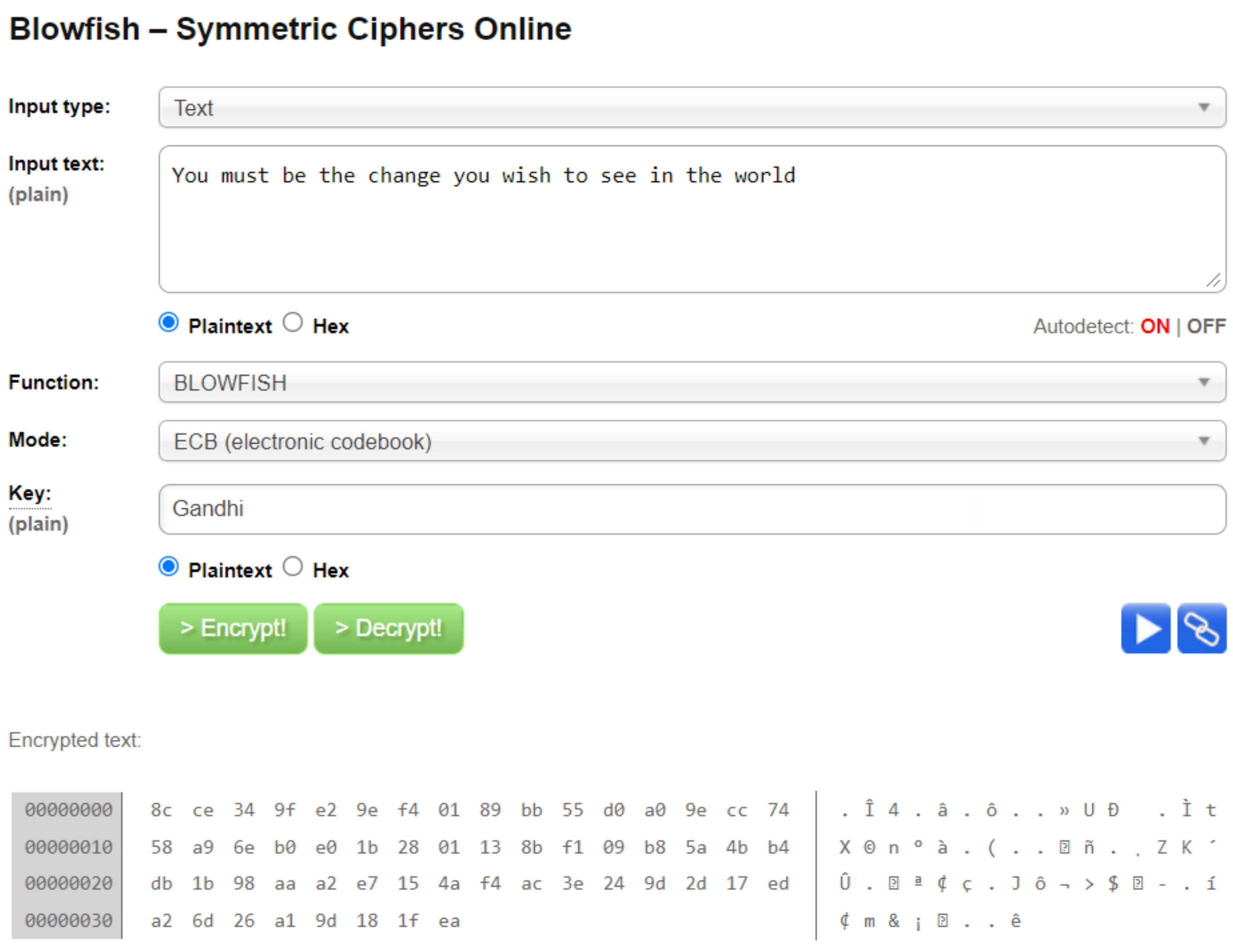
Experiment 5: Blowfish Encryption

Name: Deep Nayak **UID**: 2019130045 TE COMPS

AIM : The aim of this lab is to experiment with an online encryption tool. We will encode a message and send it to someone else in the class, who will decode it when we supply the secret key. Note that this particular tool is of limited use in a security context, since the plaintext of the message is sent to and from the encryption website! However, it could be used to prevent people from reading your email. A similar tool downloaded and running on your computer would provide a greater level of security. Some email clients even provide support for automatic encryption and decryption of all messages.
Website Used: http://blowfish.online-domain-tools.com

PROBLEM STATEMENT :

- **Go to the encryption tool website and try it out. Try the following experiments and note how they change the output:**



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
You must be the change you wish to see in the world
```

◉ Plaintext ○ Hex   Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

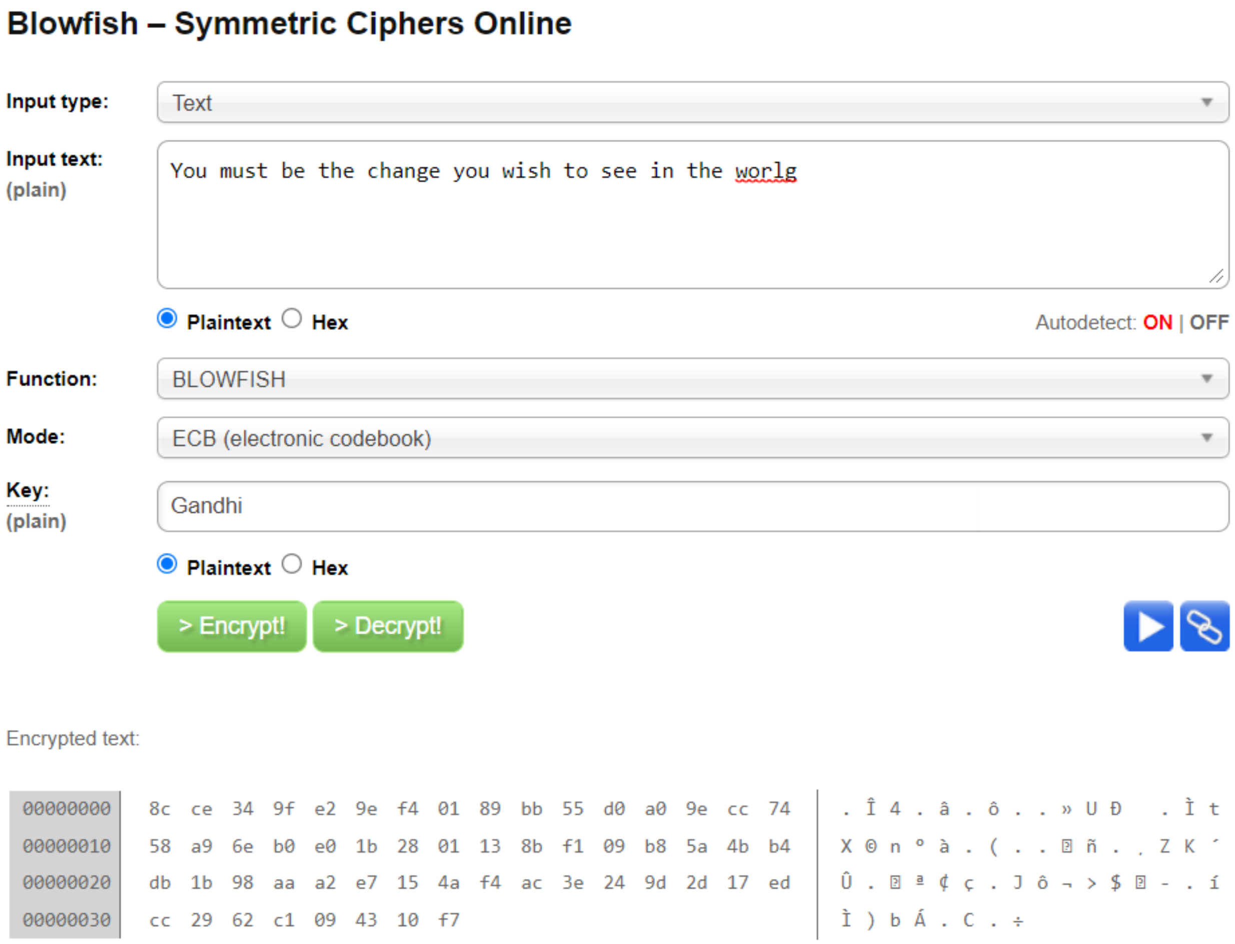
Key: (plain) Gandhi

◉ Plaintext ○ Hex

Encrypted text:

```
00000000  8c ce 34 9f e2 9e f4 01 89 bb 55 d0 a0 9e cc 74  | . Î 4 . â . ô . . » U Ð   . Ì t
00000010  58 a9 6e b0 e0 1b 28 01 13 8b f1 09 b8 5a 4b b4  | X © n ° à . ( . . � ñ . ¸ Z K ´
00000020  db 1b 98 aa a2 e7 15 4a f4 ac 3e 24 9d 2d 17 ed  | Û . � ª ¢ ç . J ô ¬ > $ � - . í
00000030  a2 6d 26 a1 9d 18 1f ea                          | ¢ m & ¡ � . . ê
```

- **Change one character at the end of the message. How much of the encoded message changes?**



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
You must be the change you wish to see in the worlg
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

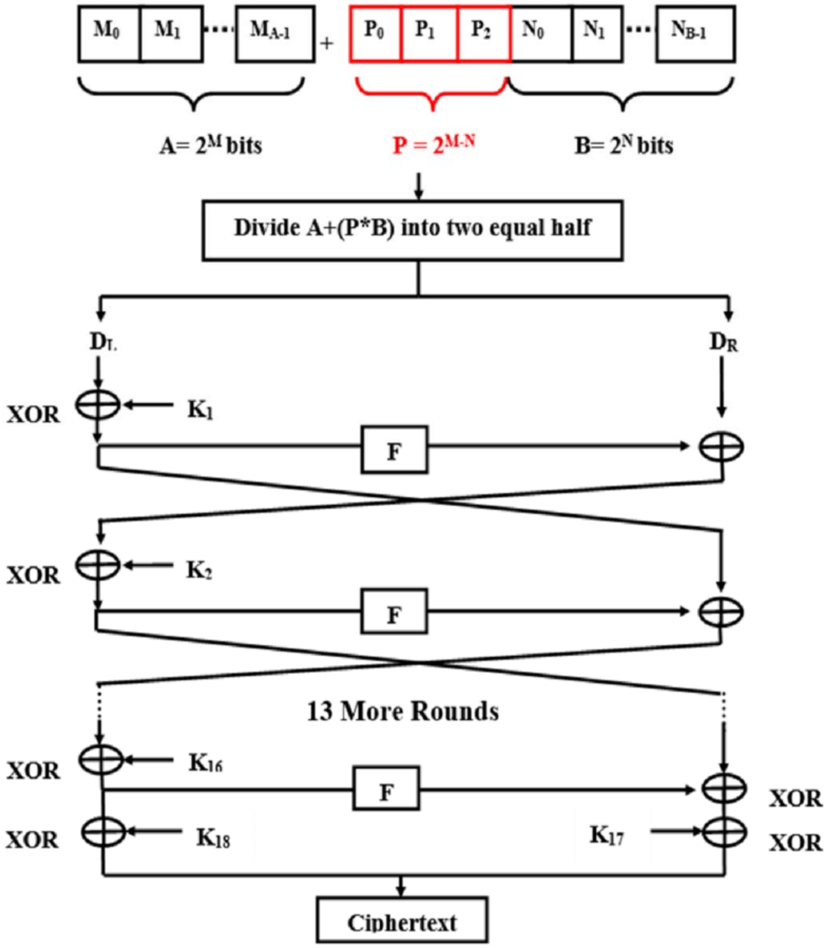
Mode: ECB (electronic codebook)

Key: (plain) Gandhi

● Plaintext ○ Hex

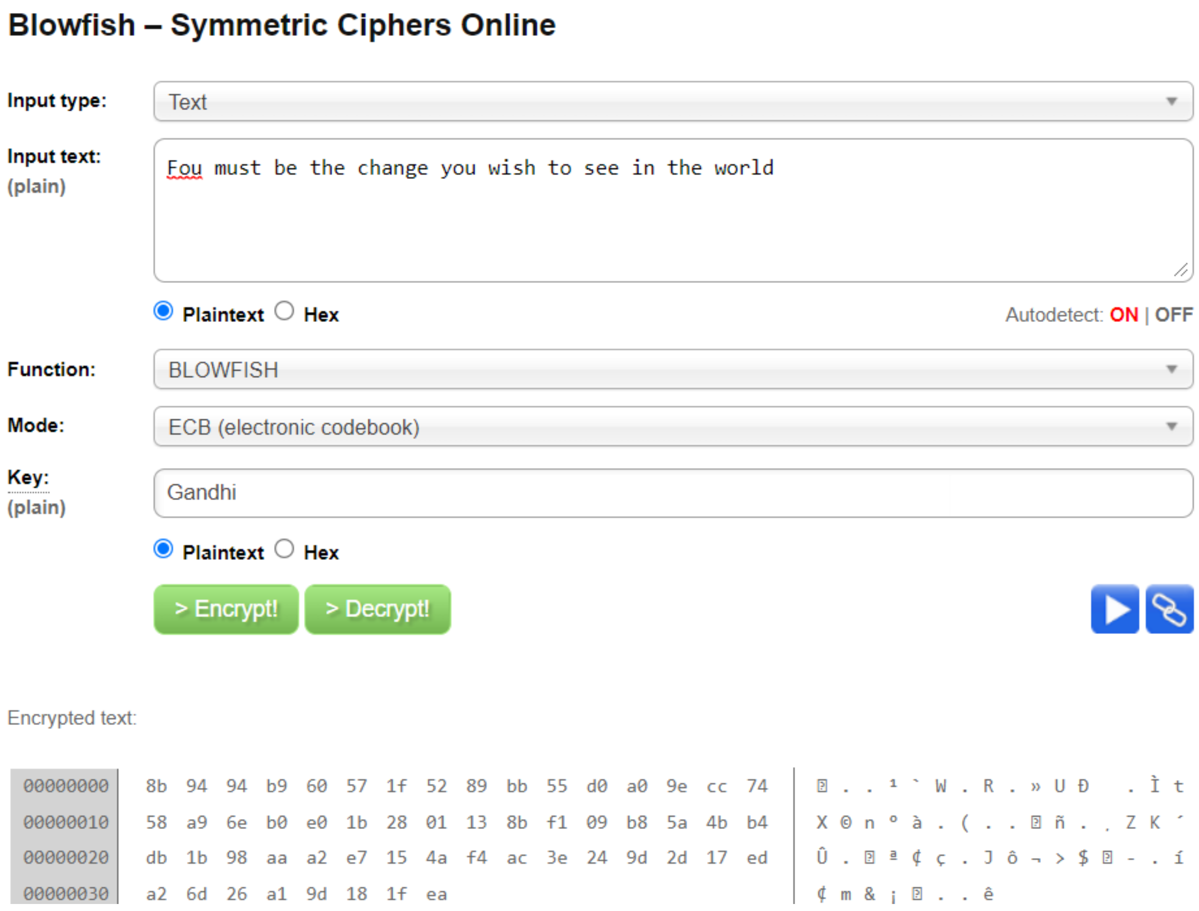
Encrypted text:

```
00000000   8c ce 34 9f e2 9e f4 01 89 bb 55 d0 a0 9e cc 74  | . Î 4 . â . ô . . » U Ð   . Ì t
00000010   58 a9 6e b0 e0 1b 28 01 13 8b f1 09 b8 5a 4b b4  | X © n ° à . ( . . ⍰ ñ . ¸ Z K ´
00000020   db 1b 98 aa a2 e7 15 4a f4 ac 3e 24 9d 2d 17 ed  | Û . ⍰ ª ¢ ç . J ô ¬ > $ ⍰ - . í
00000030   cc 29 62 c1 09 43 10 f7                          | Ì ) b Á . C . ÷
```



Every round in the blowfish algorithm, swaps the right text with the left text and performs an XOR operation. Since there are 16 rounds in total, the rightmost text remains in the right in the encrypted text as well. However, the entire right block is affected and this can be seen in the result.

- **Change one character at the beginning of the message. How much of the encoded message changes?**



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
Fou must be the change you wish to see in the world
```

● Plaintext ○ Hex Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) Gandhi

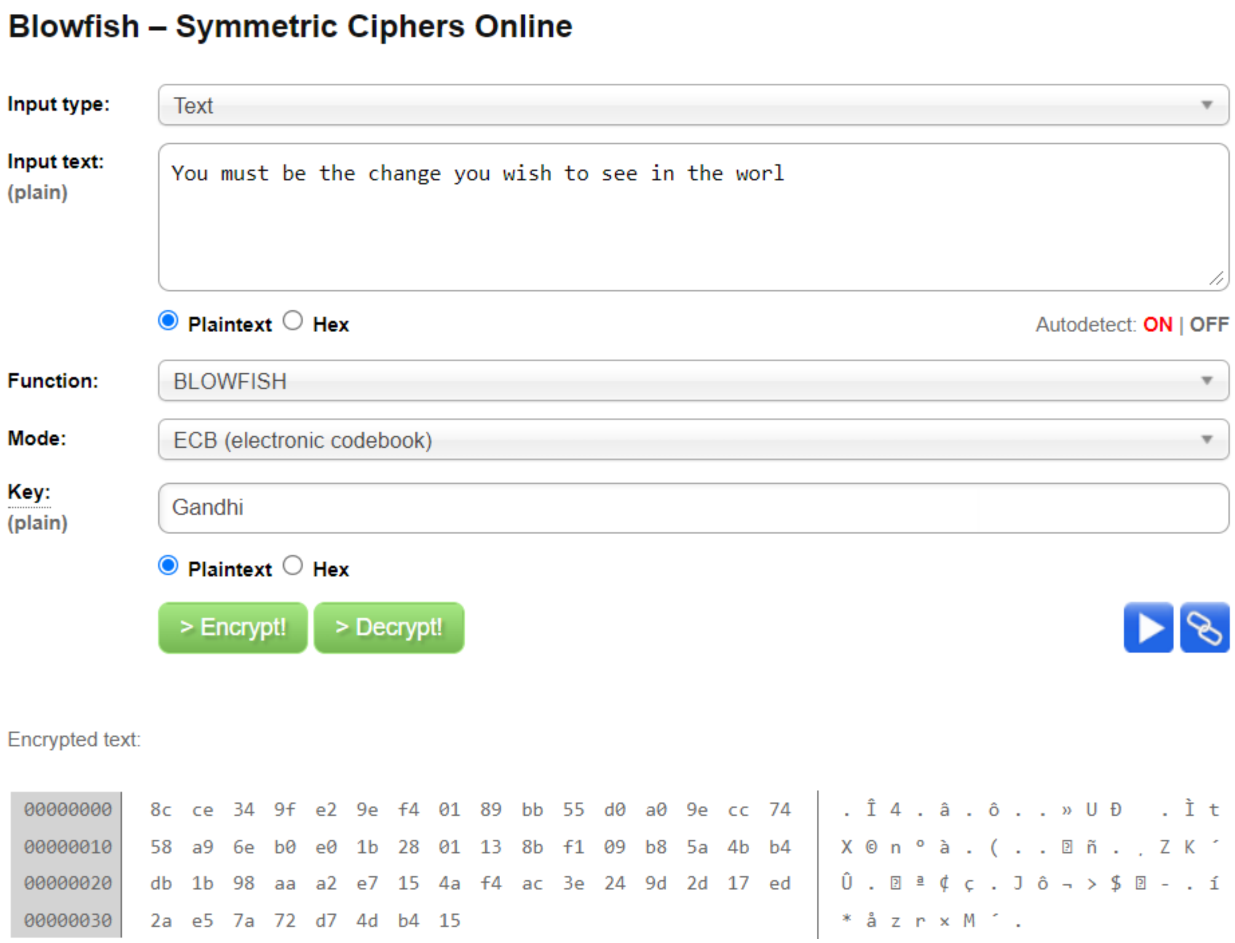
● Plaintext ○ Hex

Encrypted text:

```
00000000  8b 94 94 b9 60 57 1f 52 89 bb 55 d0 a0 9e cc 74 | ▯ . . ¹ ` W . R . » U Ð   . Ì t
00000010  58 a9 6e b0 e0 1b 28 01 13 8b f1 09 b8 5a 4b b4 | X © n ° à . ( . . ▯ ñ . ¸ Z K ´
00000020  db 1b 98 aa a2 e7 15 4a f4 ac 3e 24 9d 2d 17 ed | Û . ▯ ª ¢ ç . J ô ¬ > $ ▯ - . í
00000030  a2 6d 26 a1 9d 18 1f ea                         | ¢ m & ¡ ▯ . . ê
```

Similar to the above case the entire left block ended up changing on account of replacing a Y by F and this behavior can be mapped to the block cipher property of Blowfish.

- **Delete one character at the end of the message. How much of the encoded message changes?**



Blowfish – Symmetric Ciphers Online

Input type: Text ▾

Input text: (plain)

```
You must be the change you wish to see in the worl
```

● Plaintext ○ Hex — Autodetect: ON | OFF

Function: BLOWFISH ▾

Mode: ECB (electronic codebook) ▾

Key: (plain) Gandhi

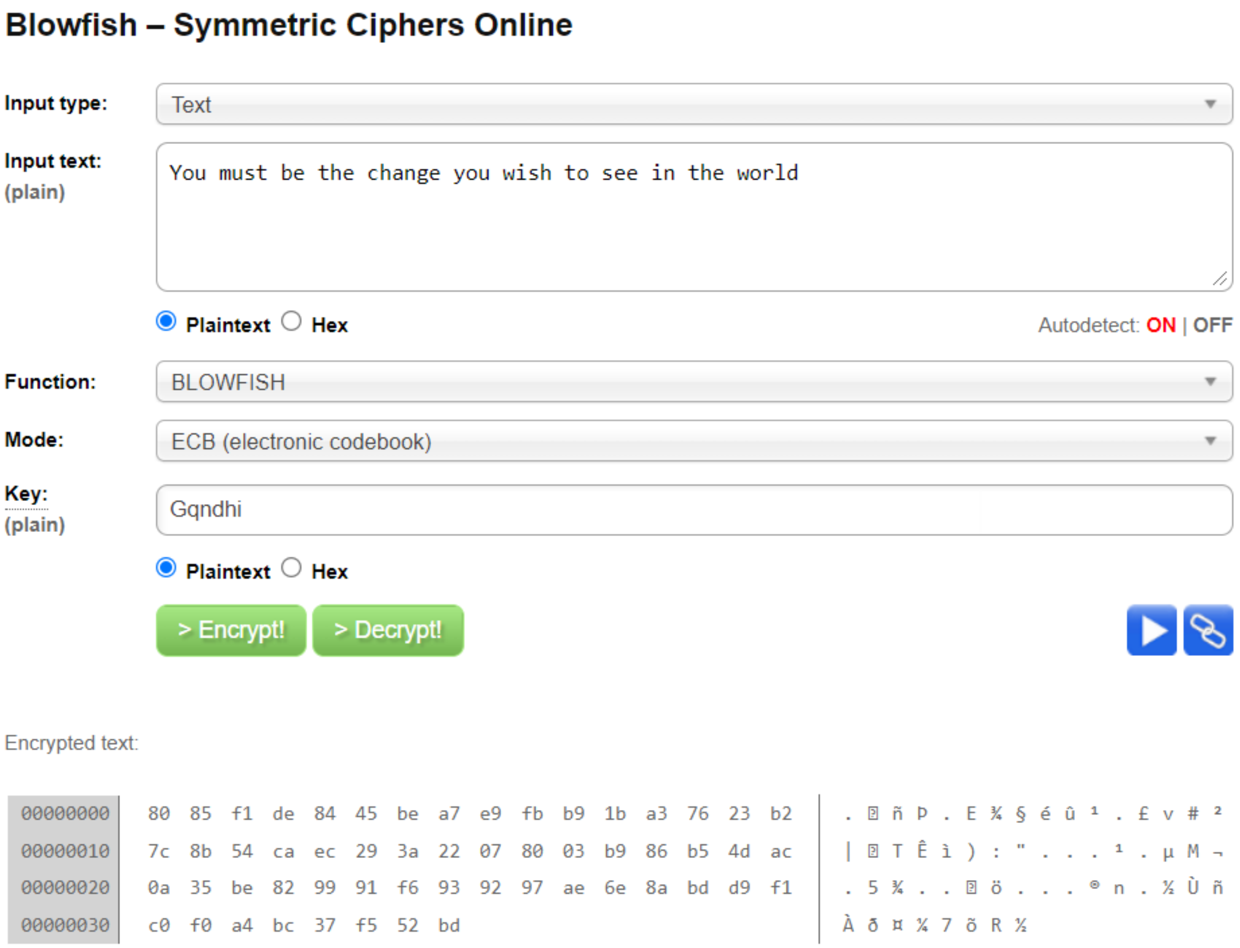
● Plaintext ○ Hex

Encrypted text:

```
00000000   8c ce 34 9f e2 9e f4 01 89 bb 55 d0 a0 9e cc 74   . Î 4 . â . ô . . » U Ð   . Ì t
00000010   58 a9 6e b0 e0 1b 28 01 13 8b f1 09 b8 5a 4b b4   X © n º à . ( . . ⍰ ñ . ¸ Z K ´
00000020   db 1b 98 aa a2 e7 15 4a f4 ac 3e 24 9d 2d 17 ed   Û . ⍰ ª ¢ ç . J ô ¬ > $ ⍰ - . í
00000030   2a e5 7a 72 d7 4d b4 15                           * å z r × M ´ .
```

After removing the last character, the entire last block changes.

- **Change one character in the key. How much of the encoded message changes?**



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
You must be the change you wish to see in the world
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) Gqndhi

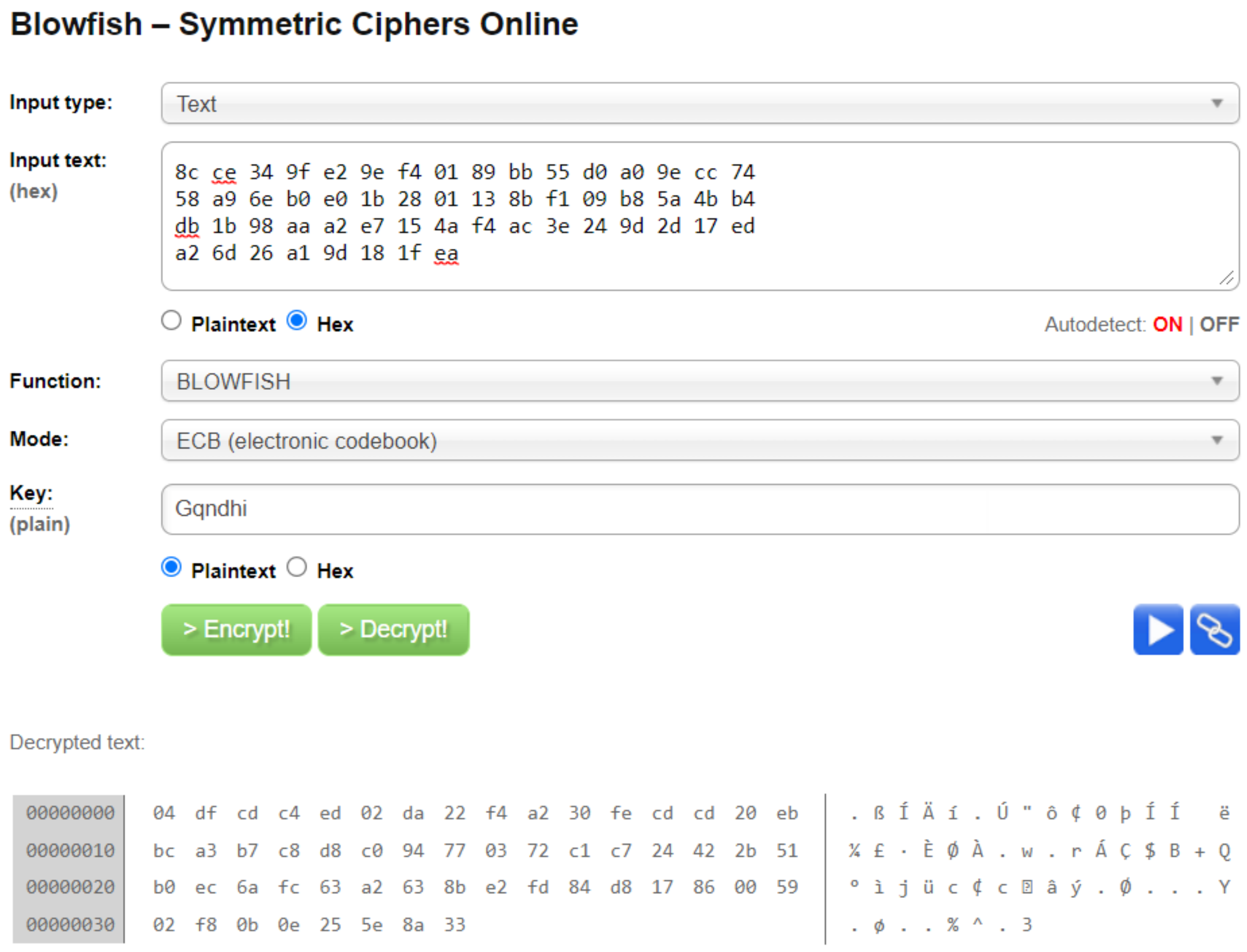
● Plaintext ○ Hex

Encrypted text:

```
00000000  80 85 f1 de 84 45 be a7 e9 fb b9 1b a3 76 23 b2  | . ⍰ ñ Þ . E ¾ § é û ¹ . £ v # ²
00000010  7c 8b 54 ca ec 29 3a 22 07 80 03 b9 86 b5 4d ac  | | ⍰ T Ê ì ) : " . . . ¹ . µ M ¬
00000020  0a 35 be 82 99 91 f6 93 92 97 ae 6e 8a bd d9 f1  | . 5 ¾ . . ⍰ ö . . . ® n . ½ Ù ñ
00000030  c0 f0 a4 bc 37 f5 52 bd                          | À ð ¤ ¼ 7 õ R ½
```

The entire encrypted text is changed. Because blowfish is a symmetric encryption technique, the value of P i(Permutation Box values) is fully reliant on the key, which changes in each loop; even a tiny change in the key will result in a completely different encrypted text.

- **Decrypt a message using a key with one character changed. Does it look anything like the original?**



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
8c ce 34 9f e2 9e f4 01 89 bb 55 d0 a0 9e cc 74
58 a9 6e b0 e0 1b 28 01 13 8b f1 09 b8 5a 4b b4
db 1b 98 aa a2 e7 15 4a f4 ac 3e 24 9d 2d 17 ed
a2 6d 26 a1 9d 18 1f ea
```

○ Plaintext ● Hex

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) Gqndhi

● Plaintext ○ Hex

Decrypted text:

```
00000000  04 df cd c4 ed 02 da 22 f4 a2 30 fe cd cd 20 eb  | . ß Í Ä í . Ú " ô ¢ 0 þ Í Í   ë
00000010  bc a3 b7 c8 d8 c0 94 77 03 72 c1 c7 24 42 2b 51  | ¼ £ · È Ø À . w . r Á Ç $ B + Q
00000020  b0 ec 6a fc 63 a2 63 8b e2 fd 84 d8 17 86 00 59  | ° ì j ü c ¢ c ⍰ â ý . Ø . . . Y
00000030  02 f8 0b 0e 25 5e 8a 33                          | . ø . . % ^ . 3
```

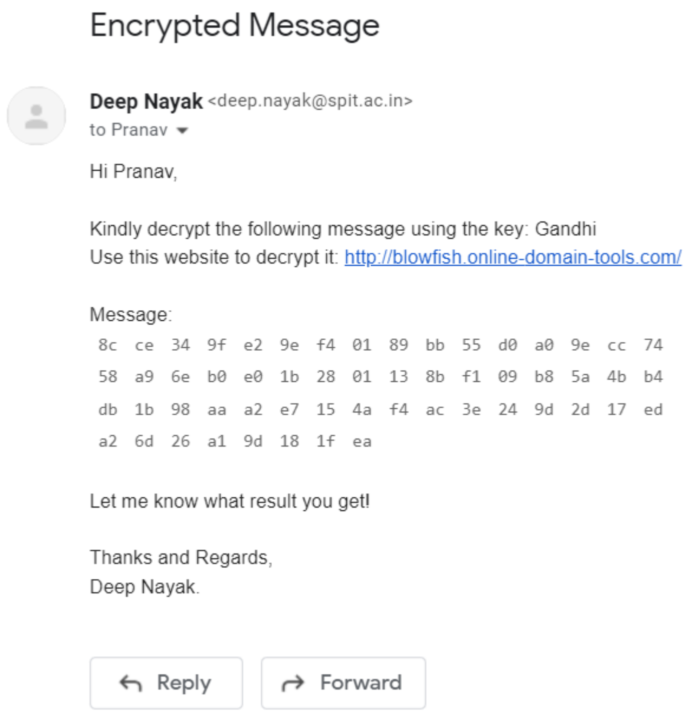
When you decrypt a message with a different key, you receive a completely new message. The real plain text and the message obtained in the latter situation have no resemblance at all.

A Secret Message When you have finished the above, see if you can decode the following message.

E2D472B6E8EA93AECD0D518D04DF3188 715D3AF7877684AC34EEB0FF3768B8DD
9E227C12E7340390987FDD12F9B9C156
F05A0748FBACFBC48D4B70C99780413F
652E6676330AC76F1DE7380E81B12E11 (Blowfish: By PV-J)

Does not work since a key is not provided

Now it is time to send a secret message to someone else in the class. Use the tool to encode your message (without your partner seeing it) and copy the encoded text into an email. Send the key in a separate email, or tell it to the recipient. She/He should be able to decode the message using the same tool.



Encrypted Message

Deep Nayak <deep.nayak@spit.ac.in>
to Pranav

Hi Pranav,

Kindly decrypt the following message using the key: Gandhi
Use this website to decrypt it: http://blowfish.online-domain-tools.com/

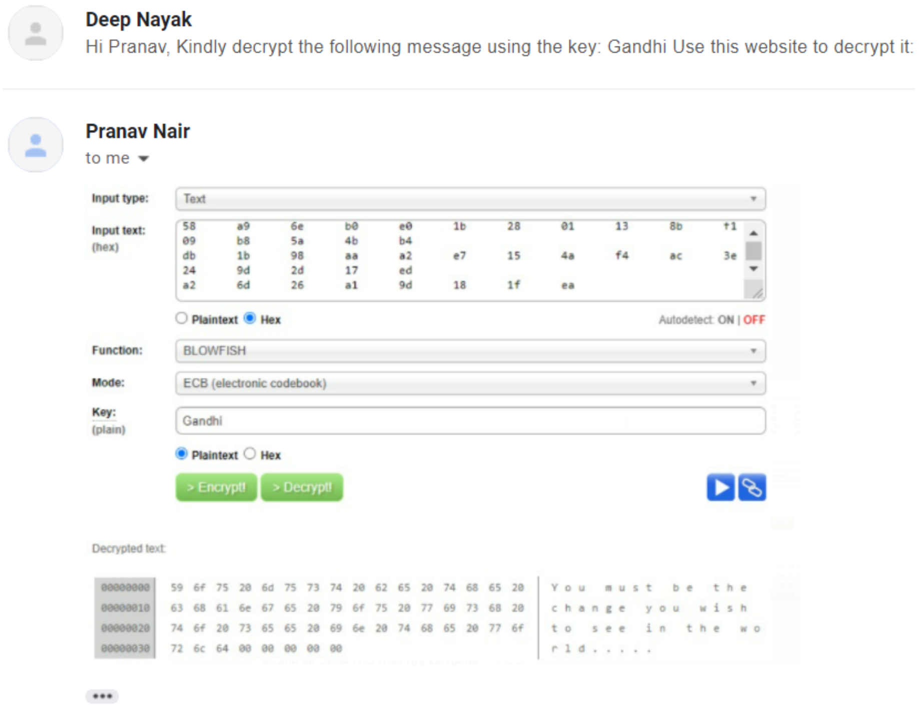
Message:

```
8c  ce  34  9f  e2  9e  f4  01  89  bb  55  d0  a0  9e  cc  74
58  a9  6e  b0  e0  1b  28  01  13  8b  f1  09  b8  5a  4b  b4
db  1b  98  aa  a2  e7  15  4a  f4  ac  3e  24  9d  2d  17  ed
a2  6d  26  a1  9d  18  1f  ea
```

Let me know what result you get!

Thanks and Regards,
Deep Nayak.

Output Obtained by friend :



Deep Nayak
Hi Pranav, Kindly decrypt the following message using the key: Gandhi Use this website to decrypt it:

Pranav Nair
to me

Input type: Text

Input text: (hex)

```
58    a9    6e    b0    e0    1b    28    01    13    8b    f1
09    b8    5a    4b    b4
db    1b    98    aa    a2    e7    15    4a    f4    ac    3e
24    9d    2d    17    ed
a2    6d    26    a1    9d    18    1f    ea
```

○ Plaintext ● Hex Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) Gandhi

● Plaintext ○ Hex

Decrypted text:

```
00000000  59 6f 75 20 6d 75 73 74 20 62 65 20 74 68 65 20 | You must be the 
00000010  63 68 61 6e 67 65 20 79 6f 75 20 77 69 73 68 20 | change you wish 
00000020  74 6f 20 73 65 65 20 69 6e 20 74 68 65 20 77 6f | to see in the wo
00000030  72 6c 64 00 00 00 00 00                         | rld.....
```

CONCLUSION

1. Through this experiment I learnt about Blowfish Encryption Algorithm and its working. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.
2. I verified that Blowfish is a block cipher since changing one character of the original text changed an entire block of the cipher text.
3. I also learnt that Blowfish is a symmetric cipher since the same key is used for encryption and decryption

Github Link:

https://github.com/deepnayak/CSS-Lab-Deep-Nayak/tree/master/Experiment%205