Experiment 5

BlowFish

Name: Sumeet Haldipur

UID: 2019130018 **Class:** TE Comps

Aim: To implement blowfish algorithm.

THEORY

BLOWFISH ALGORITHM:

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone." Notable features of the design include key-dependent S-boxes and a highly complex key schedule. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

Blowfish uses:

• blockSize: 64-bits

• **keySize**: 32-bits to 448-bits variable size

• **number of subkeys**: 18 [P-array]

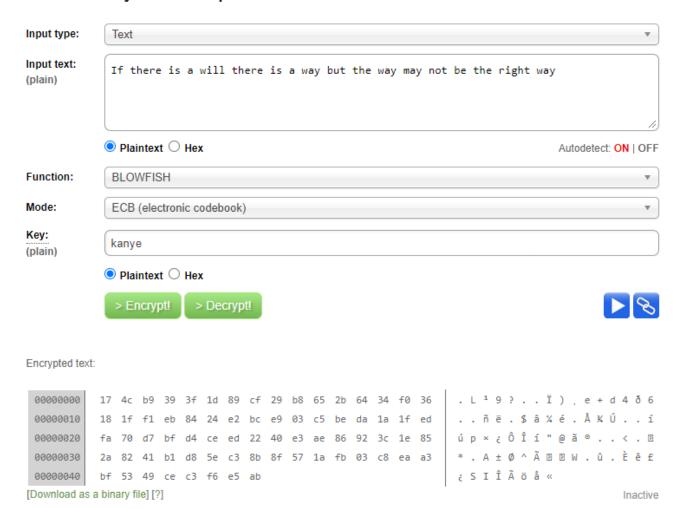
number of rounds: 16

number of substitution boxes: 4 [each having 512 entries of 32-bits each

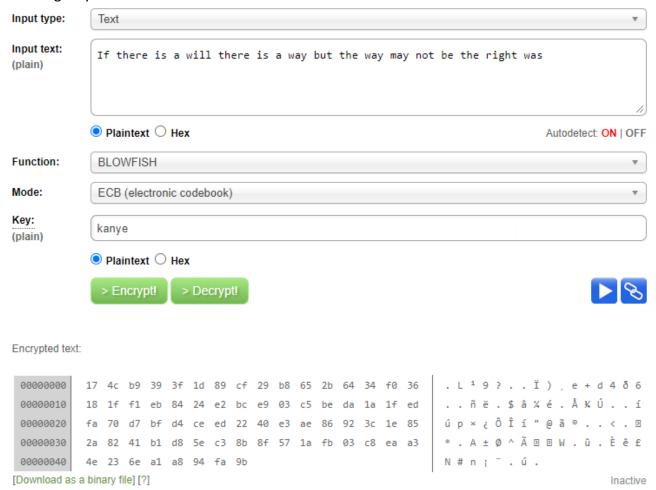
• I used http://blowfish.online-domain-tools.com/ for the experiment.

Original encoded message

Blowfish - Symmetric Ciphers Online

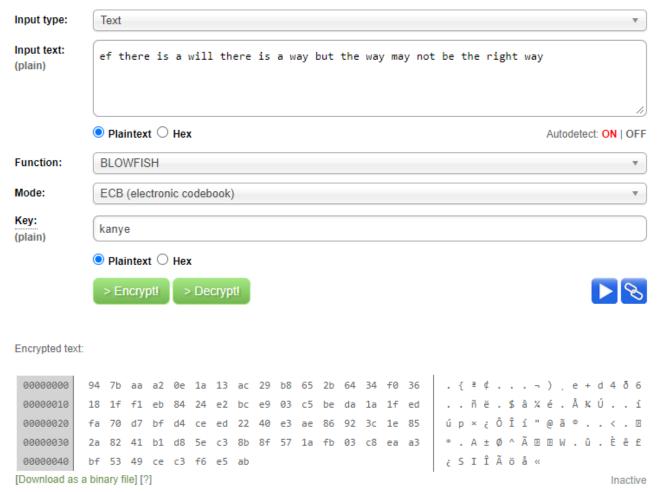


1)If you change one character at the end of the message, the encoded message changes in the following way:



Last 16 characters of the encrypted message change. The rest of the message is the same.

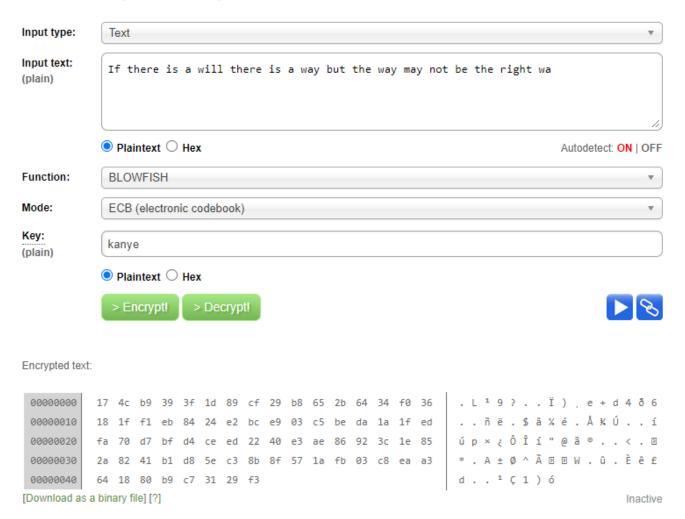
2)If you change one character at the beginning of the message, the encoded message changes as follows:



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

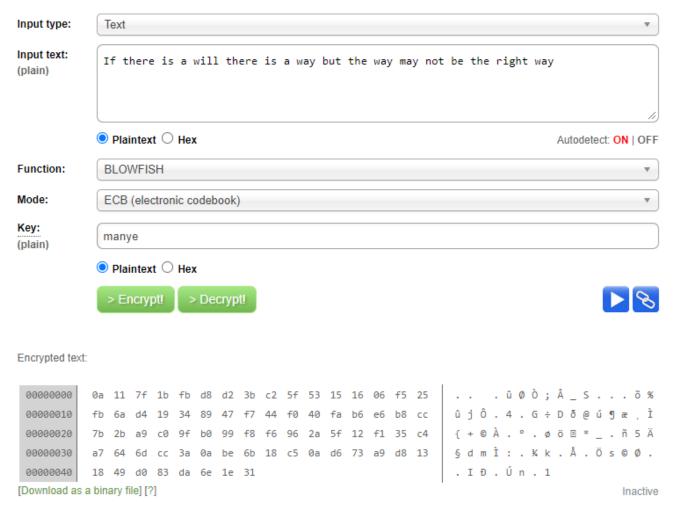
3) If you delete one character at the end of the message, the encoded message changes as follows:

Blowfish - Symmetric Ciphers Online

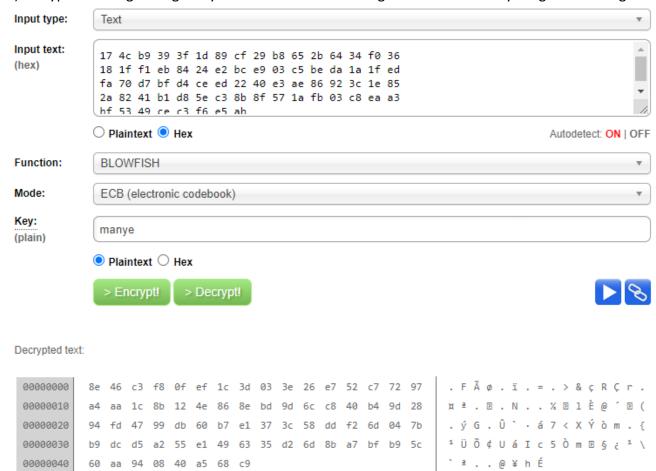


After deleting last character of plain text message, last 16 characters of the encrypted message changes, and the rest of the encrypted message remains same. Size remains the same since ECB is used which is a block cipher. 4)If you change one character in a key, the encoded message changes as follows:

Blowfish - Symmetric Ciphers Online



After changing one character in a key, entire encrypted message changes. Size of the encrypted message remains the same since the key length is the same.



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

Does not resemble original message and a lot of special characters are seen.

CONCLUSION

[Download as a binary file] [?]

- 1. Studied and understood the Blowfish algorithm.
- 2. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

Inactive

- 3. Blowfish is considered to be a block Cipher since changing one text alters that section of the block encryption.
- 4. It is also a symmetric cypher because it encrypts and decrypts with the same key. Any change in key causes the ciphered text to be incorrectly deciphered.