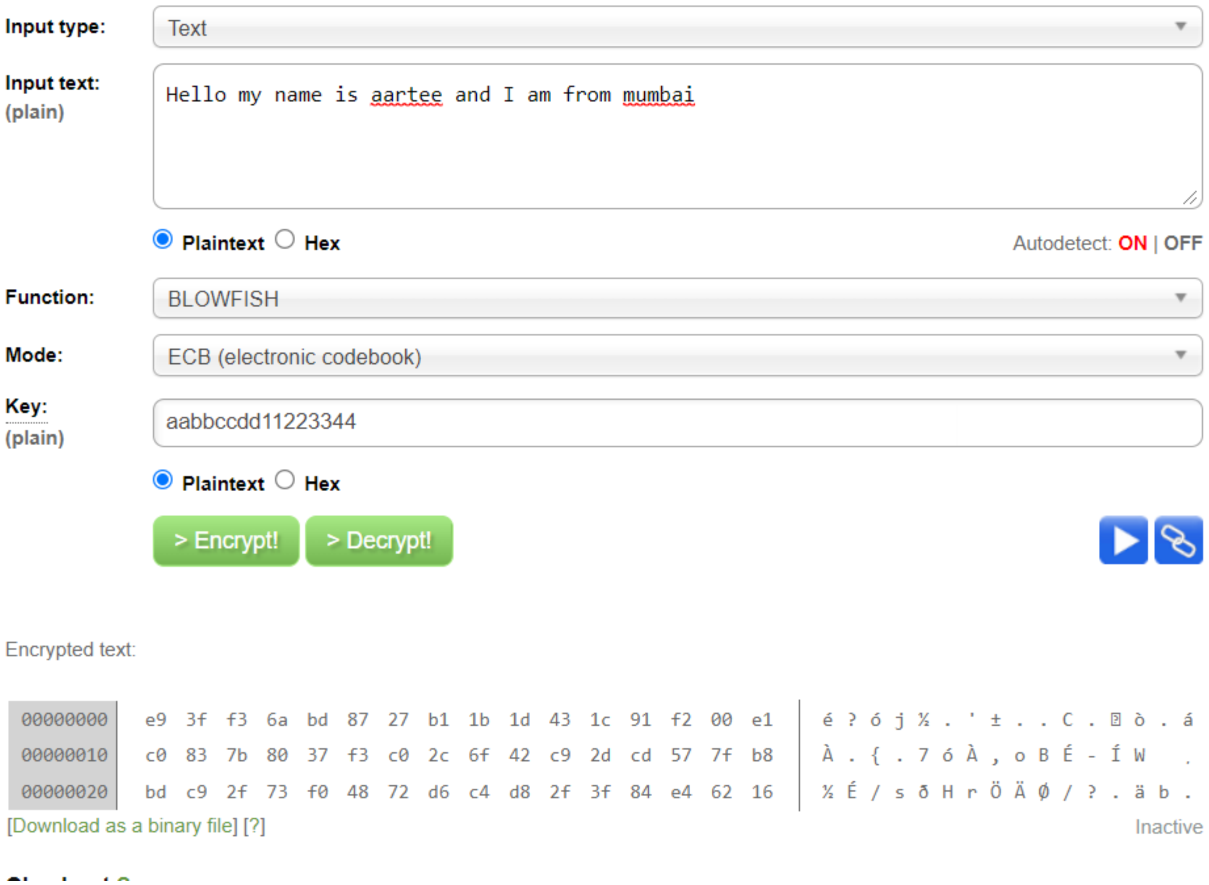
EXPERIMENT : 5

NAME : Aartee chimate
BRANCH : IT
UID : 2018140012
BATCH : A
COURSE : CSS LAB

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.

1) **Go to the encryption tool website and try it out. Enter a short key phrase and a longer piece of text to be encoded. Then submit and see what your text looks like when encrypted. Try the following experiments and note how they change the output:**



Input type: Text

Input text: (plain)

```
Hello my name is aartee and I am from mumbai
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

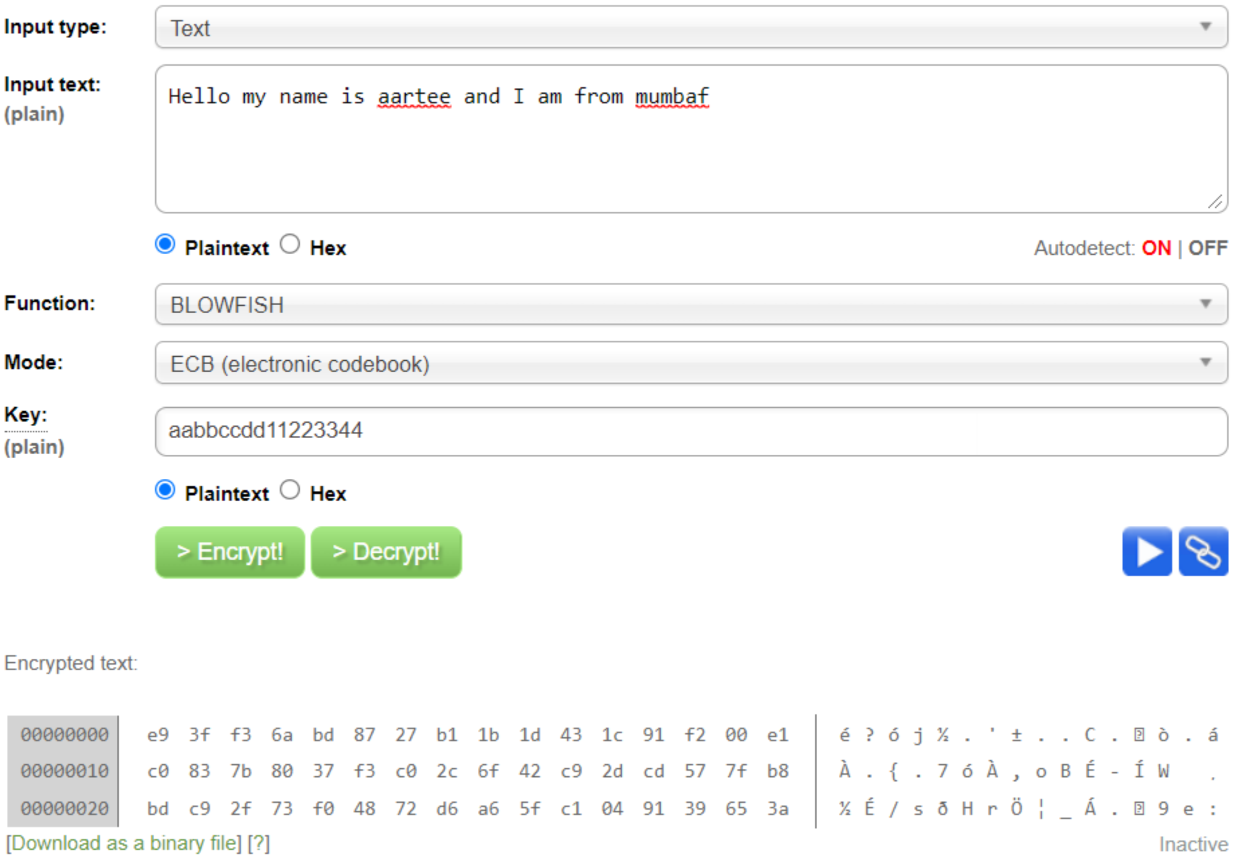
Key: (plain) aabbccdd11223344

● Plaintext ○ Hex

Encrypted text:

```
00000000   e9 3f f3 6a bd 87 27 b1 1b 1d 43 1c 91 f2 00 e1   é ? ó j ½ . ' ± . . C . ? ò . á
00000010   c0 83 7b 80 37 f3 c0 2c 6f 42 c9 2d cd 57 7f b8   À . { . 7 ó À , o B É - Í W   .
00000020   bd c9 2f 73 f0 48 72 d6 c4 d8 2f 3f 84 e4 62 16   ½ É / s ð H r Ö Ä Ø / ? . ä b .
```

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



Input type: Text

Input text: (plain)

```
Hello my name is aartee and I am from mumbaf
```

● Plaintext ○ Hex   Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) aabbccdd11223344

● Plaintext ○ Hex

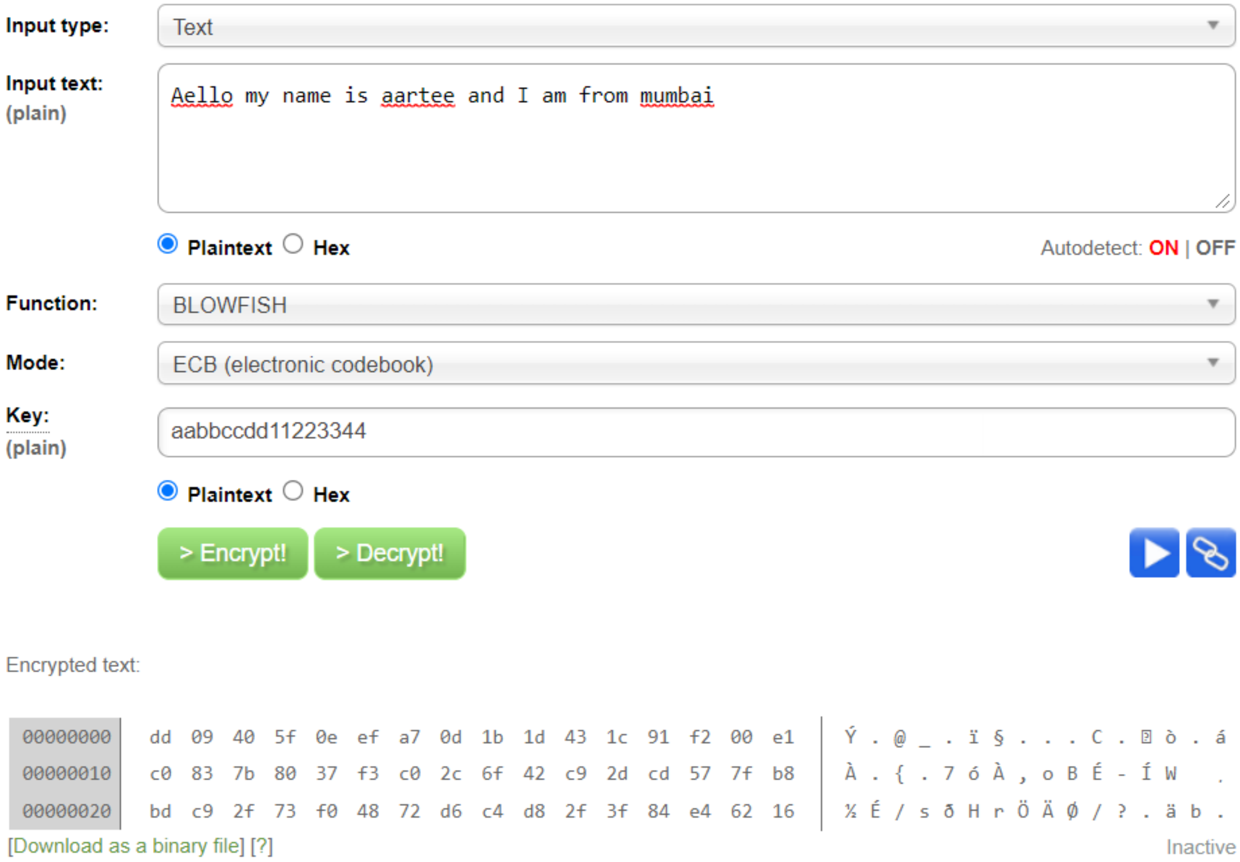
Encrypted text:

```
00000000   e9 3f f3 6a bd 87 27 b1 1b 1d 43 1c 91 f2 00 e1   é ? ó j ½ . ' ± . . C . ⍰ ò . á
00000010   c0 83 7b 80 37 f3 c0 2c 6f 42 c9 2d cd 57 7f b8   À . { . 7 ó À , o B É - Í W   .
00000020   bd c9 2f 73 f0 48 72 d6 a6 5f c1 04 91 39 65 3a   ½ É / s ð H r Ö ¦ _ Á . ⍰ 9 e :
```

[Download as a binary file] [?]   Inactive

- **Blowfish is a symmetric key block cipher. If we take 64 bit plain text and split it into half. We call the first half L and second half R. We enter a loop which we repeat 16 times.so there is change in the right part itself But then it gets inverted everytime, all the 16 times but finally when the loop ends the changed value comes back to the right most part.**
- **If we do a small change in bit in the plaintext we will get a significant change in our cipher text.**

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



Input type: Text

Input text: (plain)

```
Aello my name is aartee and I am from mumbai
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) aabbccdd11223344

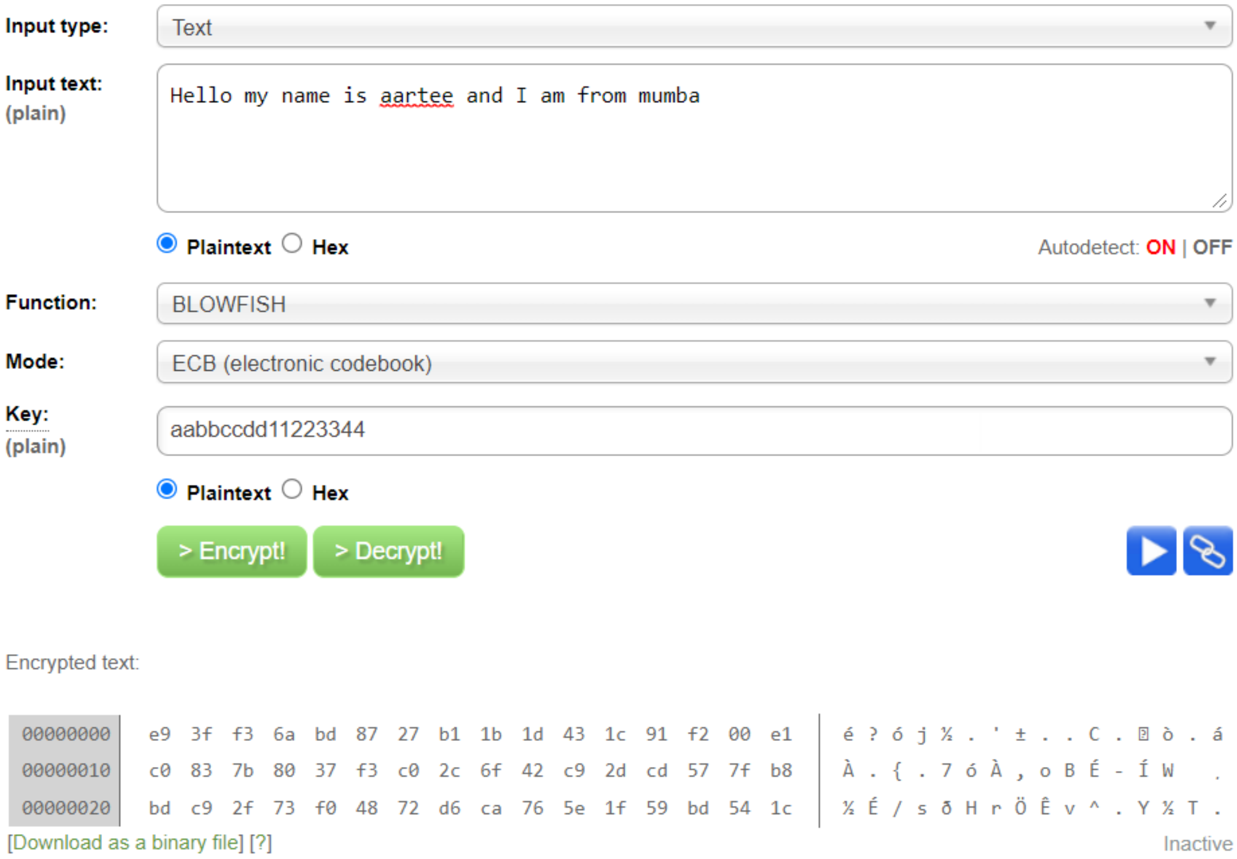
● Plaintext ○ Hex

Encrypted text:

```
00000000   dd 09 40 5f 0e ef a7 0d 1b 1d 43 1c 91 f2 00 e1   Ý . @ _ . ï § . . . C . ⍰ ò . á
00000010   c0 83 7b 80 37 f3 c0 2c 6f 42 c9 2d cd 57 7f b8   À . { . 7 ó À , o B É - Í W   .
00000020   bd c9 2f 73 f0 48 72 d6 c4 d8 2f 3f 84 e4 62 16   ½ É / s ð H r Ö Ä Ø / ? . ä b .
```

Similar to the above case the entire left block ended up changing on account of replacing an H by A.

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



Input type: Text

Input text: (plain)

```
Hello my name is aartee and I am from mumba
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) aabbccdd11223344

● Plaintext ○ Hex

Encrypted text:

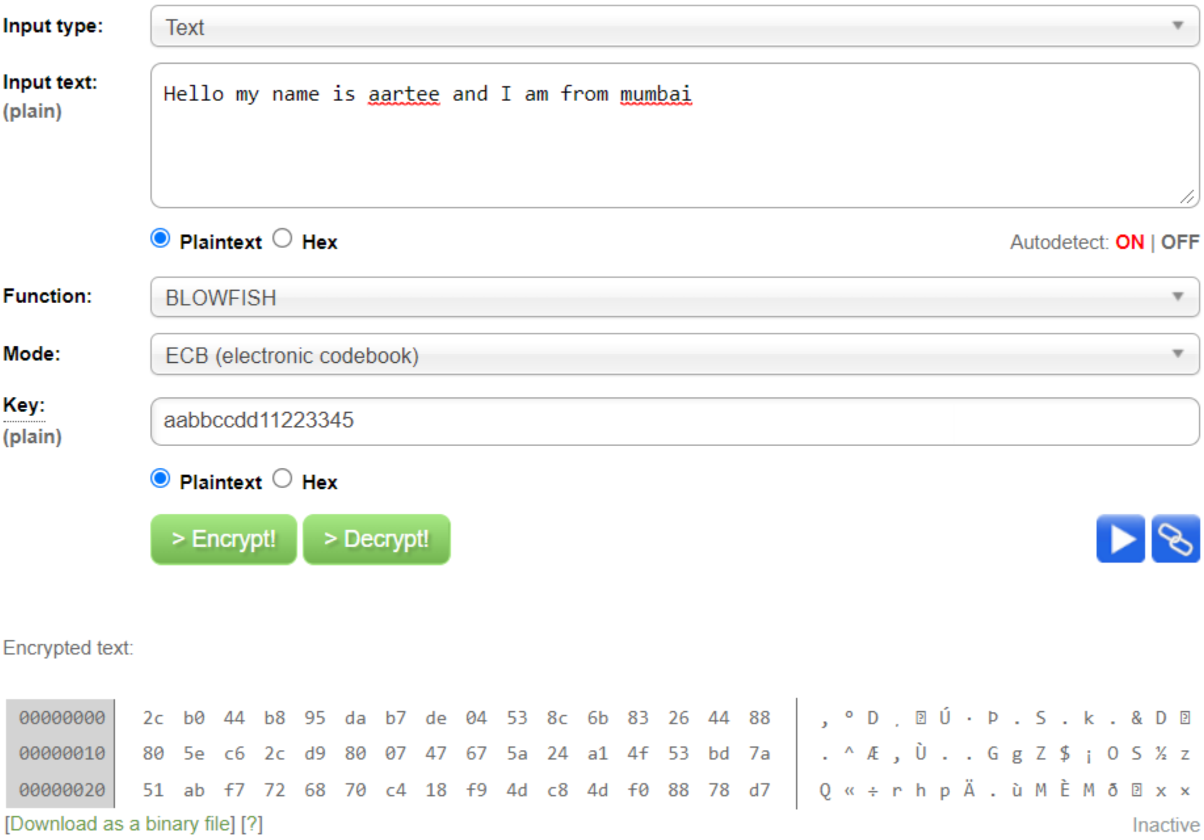
```
00000000   e9 3f f3 6a bd 87 27 b1 1b 1d 43 1c 91 f2 00 e1   é ? ó j ½ . ' ± . . C . ⍰ ò . á
00000010   c0 83 7b 80 37 f3 c0 2c 6f 42 c9 2d cd 57 7f b8   À . { . 7 ó À , o B É - Í W   .
00000020   bd c9 2f 73 f0 48 72 d6 ca 76 5e 1f 59 bd 54 1c   ½ É / s ð H r Ö Ê v ^ . Y ½ T .
```

[Download as a binary file] [?]

Inactive

After removing the last character, the entire last block is changing.

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



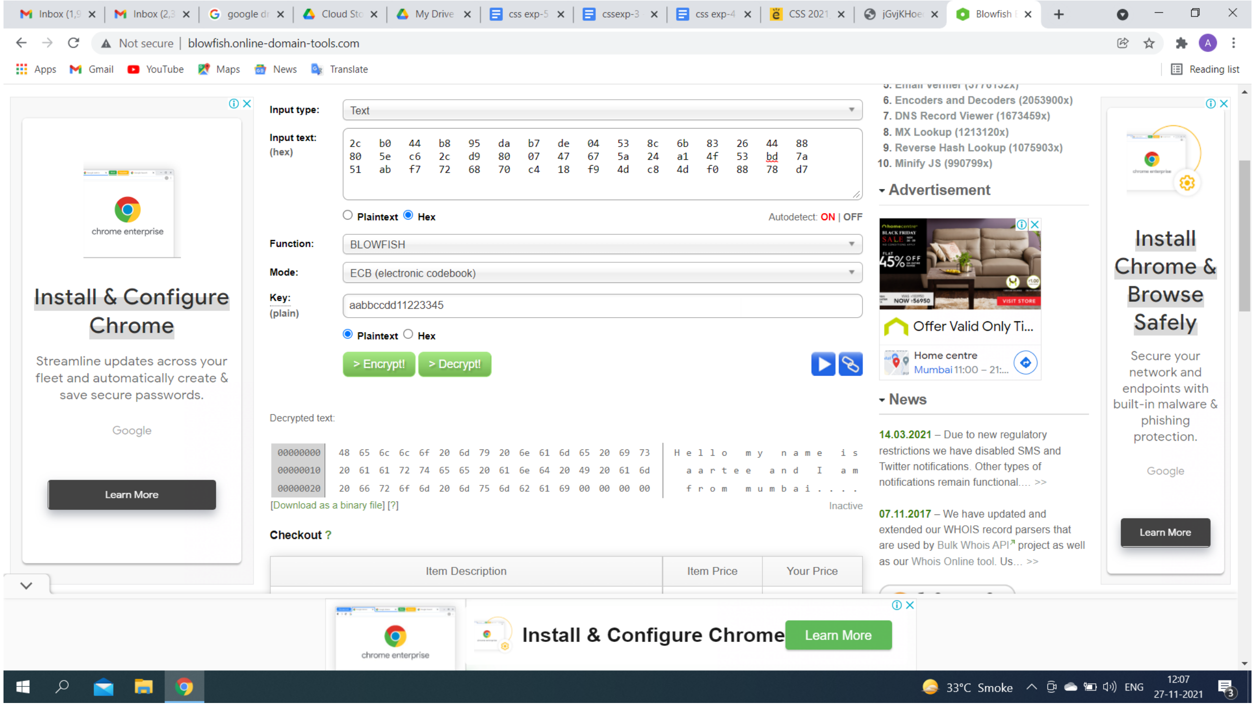
Hello my name is aartee and I am from mumbai

aabbccdd11223345

```
00000000   2c b0 44 b8 95 da b7 de 04 53 8c 6b 83 26 44 88  | , ° D ¸ ⍰ Ú · Þ . S . k . & D ⍰
00000010   80 5e c6 2c d9 80 07 47 67 5a 24 a1 4f 53 bd 7a  | . ^ Æ , Ù . . G g Z $ ¡ O S ½ z
00000020   51 ab f7 72 68 70 c4 18 f9 4d c8 4d f0 88 78 d7  | Q « ÷ r h p Ä . ù M È M ð ⍰ x ×
```

The value of p-box is dependent on the key which keeps on changing in every loop hence even a small change in the key will lead to an entirely different encrypted text.

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



Input type: Text

Input text: (hex)

```
2c   b0   44   b8   95   da   b7   de   04   53   8c   6b   83   26   44   88
80   5e   c6   2c   d9   80   07   47   67   5a   24   a1   4f   53   bd   7a
51   ab   f7   72   68   70   c4   18   f9   4d   c8   4d   f0   88   78   d7
```

○ Plaintext ● Hex   Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) aabbccdd11223345

● Plaintext ○ Hex

> Encrypt! > Decrypt!

Decrypted text:

```
00000000  48 65 6c 6c 6f 20 6d 79 20 6e 61 6d 65 20 69 73  Hello my name is
00000010  20 61 61 72 74 65 65 20 61 6e 64 20 49 20 61 6d   aartee and I am
00000020  20 66 72 6f 6d 20 6d 75 6d 62 61 69 00 00 00 00   from mumbai....
```

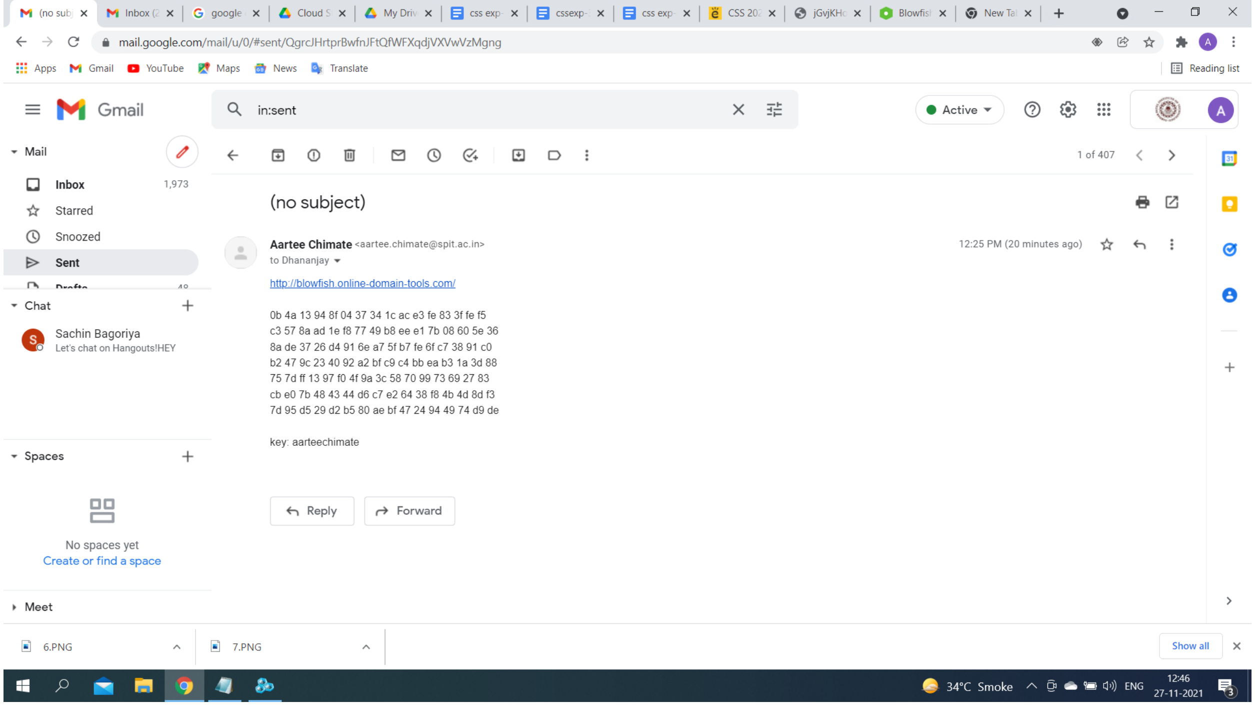
[Download as a binary file] [?]   Inactive

Checkout ?

Item Description	Item Price	Your Price

Decrypting a message with a changed key leads to a different message . There is no similarity between the actual plain text and the message obtained in the above case.

2] 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.



(no subject)

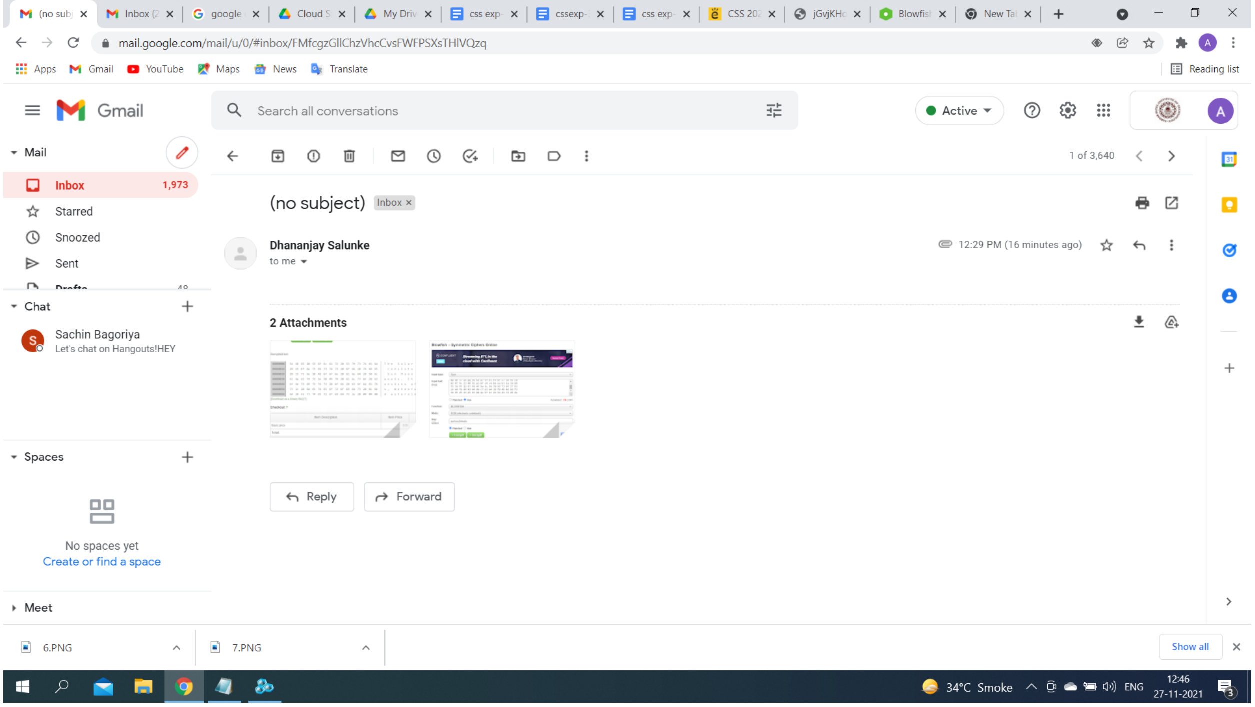
Aartee Chimate <aartee.chimate@spit.ac.in>
to Dhananjay

12:25 PM (20 minutes ago)

http://blowfish.online-domain-tools.com/

```
0b 4a 13 94 8f 04 37 34 1c ac e3 fe 83 3f fe f5
c3 57 8a ad 1e f8 77 49 b8 ee e1 7b 08 60 5e 36
8a de 37 26 d4 91 6e a7 5f b7 fe 6f c7 38 91 c0
b2 47 9c 23 40 92 a2 bf c9 c4 bb ea b3 1a 3d 88
75 7d ff 13 97 f0 4f 9a 3c 58 70 99 73 69 27 83
cb e0 7b 48 43 44 d6 c7 e2 64 38 f8 4b 4d 8d f3
7d 95 d5 29 d2 b5 80 ae bf 47 24 94 49 74 d9 de
```

key: aarteechimate

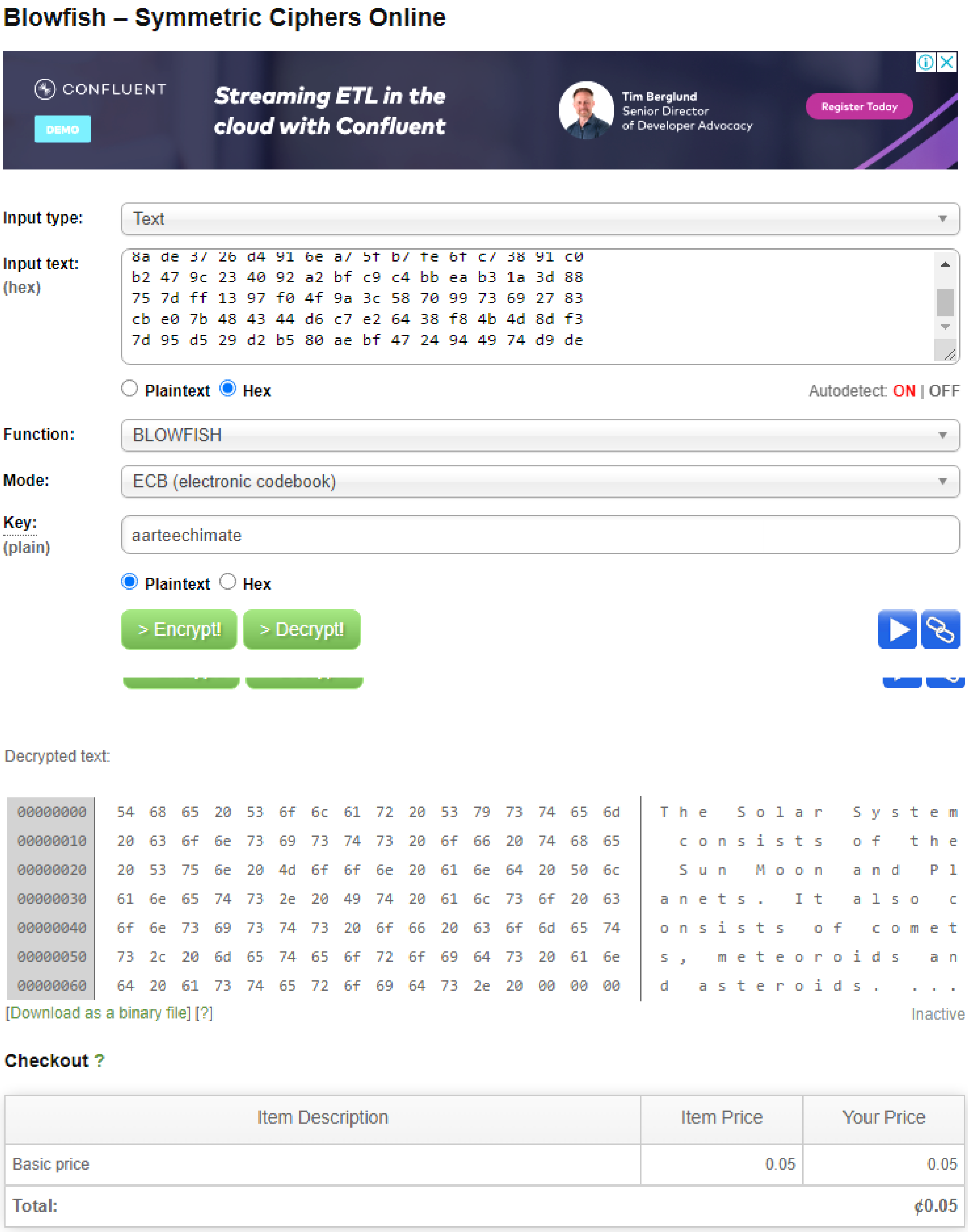


(no subject)

Dhananjay Salunke
to me

12:29 PM (16 minutes ago)

2 Attachments



Blowfish – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
8a de 37 26 d4 91 6e a7 5f b7 fe 6f c7 38 91 c0
b2 47 9c 23 40 92 a2 bf c9 c4 bb ea b3 1a 3d 88
75 7d ff 13 97 f0 4f 9a 3c 58 70 99 73 69 27 83
cb e0 7b 48 43 44 d6 c7 e2 64 38 f8 4b 4d 8d f3
7d 95 d5 29 d2 b5 80 ae bf 47 24 94 49 74 d9 de
```

○ Plaintext ● Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) aarteechimate

● Plaintext ○ Hex

Decrypted text:

```
00000000  54 68 65 20 53 6f 6c 61 72 20 53 79 73 74 65 6d  The Solar System
00000010  20 63 6f 6e 73 69 73 74 73 20 6f 66 20 74 68 65   consists of the
00000020  20 53 75 6e 20 4d 6f 6f 6e 20 61 6e 64 20 50 6c   Sun Moon and Pl
00000030  61 6e 65 74 73 2e 20 49 74 20 61 6c 73 6f 20 63  anets. It also c
00000040  6f 6e 73 69 73 74 73 20 6f 66 20 63 6f 6d 65 74  onsists of comet
00000050  73 2c 20 6d 65 74 65 6f 72 6f 69 64 73 20 61 6e  s, meteoroids an
00000060  64 20 61 73 74 65 72 6f 69 64 73 2e 20 00 00 00  d asteroids. ...
```

[Download as a binary file] [?]

Inactive

Checkout ?

Item Description	Item Price	Your Price
Basic price	0.05	0.05
Total:		**¢0.05**