**Foundations Network Security**

*Chakradhar Reddy Donuri*

*E949F496*

**Task-1**

1. Observation : A new set of 16 random keys are generated each second.
2. Observation after running code : Same Keys are being generated irrespective of time.
3. Purpose of **srand**() : Produces the set of pseudo random numbers by setting a start point. Purpose of **time**() : Gives the time value, time() is used as start point.

**Task-3**

**Below is the screenshot that shows before the mouse/keyboard movement.**

**A screenshot of a computer

Description automatically generated**

**Below is the screenshot that shows after the mouse/keyboard movement.**

**A screenshot of a computer

Description automatically generated**

**Difference of output** : Upon performing the keyboard clicks or mouse movements the entropy value is increased. Entropy increases only when the keyboard clicks or mouse movements are performed.

**Task-4**

**Below is the screenshot that shows before moving.**

A screenshot of a computer

Description automatically generated

**Below is the screenshot that shows after moving.A screenshot of a computer

Description automatically generated**

**Difference in output**: Upon mouse movements the value is changing i.e. the value is fluctuating between 0 to 63. Once the value reaches 63 again the value is changed to 0 and increases to 63 again. In this way it goes on continuously.

**Task-5**

**Below is the screenshot that shows before moving.**

A screenshot of a computer

Description automatically generated

**Below is the screenshot that shows after moving.**

A screenshot of a computer

Description automatically generated

**Below is the screenshot of Contents of file output.bin**

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Yes, the entropy that is depicted in the above screenshot is acceptable, i.e. 7.9998 bits per byte because as the rule, the higher the entropy in Pseudo-random number generation, the more secure the output. If the entropy less then the attackers may have the more ability to guess the data inputs.

**Below is the 256 Bit Key generator code**

A screenshot of a computer

Description automatically generated

**Below is the output for the code which generates the key**

A screenshot of a computer

Description automatically generated