Feistel Cipher

Akshay Abhyankar(111503001)
Aditya Jadhav(111503002)
Hamza Motiwalla(111503025)
Abhishek Jadhav(111503027)

- **Block Size**
  Following DES we used block size of 8 bytes.

- **Key Size**
  16 bytes.

- **Round Function**
  Key is being rotated 8 times. As key size is 16, rotating 8 times make it symmetric.
  Same can be used for decryption.

- **Key Generation**
  For sub-key generation, alternate characters are getting incremented and decremented.

- **Rounds**
  16

- **Sample Working:**

  Key: “ABCDEFGHIJKLMNOP”
  KeyinHex: 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50
  KeyinBin: 01000001 01000010 01000011 01000100
  01000101 01000110 01000111 01001000
  01001001 01001010 01001011 01001100
  01001101 01001110 01001111 01010000
  Message: “Feistal?”
  MessageinBin : 01000110 01100101 01101001 01110011

01110100 01100101 01101100 00111111

Block Size : 64bits
Blk1: 01000110 01100101 01101001 01110011
01110100 01100101 01101100 00111111

Splitting into Left and Right Blocks of 32bits

Left : 01000110 01100101 01101001 01110011 Feis
Right : 01110100 01100101 01101100 00111111 tal?

Key Generator:
Swaps 2 consecutive characters and then Swaps a block of Eight characters **once in the beginning**
Increments every even character of the key **every round by one**
Decrements every odd character of the key **every round by one**

Key:	ABCD	EFGH	IJKL	MNOP
RK0:	JILK	NMPO	BADC	FEHG
RK1:	KHMJ	OLQN	C@EB	GDIF
RK2:	LGNI	PKRM	D?FA	HCJE
.				
.				
.				
RK15:	Y:[<	]>_@	Q2S4	U6W8

However since the block size is 64bit and the Left and Right block are only 32bits, We use only the first 4 characters of every round key generator.

Round Function:
This function is used to combine the round key and the Right block.
The function swaps the first and second 16bit blocks of the Right32bit block.(ie cyclic rotate 16bits). And then XORS the round key with the swapped Right block.
The swapping increases Diffusion, and the XOR increases Confusion.

F(Right, Rn) = RKn XOR (cyclicrotate16(Right))

Round0:

RK0: JILK
Right: tal?
Left: Feis

Tmp = RK0 XOR cyclicrotate16(Right)
Tmp = “JILK” XOR “l?ta”
Tmp = 00100110 01110110 00111000 00101010 “&v8*”

Next, we perform XOR on Tmp and the Left Block.
Res = Left XOR Tmp
Res = 01100000 00010011 01010001 01011001 “`\x13QY”

……
…..
…

Round15:

RK0: Y:[<
Right: qNe\x1c
Left: ztM\x12

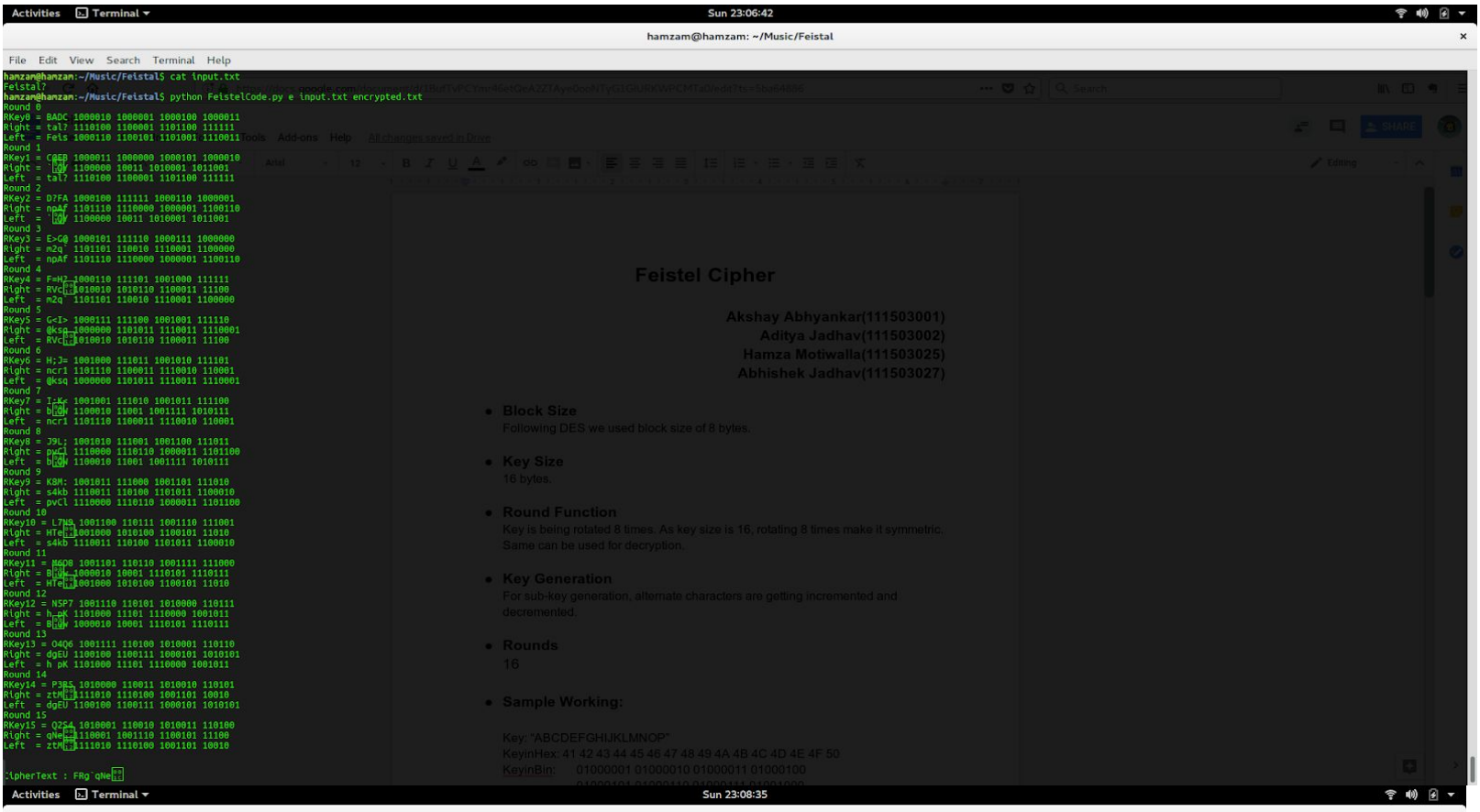
Tmp = RK15 XOR cyclicrotate16(Right)
Tmp = “Y:[<” XOR “e\x1cqN”
Tmp = 00111100 00100110 00101010 01110010 “<&*r”

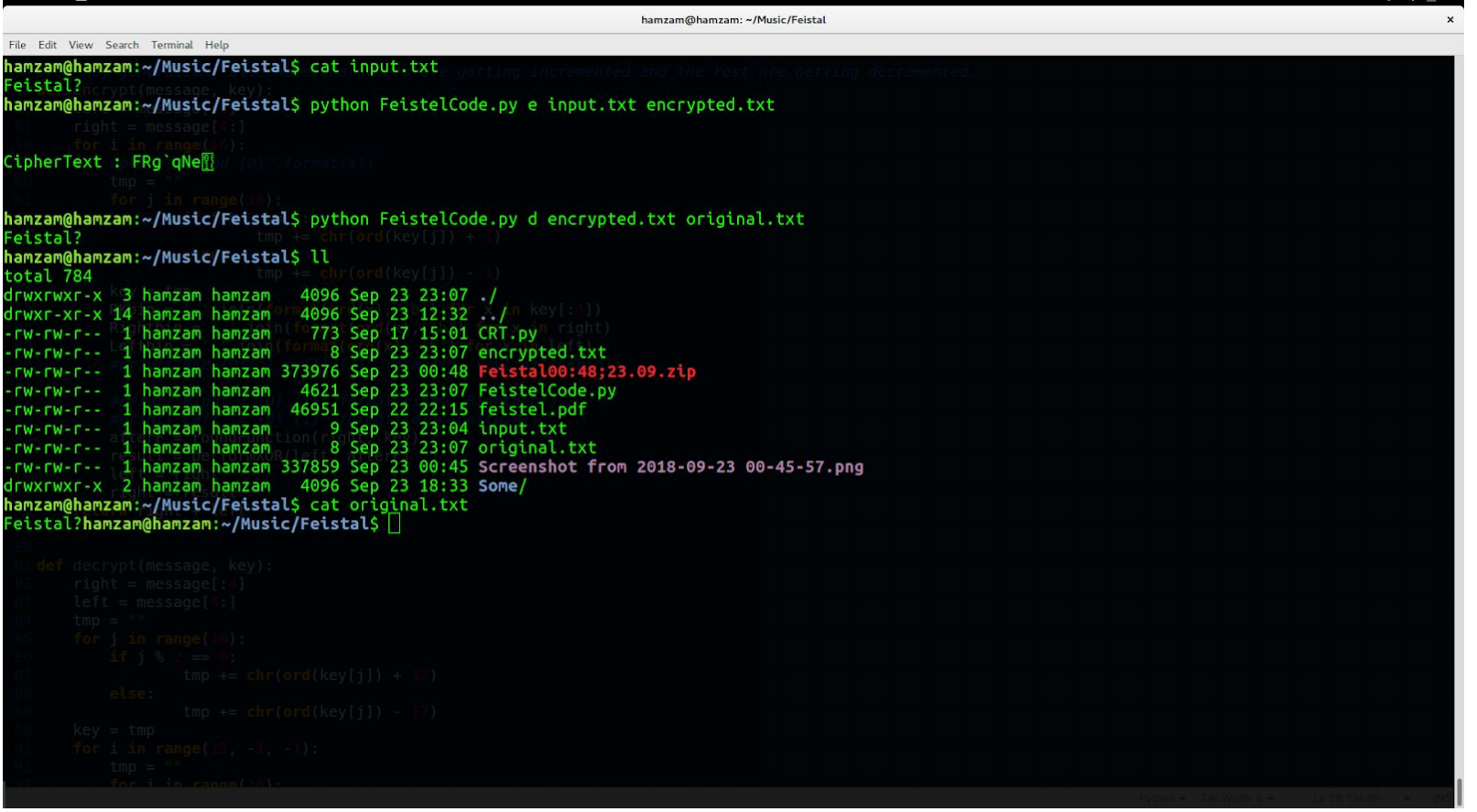
Next, we perform XOR on Tmp and the Left Block.
Res = Left XOR Tmp
Res = 01000110 01010010 01100111 01100000 “`FRg`”

----------xxxxxxx----------

Final Left : FRg`
Final Right : qNe\x1c

Orginal Msg: “Feistal?”
Encrypted Msd: “FRg`qNe\x1c”


Activities
Terminal
Sun 23:06:42
hamzam@hamzam: ~/Music/Feistal
File Edit View Search Terminal Help
hamzam@hanzan:~/Music/Feistal$ cat input.txt
Feistal?
hamzam@hanzan:~/Music/Feistal$ python FeistelCode.py e input.txt encrypted.txt
Round 0
RKey0 = BADC 1000010 1000001 1000100 1000011
Right = tal? 1110100 1100001 1101100 111111
Left = Feis 1000110 1100101 1101001 1110011
Round 1
RKey1 = C@EB 1000011 1000000 1000101 1000010
Right = [@W 1100000 10011 1010001 1011001
Left = tal? 1110100 1100001 1101100 111111
Round 2
RKey2 = D7FA 1000100 111111 1000110 1000001
Right = npAf 1101110 1110000 1000001 1100110
Left = [@W 1100000 10011 1010001 1011001
Round 3
RKey3 = E>G@ 1000101 111110 1000111 1000000
Right = m2q` 1101101 110010 1110001 1100000
Left = npAf 1101110 1110000 1000001 1100110
Round 4
RKey4 = F=H2 1000110 111101 1001000 111111
Right = RVc[1010010 1010110 1100011 11100
Left = m2q` 1101101 110010 1110001 1100000
Round 5
RKey5 = G<I> 1000111 111100 1001001 111110
Right = @ksq 1000000 1101011 1110011 1110001
Left = RVc[1010010 1010110 1100011 11100
Round 6
RKey6 = H;J= 1001000 111011 1001010 111101
Right = ncr1 1101110 1100011 1110010 110001
Left = @ksq 1000000 1101011 1110011 1110001
Round 7
RKey7 = I:K< 1001001 111010 1001011 111100
Right = b[qW 1100010 11001 1001111 1010111
Left = ncr1 1101110 1100011 1110010 110001
Round 8
RKey8 = J9L; 1001010 111001 1001100 111011
Right = pvCl 1110000 1110110 1000011 1101100
Left = b[qW 1100010 11001 1001111 1010111
Round 9
RKey9 = K8M: 1001011 111000 1001101 111010
Right = s4kb 1110011 1101100 1101011 1100010
Left = pvCl 1110000 1110110 1000011 1101100
Round 10
RKey10 = L7N9 1001100 110111 1001110 111001
Right = HTe[1001000 1010100 1100101 11010
Left = s4kb 1110011 1101100 1101011 1100010
Round 11
RKey11 = M6O8 1001101 110110 1001111 111000
Right = B[qW 1000010 10001 1110101 1110111
Left = HTe[1001000 1010100 1100101 11010
Round 12
RKey12 = N5P7 1001110 110101 1010000 110111
Right = h pK 1101000 11101 1110000 1001011
Left = B[qW 1000010 10001 1110101 1110111
Round 13
RKey13 = O4Q6 1001111 110100 1010001 110110
Right = dgEU 1100100 1100111 1000101 1010101
Left = h pK 1101000 11101 1110000 1001011
Round 14
RKey14 = P3R5 1010000 110011 1010010 110101
Right = ztM[1111010 1110100 1001101 10010
Left = dgEU 1100100 1100111 1000101 1010101
Round 15
RKey15 = Q2S4 1010001 110010 1010011 110100
Right = qNe[1110001 1001110 1100101 11100
Left = ztM[1111010 1110100 1001101 10010
CipherText : FRg`qNe[
Feistel Cipher
Akshay Abhyankar(111503001)
Aditya Jadhav(111503002)
Hamza Motiwalla(111503025)
Abhishek Jadhav(111503027)
Block Size
Following DES we used block size of 8 bytes.
Key Size
16 bytes.
Round Function
Key is being rotated 8 times. As key size is 16, rotating 8 times make it symmetric.
Same can be used for decryption.
Key Generation
For sub-key generation, alternate characters are getting incremented and decremented.
Rounds
16
Sample Working:
Key: "ABCDEFGHIJKLMNOP"
KeyinHex: 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50
KeyinBin: 01000001 01000010 01000011 01000100


Activities
Terminal
Sun 23:08:35
hamzam@hamzam: ~/Music/Feistal
File Edit View Search Terminal Help
hamzam@hamzam:~/Music/Feistal$ cat input.txt
Feistal?
hamzam@hamzam:~/Music/Feistal$ python FeistelCode.py e input.txt encrypted.txt
CipherText : FRg`qNe[
hamzam@hamzam:~/Music/Feistal$ python FeistelCode.py d encrypted.txt original.txt
Feistal?
hamzam@hamzam:~/Music/Feistal$ ll
total 784
drwxrwxr-x 3 hamzam hamzam 4096 Sep 23 23:07 ./
drwxr-xr-x 14 hamzam hamzam 4096 Sep 23 12:32 ../
-rw-rw-r-- 1 hamzam hamzam 773 Sep 17 15:01 CRT.py
-rw-rw-r-- 1 hamzam hamzam 8 Sep 23 23:07 encrypted.txt
-rw-rw-r-- 1 hamzam hamzam 373976 Sep 23 00:48 Feistal00:48;23.09.zip
-rw-rw-r-- 1 hamzam hamzam 4621 Sep 23 23:07 FeistelCode.py
-rw-rw-r-- 1 hamzam hamzam 46951 Sep 22 22:15 feistel.pdf
-rw-rw-r-- 1 hamzam hamzam 9 Sep 23 23:04 input.txt
-rw-rw-r-- 1 hamzam hamzam 8 Sep 23 23:07 original.txt
-rw-rw-r-- 1 hamzam hamzam 337859 Sep 23 00:45 Screenshot from 2018-09-23 00-45-57.png
drwxrwxr-x 2 hamzam hamzam 4096 Sep 23 18:33 Some/
hamzam@hamzam:~/Music/Feistal$ cat original.txt
Feistal?hamzam@hamzam:~/Music/Feistal$