

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.

The screenshot shows a web-based Blowfish encryption tool. At the top, a blue header bar contains the title "BLOWFISH". Below the header, a paragraph explains the tool's capabilities: "Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadding to multiples of 8 bytes." Below this, two numbered instructions are provided: 1. To Encrypt: Select "Encrypt" and paste the plain text in the "Blowfish Plain" box. 2. To Decrypt: Select "Decrypt", paste the ASCII-Hex encrypted text in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt. The interface includes a "Break at" dropdown set to "32" and "Characters". There are two radio buttons for "Encrypt/Decrypt": "Encrypt" is selected, and "Decrypt" is unselected. The "Blowfish Key" field, labeled "MAX 56 Bytes", contains the text "hgftyuioknbvcdew". The "Blowfish Plain (or ASCII HEX if Encrypted)" field contains the text "Hello my name is Shreyas". Below these fields, there are two output boxes. The left box, labeled "Blowfish Encrypted Text (Hexadecimal)", contains the text "ECC276FA476C36B24158C59524609C0F51E63D3C8C6E45F5". The right box contains the text "ecc276fa476c36b24158c59524609c0f51e63d3c8c6e45f5".

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?

BLOWFISH

Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadded to multiples of 8 bytes.

① To Encrypt plain text Select "Encrypt" and paste the plain text in the "Blowfish Plain" box.
① To Decrypt, select "Decrypt", paste the ASCII-Hex encrypted text in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt.

Encrypt/Decrypt ☒ Encrypt Break at Characters ☐ Decrypt

Blowfish Key
MAX 56 Bytes hgftyuioknbvcdew

Blowfish Plain (or ASCII
HEX if
Encrypted)
Hello my name is Shreya0

Blowfish Encrypted Text (Hexadecimal)

ECC276FA476C36B24158C59524609C0F 660CE9BDBD67FF81	ecc276fa476c36b24158c59524609c0f 660ce9bdbbd67ff81
--	---

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?

BLOWFISH

Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadded to multiples of 8 bytes.

① To Encrypt plain text Select "Encrypt" and paste the plain text in the "Blowfish Plain" box.
① To Decrypt, select "Decrypt", paste the ASCII-Hex encrypted text in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt.

Encrypt/Decrypt ☒ Encrypt Break at Characters ☐ Decrypt

Blowfish Key
MAX 56 Bytes hgftyuioknbvcdew

Blowfish Plain (or ASCII
HEX if
Encrypted)
Yello my name is Shreyas

Blowfish Encrypted Text (Hexadecimal)

445B72365961769A4158C59524609C0F 51E63D3C8C6E45F5	445b72365961769a4158c59524609c0f 51e63d3c8c6e45f5
--	--

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?

BLOWFISH

Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadded to multiples of 8 bytes.

① To **Encrypt** plain text Select "Encrypt" and paste the plain text in the "Blowfish Plain" box.
① To **Decrypt**, select "Decrypt", paste the ASCII-Hex **encrypted** text in in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt.

Encrypt/Decrypt ☒ Encrypt Break at Characters ☐ Decrypt

Blowfish Key
MAX 56 Bytes hgftyuioknbvcdew

Blowfish Plain (or ASCII
HEX if
Encrypted)
Hello my name is Shreya

Blowfish Encrypted Text
(Hexadecimal)
padded with 1
bytes

ECC276FA476C36B24158C59524609C0F A241A0F46ACA26DB	ecc276fa476c36b24158c59524609c0f a241a0f46aca26db
--	--

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?

BLOWFISH

Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadded to multiples of 8 bytes.

① To **Encrypt** plain text Select "Encrypt" and paste the plain text in the "Blowfish Plain" box.
① To **Decrypt**, select "Decrypt", paste the ASCII-Hex **encrypted** text in in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt.

Encrypt/Decrypt ☒ Encrypt Break at Characters ☐ Decrypt

Blowfish Key
MAX 56 Bytes hgftyuioknbvcdes

Blowfish Plain (or ASCII
HEX if
Encrypted)
Hello my name is Shreyas

Blowfish Encrypted Text
(Hexadecimal)

49AEF241224C0F53BF815F266FC213F1 3AA44D2E7F71BAAB	49aef241224c0f53bf815f266fc213f1 3aa44d2e7f71baab
--	--

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 anything like the original?

The screenshot shows a web-based BLOWFISH encryption tool. At the top, a blue header reads "BLOWFISH". Below it, a paragraph explains that Blowfish can use key sizes up to 56 bytes (448 bits) and that the key must be a multiple of 8 bytes. It also notes that the output is padded to multiples of 8 bytes. Two numbered instructions follow: 1. To encrypt, select "Encrypt" and paste plain text into the "Blowfish Plain" box. 2. To decrypt, select "Decrypt", paste the ASCII-Hex encrypted text into the "Blowfish Plain" box, and ensure the password is the same as the one used for encryption. The interface includes a "Blowfish Key" field with a dropdown menu set to "MAX 56 Bytes" and a text input containing "hgftyuioknbvodes". Below the key field is a large blue box labeled "Blowfish Plain (or ASCII HEX if Encrypted)" containing the text "Hello my name is Shreyas". At the bottom, there are two empty text boxes: "Blowfish Encrypted Text (Hexadecimal)" on the left and "Nothing to do" on the right. The "Encrypt/Decrypt" section has two radio buttons: "Encrypt" (selected) and "Decrypt". A "Break at" dropdown is set to "32" characters.

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
E2D472B6E8EA93AECDD0D518D04DF3188
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:

BLOWFISH

Blowfish is capable of strong encryption and can use key sizes up to 56 bytes (a 448 bit key). The key must be a multiple of 8 bytes (up to a maximum of 56). This example will automatically pad and unpad the key to size. Because Blowfish creates blocks of 8 byte encrypted output, the output is also padded and unpadded to multiples of 8 bytes.

❶ To Encrypt plain text Select "Encrypt" and paste the plain text in the "Blowfish Plain" box.
 ❶ To Decrypt, select "Decrypt", paste the ASCII-Hex encrypted text in in the "Blowfish Plain" box and make sure the password is the same as the one you used to Encrypt.

Encrypt/Decrypt ☒ **Encrypt** Break at Characters ☐ Decrypt

Blowfish Key
MAX 56 Bytes

shreyasprerak padded with 3 bytes

Blowfish Plain (or ASCII HEX if Encrypted)

ED85E0929D1248116C52FA6AFFB1DAC1

Blowfish Encrypted Text (Hexadecimal)
padded with 4 bytes

A6BEFFB105E93280B6BE8D6454C51349
 BA905D07DA413899884907A5111C8210
 18FAD827B51D2BCD3949D02C21CE0EE3
 AC01EEF262E17B8CEDC7DEEEB8A0CC72
 A068691BAA9B677EABFB0524832A408E
 A6E2E5E4A84EE7D71667470DD5320609

79c02c9ab20a408f63b676cf8b5a6046
 82fb266b8e18d056928cc9d2c23ecd1c
 dde9002722b9ac9e732215689cf4ad53
 eced512f4861240a5d05c237dc50dfc7
 1429b9a43c82267b15fd7e53e6753f81
 638dfb7d2324afb6bcc15a35450a7235
 eb0a317ae1078173111dd262905233d2

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 decryption.