Lab 1 report

In this lab, we want to check the whether the key stream generated by rc4 algorithm is random or not. To do that we defined a value known as randomness. Higher the value of the randomness, less random is the key stream generated by rc4. If the keystream generated by rc4 is perfectly random, if we change a single input key bit, half of the keystream bits should flip. We want to see if that is happening via plotting randomness against the number of bits toggled.

To calculate randomness, we will take keystream of different sizes.

For each keystream size, we will create a key and a toggled key by flipping n number of bytes of the key. We will also take a counter array of size 256.Then we will find the XOR of key and toggled key pairwise 8 bits at a time and then update the counter with above XOR result index by 1. This way we would fill the counter array. We will then repeat the above process for 40 times for each keystream size and calculate the randomness value and plot it against number of bits toggled. We would get different lines in the same graph for different keystream sizes.

Chart, line chart

Description automatically generated

We plotted the randomness vs the number of toggled bits on python. The above graph shows this plot.

**Observations:**

1.The 2B keystream size has high and varying randomness value irrespective of the number of bits toggled.

2. The 512B keystream size plot line has strictly greater than zero randomness until 2 bits and later fluctuated up and down from zero until 10 bits before finally stabilizing at zero.

3. The graphs with keystream size in between 2B and 512B have in ascending order of bytes stabilized at zero at higher and higher number of bits.

**Conclusions:**

We can see that if the key stream generated by the algorithm is only 2 bytes size, the key stream is far from random. But as we go considering larger and larger size of keystreams, the randomness value is closing into zero with a smaller number of bits toggling. i.e., if we consider the large keystream rather than taking small keystream generated by rc4 as a secret key, then only we can say that it is truly random.