NAME : SHREYAS PATEL
ROLL NO : 42
BRANCH : TE COMPS

CEL 62, Winter 2020
Lab 5: Blowfish Encryption

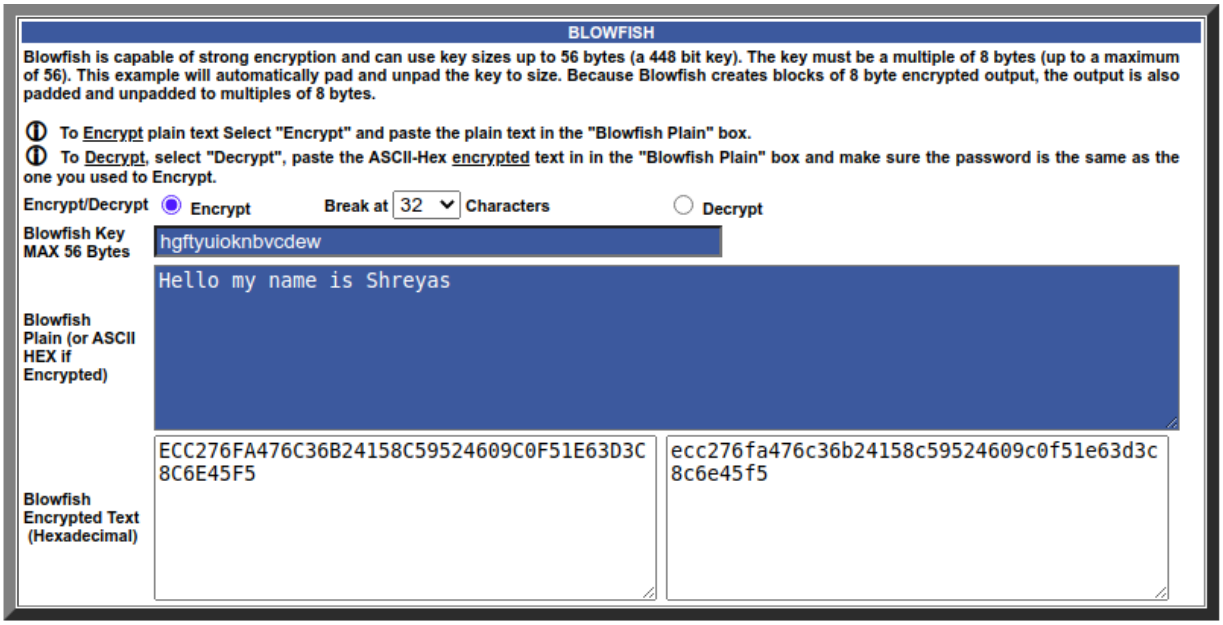
1. Objective

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

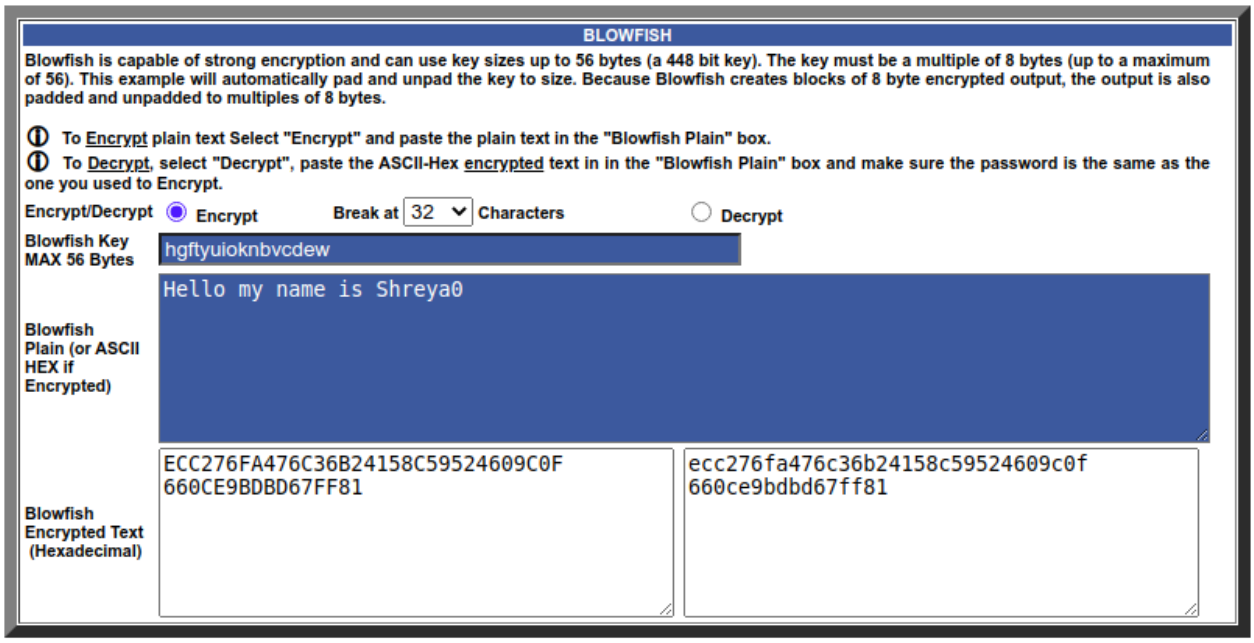
Laboratory Task: Testing Blowfish

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.



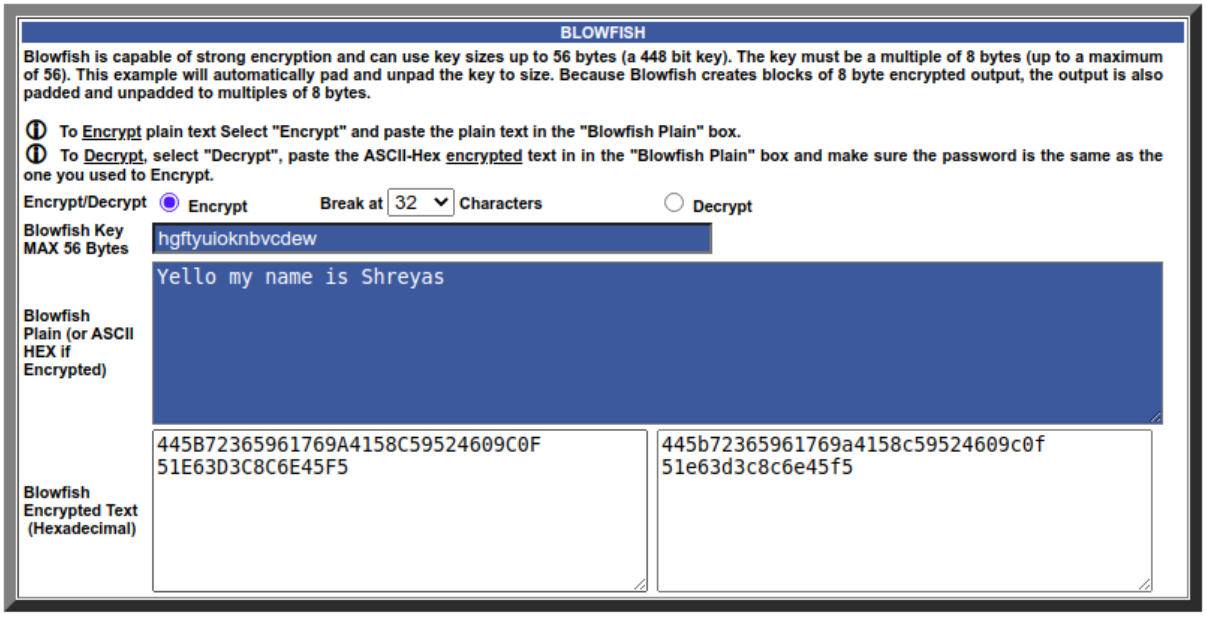
Try the following experiments and note how they change the output:

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



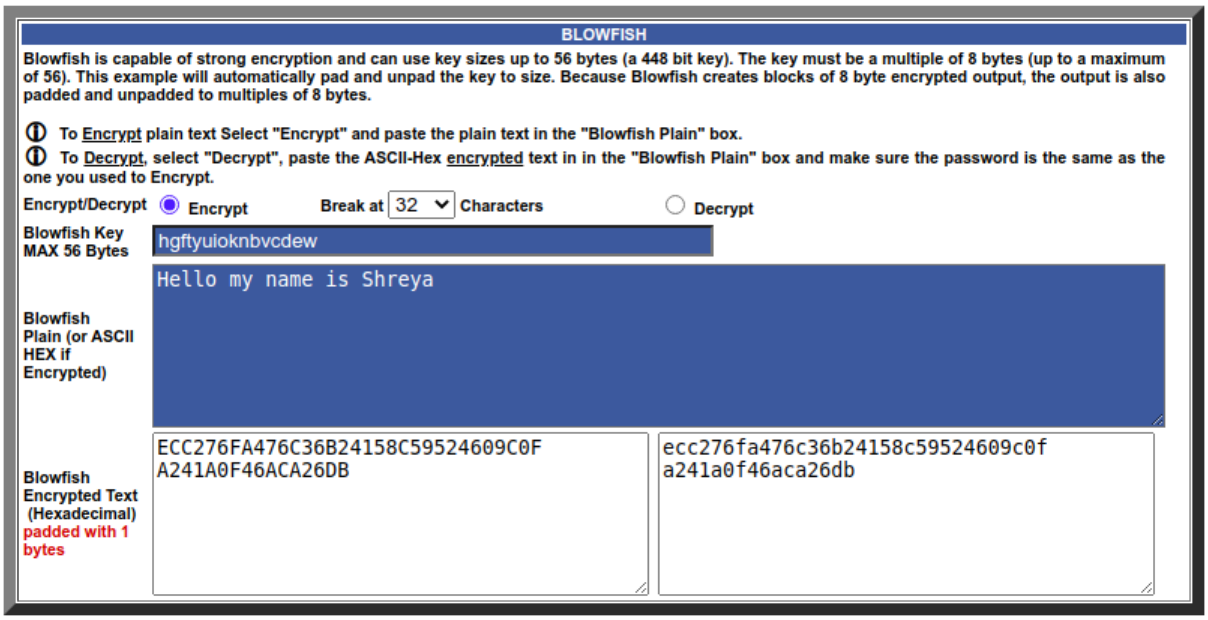
So we can see that 16 characters of the encrypted message is changed as it is a hexadecimal message

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



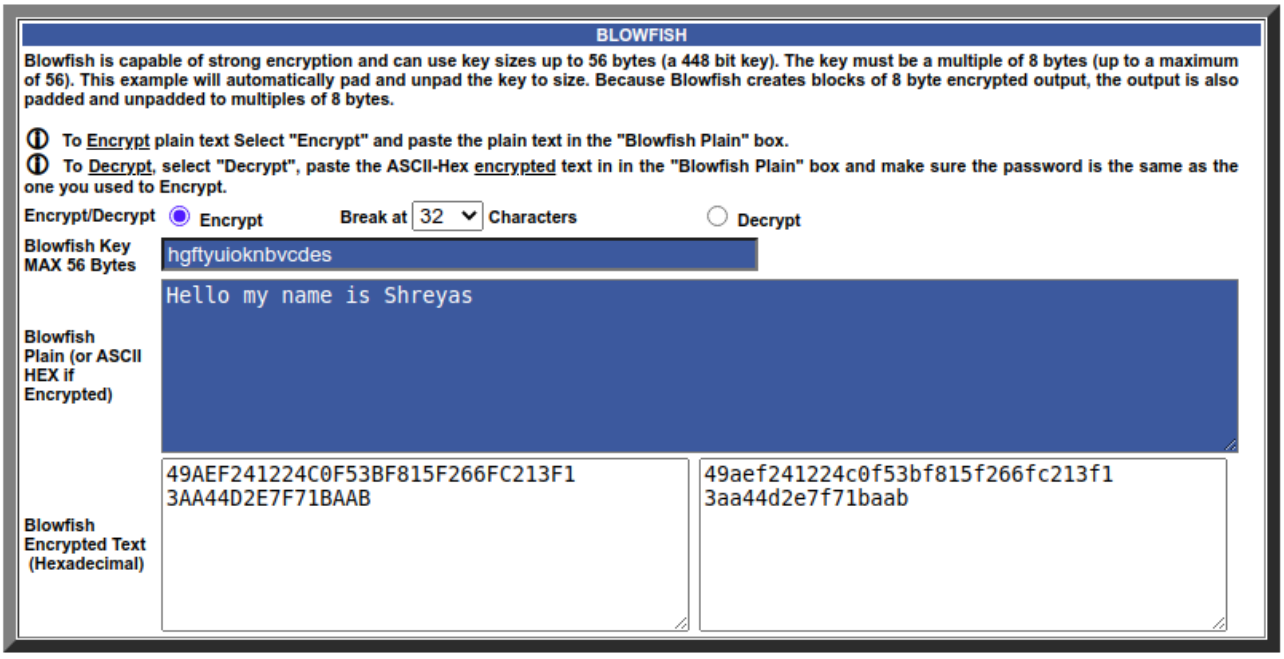
So we can see that the first 16 characters of the encrypted message have been changed, the reason also being it is a hexadecimal message.

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



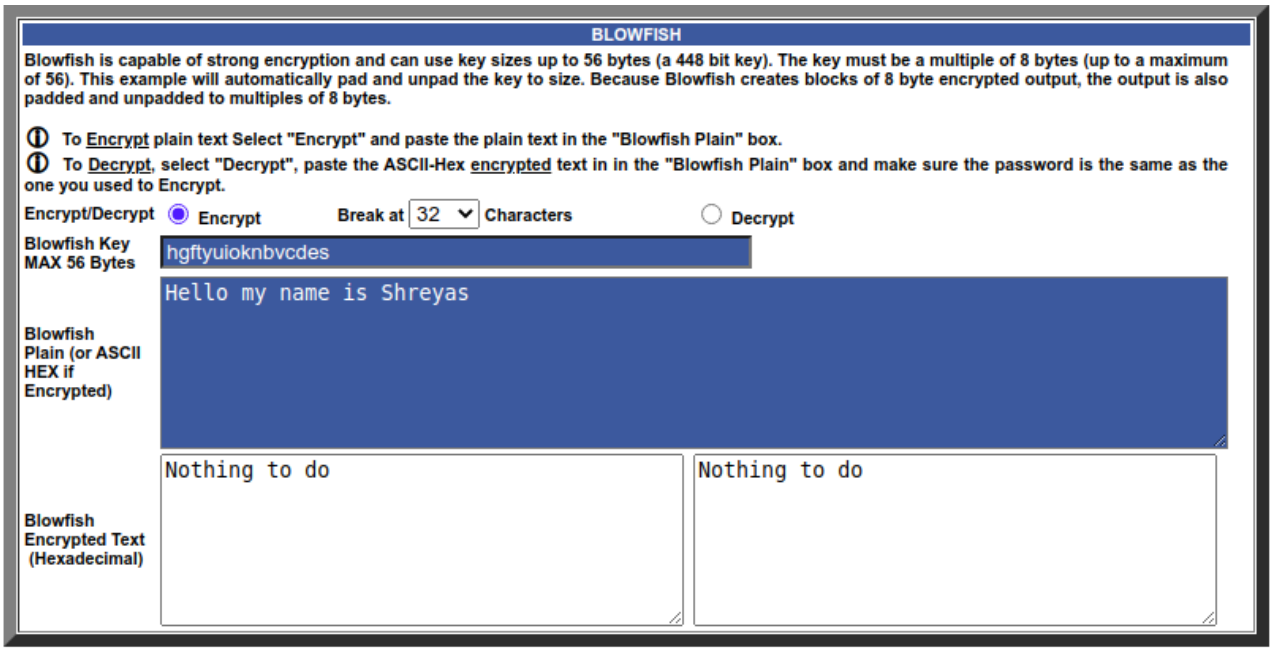
So we can see that some of the characters at the end changed. Again the number is 16

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



We can see that the whole encoded message has been changed.

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



So by changing one character in the key and decrypting, we can see that we have lost the original message

A Secret Message

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

```
ED85E0929D1248116C52FA6AFFB1DAC1
E2D472B6E8EA93AECD0D518D04DF3188
715D3AF7877684AC34EEB0FF3768B8DD
9E227C12E7340390987FDD12F9B9C156
F05A0748FBACFBC48D4B70C99780413F
652E6676330AC76F1DE7380E81B12E11
```

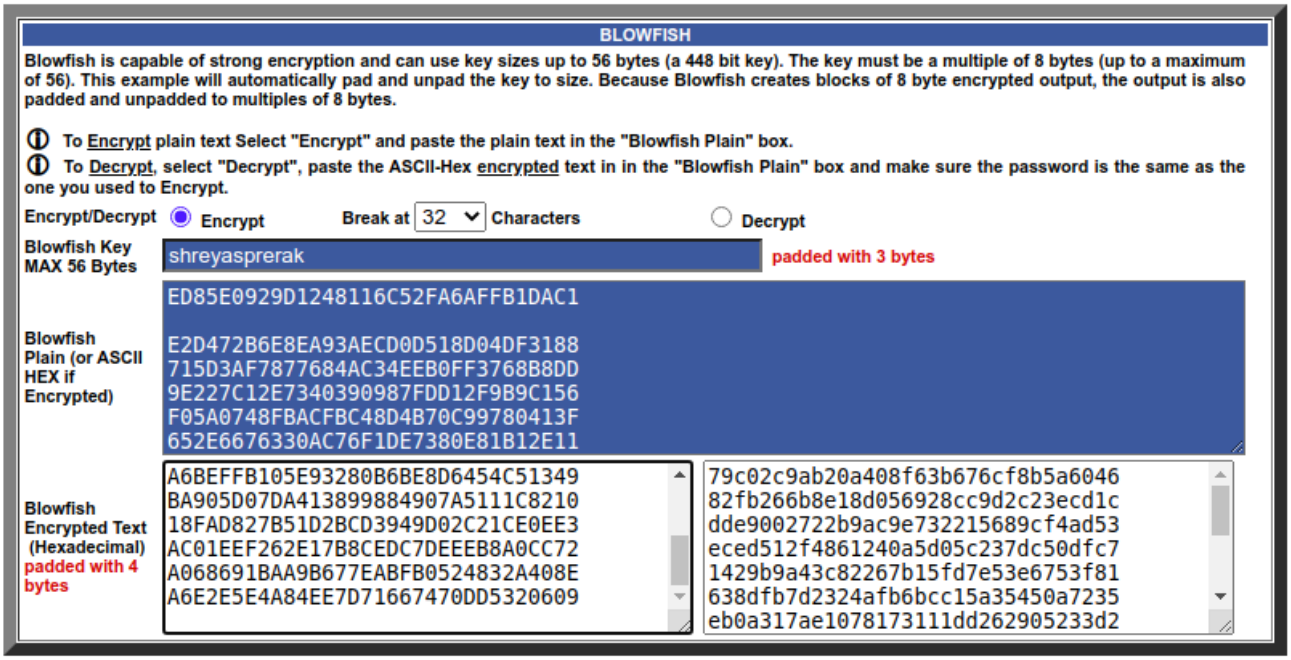
(Blowfish: By PV-J)

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) 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.

Public Key Cryptography

Experiment with this page designed to demo cryptography with public/private key pairs. Note how a message encrypted with one key can be decrypted using the other.

This is my encoded message which I sent my friend:



And here's what my friend got after decoding the encoded message I sent to him:

ED85E0929D1248116C52FA6AFFB1DA
E2D472B6E8EA93AECD0D518D04DF31
715D3AF7877684AC34EEB0FF3768B8
9E227C12E7340390987FDD12F9B9C1
F05A0748FBACFBC48D4B70C9978041
652E6676330AC76F1DE7380E81B12E

This is the original secret message!

CONCLUSION : Through this experient I came to know the usage of Blowfish Algorithm and its tool to send secret messages securely through encryption and decrypion.