in keys.txt file.

**Code:**



**Output:**

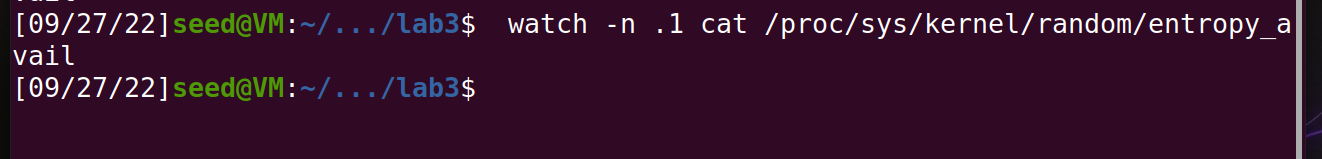


**Observation:**

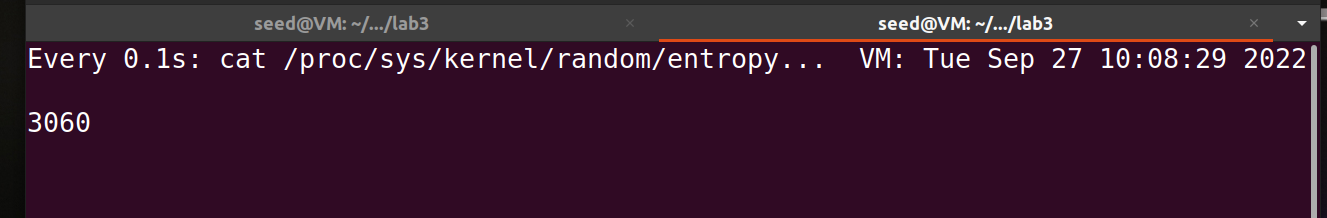
Commenting out the unwanted output we now check if the cipher text we need is present in the list of encrypted values.

**Task 3: Measure the Entropy of Kernel**

**Code:**



**Output:**



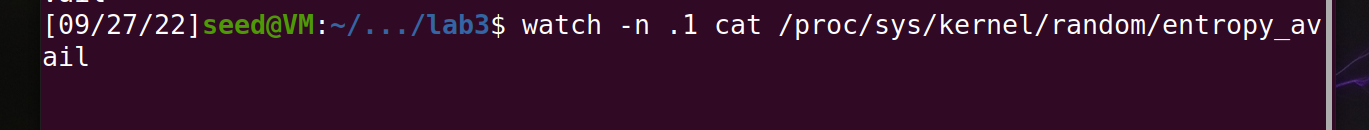
**Observation:**

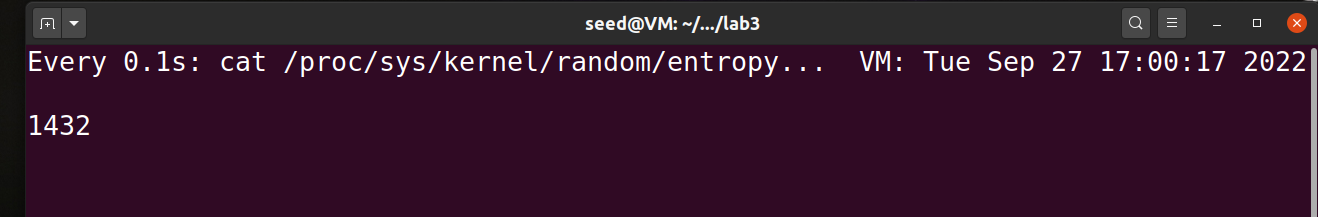
The entropy changes quickly when the mouse is moved faster and slower if it is not moved around.

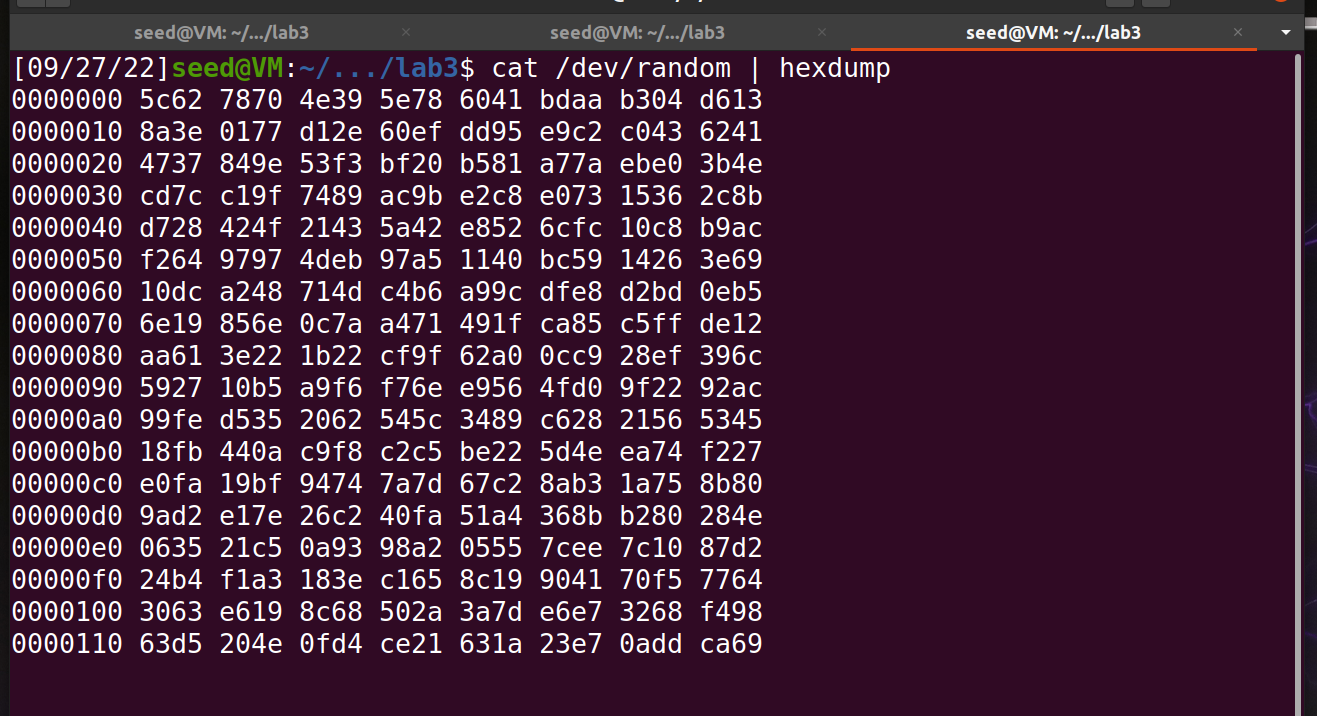
**Task 4: Get Pseudo Random Numbers from /dev/random**

Step 1:-

**Output:**







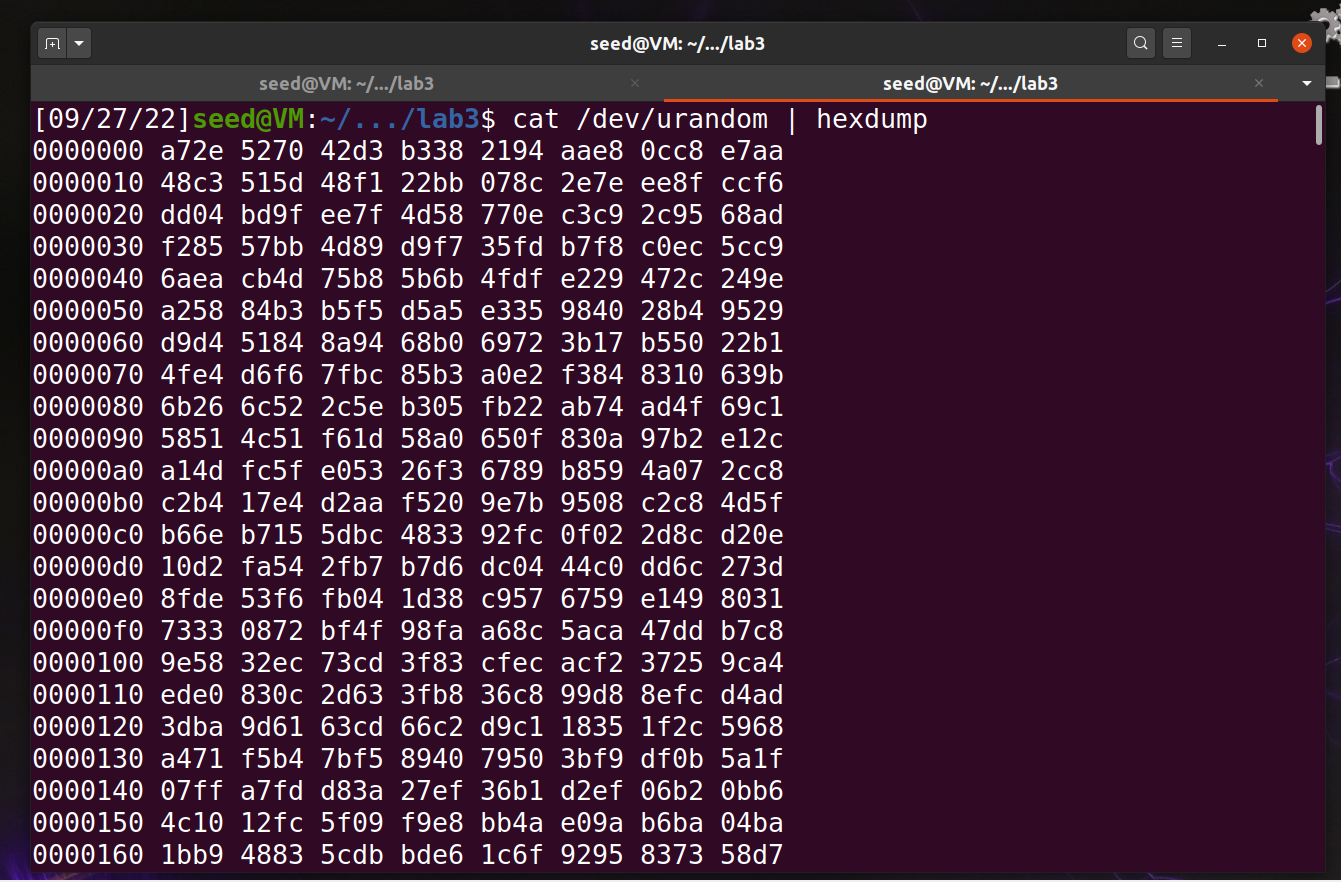
**Observation:**

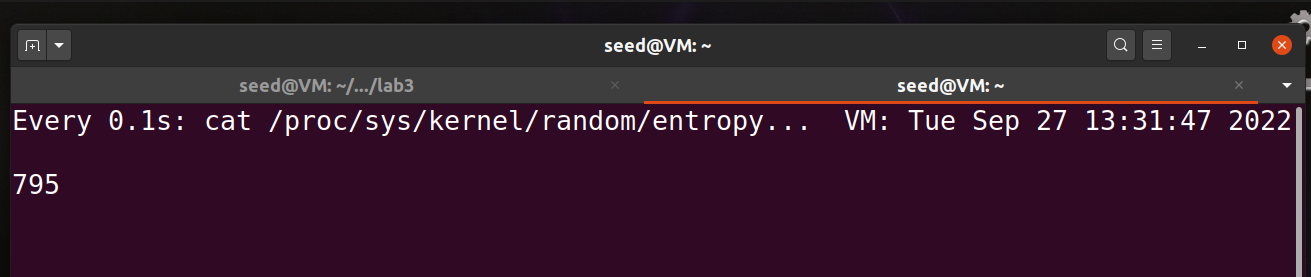
Movement of mouse and keyboard increases the entropy and low activity reduces the change rate of entropy.

**Task 5: Get Pseudo Random Numbers from /dev/urandom**

Step 1:-

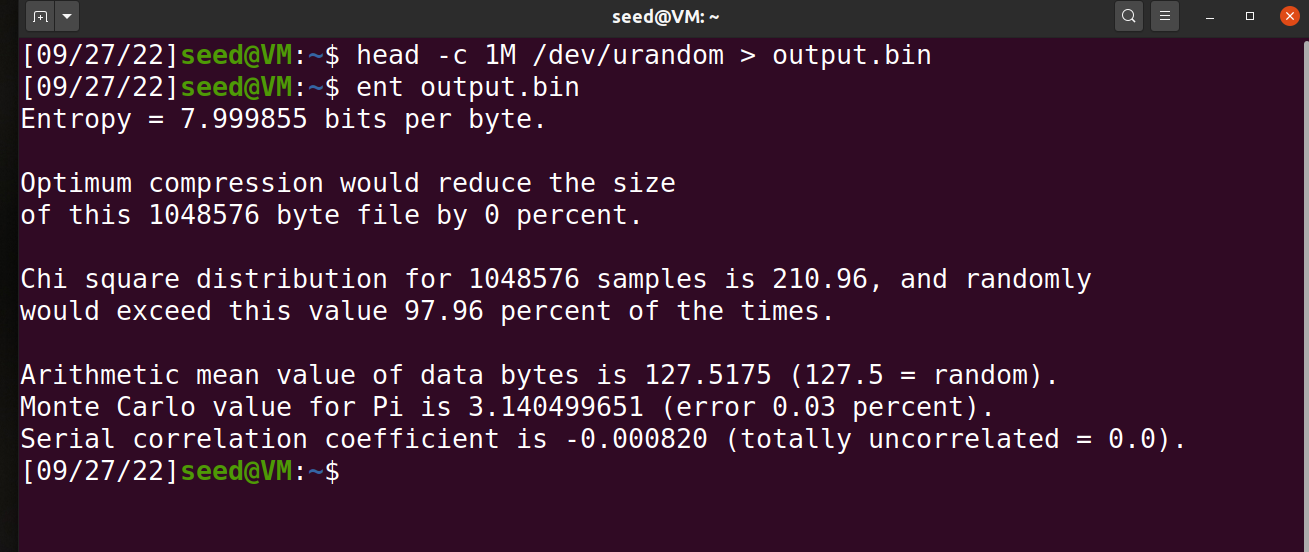
**Output:**





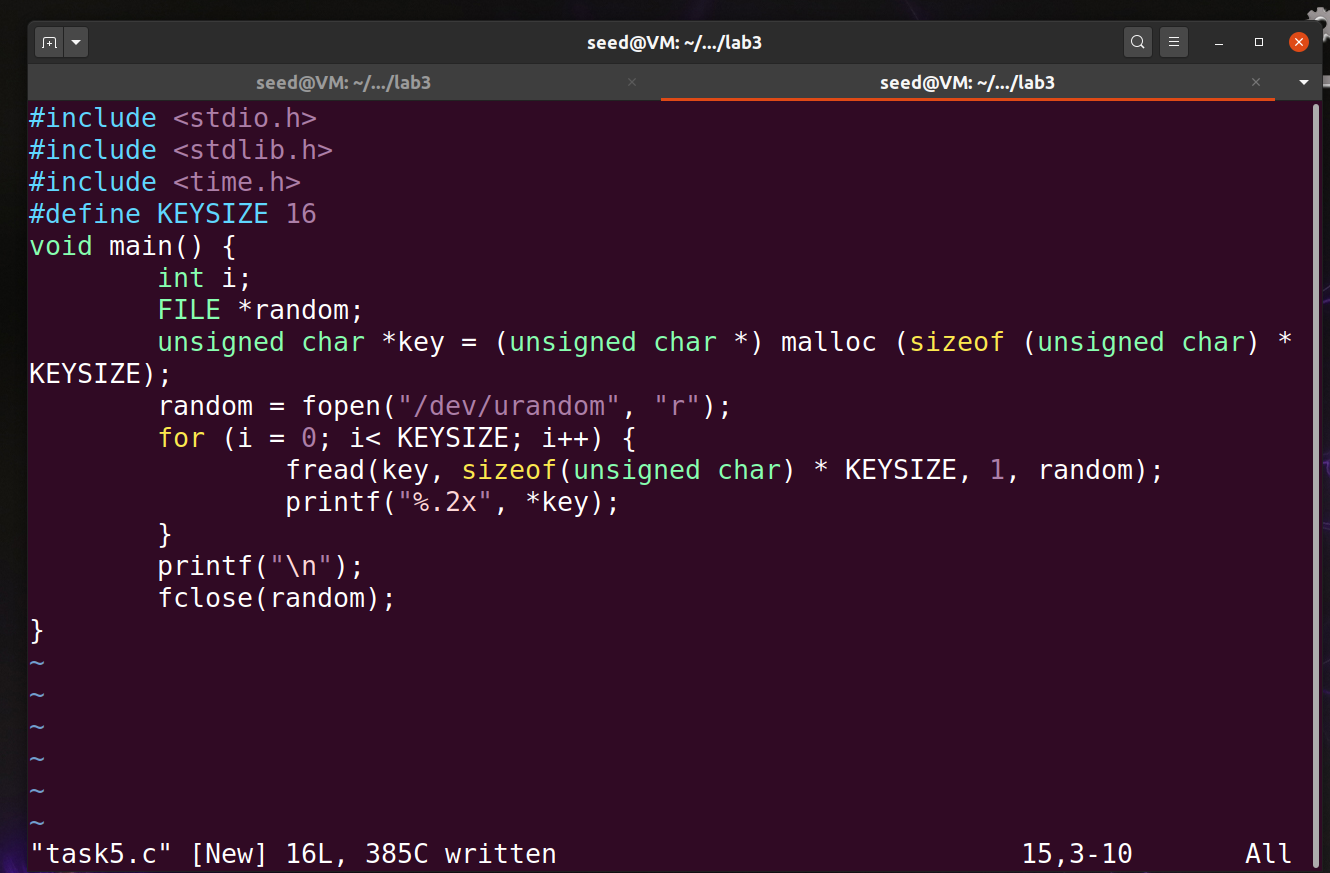
Step 2:-

**Output:**

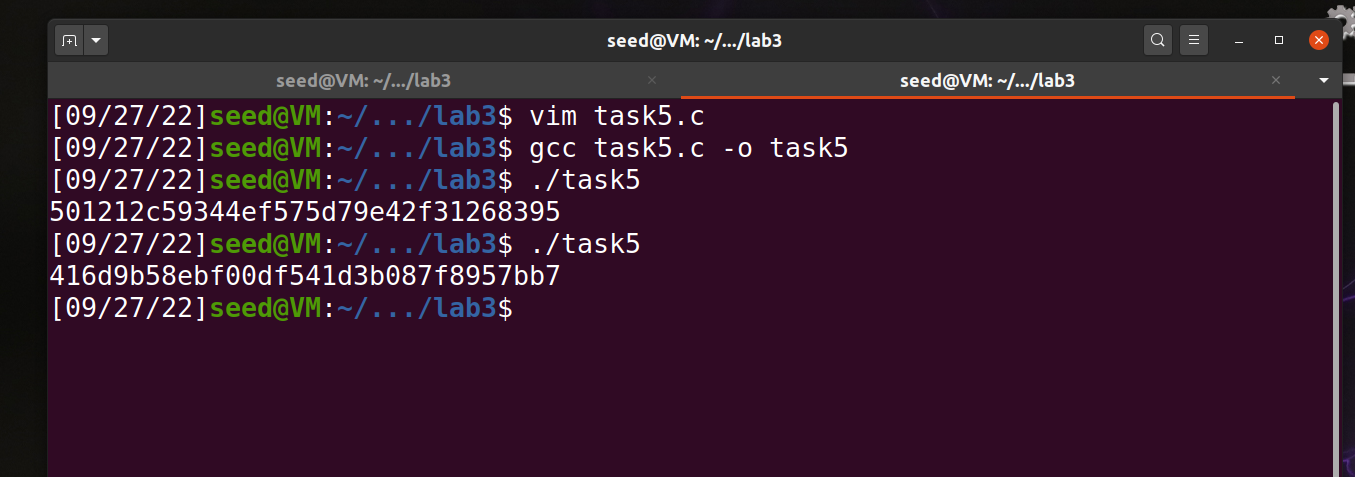


Step 3:-

**Code:**



**Output:**



**Observation:**

We use a better way of generating key using PRNG rather than relying on seed and time values.