Divya Shah
2019130057
TE Comps

Lab 5: Blowfish Encryption

1. Objective

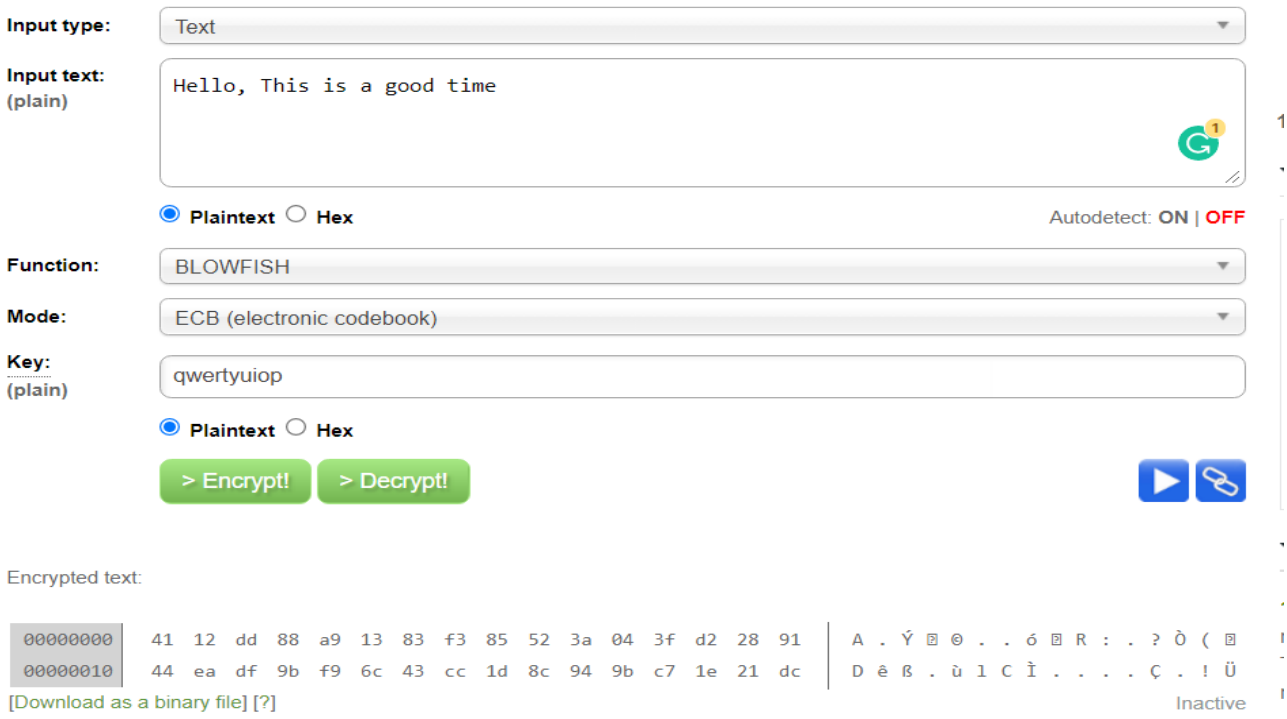
This lab will give you the chance to experiment with an online encryption tool. You will encode a message and send it to someone else in the class, who will decode it when you supply the secret key. Note that this particular tool is of limited use in a security context, since the plaintext of the message is sent to and from the encryption web site! 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.

The tool we will use implements the Blowfish cipher system. Blowfish is a public domain algorithm designed and released by Bruce Schneier, a noted security expert. Although it was originally designed in 1993, it remains in use and no compromising errors are known in its design

Laboratory Task: Testing Blowfish

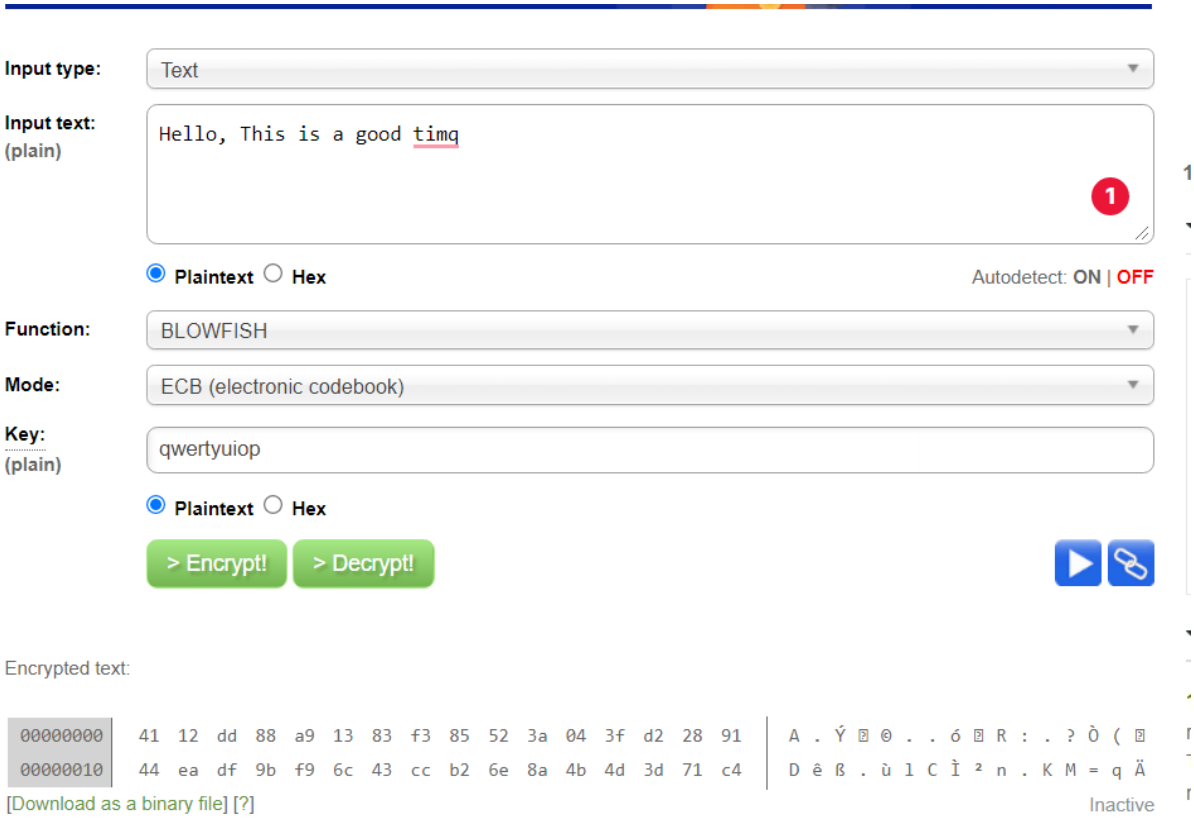
Go to the encryption tool web site and try it out. Enter a short key phrase and a longer piece of text to be encoded. Then submit and see what your text looks like when encrypted.

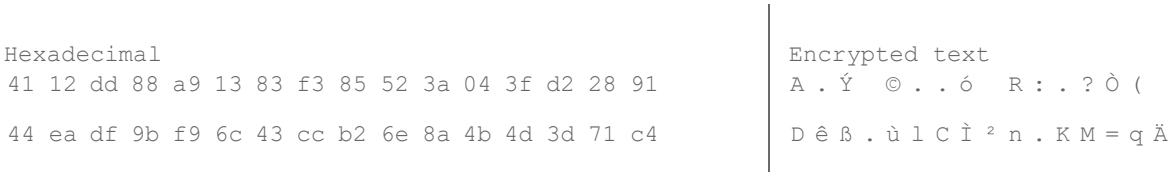
41 12 dd 88 a9 13 83 f3 85 52 3a 04 3f d2 28 91	A . Ý © . . ó R : . ? Ò (
44 ea df 9b f9 6c 43 cc 1d 8c 94 9b c7 1e 21 dc	D ê ß . ù l C Ì . . . . Ç . ! Ü
Hexadecimal Numbers	Encrypted Text



Try the following experiments and note how they change the output:

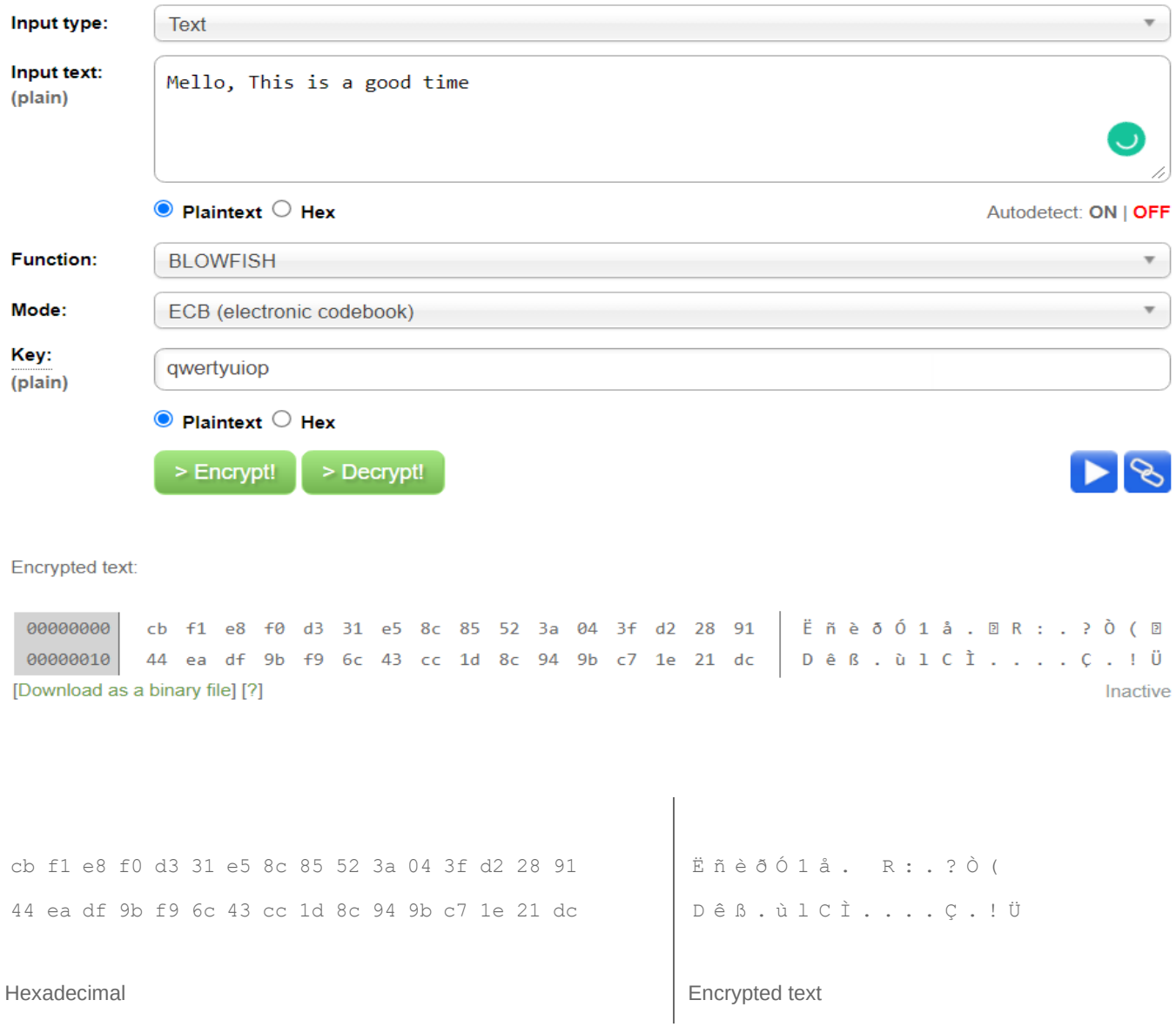
1. Change one character at the end of the message. How much of the encoded message changes?





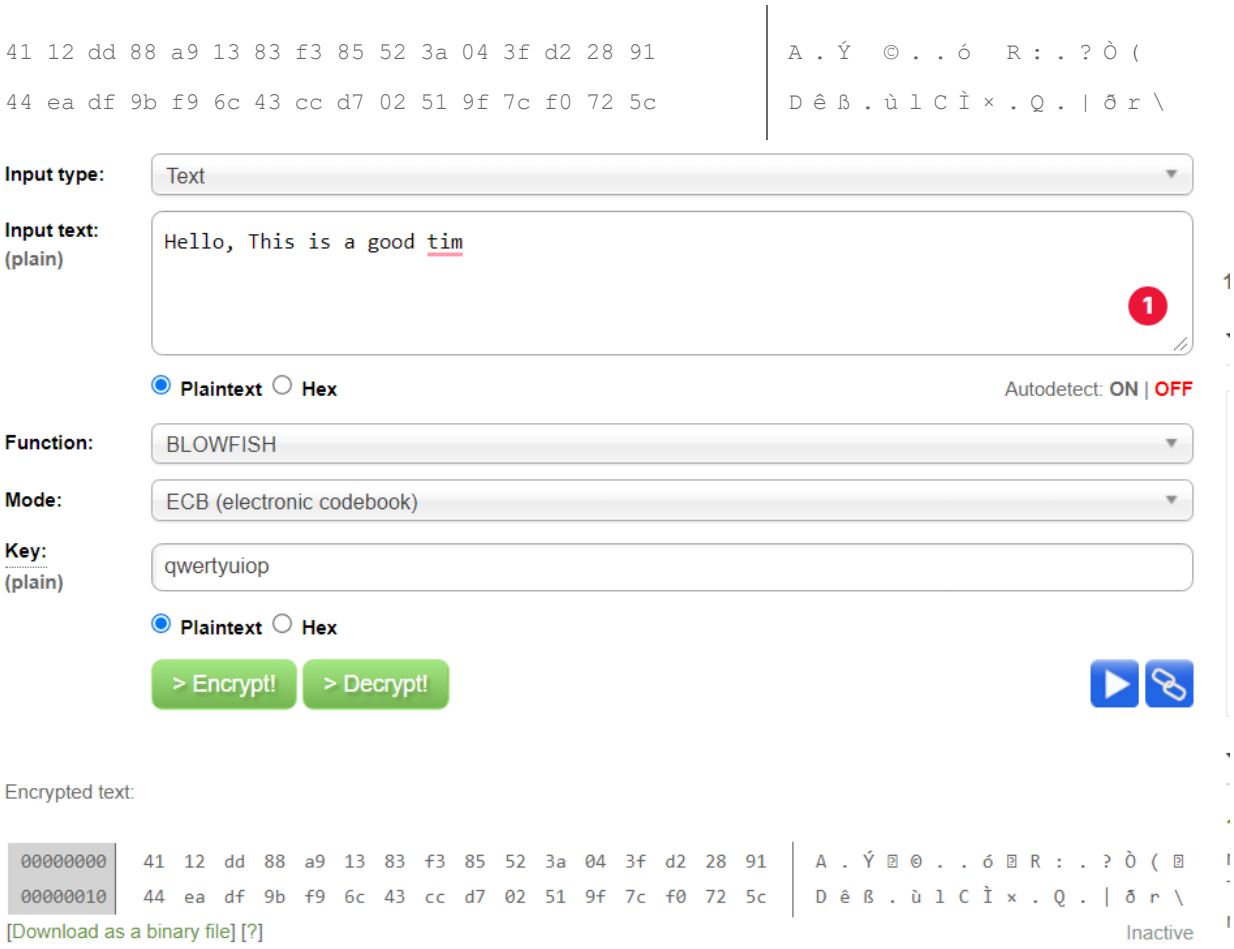
After changing the last character of the plain text message, the last 16 characters of the encrypted message change, and the rest of the encrypted message remains the same.

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



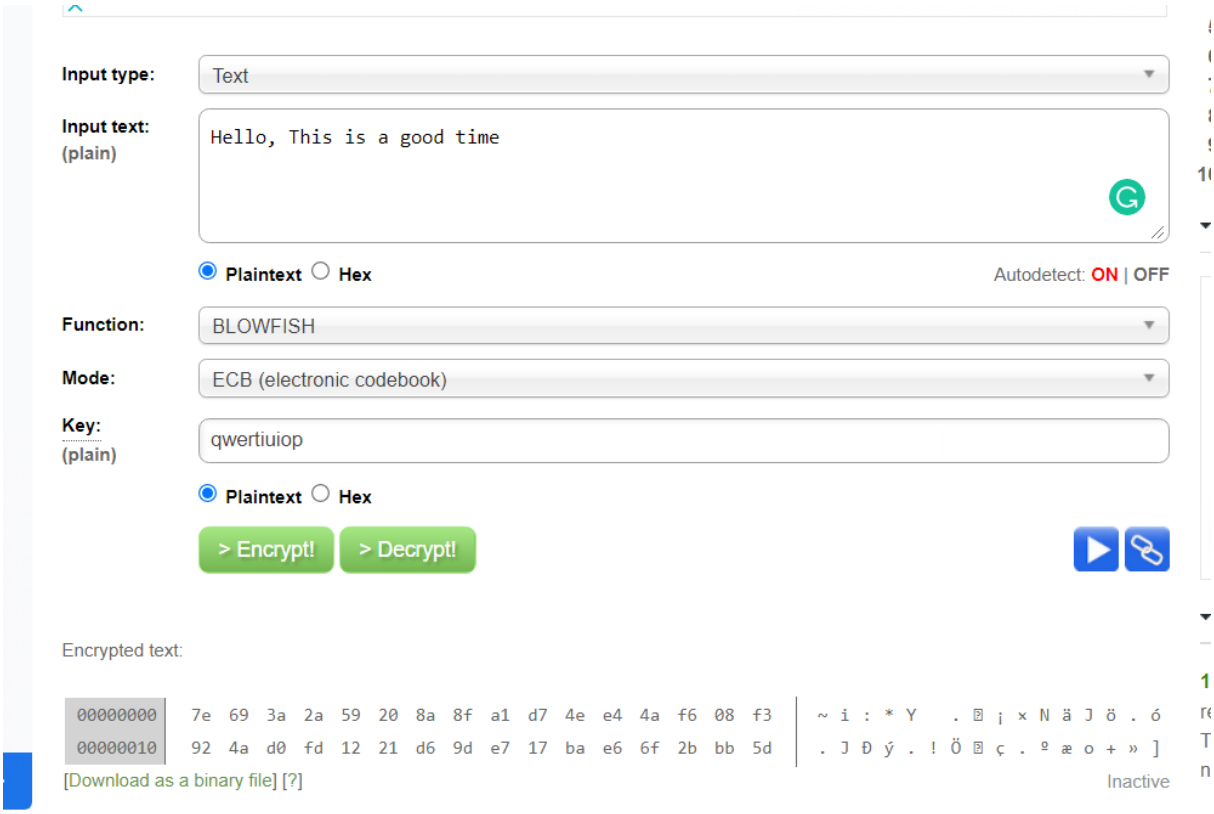
The first 16 characters of the encrypted message changes.

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



The last 16 characters of the encrypted message changes, the rest of the encrypted message remains same.

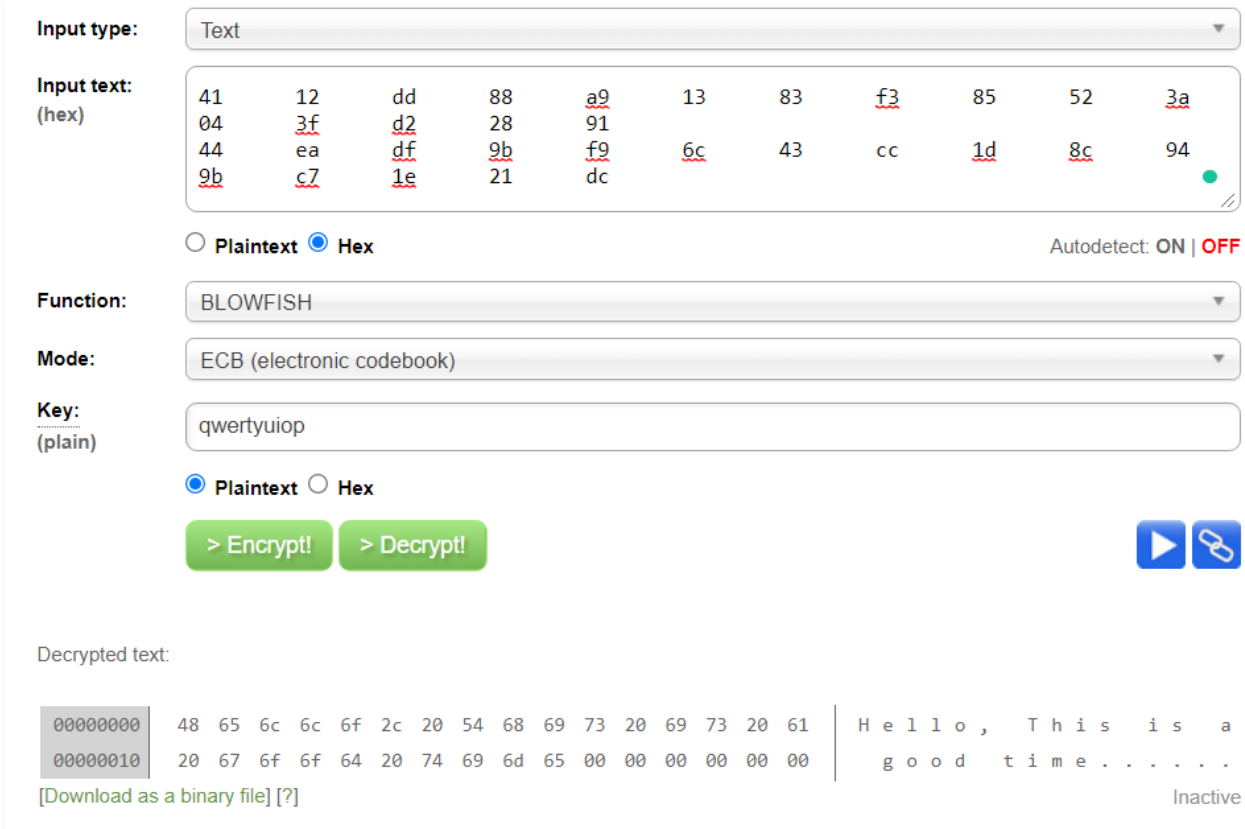
4. Change one character in the key. How much of the encoded message changes?



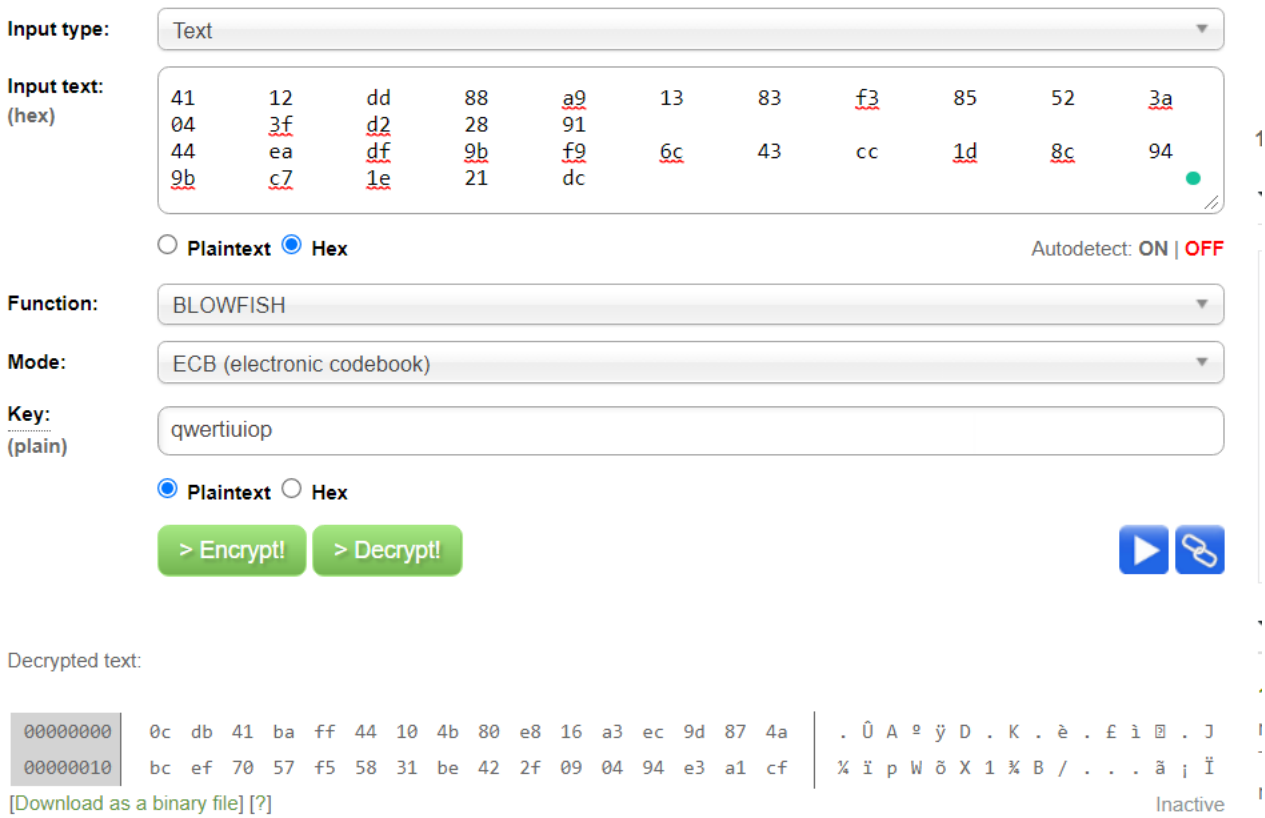

```
7e 69 3a 2a 59 20 8a 8f a1 d7 4e e4 4a f6 08 f3
92 4a d0 fd 12 21 d6 9d e7 17 ba e6 6f 2b bb 5d
```

The entire encrypted message changes significantly.

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



Decryption with the original key



Decryption with changed key.

No it doesnt look anything like the original.

Conclusion:

It is understood that blowfish is a block cipher because changing of one text changes that part of block encryption. It can also be understood that it is a symmetric cipher because it encrypts and decrypts using the same key. Any change in key does not decipher the ciphered text properly.

Github Link: https://github.com/Divya-127/CSS-Lab/tree/main/Exp5