## SECTION – 2

**12. Show formally and with figures and code, the most deadly linear trail in your cipher. Ensure that an attacker would find linear cryptanalysis more difficult than brute force.**

Using the linear and differential trails in the cipher, I found that the no. of I proposed were too high. I have also took advise from a friend and found 3 new sboxes. Thus making the linear and differential attack much more harder. In the files I have attached along with the report, the output of the code gives the the linear approximation table and also the maximum bias in each row. So, using the linear approximation tables for each sbox I proposed, we can find the deadliest path which is nothing but the path with the maximum bias and using the fact that,

Maximum bias in any sbox is $\frac{16}{64}$

After each round, the bias is multiplied by $2^{15} * (\frac{16}{64})^{16}$

For N such rounds, we have an upperbound which is that the brute force is more easier than the linear cryptanalysis.

$$2^{16N-1} * \epsilon^{16N} \geqslant \frac{1}{2^k}$$

where k = 128/2 = 64 and N is no. of rounds

This gives and upper bound of 8.

Choosing the best trial for the linear cryptanalysis (I have arranges the sboxes, s1,s2,s3,s4,s1,s2,s3...) the maximum bias was $\frac{0.42}{2^{32}}$ which gives an upperbound of 5 rounds for the condition.

**13. Show formally and with figures and code, the most deadly differential trail in your cipher. Ensure that an attacker would find differential cryptanalysis more difficult than brute force.**

Using the same method above and the differential approximation tables , we get a bias of $\frac{0.000002}{2^{32}}$ which gives and upper bound of 6 rounds.

Thus as we are choosing the maximum of linear and differential cryptanalysis, I optimmaly chose 7 rounds for the cipher.

**14. Revsit all questions in Section 1. If you decide to make changes in any of the answers, mention them here and justify why you are making the changes.**

The number of rounds for the cipher I chose changes which is 7 now. I chose 4 sboxes to make the linear and differrntial cryptanalysis much more difficult. The sboxes proposed are gven in the code itself.