Block Cipher

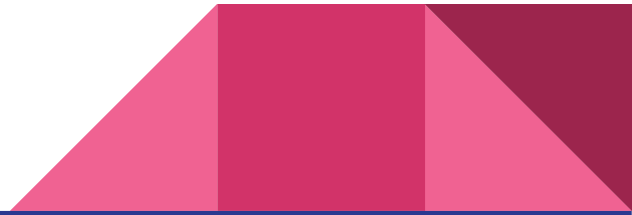
Y.Saikumar, EE14B067

Design Idea

The name of the cipher is Descartes named after the mathematician René Descartes.

I chose a feistel cipher for the design taking into account the conveniences for the implementation.

The design of the cipher is similar to that of any feistel cipher.



Design Idea

I initially analyzed the brute force difficulty over the linear and differential cryptanalysis and designed the cipher for ~18 rounds.

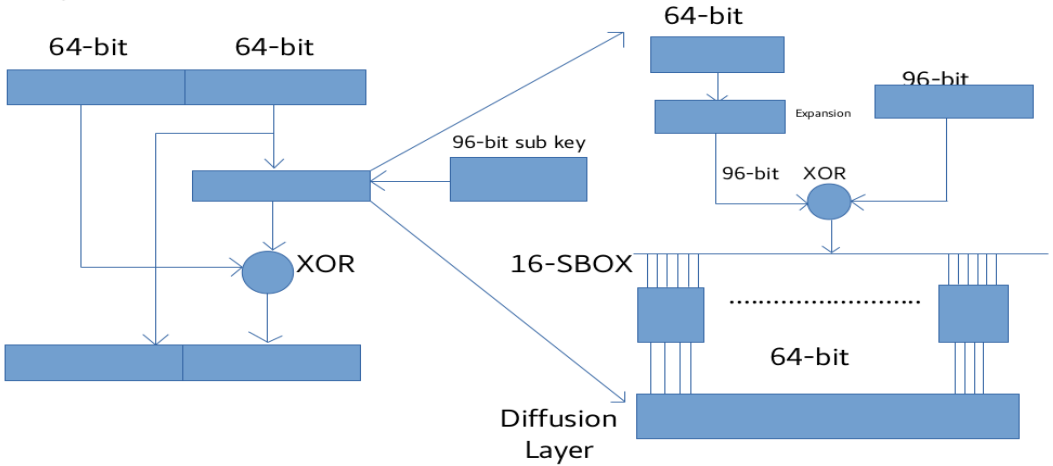
Following the second submission, I analyzed the differential and linear trails and using the equations below -

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

where n is the number of rounds and k is the keyspace, I got an estimate on the number of rounds required.

Design Idea

A single round in the cipher is -



SBOX

I used 4 different sboxes on a friend’s suggestion.

int sbox1[64]=
{14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7,0,15,4,7,14,2,13,1,10,6,12,11,9,5,3,8,4,1,14,8,13,
6,2,11,15,12,9,7,3,10,6,0,15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13};

int sbox2[64]=
{10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8,13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1,13,6,4,9,8,1
5,3,0,11,1,2,12,5,10,14,7,1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12};

SBOX

int sbox3[64]=
{7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15,13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9,10,6,9,0,12,
11,7,13,15,1,3,14,5,2,8,4,3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14};

int sbox4[64]=
{13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7,1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2,7,11,4,1,9,1
2,14,2,0,6,10,13,15,3,5,8,2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11};

SBOX

The linear and differential trails are shown in the following slides.

I used a C++ script to print the tables.

All the sboxes I chose are 16X4 compression sboxes. All of them doesn’t obey all the desired properties.

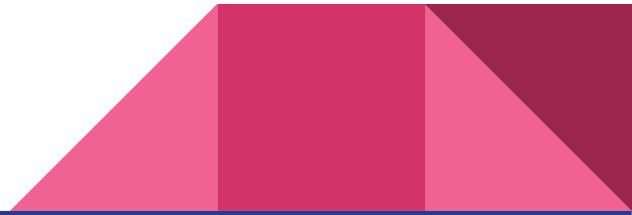
The analysis of a single sbox is given in my first report.

It doesn’t obey SAC property. It has a strong linearity property.

SBOX

A C++ code to check for non linearity is available in my submission. It just compares the output of the suggested sbox and checks it with affine transformations.

The following are the linear and differential trails in the sbox -



Linear Approximation Table

Linear Approximation tables for sboxes 1 and 2 -

64,33,31,32,32,31,33,32,32,33,31,32,32,31,33,32,
32,33,31,28,30,29,27,38,34,35,33,38,36,27,25,36,
32,33,31,28,30,33,27,26,30,35,41,34,32,31,25,44,
32,29,31,36,32,39,33,32,32,25,35,36,32,35,29,24,
32,35,31,38,26,27,31,28,28,27,35,30,34,31,31,32,
32,31,35,34,32,37,37,34,30,33,33,36,30,31,27,36,
32,31,31,38,32,33,33,34,34,33,37,28,34,27,39,32,
32,31,27,30,34,35,35,32,36,35,35,30,34,35,31,36,
32,33,35,32,30,33,35,26,32,37,35,28,38,29,27,14,
32,37,35,32,28,35,29,36,26,35,37,38,34,37,35,22,
32,37,31,36,24,27,37,32,34,39,29,34,38,33,31,34,
32,37,31,32,34,29,35,34,36,33,31,32,30,33,35,34,
32,35,39,34,32,37,37,34,36,31,35,38,32,29,29,34,
32,35,27,34,30,27,35,36,30,33,33,32,28,33,33,34,
32,27,35,34,34,27,31,28,30,29,37,32,32,37,33,34,
32,31,31,30,36,33,33,30,32,35,27,30,32,33,33,34,
32,33,31,32,32,31,33,32,32,33,31,32,32,31,33,32,
32,29,27,28,30,33,31,38,34,39,29,30,36,39,29,28,
32,29,31,32,30,29,27,30,34,27,29,34,36,23,29,28,
32,29,35,40,32,31,29,36,36,29,27,28,36,31,29,32,
32,31,39,26,30,27,35,28,32,27,31,38,34,27,31,28,
32,31,23,30,28,25,37,34,26,37,33,36,30,31,31,32,
32,39,31,38,36,29,29,30,34,33,37,36,30,39,27,28,
32,35,31,38,30,27,35,28,28,31,31,30,30,27,31,32,
32,33,31,28,34,29,27,42,28,33,35,28,30,29,31,26,
32,33,27,28,32,35,25,20,30,27,25,38,34,41,35,34,
32,33,35,28,28,35,37,28,42,35,33,34,26,33,39,30,
32,37,39,24,38,33,31,30,20,33,31,32,26,29,31,30,
32,31,35,26,32,25,33,34,36,27,39,38,32,33,33,26,
32,35,35,34,22,35,27,36,30,25,33,32,36,33,33,34,
32,35,31,30,34,27,27,32,34,33,29,32,20,33,25,26,
32,35,31,34,28,29,33,34,36,27,39,30,28,33,29,34,
32,31,33,32,32,33,31,32,32,31,33,32,32,33,31,32,
32,35,33,32,34,31,29,38,30,33,31,38,36,41,39,32,
32,35,25,24,34,35,37,34,34,33,31,34,32,37,23,32,
32,35,33,28,40,25,39,32,32,23,29,28,32,37,35,32,
32,37,29,30,30,29,29,32,36,37,33,38,30,25,45,36,
32,37,33,30,32,31,31,30,34,27,27,28,34,29,33,28,

64,32,32,32,32,32,32,32,32,32,32,32,32,32,32,32,
32,34,30,28,32,30,26,36,32,38,30,24,36,30,30,28,
32,28,32,32,34,30,26,34,32,36,36,28,26,22,38,30,
32,30,34,32,34,28,32,34,32,26,30,32,30,36,40,30,
32,32,38,26,32,32,34,30,30,34,32,40,38,34,36,28,
32,30,40,30,32,34,24,26,34,32,38,36,30,32,34,28,
32,32,30,30,34,42,36,28,34,30,32,28,36,24,38,26,
32,30,28,30,34,28,30,28,30,36,34,36,36,30,24,30,
32,32,34,30,34,34,40,36,34,38,28,44,28,24,34,42,
32,30,36,34,30,32,34,36,30,28,26,32,32,18,36,30,
32,36,26,30,28,32,34,30,34,26,24,32,38,30,32,32,
32,34,32,22,32,38,32,34,30,32,34,32,34,32,30,32,
32,32,36,28,34,34,30,30,28,36,36,36,30,38,38,30,
32,26,34,32,30,36,28,30,28,34,34,36,38,32,32,30,
32,32,28,32,28,36,24,36,32,24,36,32,28,36,40,36,
32,26,38,32,32,30,34,32,24,30,30,28,36,30,30,32,
32,32,32,32,32,32,32,32,32,32,32,32,32,32,32,32,
32,30,30,32,36,30,30,28,28,30,34,32,28,34,30,32,
32,32,32,28,34,34,34,38,32,32,36,32,34,26,38,34,
32,30,34,32,30,40,36,38,28,30,34,28,22,36,32,30,
32,32,34,30,32,24,30,26,30,34,28,28,30,34,40,32,
32,34,28,38,36,34,32,30,30,32,30,32,30,28,30,36,
32,28,34,30,34,30,32,44,34,34,36,36,36,36,34,34,
32,30,24,34,30,32,30,28,26,24,34,36,36,30,36,34,
32,32,30,34,30,30,32,36,30,34,36,28,36,32,22,38,
32,34,32,34,30,36,30,20,30,32,30,40,24,30,32,30,
32,40,30,38,32,40,34,34,30,34,24,28,30,34,36,32,
32,42,36,26,32,30,28,30,30,32,30,36,34,32,34,28,
32,40,28,28,30,30,34,34,32,32,32,40,22,30,22,30,
32,30,34,28,30,32,28,34,36,30,34,32,30,36,32,34,
32,36,36,36,32,36,28,28,36,40,32,32,36,32,32,40,
32,26,22,32,32,38,26,32,32,30,30,36,36,30,30,32,
32,32,32,32,32,32,32,32,32,32,32,32,32,32,32,32,
32,30,30,32,32,34,34,24,32,34,30,28,36,34,38,48,
32,36,32,40,34,30,26,34,36,32,24,40,38,34,34,26,
32,34,26,20,34,32,32,30,28,26,34,32,34,28,28,30,
32,32,34,30,32,40,38,34,30,26,28,36,30,42,32,32,
32,34,36,30,40,30,28,34,34,28,34,28,30,28,30,36,

Linear Approximation Table

Linear Approximation tables for sboxes 3 and 4 -

Implementation aspects and results

The implementation is trivial.

The components that needed attention were expansion box, diffusion layer.

The diffusion layer took 94 bit input and compressed it to 64 bits.

To ensure maximum diffusion, 24 bit inputs were taken and 16 bit outputs were given.

This was used 4 times.

Implementation aspects and results

In the diffusion box, the first four inputs were transmitted to the 0th, 4th, 8th, 12th bits of the output from the left respectively.

The Expansion box takes a 64-bit input and gives a 96-bit output.

This also uses a 16X24 plan.

Then we have the direct feistel implementation.

We are reading from the file one character at a time and storing 8 of these and calling the cipher.

Implementation aspects and results

The decryption is very much similar as this is a feistel cipher.

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

For Encryption

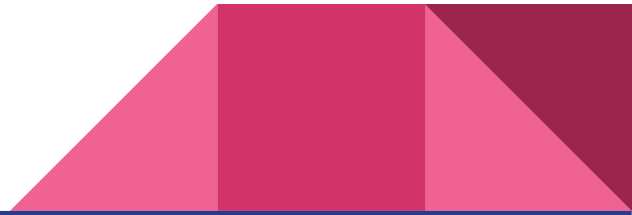
$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i).$$

For Decryption

Implementation aspects and results

Those were about the changes that needed to be done for decryption.

Working of the cipher will be demonstrated.



The End