Họ tên: Ngô Trung Hiếu

Lớp: CNTT4 – K60

MSV: 191213136

BÀI TẬP ONLINE DES (Đề số 20)

K: 9CA2FA3E9343770F

M: 455D56BDA4913149

K nhị phân:
1001110010100010111110100011111010010011010000110111011100001111
K hoán vị:
00010111011001000100111001011111111011001001100011011101

Round Number	Bits Rotated	C_i	D_i
0		0001011101100100010011100101	1111111011001001100011011101
1	1	0010111011001000100111001010	1111110110010011000110111011
2	1	0101110110010001001110010100	1111101100100110001101110111
3	2	0111011001000100111001010001	1110110010011000110111011111
4	2	1101100100010011100101000101	1011001001100011011101111111
5	2	0110010001001110010100010111	1100100110001101110111111110
6	2	1001000100111001010001011101	0010011000110111011111111011
7	2	0100010011100101000101110110	1001100011011101111111101100
8	2	0001001110010100010111011001	0110001101110111111110110010
9	1	0010011100101000101110110010	1100011011101111111101100100
10	2	1001110010100010111011001000	0001101110111111110110010011
11	2	0111001010001011101100100010	0110111011111111011001001100
12	2	1100101000101110110010001001	1011101111111101100100110001
13	2	0010100010111011001000100111	1110111111110110010011000110
14	2	1010001011101100100010011100	1011111111011001001100011011
15	2	1000101110110010001001110010	1111111101100100110001101110
16	1	0001011101100100010011100101	1111111011001001100011011101

Round Number	K_i
1	010001100111000000011110011101111011110111000111
2	000101000110011111100101011011101011001100011111
3	110100110101010100010001111101110111010111101010
4	010011011000001111100101011011001001101101101011
5	100100111101000010001111110101101111110001111110
6	001110010000000111110001001101101100111111111000
7	101100000101100010101101100110011111110001111011
8	100100010010001101010100011011111101111000110100
9	011100100110110001011110100110101101101010111010
10	011011001110010100000000110101010111111100110101
11	010000101000110100111111011101100101010111111000
12	111011011010000000001001111110001111101100010111
13	001001111000111010101010001101110010011010111110
14	111110100011000010010010111111010011100111000111
15	001111001000111001011000001001101110001011111111
16	101000010111100111010000111100100110110111001011

L0:10000111011011100001111111101011
R0:00111000010110001000101000000100

-- Round1---
--
L1:00111000010110001000101000000100
E(R0):000111110000001011110001010001010100000000001000
K1:010001100111000000011110011101111011110111000111
ER0XORK1:010110010111001011101111001100101111110111001111
SBox_Out1:010110010111001011101111001100101111110111001111
S1B1:11001010010010001011101011110100
F(R0K1):01110011101110011000010011100001
L0:10000111011011100001111111101011
R1:11110100110101111001101100001010

-- Round 2---
L2:11110100110101111001101100001010
E(R1):011110101001011010101111110011110110100001010101
K2:000101000110011111100101011011101011001100011111
ER1XORK2:011011101111000101001010101000011101101101001010

```
SBox_Out2:011011101111000101001010101000011101101101001010
S2B2:01010010000001101010001110101111
F(R1K2):01001001011000101011110010100011
L1:00111000010110001000101000000100
R2:01110001001110100011011010100111

---------------------------------------- Round 3-----------------------------------------
L3:01110001001110100011011010100111
E(R2):101110100010100111110100000110101101010100001110
K3:110100110101010100010001111011101110101111101010
ER2XORK3:011010010111110011100101111011011010000011100100
SBox_Out3:011010010111110011100101111011011010000011100100
S3B3:10011010111100000100011100000100
F(R2K3):01000100101011010010000100101110
L2:11110100110101111001101100001010
R3:10110000011110101011101000100100

---------------------------------------- Round 4-----------------------------------------
L4:10110000011110101011101000100100
E(R3):010110100000001111110101010111110100000100001001
K4:010011011000001111100101011011001001101101101011
ER3XORK4:000101111000000000010000001100111101101001100010
SBox_Out4:000101111000000000010000001100111101101001100010
S4B4:01111001101000011011100000011011
F(R3K4):10111011000010101100101110000110
L3:01110001001110100011011010100111
R4:11001010001100001111110100100001

---------------------------------------- Round 5-----------------------------------------
L5:11001010001100001111110100100001
E(R4):111001010100000110100001011111111010100100000011
K5:100100111101000010001111110101101111110001111110
ER4XORK5:011101101001000100101110101001010101010101111101
SBox_Out5:011101101001000100101110101001010101010101111101
S5B5:00110011100111011101110101010110
F(R4K5):11110111000101100111001101101010
L4:10110000011110101011101000100100
R5:01000111011011001100100101001110
```

```
-------------------------------------------------- Round 6---------------------------------------------------
L6:01000111011011001100100101001110
E(R5):001000001110101101011001011001010010101001011100
K6:001110010000001111100010011011011001111111111000
ER5XORK6:000110011110100010111011000010001011010110100100
SBox_Out6:000110011110100010111011000010001011010110100100
S6B6:00011010011001111100110001110100
F(R5K6):11010011010111010001010000101110
L5:11001010001100001111110100100001
R6:00011001011011011110100100001111

-------------------------------------------------- Round 7---------------------------------------------------
L7:00011001011011011110100100001111
E(R6):100011110010101101011011111101010010100001011110
K7:101100000101100010101101100110011111110001111011
ER6XORK7:001111110111001111110110011011001101010000100101
SBox_Out7:001111110111001111110110011011001101010000100101
S7B7:00011100101011101001100100111110
F(R6K7):00111011010010100011010101110110
L6:01000111011011001100100101001110
R7:01111100001001101111110000111000

-------------------------------------------------- Round 8---------------------------------------------------
L8:01111100001001101111110000111000
E(R7):001111111000000100001101011111111000000111110000
K8:100100010010001101010100011011111101111000110100
ER7XORK8:101011101010001001011001000100000101111111000100
SBox_Out8:101011101010001001011001000100000101111111000100
S8B8:10010100001100010100010011001000
F(R7K8):10001100100101000000000000011111
L7:00011001011011011110100100001111
R8:10010101111110011110100100010000

-------------------------------------------------- Round 9---------------------------------------------------
L9:10010101111110011110100100010000
E(R8):010010101011111111110011111101010010100010100001
K9:011100100110110001011110100110101101101010111010
```

```
ER8XORK9:001110001101001110101101011011111111001000011011
SBox_Out9:001110001101001110101101011011111111001000011011
S9B9:10001000010111011001110111111110
F(R8K9):10111111100110110011010001101001
L8:01111100001001101111110000111000
R9:11000011101111011100100001010001

---------------------------------------- Round 10----------------------------------------
L10:11000011101111011100100001010001
E(R9):111000000111110111111011111001010000001010100011
K10:011011001110010100000000110101010111111100110101
ER9XORK10:100011001001100011111011001100000111110110010110
SBox_Out10:100011001001100011111011001100000111110110010110
S10B10:11001111101001111011001010001110
F(R9K10):11101001111010101101000110110101
L9:10010101111110011110100100010000
R10:01111100000100110011100010100101

---------------------------------------- Round 11----------------------------------------
L11:01111100000100110011100010100101
E(R10):101111111000000010100110100111110001010100001010
K11:010000101000110100111111011101100101010111111000
ER10XORK11:111111010000110110011001001001000011111111110010
SBox_Out11:111111010000110110011001001001000011111111110010
S11B11:11011001110000010100111111000110
F(R10K11):10010000101111111110000100101011
L10:11000011101111011100100001010001
R11:01010011000000100010100101111010

---------------------------------------- Round 12----------------------------------------
L12:01010011000000100010100101111010
E(R11):001010100110100000000010000010101001010111110100
K12:111011011010000000010011111100011111101100010111
ER11XORK12:110001111100100000010111111001001101000011100011
SBox_Out12:110001111100100000010111111001001101000011100011
S12B12:01010010110111001010100100000001
F(R11K12):01010101000000011011100111000010
L11:01111100000100110011100010100101
```

```
R12:00101001000100101000000101100111

---------------------------------------- Round 13----------------------------------------
L13:00101001000100101000000101100111
E(R12):100101010010100010100101010000000010101100001110
K13:001001111000111010101010001101110010011010111110
ER12XORK13:101100101010011000001111011101110000110110110000
SBox_Out13:101100101010011000001111011101110000110110110000
S13B13:00100100101100111000011110000000
F(R12K13):10000101011000000010001100011101
L12:01010011000000100010100101111010
R13:11010110011000100000101001100111

---------------------------------------- Round 14----------------------------------------
L14:11010110011000100000101001100111
E(R13):111010101100001100000100000001010100001100001111
K14:111110100011000010010010111111010011100111000111
ER13XORK14:000100001111001110010110111110000111101011001000
SBox_Out14:000100001111001110010110111110000111101011001000
S14B14:11011110010101011110001001000110
F(R13K14):11000101101111111001000010110010
L13:00101001000100101000000101100111
R14:11101100101011010001000111010101

---------------------------------------- Round 15----------------------------------------
L15:11101100101011010001000111010101
E(R14):111101011001010101011010100010100011111010101011
K15:001111001000111001011000001001101110001011111111
ER14XORK15:110010010001101100000010101011001101110001010100
SBox_Out15:110010010001101100000010101011001101110001010100
S15B15:11001100001111011110100110010011
F(R14K15):10010111100011101011100011010101
L14:11010110011000100000101001100111
R15:01000001111011001011001010110010

---------------------------------------- Round 16----------------------------------------
L16:01000001111011001011001010110010
E(R15):001000000011111101011001010110100101010110100100
```

K16:101000010111100111010000111100100110110111001011
ER15XORK16:100000010100011010001001101010000011100001101111
SBox_Out16:100000010100011010001001101010000011100001101111
S16B16:01000010010001101101111101101101
F(R15K16):01111001011101011011110000101000
L15:11101100101011010001000111010101
R16:10010101110110001010110111111101

IP-1:
1100010100001010011001010011010101011011001011111011000101111111
Bản mã của đoạn : C50A65355B2FB17F