Homework for section#4 (approximate due date Sept 7th, 2020)

- Find the 32-bit substitutions of the following 48-bit data streams with the S-Box of DES:

1. Stream #1 111010 001010 011010 101001 101110 110101 010001 110010

Applying 8 S-box to the stream

1[1101]0 => 10 = 1010

0[0101]0 => 11 = 1011

0[1101]0 => 4 = 0100

1[0100]1 => 10 = 1010

1[0111]0 => 8 = 1000

1[1010]1 => 1 = 0001

0[1000]1 => 14 = 1110

1[1001]0 => 6 = 0110

1010 1011 0100 1010 1000 0001 1110 0110

2. Stream #2 010101 110011 011011 101110 110101 101011 101010 111001

Applying 8 S-box to the stream

0[1010]1 => 12 = 1100

1[1001]1 => 6 = 0110

0[1101]1 => 11 = 1011

1[0111]0 => 13 = 1101

1[1010]1 => 0 = 0000

1[0101]1 => 5 = 0101

1[0101]0 => 3 = 0011

1[1100]1 => 3 = 0011

1100 0110 1011 1101 0000 0101 0011 0011

- Using DES key processor, find the first 4 sub-keys of:

Key#1 □ 0110110101100101011010010111010101010001101001101101000101010110

Here, K0 = 0110110101100101011010010111010101010001101001101101000101010110

Applying initial permutation PC1 to K0

0110000011011111001011111101 1010000010101011000001011000

C0 = 0110000011011111001011111101

D0 = 1010000010101011000001011000

Applying Left shift to C0 and D0

C1 = 1100000110111110010111111010

D1 = 0100000101010110000010110001

Applying permutation PC2 to C1 + D1

K1 = 101110001010101001001111010000111000010100010100

===

Applying Left shift to C1 and D1

C2 = 1000001101111100101111110101

D2 = 1000001010101100000101100010

Applying permutation PC2 to C2 + D2

K2 = 111110010011111011010110100101001001001000011010

===

Applying Left shift to C2 and D2

C3 = 0000110111110010111111010110

D3 = 0000101010110000010110001010

Applying permutation PC2 to C3 + D3

K3 = 011101001111011011001100000101010011011001100000

===

Applying Left shift to C3 and D3

C4 = 0011011111001011111101011000

D4 = 0010101011000001011000101000

Applying permutation PC2 to C4 + D4

K4 = 010100101101010101110110001110001010100001100000

==

Key#2 1101001001101011001000110101010101110110010011101011101010001101

Here, K0 = 1101001001101011001000110101010101110110010011101011101010001101

Applying initial permutation PC1 to K0

0110000011011111001011111101 1010000010101011000001011000

C0 = 1100000100111011010101100101

D0 = 0111011110111000111000101001

Applying Left shift to C0 and D0

C1 = 1000001001110110101011001011

D1 = 1110111101110001110001010010

Applying permutation PC2 to C1 + D1

K1 = 111010011011011000011000011001110110101010101110

==

Applying Left shift to C1 and D1

C2 = 0000010011101101010110010111

D2 = 1101111011100011100010100101

Applying permutation PC2 to C2 + D2

K2 = 101100010111000010101110000100101110111110000011

==

Applying Left shift to C2 and D2

C3 = 0001001110110101011001011100

D3 = 0111101110001110001010010111

Applying permutation PC2 to C3 + D3

K3 = 101100000000011111110000111111100010010100010101

==

Applying Left shift to C3 and D3

C4 = 0100111011010101100101110000

D4 = 1110111000111000101001011101

Applying permutation PC2 to C4 + D4

K4 = 110101000101101000110101111010110110001111001010

==

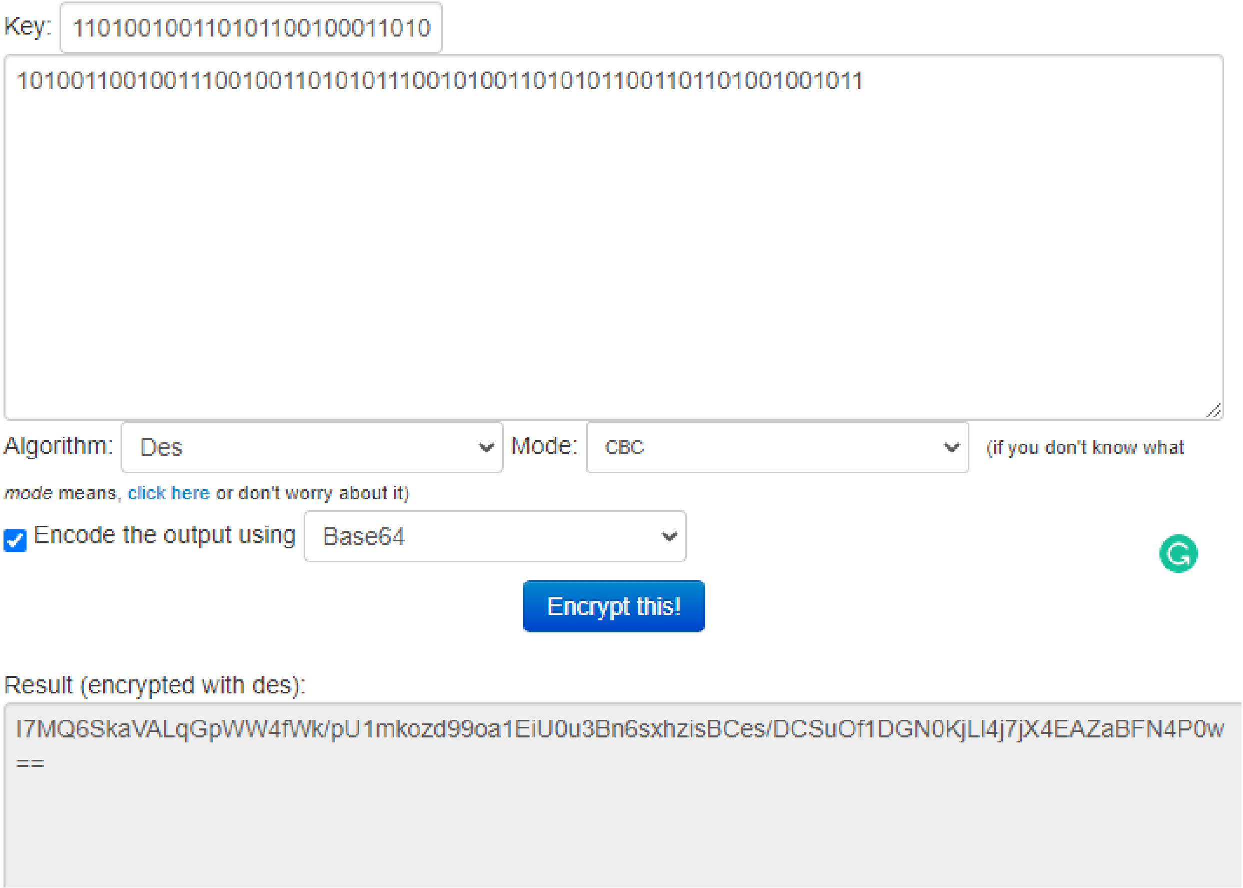
- Using DES online tool, find the cipher text of the following data streams:

Stream#1 1010011001001110010011010101110010100110101011001101101001001011

Key: 1101001001101011001000110101010101110110010011101011101010001101

Mode: CBC (cipher block chaining)

Cipher Text:
I7MQ6SkaVALqGpWW4fWk/pU1mkozd99oa1EiU0u3Bn6sxhzisBCes/DCSuOf1DGN0KjLl4j7jX4EA
ZaBFN4P0w==



Key: 110100100110101100100011010

1010011001001110010011010101110010100110101011001101101001001011

Algorithm: Des

Mode: CBC

(if you don't know what *mode* means, click here or don't worry about it)

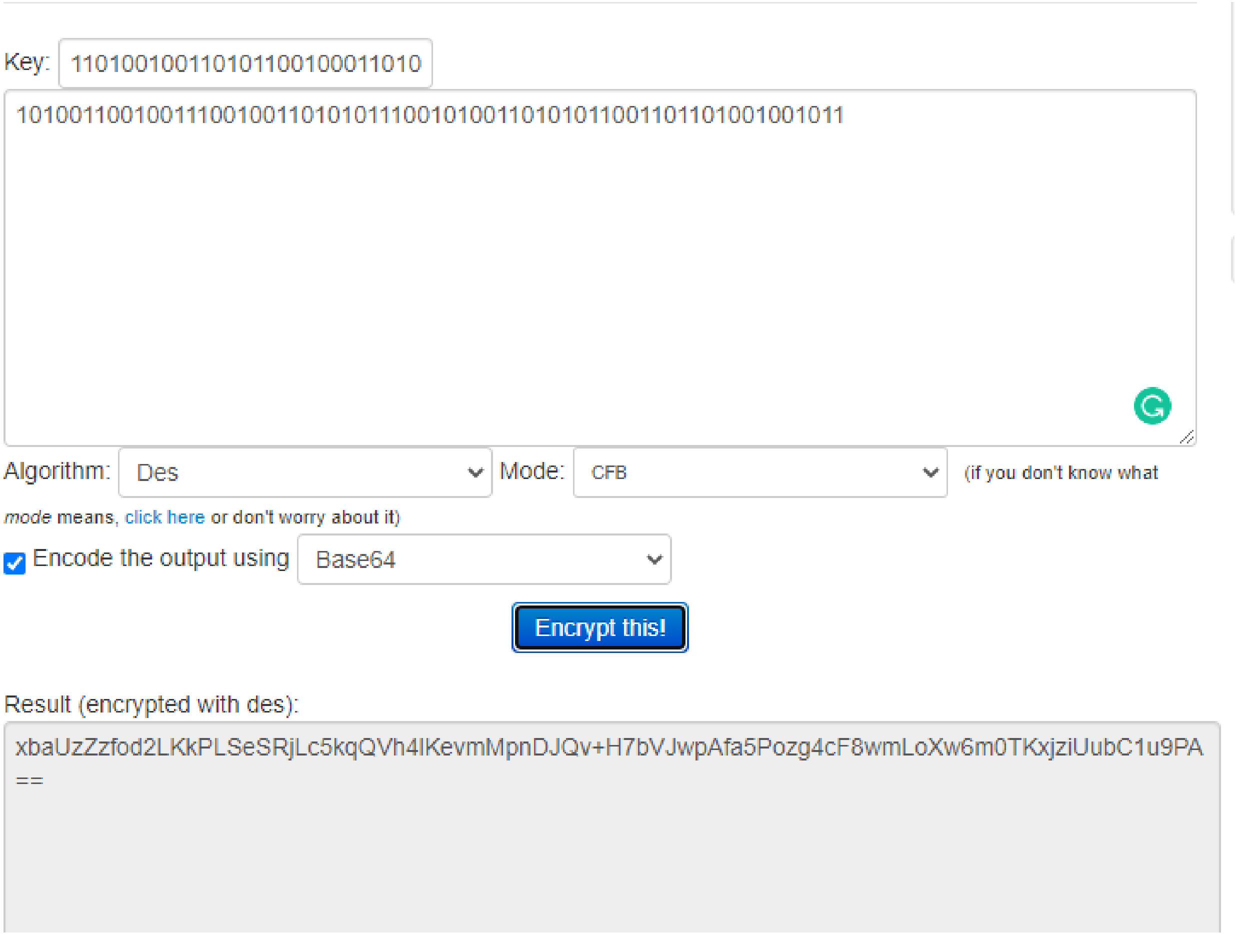
☑ Encode the output using Base64

Result (encrypted with des):

I7MQ6SkaVALqGpWW4fWk/pU1mkozd99oa1EiU0u3Bn6sxhzisBCes/DCSuOf1DGN0KjLl4j7jX4EAZaBFN4P0w
==

Mode: CFB (cipher feedback)

Cipher Text: xbaUzZzfod2LKkPLSeSRjLc5kqQVh4lKevmMpnDJQv+H7bVJwpAfa5Pozg4cF8wmLoXw6m0TKxjziUubC1u9PA==



Key: 110100100110101100100011010

1010011001001110010011010101110010100110101011001101101001001011

Algorithm: Des

Mode: CFB

(if you don't know what *mode* means, click here or don't worry about it)

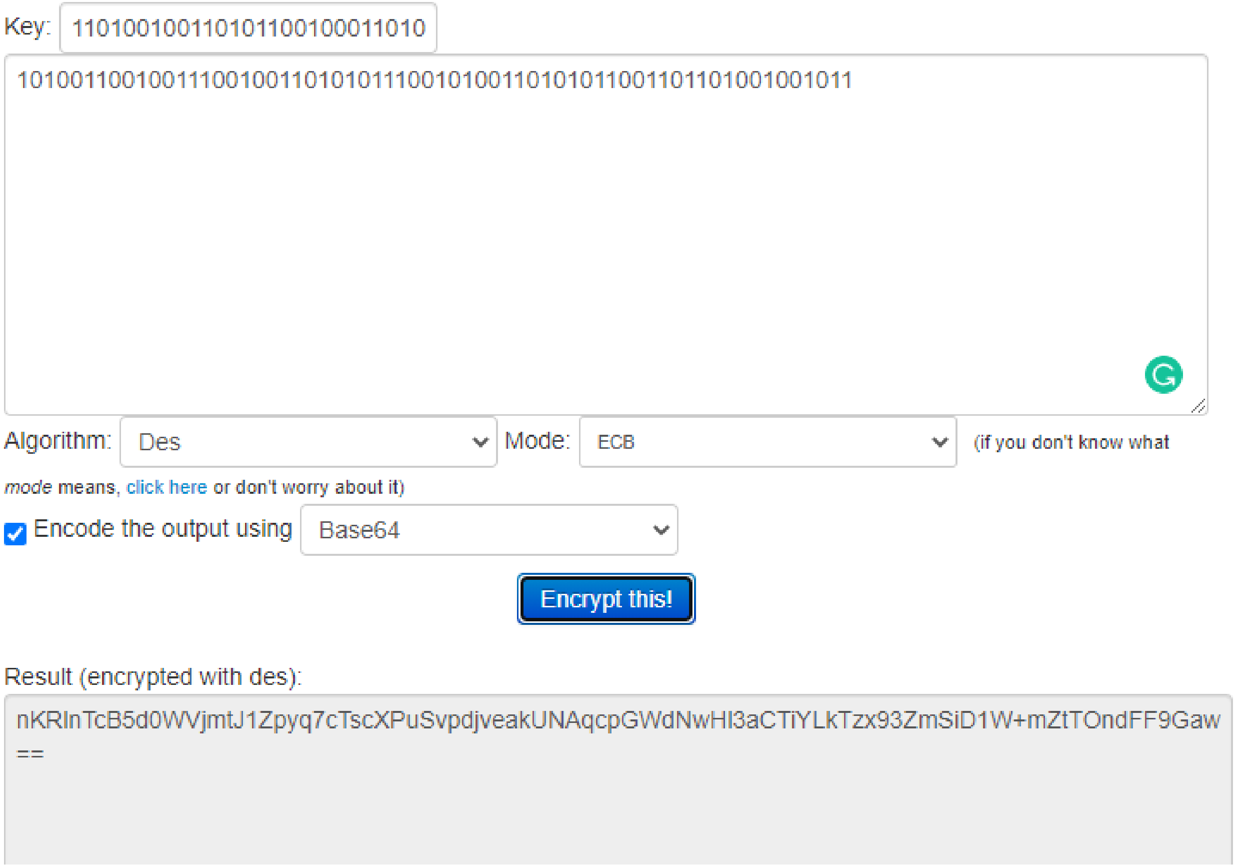
☑ Encode the output using Base64

Result (encrypted with des):

xbaUzZzfod2LKkPLSeSRjLc5kqQVh4lKevmMpnDJQv+H7bVJwpAfa5Pozg4cF8wmLoXw6m0TKxjziUubC1u9PA==

Mode: ECB (electronic codebook)

Cipher Text:
nKRlnTcB5d0WVjmtJ1Zpyq7cTscXPuSvpdjveakUNAqcpGWdNwHl3aCTiYLkTzx93ZmSiD1W+mZtT
OndFF9Gaw==



Key: 110100100110101100100011010

1010011001001110010011010101110010100110101011001101101001001011

Algorithm: Des ⌄ Mode: ECB ⌄ (if you don't know what *mode* means, click here or don't worry about it)

☑ Encode the output using Base64 ⌄

Result (encrypted with des):

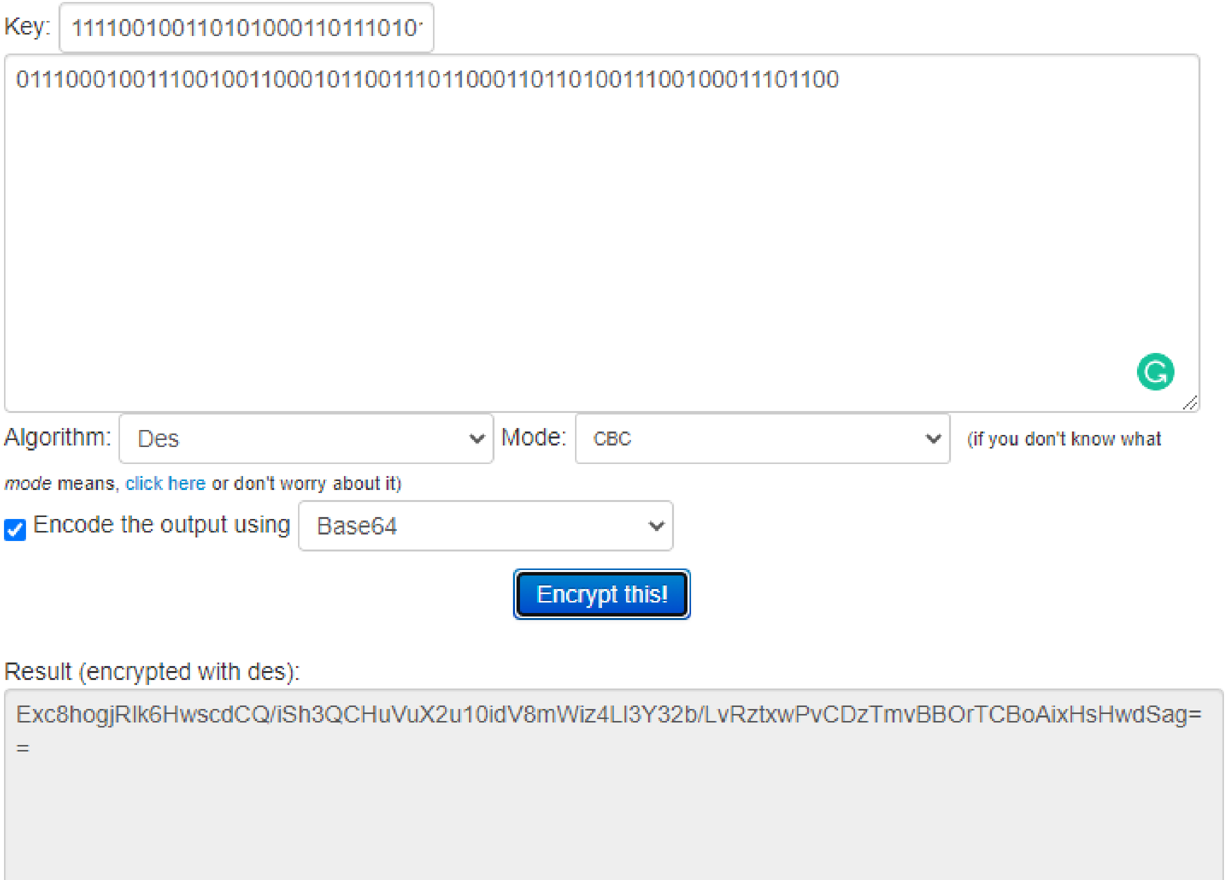
nKRlnTcB5d0WVjmtJ1Zpyq7cTscXPuSvpdjveakUNAqcpGWdNwHl3aCTiYLkTzx93ZmSiD1W+mZtTOndFF9Gaw
==

Stream#2 0111000100111001001100010110011101100011011010011100100011101100

key: 1111001001101010001101110101010101110110010011101011101011101001

Mode: CBC (cipher block chaining)

Cipher Text:
Exc8hogjRlk6HwscdCQ/iSh3QCHuVuX2u10idV8mWiz4Ll3Y32b/LvRztxwPvCDzTmvBBOrTCBoAixHsHwdSag==



Key: 11110010011010100011011101

0111000100111001001100010110011101100011011010011100100011101100

Algorithm: Des Mode: CBC (if you don't know what *mode* means, click here or don't worry about it)

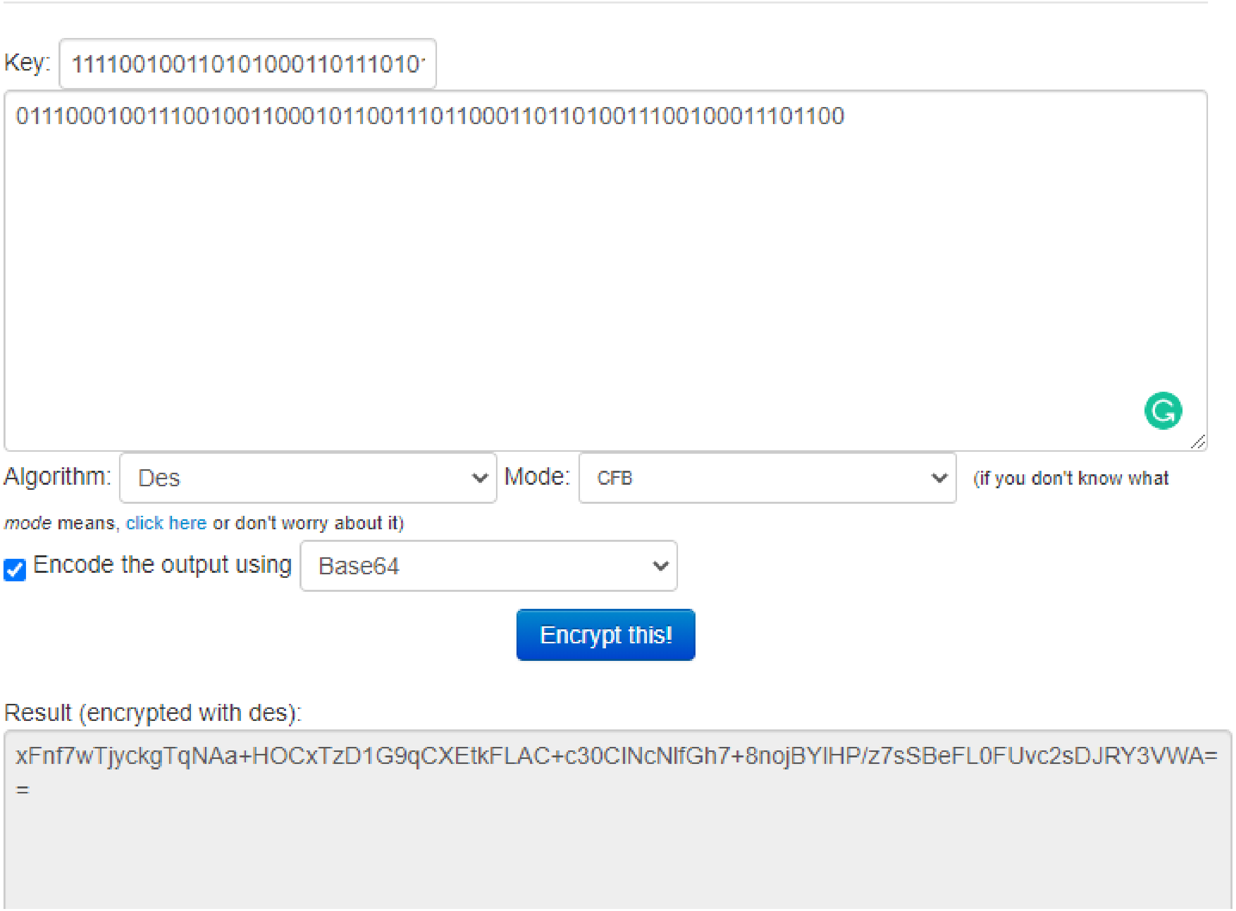
☑ Encode the output using Base64

Result (encrypted with des):

Exc8hogjRlk6HwscdCQ/iSh3QCHuVuX2u10idV8mWiz4Ll3Y32b/LvRztxwPvCDzTmvBBOrTCBoAixHsHwdSag==

Mode: CFB (cipher feedback)

Cipher Text:
xFnf7wTjyckgTqNAa+HOCxTzD1G9qCXEtkFLAC+c30ClNcNlfGh7+8nojBYlHP/z7sSBeFL0FUvc2sDJR
Y3VWA==



Key: 111100100110101000110111010

01110001001110010011000101100111011000110110100111001000111 01100

Algorithm: Des Mode: CFB (if you don't know what *mode* means, click here or don't worry about it)

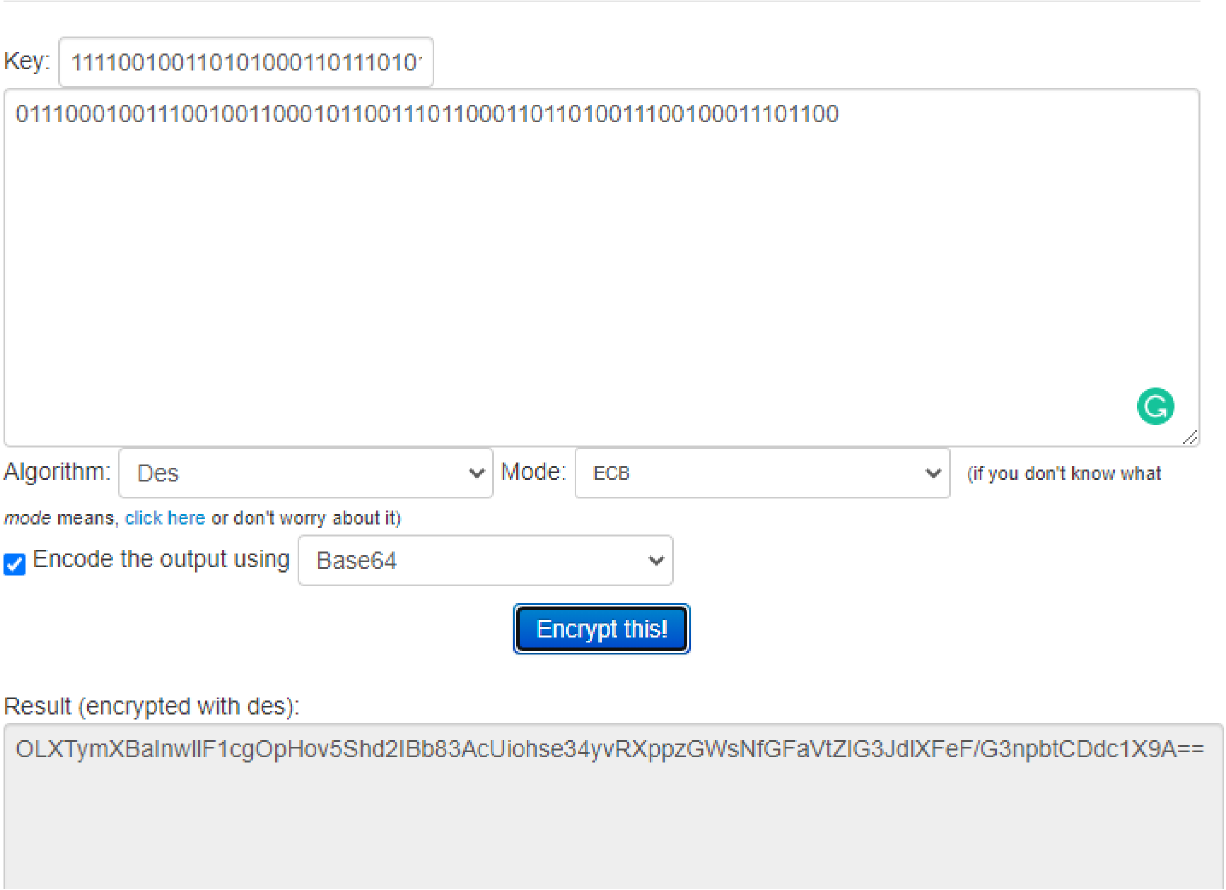
☑ Encode the output using Base64

Result (encrypted with des):

xFnf7wTjyckgTqNAa+HOCxTzD1G9qCXEtkFLAC+c30ClNcNlfGh7+8nojBYlHP/z7sSBeFL0FUvc2sDJRY3VWA=
=

Mode: ECB (electronic codebook)

Cipher Text:
OLXTymXBaInwllF1cgOpHov5Shd2IBb83AcUiohse34yvRXppzGWsNfGFaVtZlG3JdlXFeF/G3npbtC
Ddc1X9A==



Key: 111100100110101000110111010

0111000100111001001100010110011101100011011010011100100011101100

Algorithm: Des

Mode: ECB

(if you don't know what *mode* means, click here or don't worry about it)

☑ Encode the output using Base64

Result (encrypted with des):

OLXTymXBaInwllF1cgOpHov5Shd2IBb83AcUiohse34yvRXppzGWsNfGFaVtZlG3JdlXFeF/G3npbtCDdc1X9A==

Example of resource: https://www.tools4noobs.com/online_tools/encrypt/