S3 REPORT

Q5 a)

OUTPUT

```
Via XORing Random Seed
0 -> 49.944343
1 -> 50.055557
Via Random
0 -> 49.916739
1 -> 50.083161
```

We can see from the output that the Probability Distribution of 0/1 in a sample Key (128 to 1e6 numbered bits) using XORing Technique from a random 127-bit Seed or via rand () % 2 approach is almost equal & stands at approx. 50%.

Q5 b)

OUTPUT

```
Via XORing Random Seed
P(x[i]= 0/x[i-1]= 0) = 0.248997
P(x[i]= 0/x[i-1]= 1) = 0.250333
Via Random Method
P(x[i]= 0/x[i-1]= 0) = 0.249346
P(x[i]= 0/x[i-1]= 1) = 0.249902
```

We can see from the output that the Probability that we get 0 after a 0 or 0 after a 1 is close to 0.25 in any of the methods, which is the theoretical expected value (for 128 to 1e6 numbered bits).

Also, the values are closer to 0.25 in the Random Method, due to its pure randomization.

Q5 c)

We are successfully able to encrypt any file using just a 127-bit Random Key.

Also, the decrypt program was easily able to convert back the encrypted file into the original file using the same 127-bit Key.

The Program was easily able to handle file/s of multiple size & formats (like txt, image, pdf, etc.)

$$e_i = b_i \bigoplus x_{i+127}$$

$$b_i = e_i \bigoplus x_{i+127}$$

$$(where\ b_i\ is\ the\ corresponding\ bit\ of\ the\ original\ Data,\ e_i\ is\ the\ encryped\ bit)$$

$$\left(x_{i+127}\ is\ the\ \sec r\ et\ bit\ generated\ u\sin g\ \ the\ formula\ x_{i+127} = x_{i+126} \bigoplus x_i\right)$$