Name: Vishal Salvi
UID: 2019230069
Batch: C
Class: TE Comps
CEL 62, Winter 2020
Lab 5: Blowfish Encryption

1. Objective

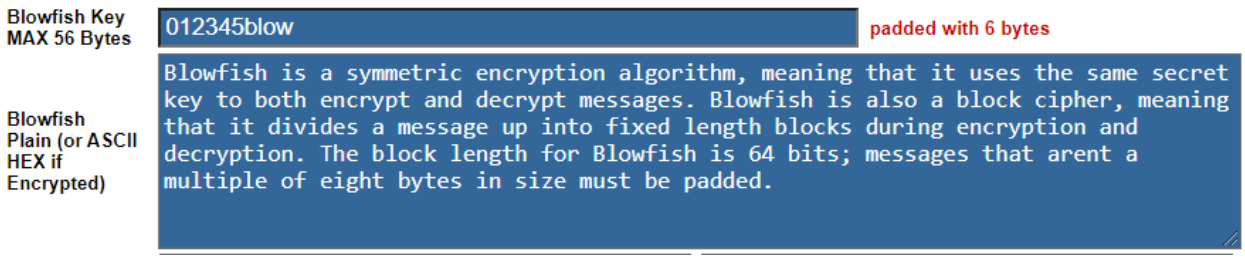
This lab will give you the chance to experiment with an online encryption tool. You will encode a message and send it to someone else in the class, who will decode it when you supply the secret key. Note that this particular tool is of limited use in a security context, since the plaintext of the message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

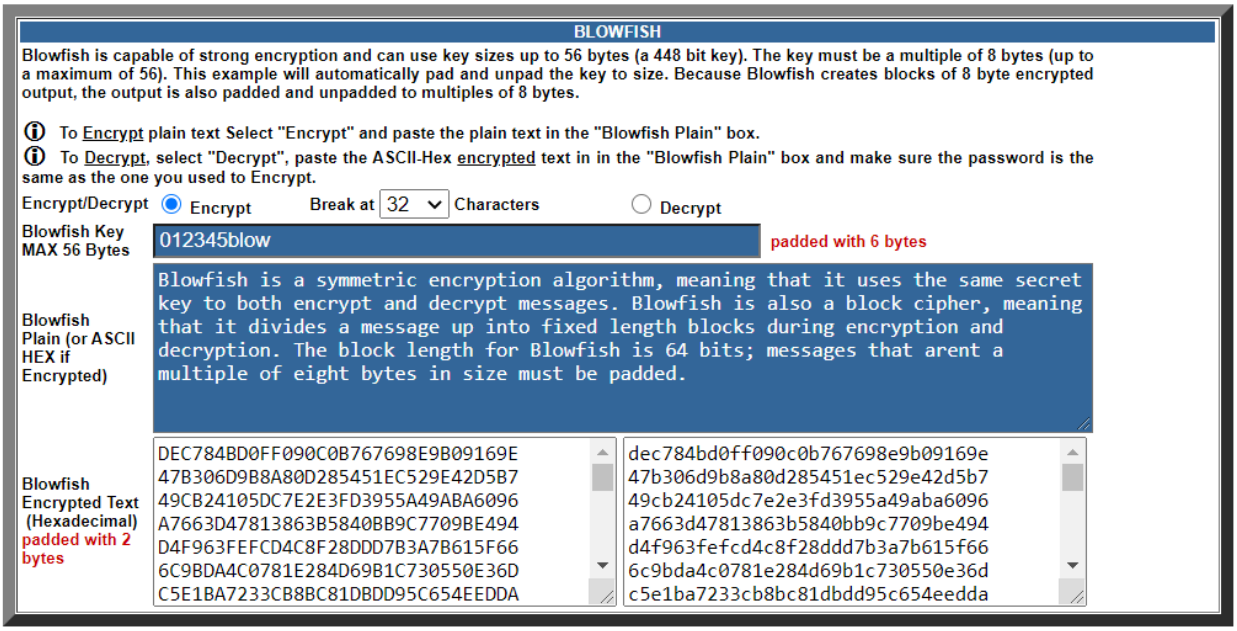
Laboratory Task: Testing Blowfish

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:

Plain Text:

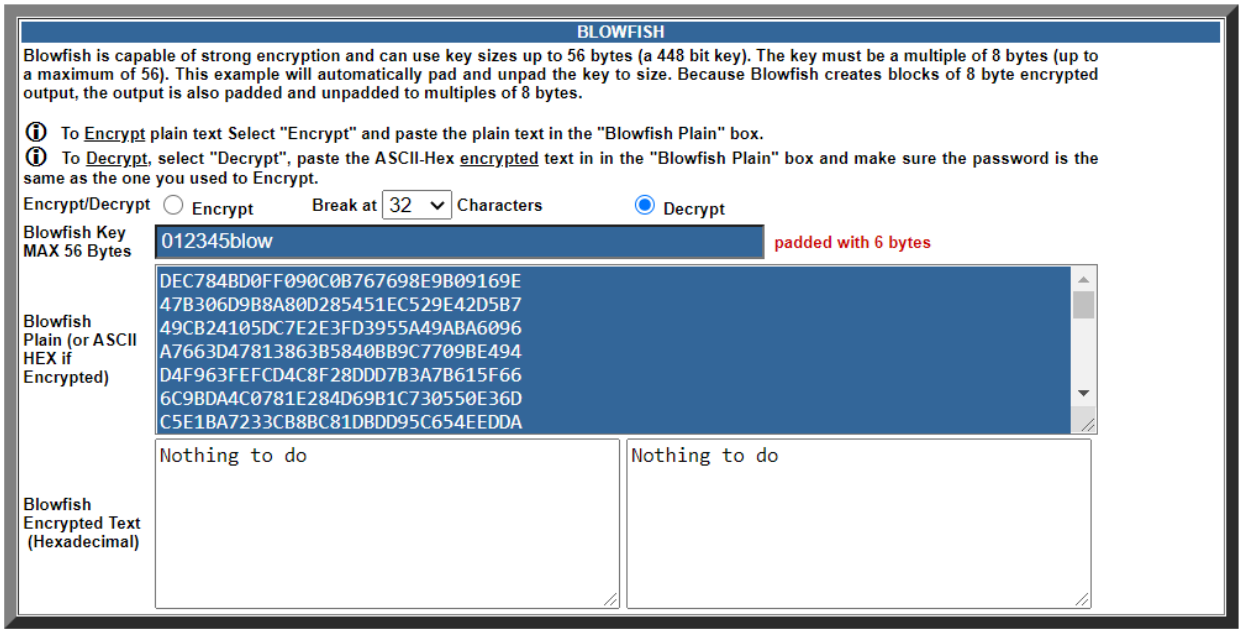


Encrypted Message:

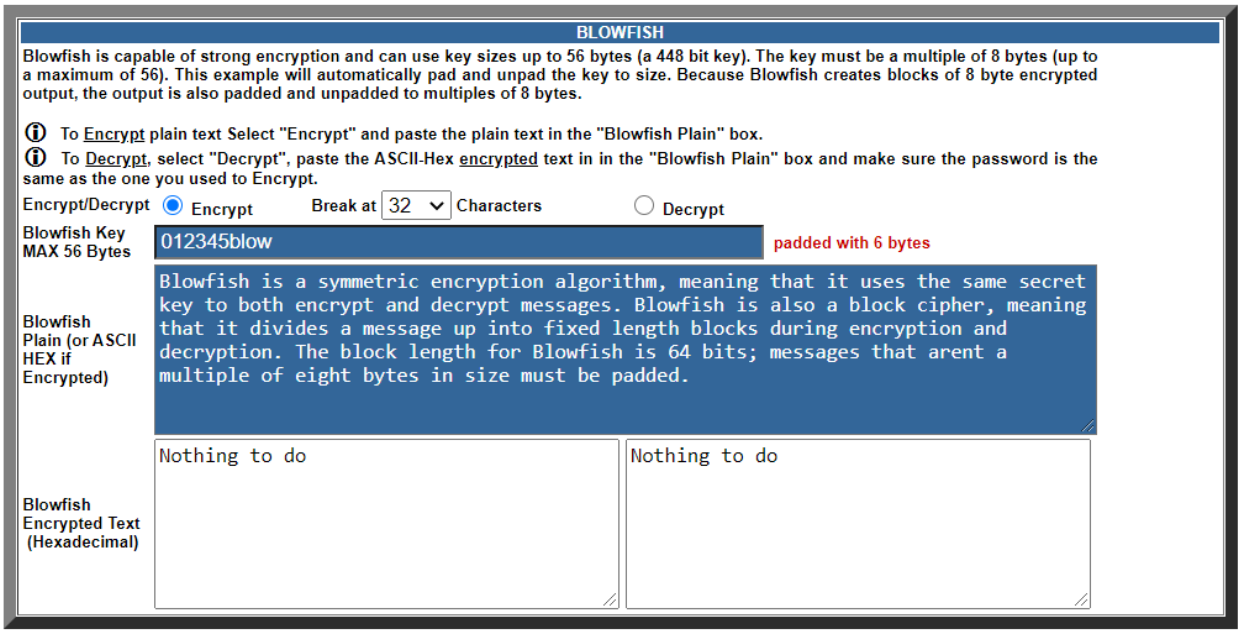


DEC784BD0FF090C0B767698E9B09169E
47B306D9B8A80D285451EC529E42D5B7
49CB24105DC7E2E3FD3955A49ABA6096
A7663D47813863B5840BB9C7709BE494
D4F963FEFCD4C8F28DDD7B3A7B615F66
6C9BDA4C0781E284D69B1C730550E36D
C5E1BA7233CB8BC81DBDD95C654EEDDA
DBDD884E9A8542BCD2450ACD3F6ADEC5
41495570EA9DF6A5EE299A5E87F5C5D3
39C2CC0224E9D916A54454C88A9C2A91
A7663D47813863B5BBB68497F8CB6185
93A15B736EC722A2468393333E304480
5F84BC91948BC70EB79365216D49864F
8682EEE45D911393E25267EF532C0E63
8E28C6D38F991DDFC47B72C652FF850B
3DF3F9D191E1AEC45E88F728C7AF6AB5
7F49E49444B1A466C033C676971F0784
21C59CE7802F305B2F7302AB787FC9D5
E63DB07F357434A78B12352E92D26D9C
F83580F0798EFB91B1A4325BEA41ED8D
41D16A2F67C5B6D5AEAC885B7D22BF93
F767063E55469678CE8D2A6C1AC47A8E
4740D1C6F82A7672BDB83645FF268317

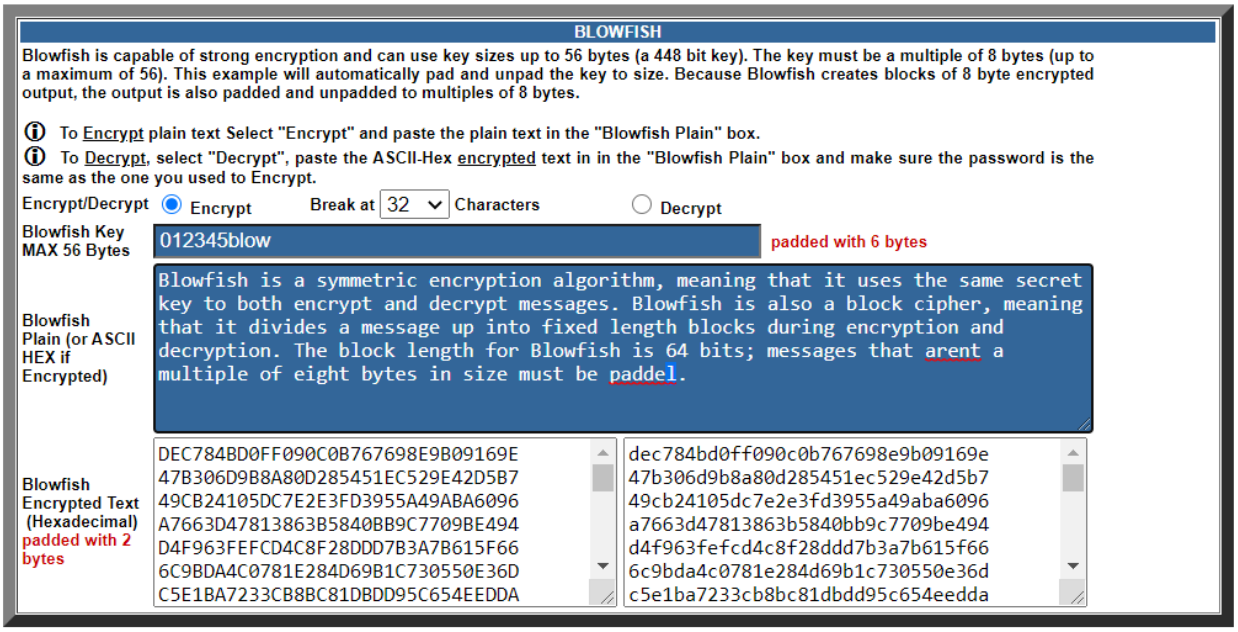
Decrypted Message:



After Decryption of message:

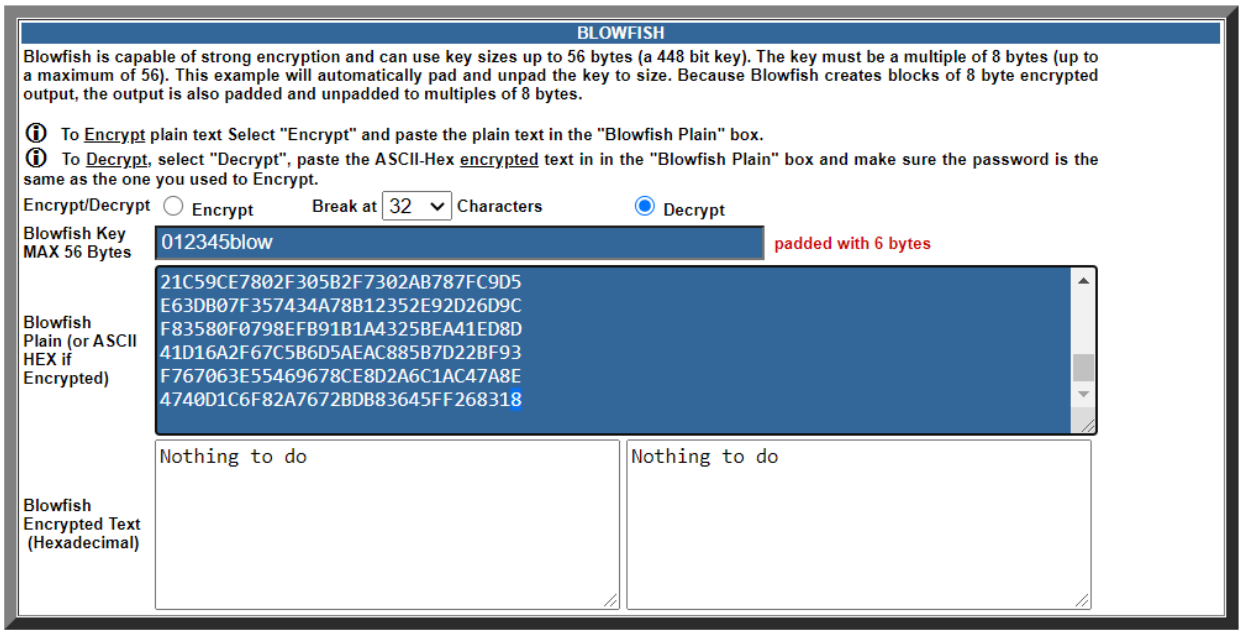


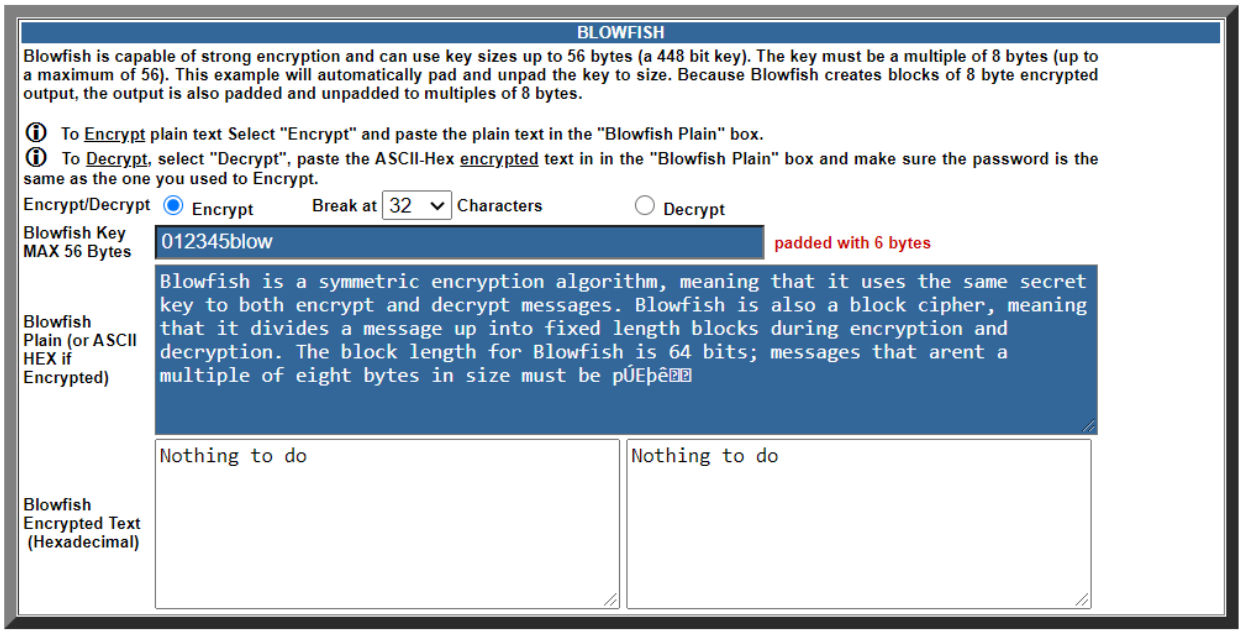
1. **Change one character at the end of the message. How much of the encoded message changes?**



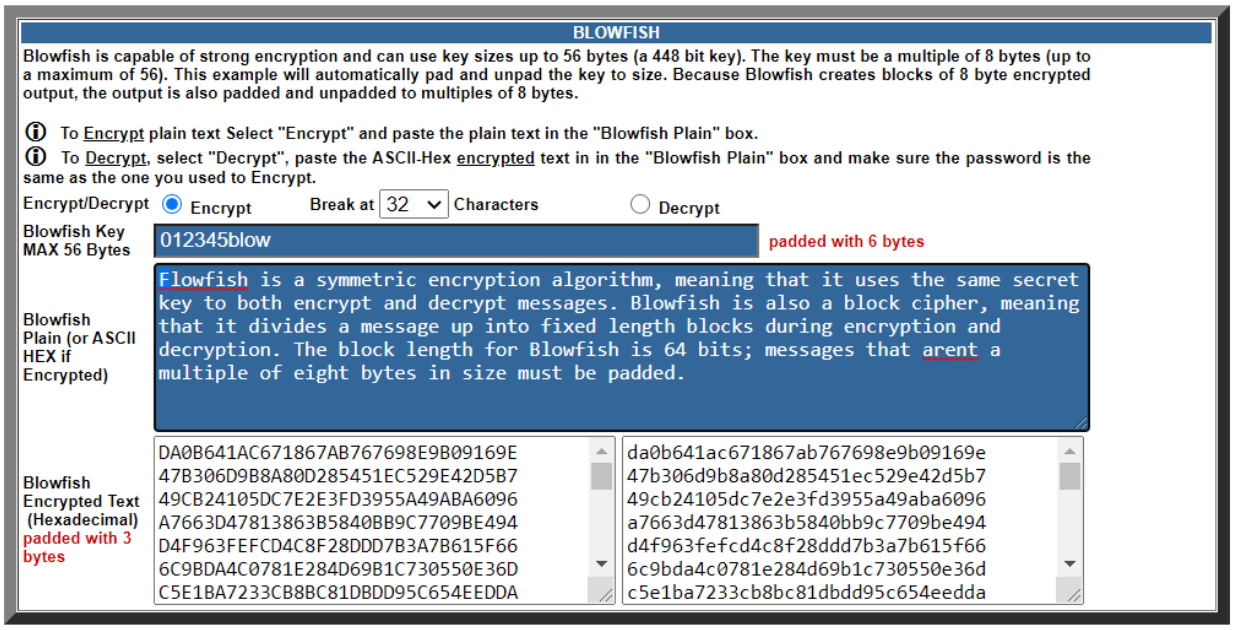
DEC784BD0FF090C0B767698E9B09169E
47B306D9B8A80D285451EC529E42D5B7
49CB24105DC7E2E3FD3955A49ABA6096
A7663D47813863B5840BB9C7709BE494
D4F963FEFCD4C8F28DDD7B3A7B615F66
6C9BDA4C0781E284D69B1C730550E36D
C5E1BA7233CB8BC81DBDD95C654EEDDA
DBDD884E9A8542BCD2450ACD3F6ADEC5
41495570EA9DF6A5EE299A5E87F5C5D3
39C2CC0224E9D916A54454C88A9C2A91
A7663D47813863B5BBB68497F8CB6185
93A15B736EC722A2468393333E304480
5F84BC91948BC70EB79365216D49864F
8682EEE45D911393E25267EF532C0E63
8E28C6D38F991DDFC47B72C652FF850B
3DF3F9D191E1AEC45E88F728C7AF6AB5
7F49E49444B1A466C033C676971F0784
21C59CE7802F305B2F7302AB787FC9D5
E63DB07F357434A78B12352E92D26D9C
F83580F0798EFB91B1A4325BEA41ED8D
41D16A2F67C5B6D5AEAC885B7D22BF93
F767063E55469678CE8D2A6C1AC47A8E
4740D1C6F82A7672**0257E635134A3F1F**

Also change in Encrypted message:



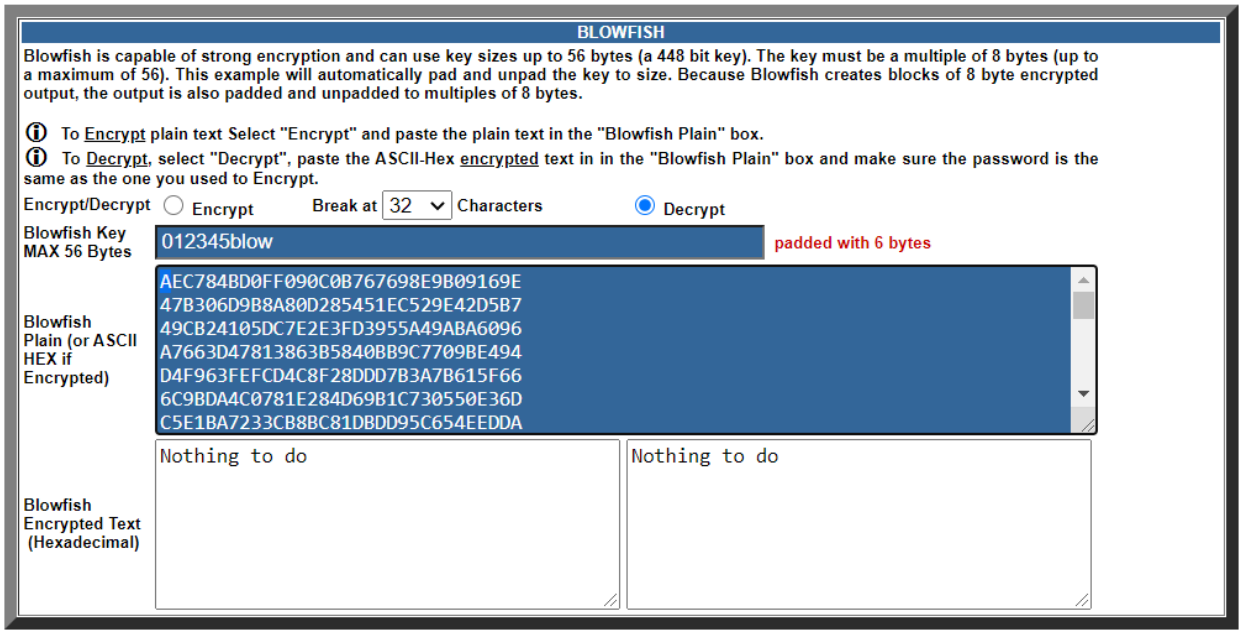


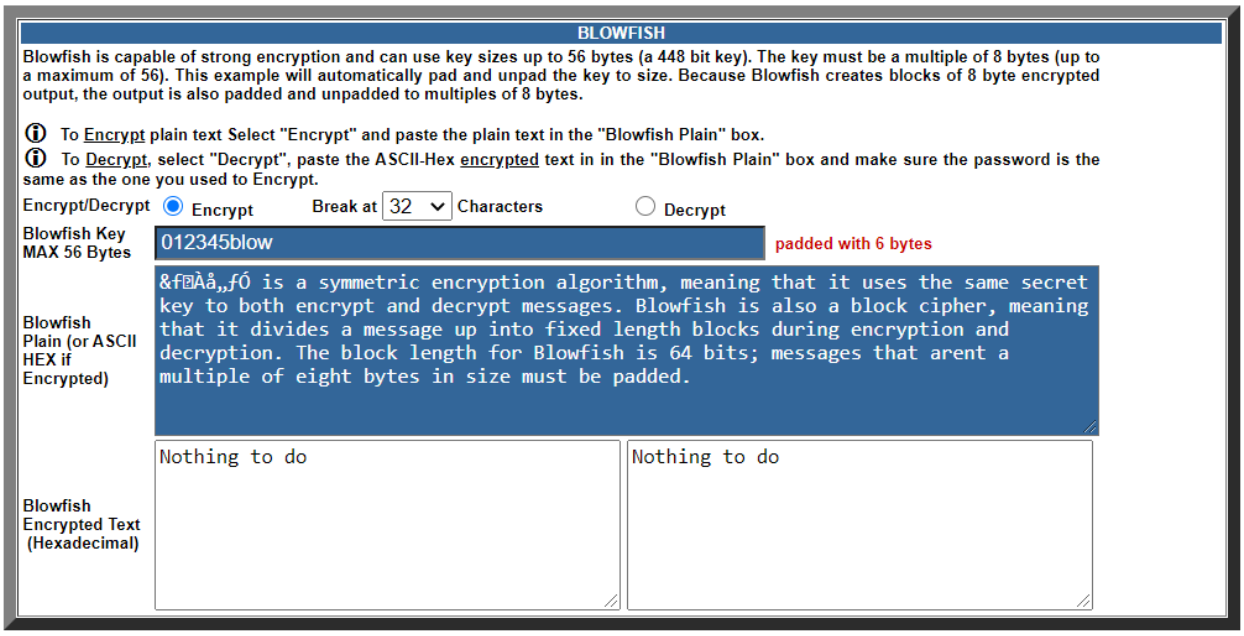
2. **Change one character at the beginning of the message. How much of the encoded message changes?**



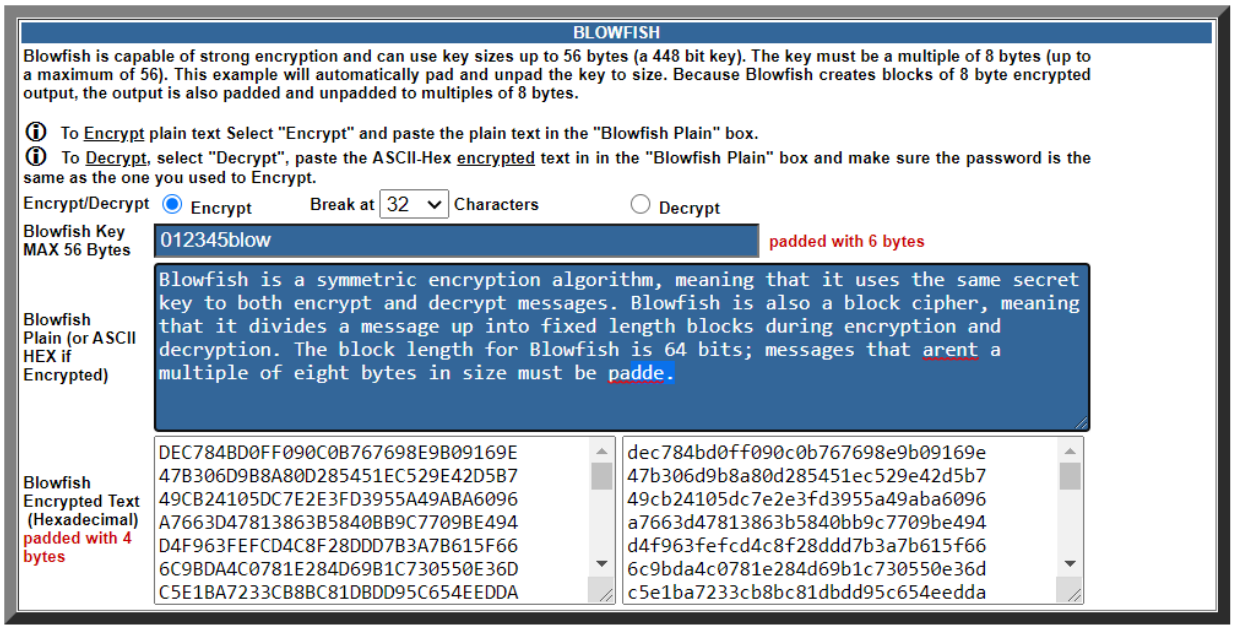
DA0B641AC671867AB767698E9B09169E
47B306D9B8A80D285451EC529E42D5B7
49CB24105DC7E2E3FD3955A49ABA6096
A7663D47813863B5840BB9C7709BE494
D4F963FEFCD4C8F28DDD7B3A7B615F66
6C9BDA4C0781E284D69B1C730550E36D
C5E1BA7233CB8BC81DBDD95C654EEDDA
DBDD884E9A8542BCD2450ACD3F6ADEC5
41495570EA9DF6A5EE299A5E87F5C5D3
39C2CC0224E9D916A54454C88A9C2A91
A7663D47813863B5BBB68497F8CB6185
93A15B736EC722A2468393333E304480
5F84BC91948BC70EB79365216D49864F
8682EEE45D911393E25267EF532C0E63
8E28C6D38F991DDFC47B72C652FF850B
3DF3F9D191E1AEC45E88F728C7AF6AB5
7F49E49444B1A466C033C676971F0784
21C59CE7802F305B2F7302AB787FC9D5
E63DB07F357434A78B12352E92D26D9C
F83580F0798EFB91F721408DC6E2E4CA
13B6384148E98549EF0A4BC60A901C9C
29C20F8C8868231246611EB07355C88F
E16AB98EE474C9D6856AE3FA28EE3433

Also change in Encrypted message:



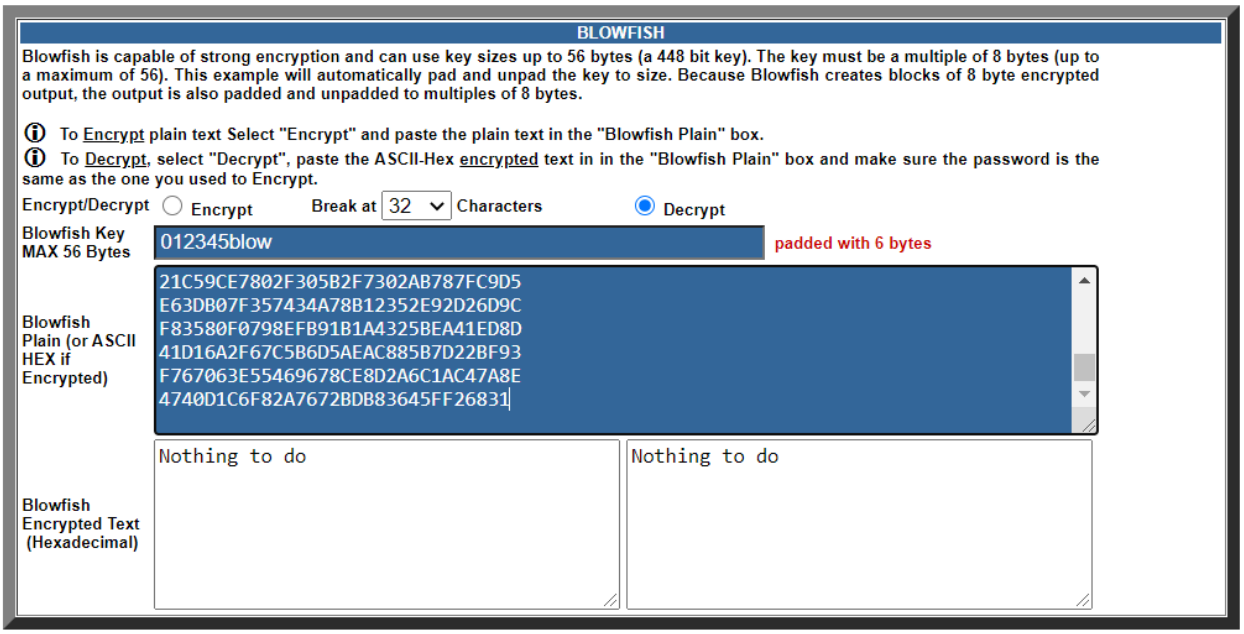


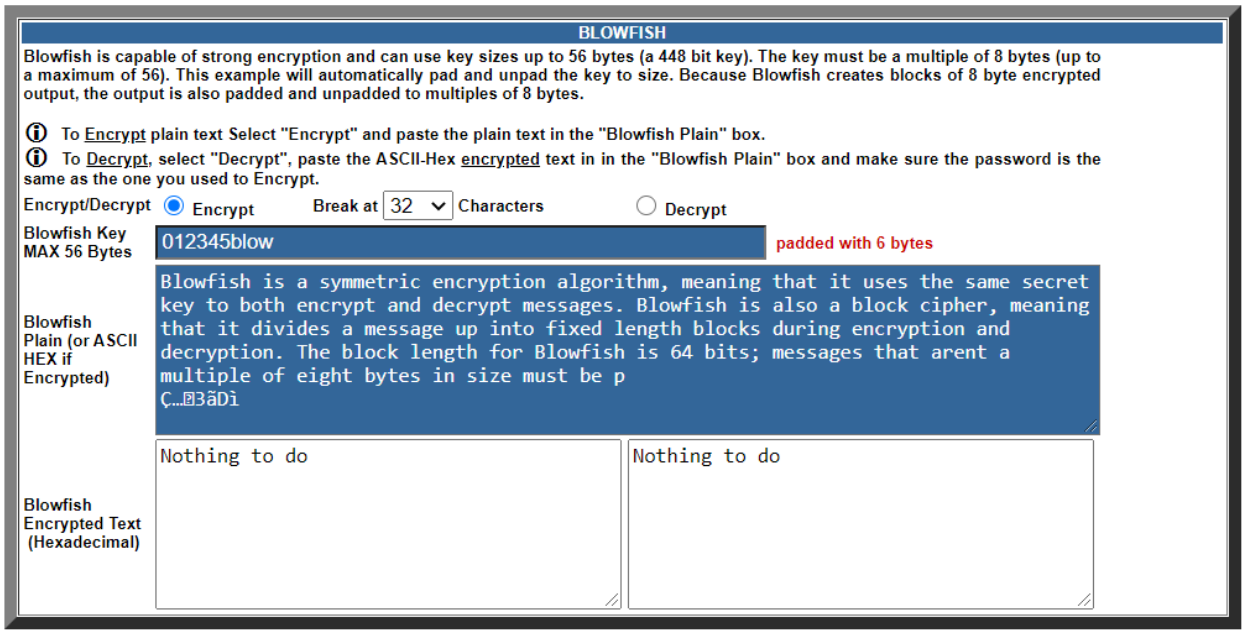
3. **Delete one character at the end of the message. How much of the encoded message changes?**



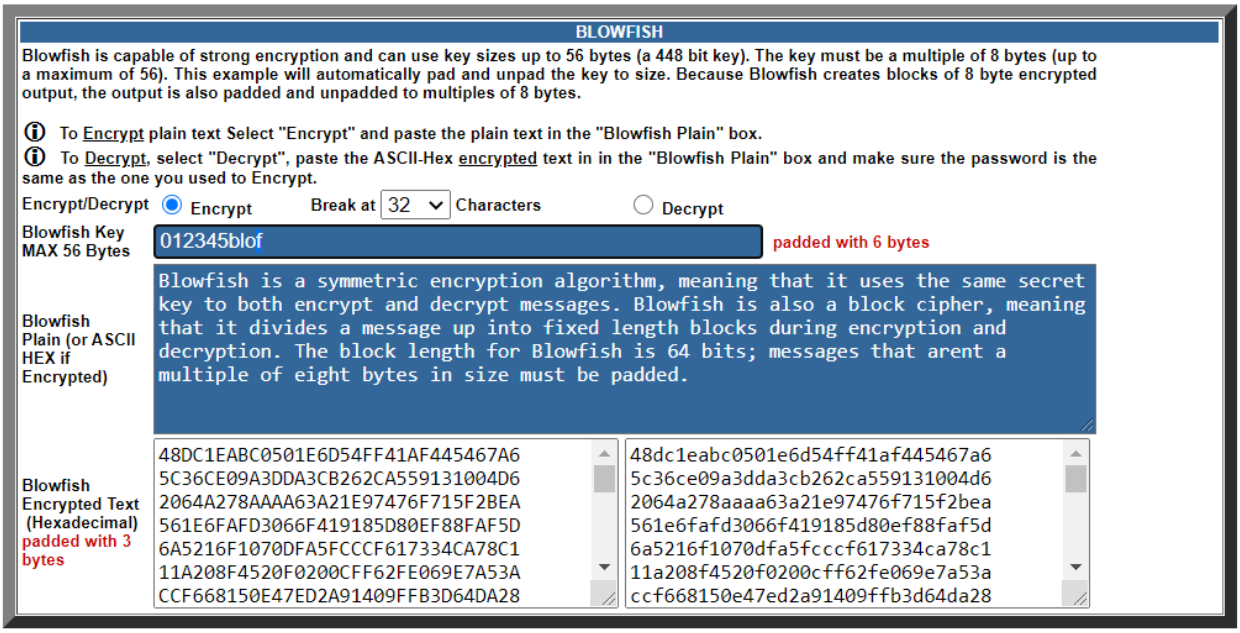
DEC784BD0FF090C0B767698E9B09169E
47B306D9B8A80D285451EC529E42D5B7
49CB24105DC7E2E3FD3955A49ABA6096
A7663D47813863B5840BB9C7709BE494
D4F963FEFCD4C8F28DDD7B3A7B615F66
6C9BDA4C0781E284D69B1C730550E36D
C5E1BA7233CB8BC81DBDD95C654EEDDA
DBDD884E9A8542BCD2450ACD3F6ADEC5
41495570EA9DF6A5EE299A5E87F5C5D3
39C2CC0224E9D916A54454C88A9C2A91
A7663D47813863B5BBB68497F8CB6185
93A15B736EC722A2468393333E304480
5F84BC91948BC70EB79365216D49864F
8682EEE45D911393E25267EF532C0E63
8E28C6D38F991DDFC47B72C652FF850B
3DF3F9D191E1AEC45E88F728C7AF6AB5
7F49E49444B1A466C033C676971F0784
21C59CE7802F305B2F7302AB787FC9D5
E63DB07F357434A78B12352E92D26D9C
F83580F0798EFB91F721408DC6E2E4CA
13B6384148E98549EF0A4BC60A901C9C
29C20F8C8868231246611EB07355C88F
E16AB98EE474C9D6**AE81ED66E5F38CF2**

Also change in Encrypted message:





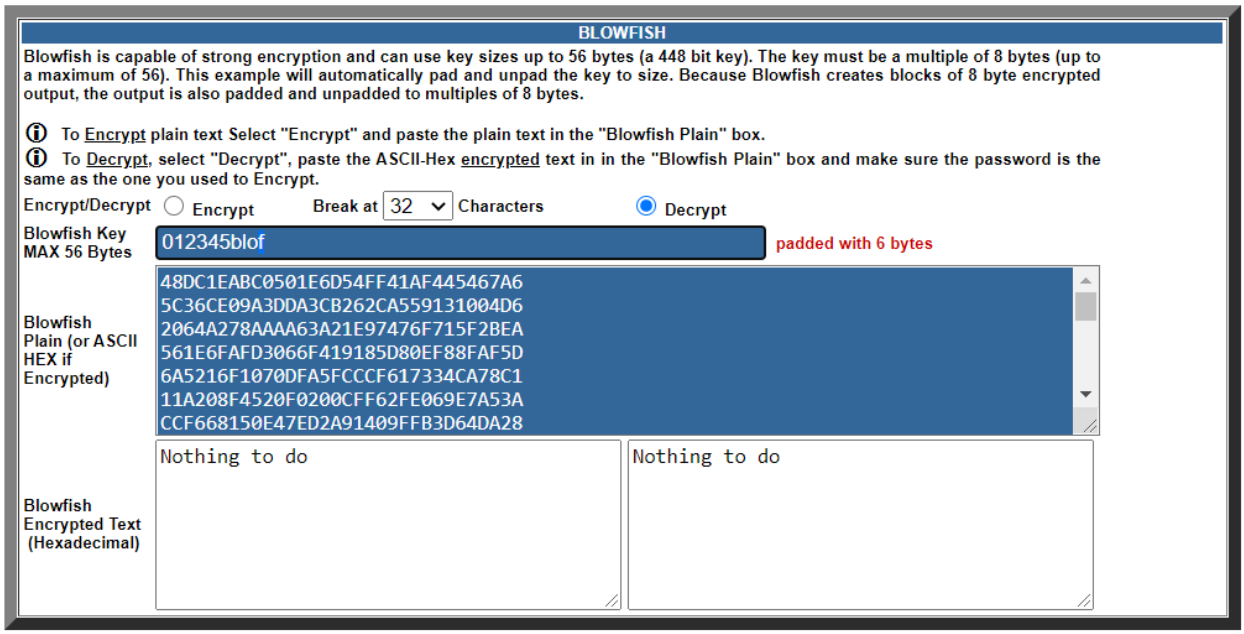
4. **Change one character in the key. How much of the encoded message changes?**

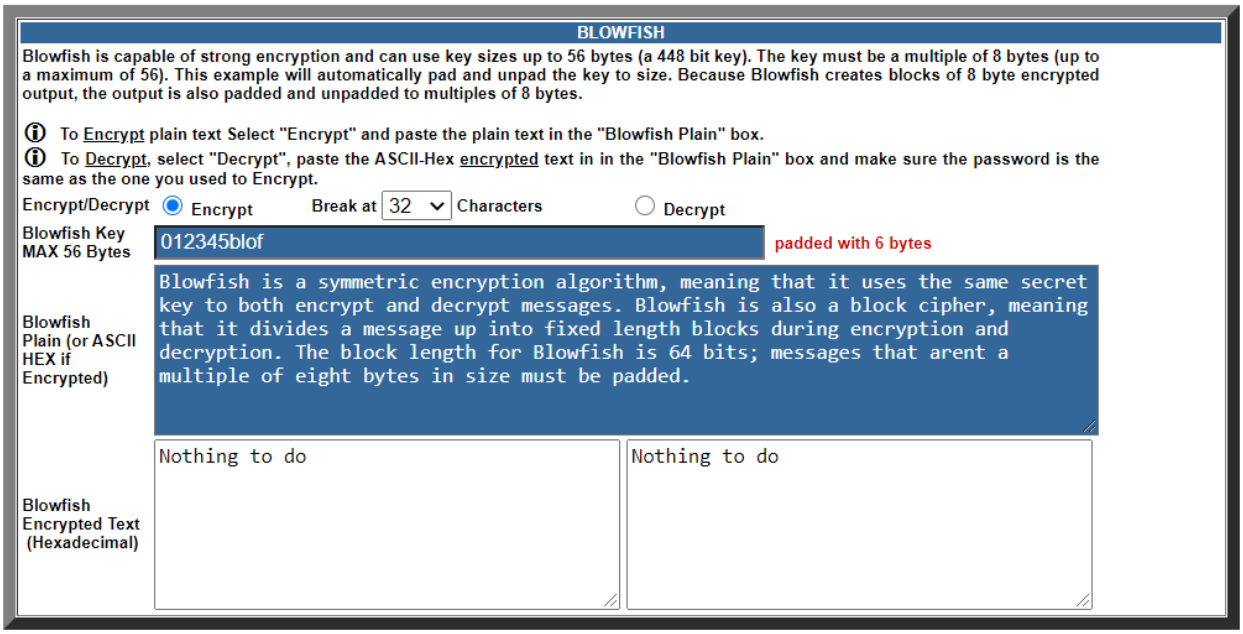


Encrypted message:

48DC1EABC0501E6D54FF41AF445467A6
5C36CE09A3DDA3CB262CA559131004D6
2064A278AAAA63A21E97476F715F2BEA
561E6FAFD3066F419185D80EF88FAF5D
6A5216F1070DFA5FCCCF617334CA78C1
11A208F4520F0200CFF62FE069E7A53A
CCF668150E47ED2A91409FFB3D64DA28
C771F55D9C101C02829875138914CEA9
19656FC6DB6325474DDB532CC7785801
5438EE9121595EE18A84E6203766FA8D
561E6FAFD3066F41E304B6F65BA3E165
1AC442785BAB2849D7FE66693BFA142C
4D51B4716A1F0F05CD77239AF16C5521
83A08268A5367E7E07BACCFEA45132DA
0C90AE8A6E3B7E6FE7720D67E2BCD56E
E0278E0B1606F5BD30728F88C9F6CA27
9954B21030C551FC26AF6AEBF28A399B
3B5094A5F80D523C997EC12F37262CF6
5320955C8FB5D6DF61149C2E7C55B3AB
D5D5C604F39BA94A01D8AD9F1818FA78
53D103F7959EC15FA64B6EA0F13151B4
85BD2547968C098CEFB6069C1F849B04
4C1A32FB1EE6C60B1A8297B9B0A33521

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

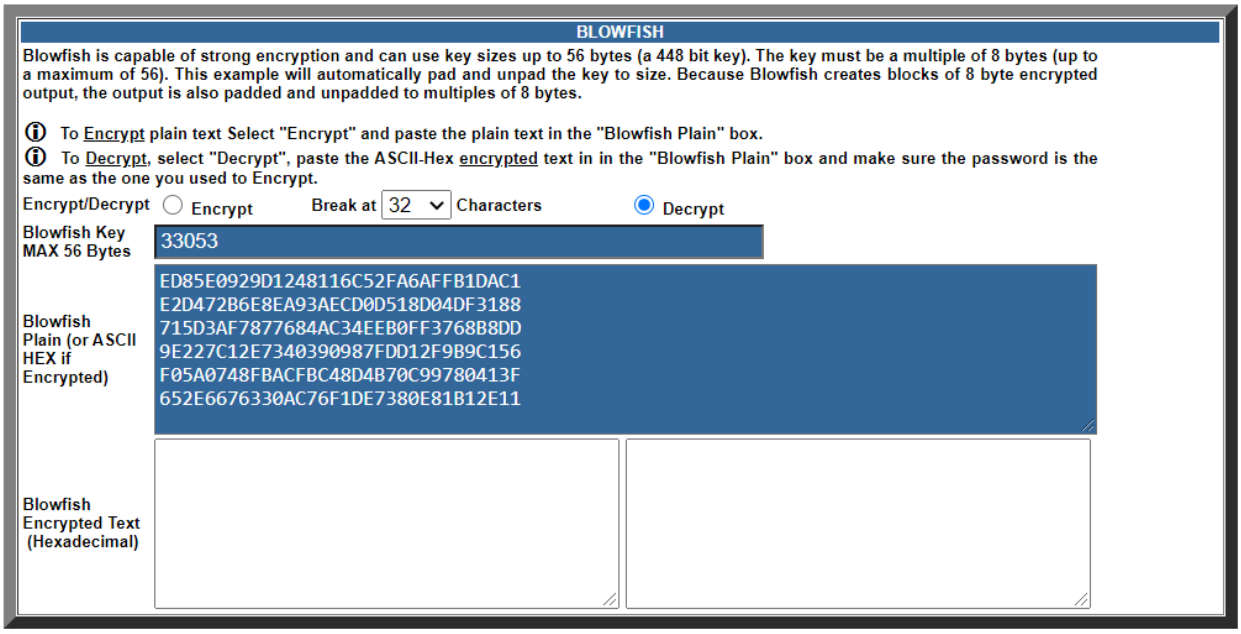


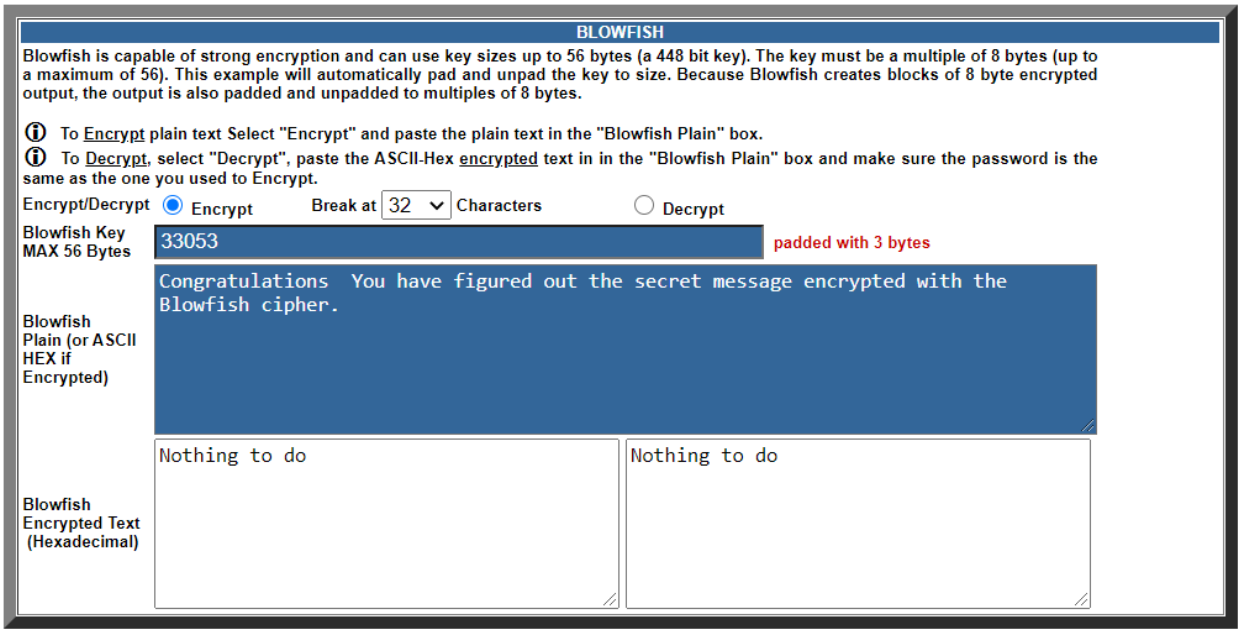


A Secret Message

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

ED85E0929D1248116C52FA6AFFB1DAC1
E2D472B6E8EA93AECD0D518D04DF3188
715D3AF7877684AC34EEB0FF3768B8DD
9E227C12E7340390987FDD12F9B9C156
F05A0748FBACFBC48D4B70C99780413F
652E6676330AC76F1DE7380E81B12E11





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.

(Blowfish: By PV-J)

Conclusion:

1. Blowfish Algorithm can achieve efficient data encryption up to 4 bits per clock. It is a variable-length key block cipher.
2. It is fit for applications where the key is more consistent, for example, a communication link. Blowfish is a 16 rounds block encryption algorithm that is very secured.
3. Blowfish is frequent and consistently used since it has gone through repetitive tests. It is efficient due to it taking advantage of built-in instructions on the current microprocessors for basic-bit shuffling operations.
4. The advanced algorithm can be invented for future enhancement. It is required for better security, to encrypt a more complicated image.