CS6500 Network Security
Assignment - 1

Cryptanalysis of RC4 encryption algorithm

Report By - Pankaj Verma CS20M043

In the code I used various utility functions for the completion of this assignment and they are listed below (common ones not included) :

1. Toggle() - this function is used to toggle the bits.
2. KSA() - key-scheduling algorithm's implementation
3. PRGA() - Implementation of pseudo-random generation algorithm

I have an array diff[] which stores the difference between the two keystreams and then counter value is updated accordingly. An array std_dev[] is used to store the standard deviation value for the particular number of bits toggled. The values from this array are used to calculate the randomness and stored in array Randomness.

For e.g. is number of bits toggled are 20, then all the samples are observed, counters are updated and standard deviation is calculated and the result is then stored at index 19.

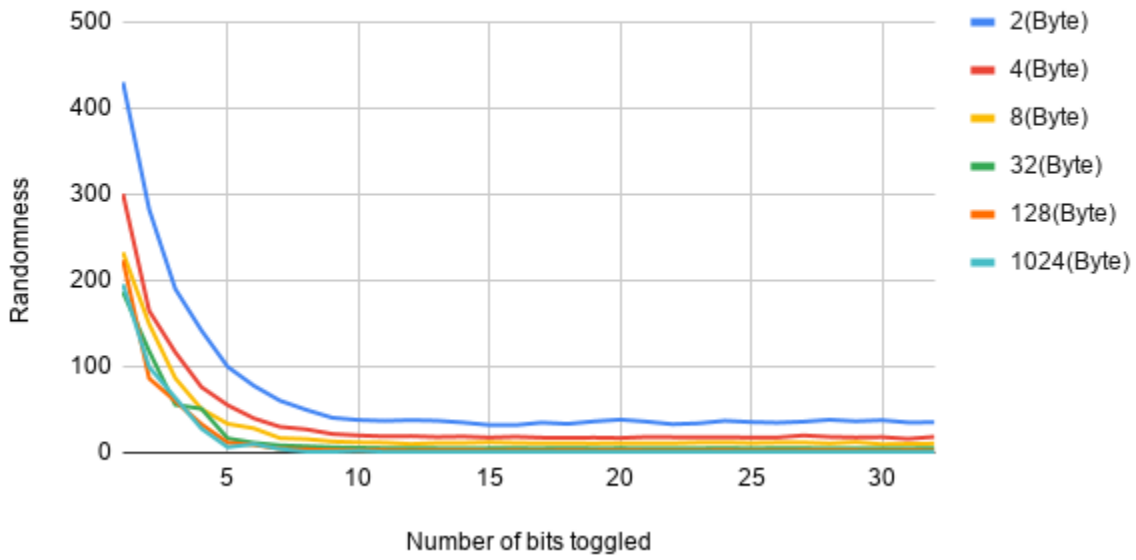
OBSERVATION

Regarding Output Length - It is observed that larger the length of the output more random will be the result.

Regarding the number of bits toggled - As the amount of bits different from the original key increases the result becomes more random and the graph line for the particular output length approaches to zero quickly.

Randomness for diff O/P lengths

Observed graph - 1



Randomness for diff O/P lenghts

Observed graph - 2