**S-DES Differential Analysis Project Documentation**

**Group Members:** Lateef Almajed, Jacqueline Kosky and Shane Geller

We implemented the following:

1. Round Expansion

The possible number of rounds was modified to accept N number of rounds instead of only 2 rounds.

The following snapshots demonstrates how the user specifies the number of rounds and enter the key.

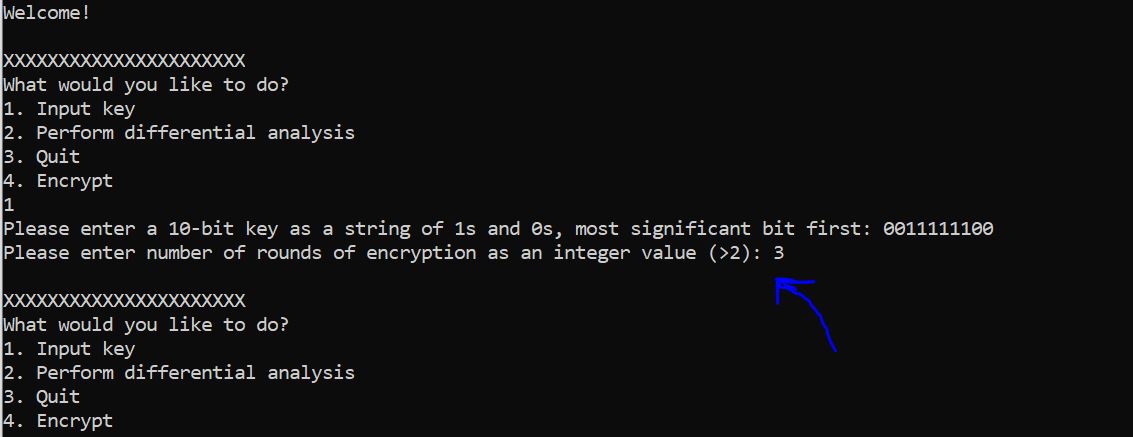


Figure 1.

Fig.1 Shows how the program was modified to prompt for the number of rounds when the user tries to input a key (option 1). The user entered 3 rounds in the shown example.

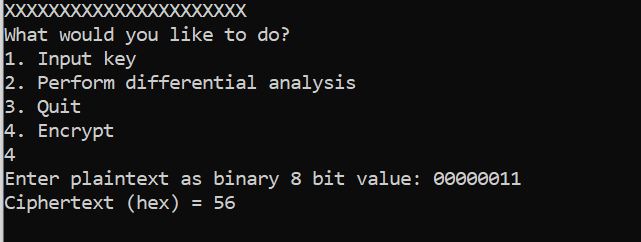


Figure 2.

In Fig.2 we see an example of running encryption (option 4) on the 8-bit string 00000011 with 3 rounds as specified in Fig.1 previously.

1. Key voting system

A system that, for a given master key, votes for a list of possible subkeys that are most likely to be part of the given master key in each specific round. Then, it verifies these lists of subkeys by checking for the existence of the original subkey in each list. The following snapshot shows a simple example of the key voting system on a 3-round S-DES.

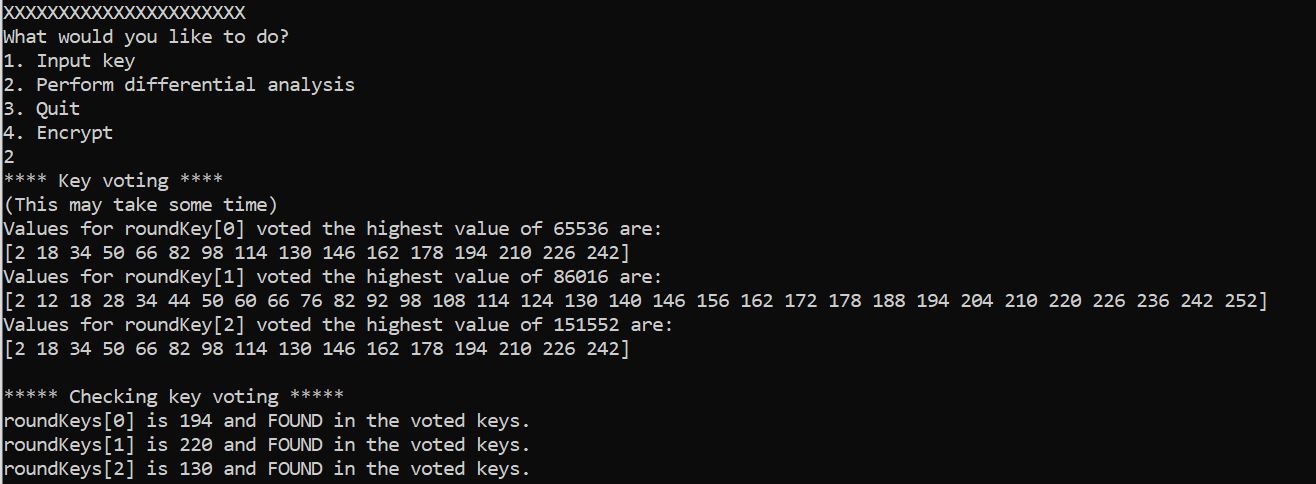


Figure 3.

In Fig.3 we notice that the system was able to vote for the round keys of each of the 3 rounds which are 194, 220 and 130 for rounds 0, 1 and 2 respectively.

Further key voting system to test the found round keys to find a single master key was explored and a start to such code is located in the analysis.cpp file. However, it does not have full functionality and has been commented out. Issue and errors occurred when back tracing through key scheduling.