Lab-5
Cryptography
DES and AES
Name: Smraddhi Rathore
Roll No.: 2021bcy0025

Implementation of DES in python:

```
from math import perm



def padToX(binaryNum, X):
   while len(binaryNum) < X:
       binaryNum = '0' + binaryNum
   return binaryNum

def splitBitByN(bits, step):
   bitSplits = []
   for i in range(len(bits)//step):
       bitSplits.append(bits[(i * step):((i+1) * step)])
   return bitSplits

def makeReadable(bits, step):
   readableBit = ""
   count = 1
   for i in bits:
       if count % step == 1:
           readableBit += f' {i}'
       else:
           readableBit += i
       count += 1
   return readableBit[1:]

#main functions
def createSubkeys(originalKey):
   PC1 = [57, 49, 41, 33, 25, 17, 9,
          1, 58, 50, 42, 34, 26, 18,
          10, 2, 59, 51, 43, 35, 27,
          19, 11, 3, 60, 52, 44, 36,
          63, 55, 47, 39, 31, 23, 15,
          7, 62, 54, 46, 38, 30, 22,
          14, 6, 61, 53, 45, 37, 29,
          21, 13, 5, 28, 20, 12, 4]

   perm56 = ""
   for i in range(len(PC1)):
```

```
        perm56 += originalKey[PC1[i]-1]

    currentC = perm56[:28]
    currentD = perm56[28:]
    concatenatedPairs = []
    numOfLeftShifts = [1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1]

    for i in numOfLeftShifts:
        currentC = currentC[i:] + currentC[:i]
        currentD = currentD[i:] + currentD[:i]
        concatenatedPairs.append(currentC + currentD)

    PC2 =[14,  17,  11,  24,  1,  5,
          3,  28,  15,  6,  21,  10,
          23,  19,  12,  4,  26,  8,
          16,   7,  27,  20,  13,  2,
          41,  52,  31,  37,  47,  55,
          30,  40,  51,  45,  33,  48,
          44,  49,  39,  56,  34,  53,
          46,  42,  50,  36,  29,  32]

    keys = []
    for currentCandD in concatenatedPairs:
        perm48 = ""
        for i in range(len(PC2)):
            perm48 += currentCandD[PC2[i]-1]
        keys.append(perm48)

    return keys

def SBoxes(bitSplit, Snum):

    bitsShrink6To4 = []
    S1 = [[14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7],
          [0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8],
          [4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0],
          [15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13]]

    S2 = [[15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10],
          [3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5],
          [0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15],
          [13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9]]

    S3 = [[10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8],
          [13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1],
```

```
        [13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7],
        [1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12]]

S4 = [[7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15],
        [13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9],
        [10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4],
        [3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14]]

S5 = [[2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9],
        [14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6],
        [4, 2, 1, 11, 10, 13, 7, 8, 15, 9, 12, 5, 6, 3, 0, 14],
        [11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9, 10, 4, 5, 3]]

S6 = [[12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11],
        [10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8],
        [9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6],
        [4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13]]

S7 = [[4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1],
        [13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6],
        [1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2],
        [6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12]]

S8 = [[13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7],
        [1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2],
        [7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8],
        [2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11]]

SMap = {1 : S1,
    2: S2,
    3: S3,
    4: S4,
    5: S5,
    6: S6,
    7: S7,
    8: S8
    }

S = SMap[Snum]

row = int((bitSplit[0] + bitSplit[5]), 2)
column = int(bitSplit[1:5], 2)

return padToX(bin(S[row][column])[2:], 4)
```

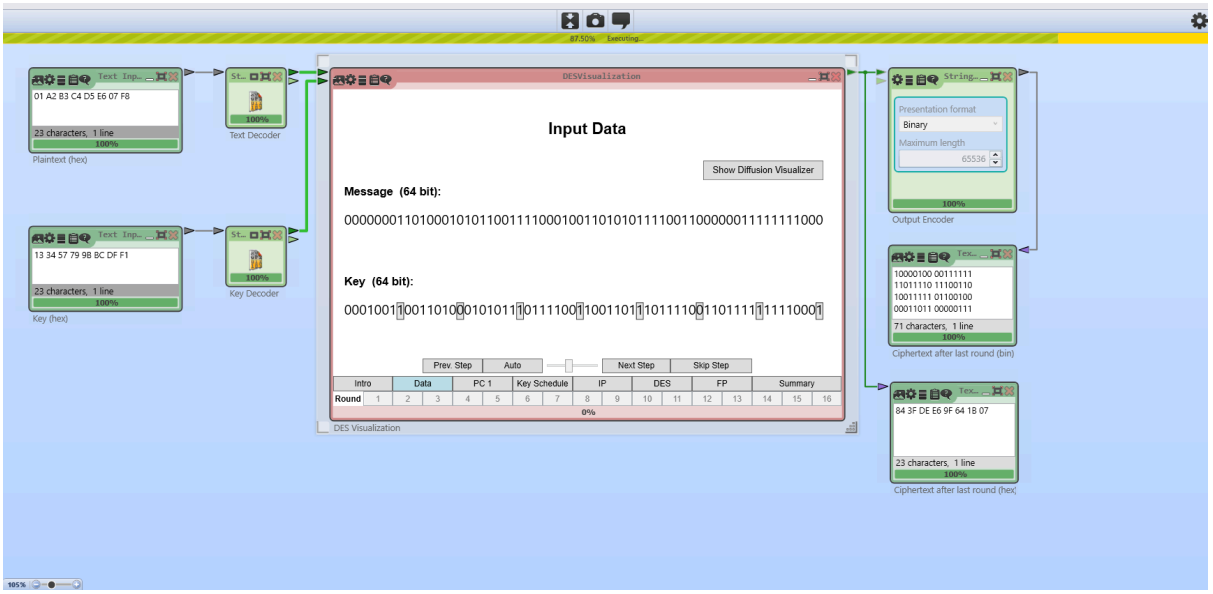
```
def XORBinaryStrings(string1, string2):

    if (len(string1) != len(string2)):
        raise "Strings must be of equal length to XOR"
    xorOutput = ""
    xorMap = {
    ('0', '0'): '0', ('0', '1'): '1', ('1', '0'): '1', ('1', '1'): '0'
    }
    for bit in range(len(string1)):
        xorOutput += xorMap[(f'{string1[bit]}', f'{string2[bit]}')]
    return xorOutput

def fFunction(right, keyN):

    expansionTable = [32, 1, 2, 3, 4, 5,
                      4, 5, 6, 7, 8, 9,
                      8, 9, 10, 11, 12, 13,
                      12, 13, 14, 15, 16, 17,
                      16, 17, 18, 19, 20, 21,
                      20, 21, 22, 23, 24, 25,
                      24, 25, 26, 27, 28, 29,
                      28, 29, 30, 31, 32, 1]
    expansionOfRight = ""
    for i in range(len(expansionTable)):
        expansionOfRight += right[expansionTable[i]-1]

    xorMap = {
        ('0', '0'): '0', ('0', '1'): '1', ('1', '0'): '1', ('1', '1'): '0'
        }
    XORExpansionAndKey = ""
    for bit in range(len(keyN)):

        XORExpansionAndKey += xorMap[(f'{keyN[bit]}', f'{expansionOfRight[bit]}')]

    bitSplits = splitBitByN(XORExpansionAndKey, 6)


    shrink48to32 = ""
    for i in range(len(bitSplits)):
        shrink48to32 += SBoxes(bitSplits[i], i+1)

    P = [16, 7, 20, 21,
        29, 12, 28, 17,
         1, 15, 23, 26,
         5, 18, 31, 10,
```

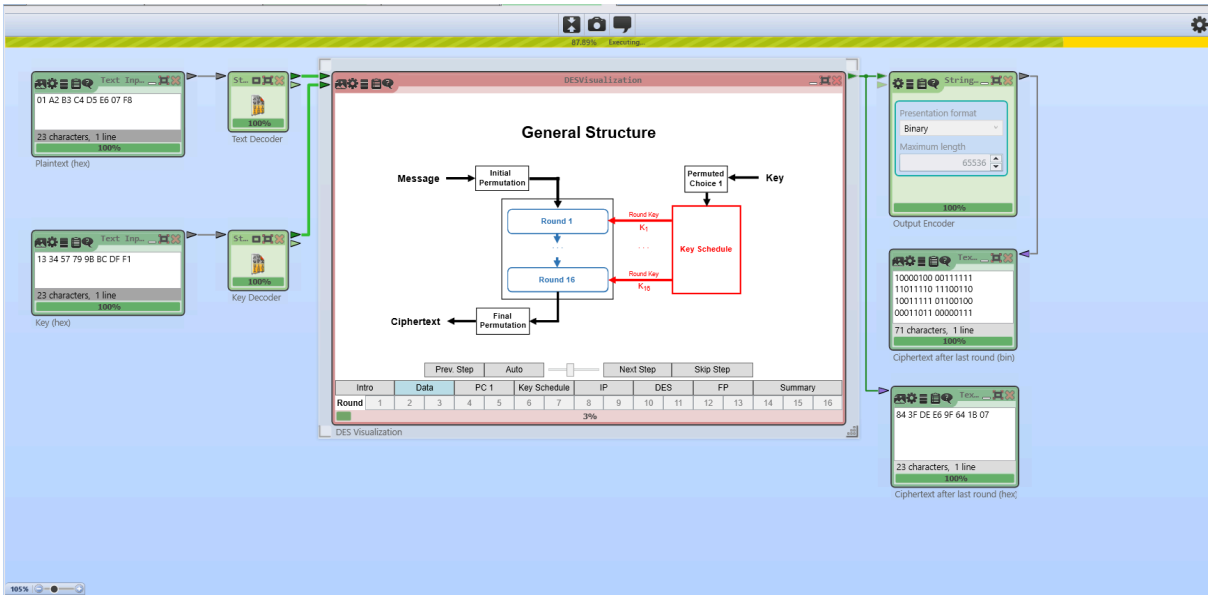
```
         2, 8, 24, 14,
         32, 27, 3, 9,
        19, 13, 30, 6,
        22, 11, 4, 25]

    permutatedSBoxes = ""
    for i in range((len(P))):
        permutatedSBoxes += shrink48to32[P[i]-1]

    return permutatedSBoxes

def encodeData(plainText, key):

    plainText = padToX(bin(int(plainText, 16))[2:], 64)
    key = padToX(bin(int(key, 16))[2:], 64)
    keys = createSubkeys(key)
    #Initial Permutation
    mPermutated = ""
    IP = [58, 50, 42, 34, 26, 18, 10, 2,
          60, 52, 44, 36, 28, 20, 12, 4,
          62, 54, 46, 38, 30, 22, 14, 6,
          64, 56, 48, 40, 32, 24, 16, 8,
          57, 49, 41, 33, 25, 17,  9, 1,
          59, 51, 43, 35, 27, 19, 11, 3,
          61, 53, 45, 37, 29, 21, 13, 5,
          63, 55, 47, 39, 31, 23, 15, 7]
    for i in range(len(IP)):
        mPermutated += plainText[IP[i]-1]

    left = mPermutated[:32]
    right = mPermutated[32:]

    for i in range(16):
        rightBefore = right
        leftBefore = left
        right = XORBinaryStrings(leftBefore, fFunction(rightBefore, keys[i]))
        left = rightBefore
    R16permL16 = right + left

    IPInverse = [40, 8, 48, 16, 56, 24, 64, 32,
                 39, 7, 47, 15, 55, 23, 63, 31,
                 38, 6, 46, 14, 54, 22, 62, 30,
                 37, 5, 45, 13, 53, 21, 61, 29,
                 36, 4, 44, 12, 52, 20, 60, 28,
                 35, 3, 43, 11, 51, 19, 59, 27,
```

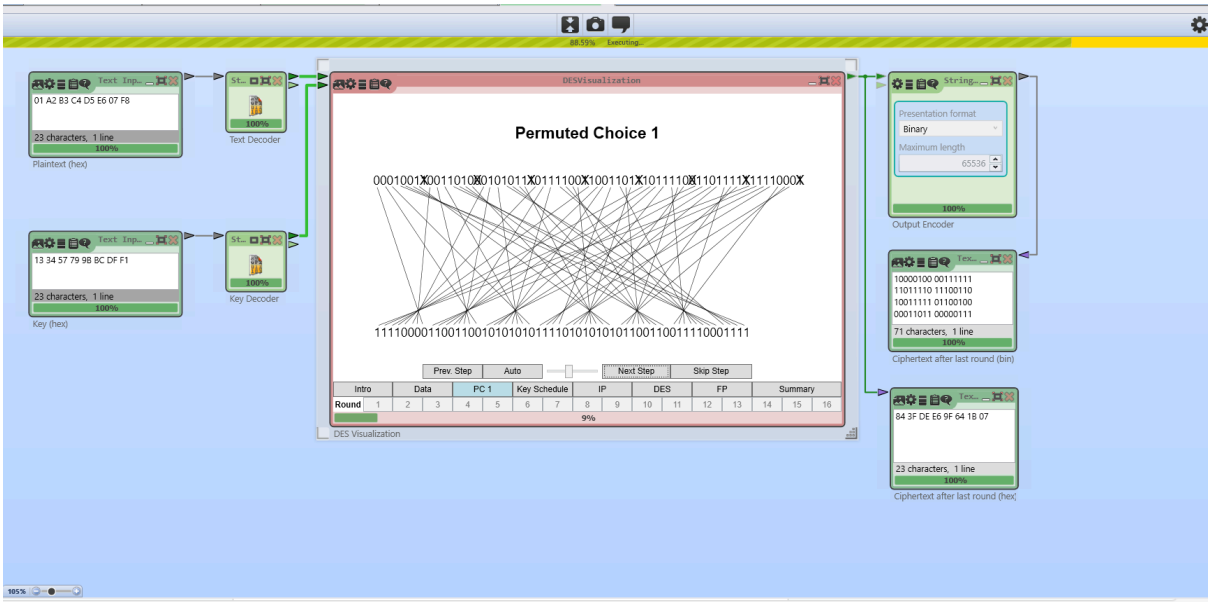
```
                34, 2, 42, 10, 50, 18, 58, 26,
                33, 1, 41,  9, 49, 17, 57, 25]
    finalPermutation = ""
    for i in range(len(IPInverse)):
        finalPermutation += R16permL16[IPInverse[i]-1]

    return hex(int(finalPermutation, 2))


def main():

    plainText = input("Enter a hexadecimal plain text message: ")
    key = input("Enter a hexadecimal key: ")
    print("Encrypted output using DES Encryption:", encodeData(plainText, key))

if __name__ == "__main__":
    main()
```

```
smraddhi@smraddhis-MacBook-Air Cryptography % python -u "/Users/smraddhi/Documents/Cryptography/Des2.py"
Enter a hexadecimal plain text message: 123456ABCD132536
Enter a hexadecimal key: AABB09182736CCDD
Encrypted output using DES Encryption: 0xc0b7a8d05f3a829c
```

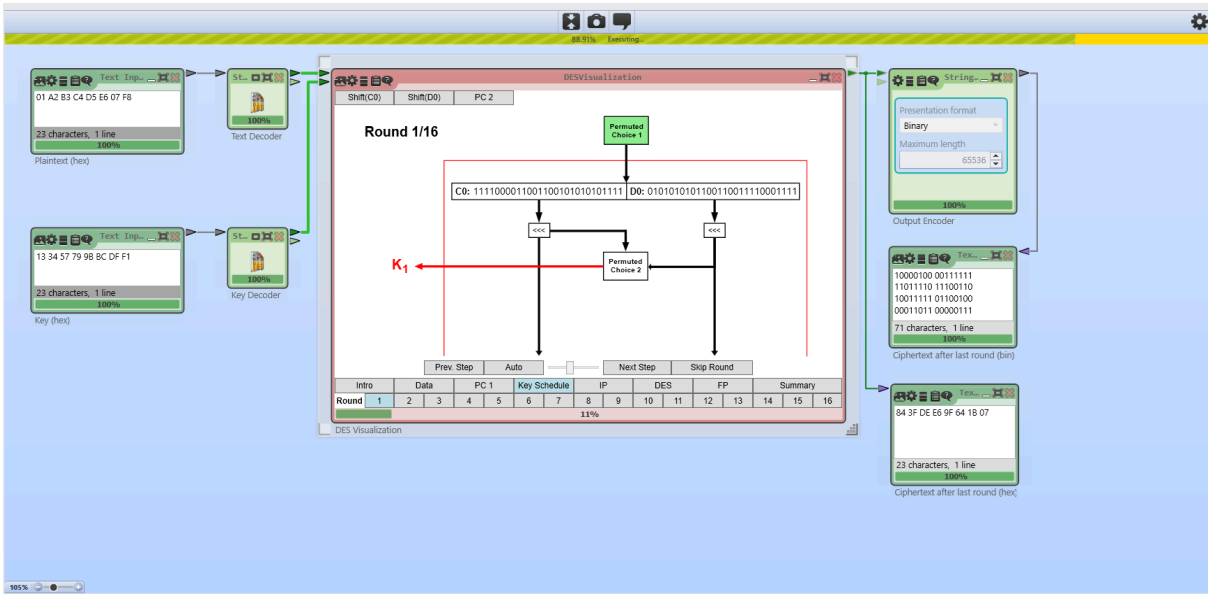
Visualisation of des:

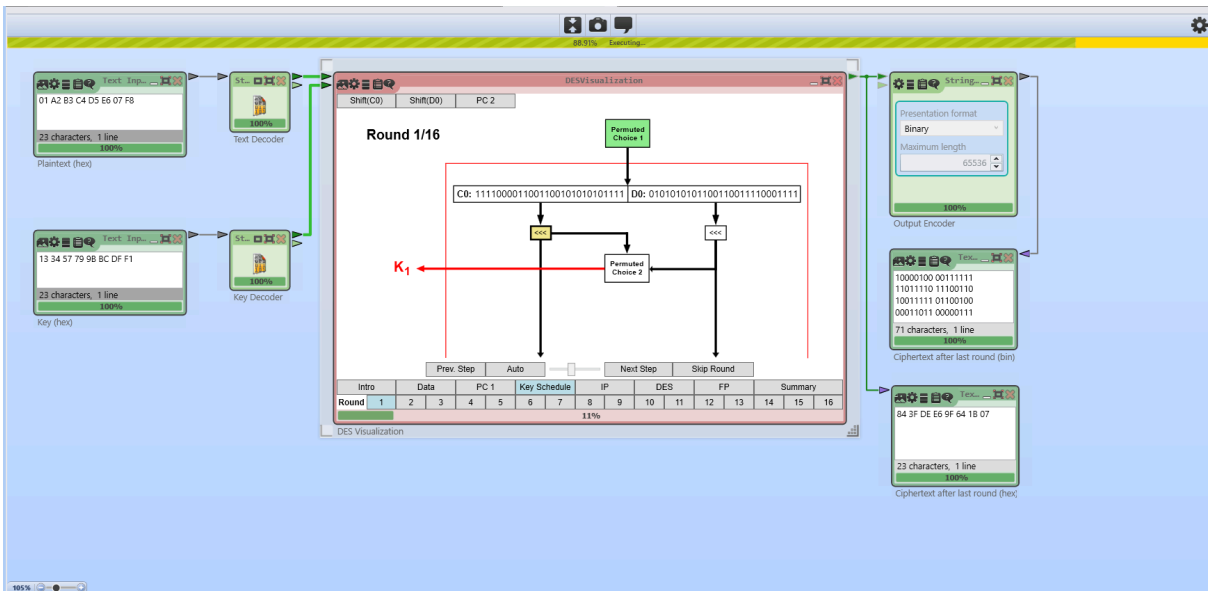


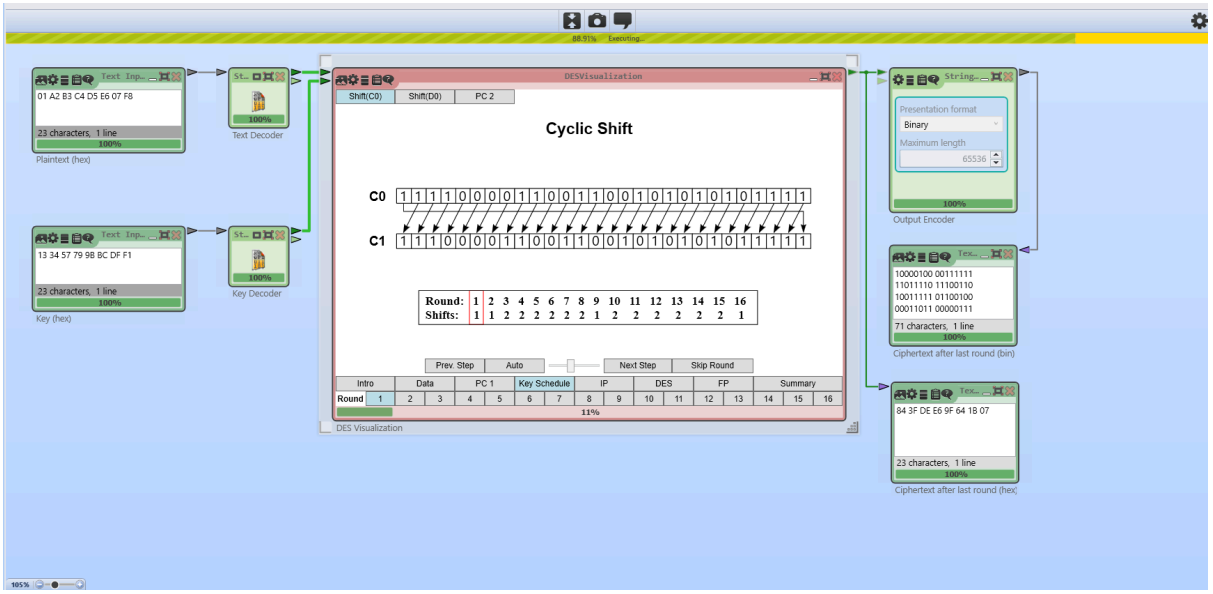

DESVisualization
General Structure
Message
Initial Permutation
Permuted Choice 1
Key
Round 1
Round 16
Round Key
Key Schedule
Ciphertext
Final Permutation
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
DES Visualization
01 A2 B3 C4 D5 E6 07 F8
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
Key (hex)
Key Decoder
Output Encoder
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
Ciphertext after last round (hex)

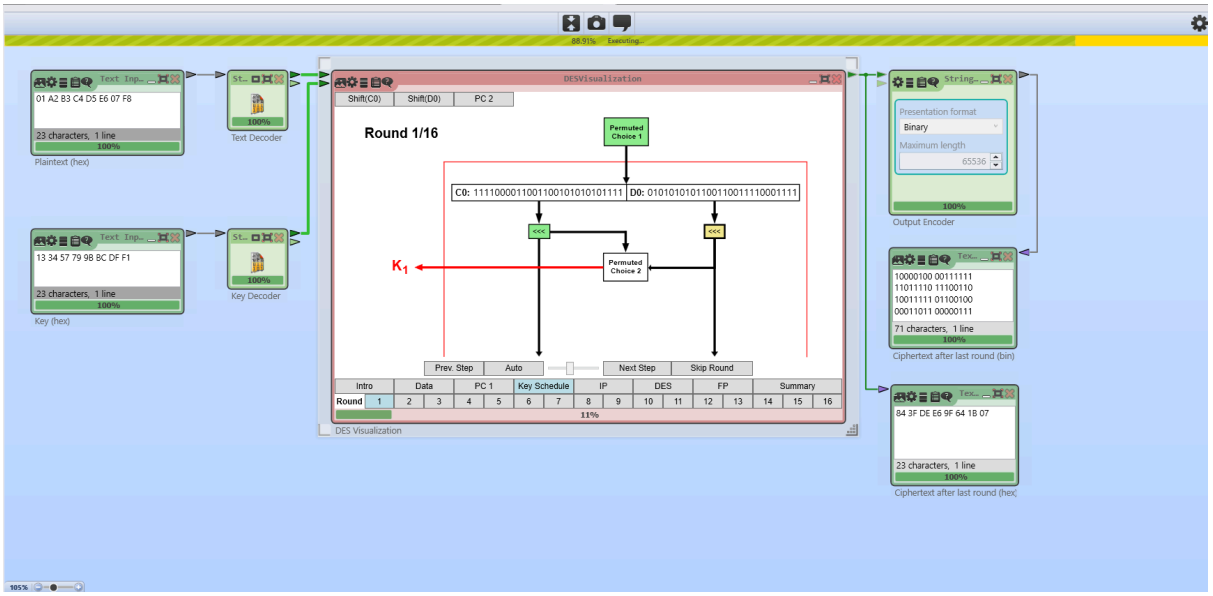

DESVisualization
Permuted Choice 1
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
DES Visualization
01 A2 B3 C4 D5 E6 07 F8
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
Key (hex)
Key Decoder
Output Encoder
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
Ciphertext after last round (hex)

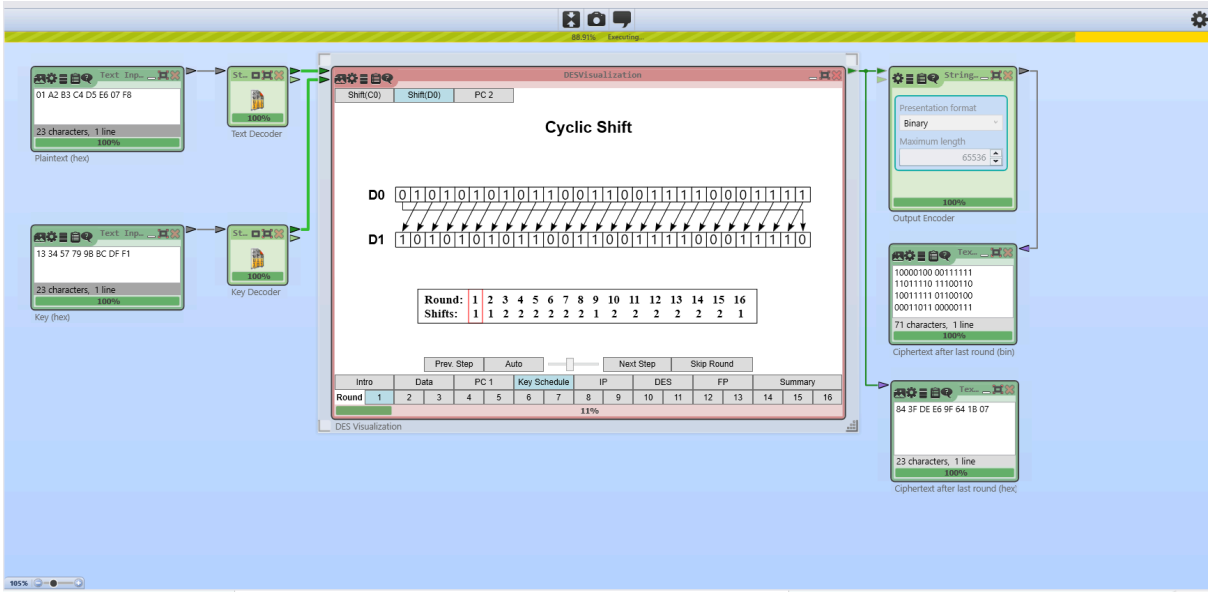
Round 1:

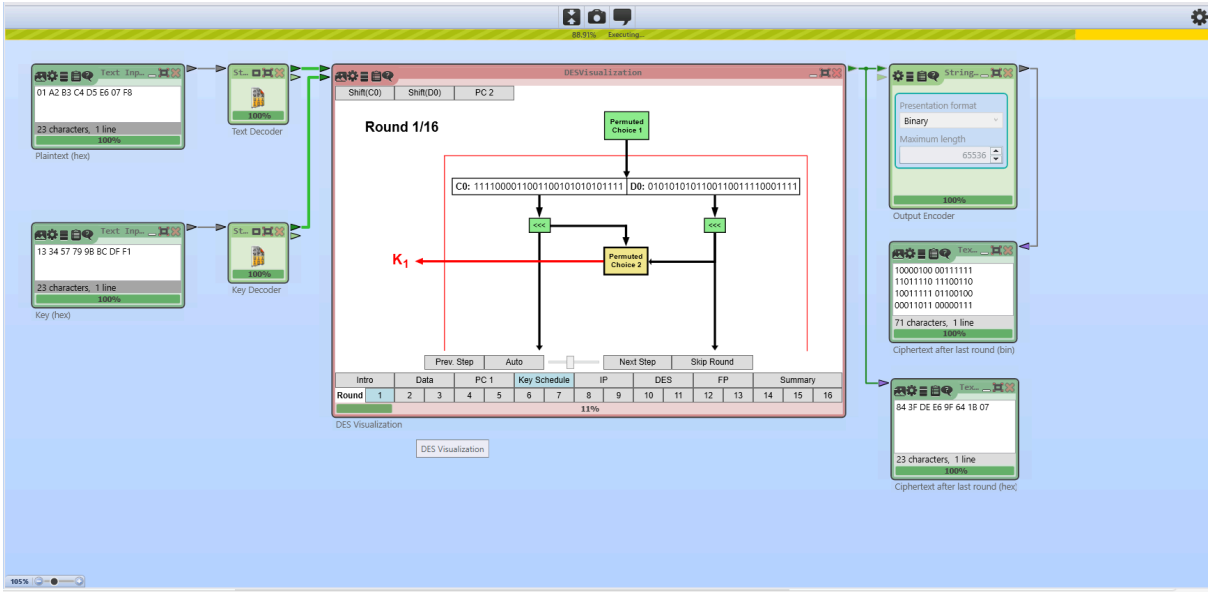

DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round 1/16
Permuted Choice 1
C0: 1111000011001100101010101111
D0: 0101010101100110011110001111
Permuted Choice 2
K1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
DES Visualization
01 A2 B3 C4 D5 E6 07 F8
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
Key (hex)
Key Decoder
Output Encoder
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
Ciphertext after last round (hex)

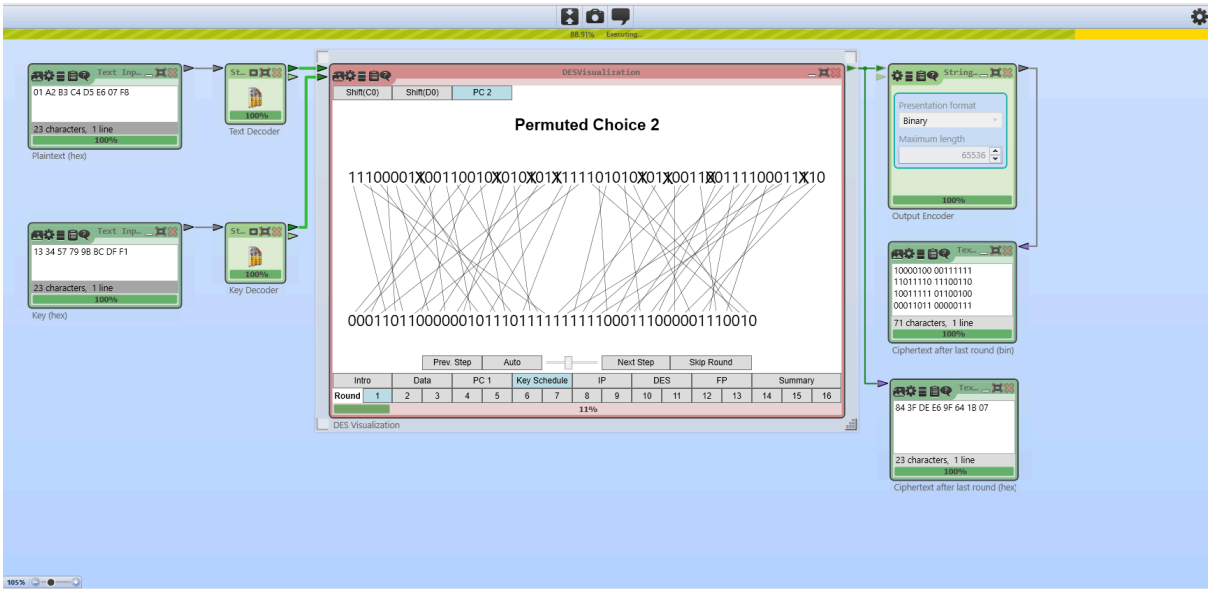

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round 1/16
Permuted Choice 1
C0: 1111000011001100101010101111
D0: 0101010101100110011110001111
<<<
<<<
K1
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

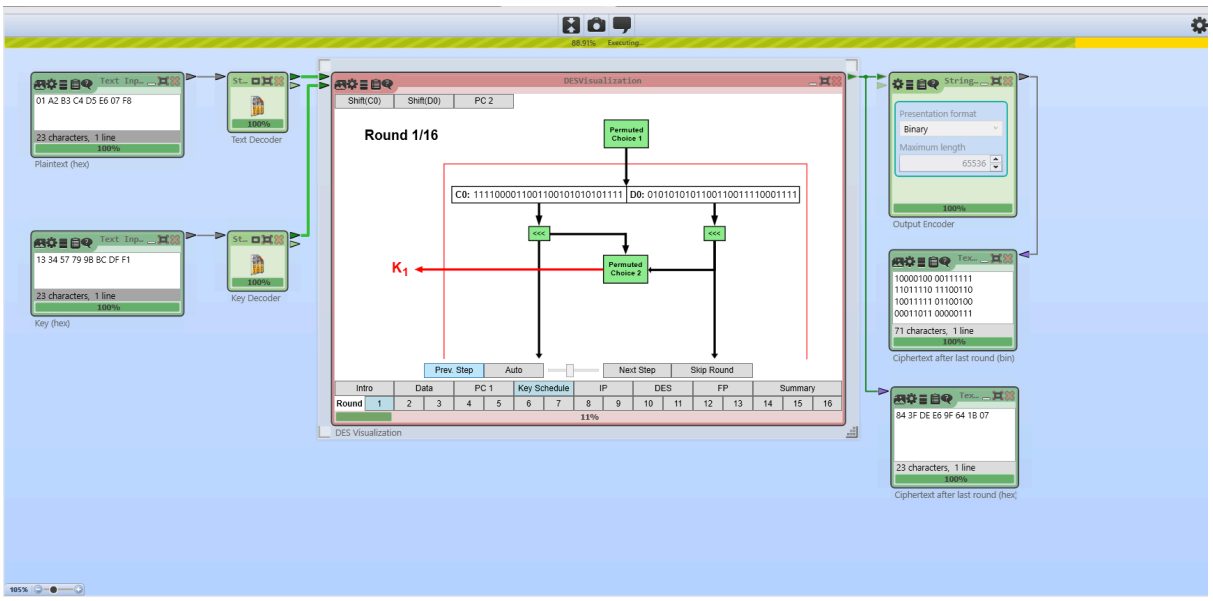

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Cyclic Shift
C0 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1
C1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

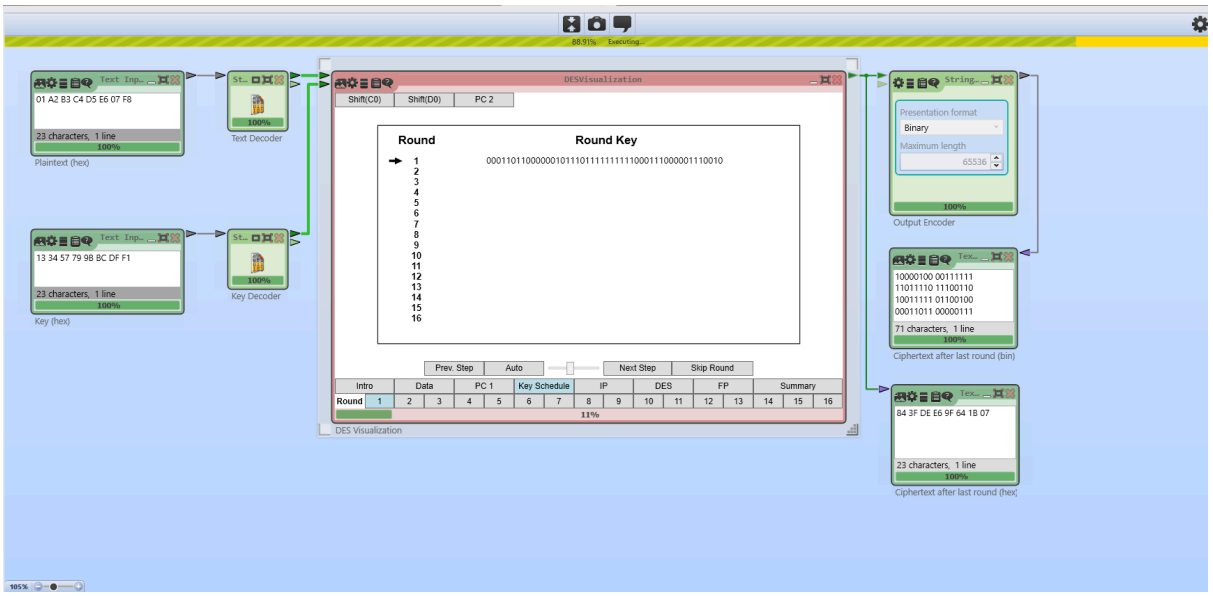

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round 1/16
Permuted Choice 1
C0: 1111000011001100101010101111
D0: 0101010101100110011110001111
<<<
<<<
K1
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Cyclic Shift
D0 0 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 1 0 0 0 1 1 1 1
D1 1 0 1 0 1 0 1 0 1 1 0 0 1 1 1 0 0 1 1 1 1 1 0 0 0 1 1 1 1 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

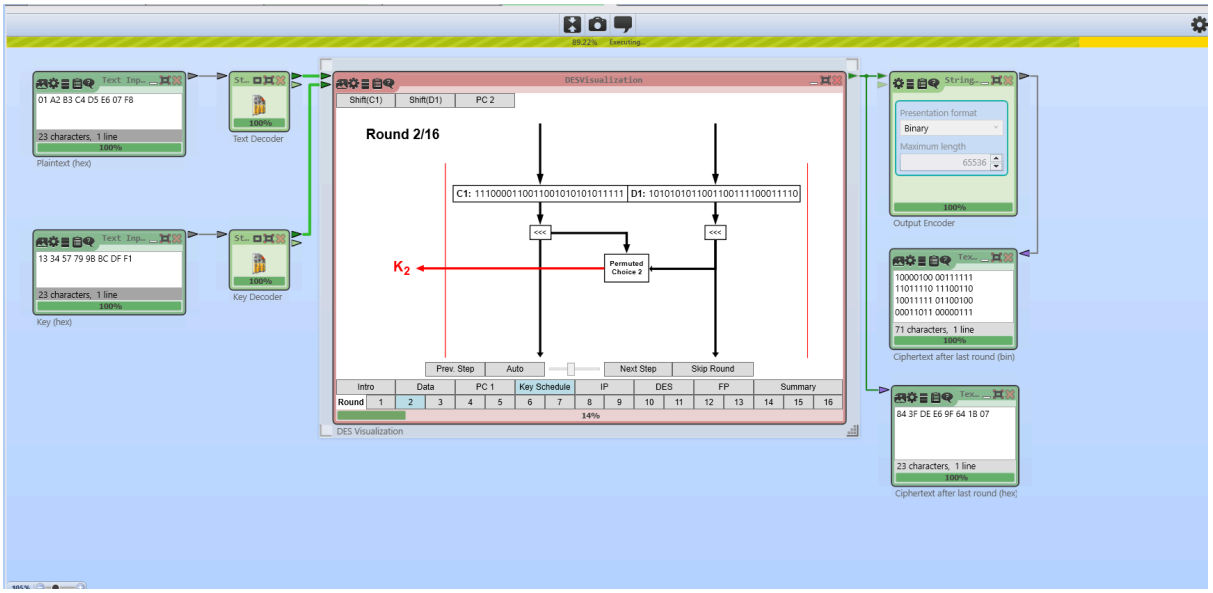

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round 1/16
Permuted Choice 1
C0: 1111000011001100101010101111
D0: 0101010101100110011110001111
<<<
<<<
K1
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

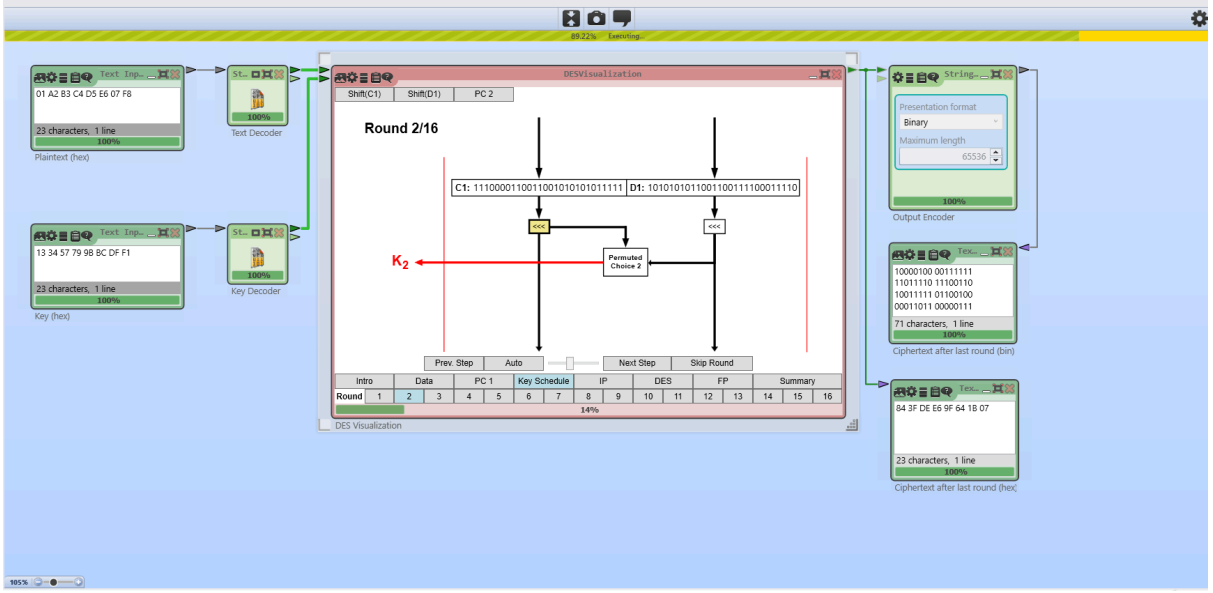

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Permuted Choice 2
11100001X00110010X010X01X1111010101X01X0011X0111100011X10
0001101100000010111011111111110001110000011100 10
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

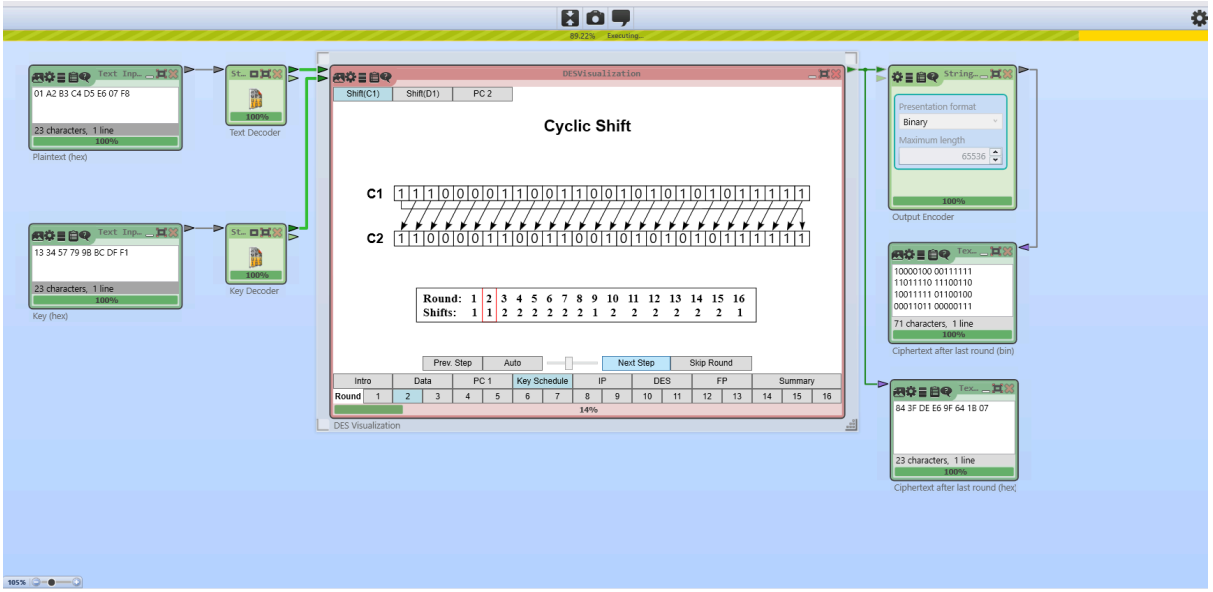

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round 1/16
Permuted Choice 1
C0: 1111000011001100101010101111
D0: 0101010101100110011110001111
<<<
<<<
K1
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

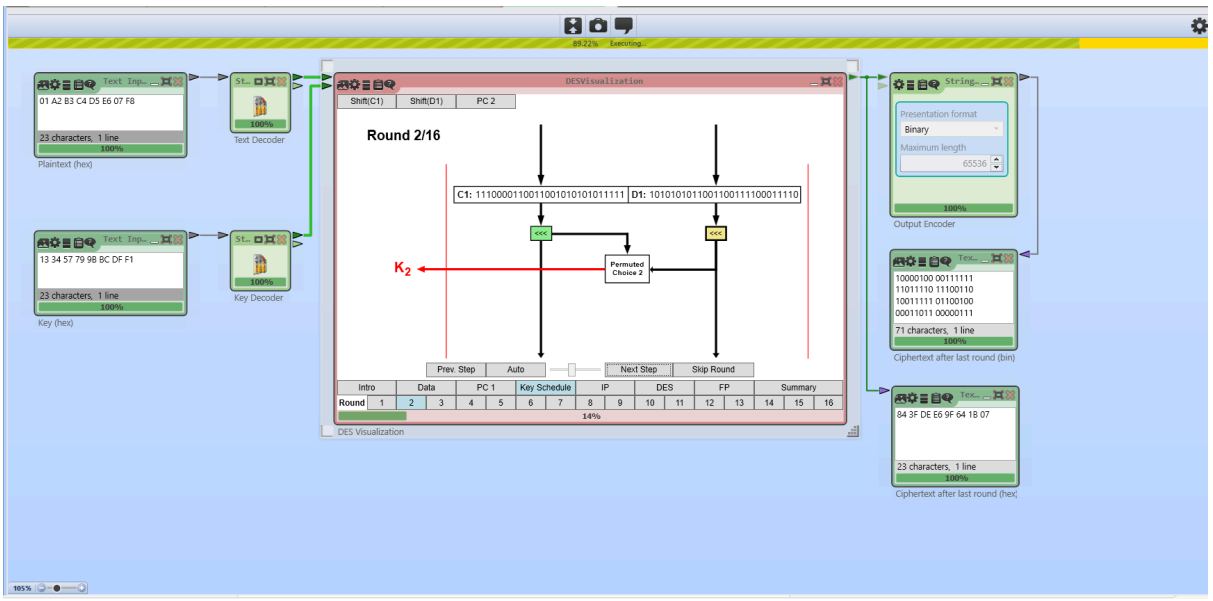

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C0)
Shift(D0)
PC 2
Round
Round Key
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
0001101100000010110111111111100011100000111 0010
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
11%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

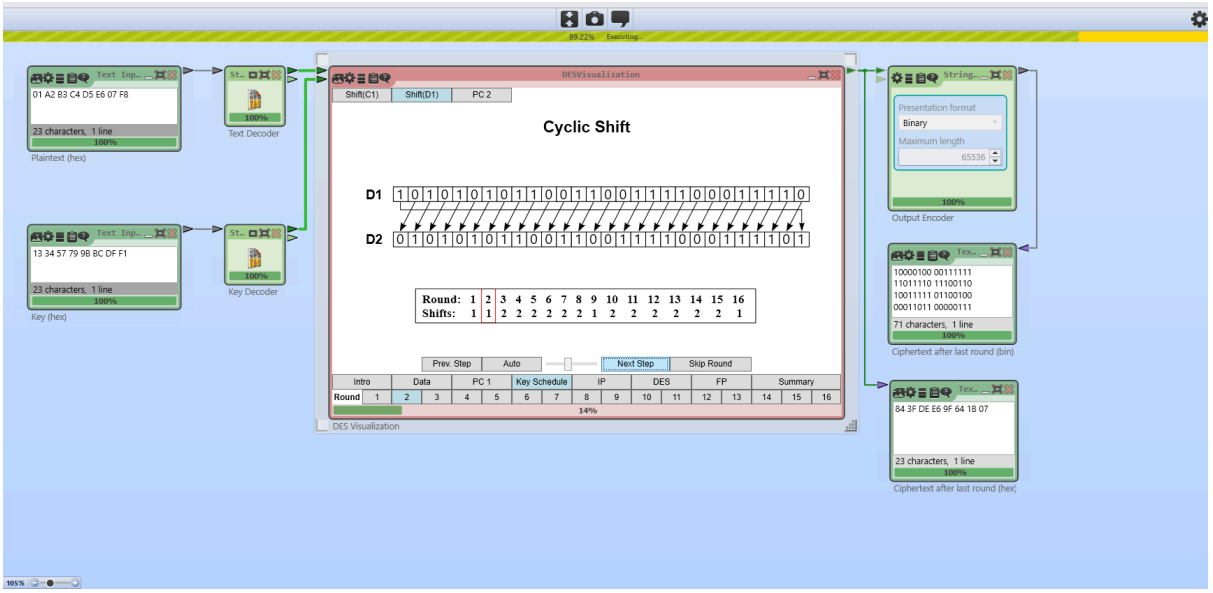
Round 2:

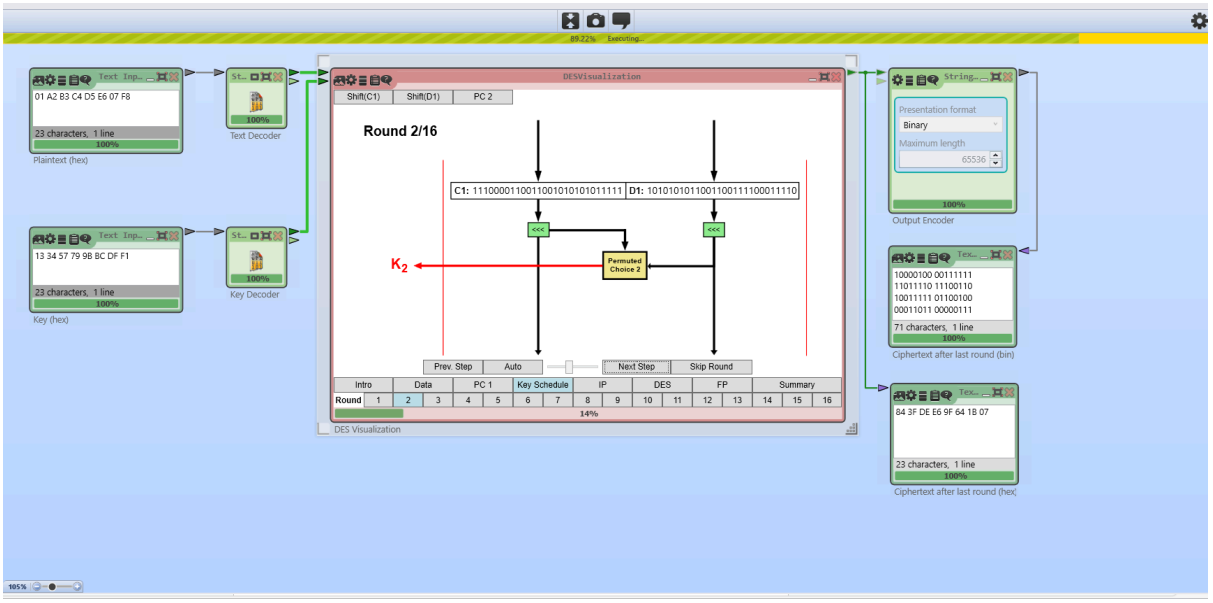

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Round 2/16
C1: 1110000110011001010101011111
D1: 1010101011001100111100011110
<<<
<<<
K2
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

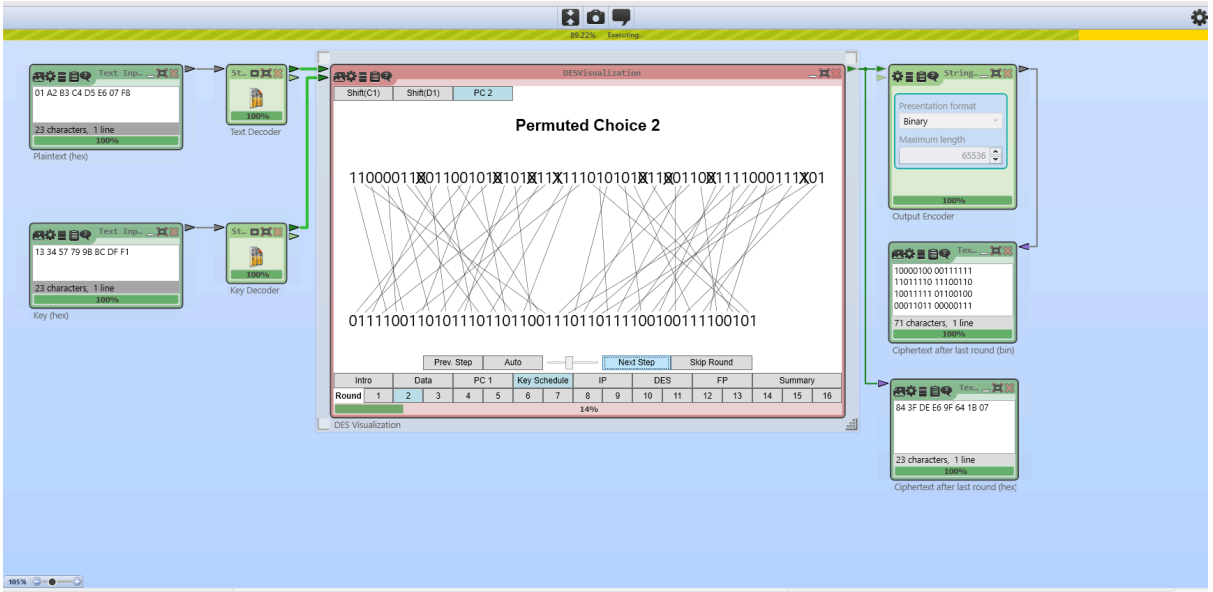

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Round 2/16
C1: 1110000110011001010101011111
D1: 1010101011001100111100011110
<<<
<<<
K2
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

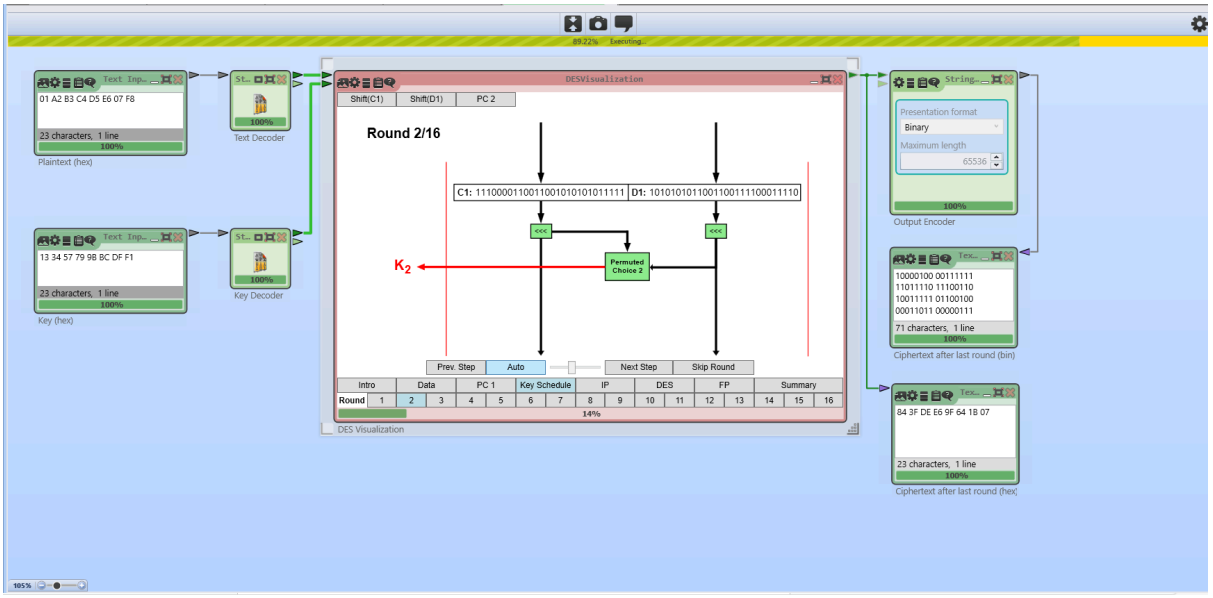

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Cyclic Shift
C1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1
C2 1 1 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

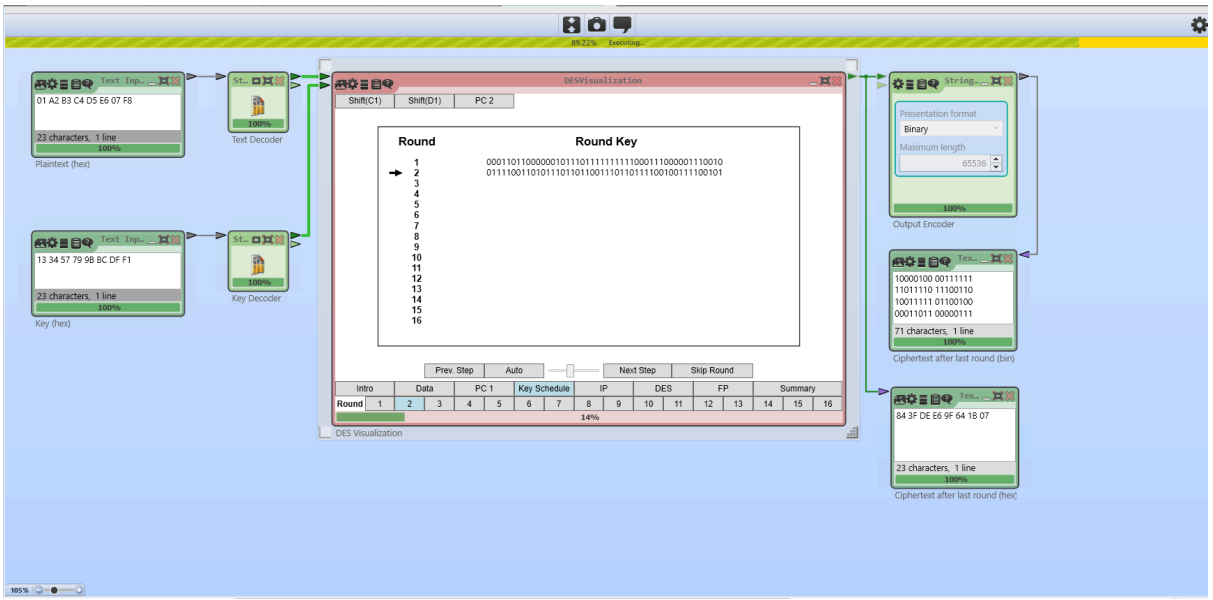

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Round 2/16
C1: 1110000110011001010101011111
D1: 1010101011001100111100011110
<<<
<<<
Permuted Choice 2
K2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Cyclic Shift
D1
1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0
D2
0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

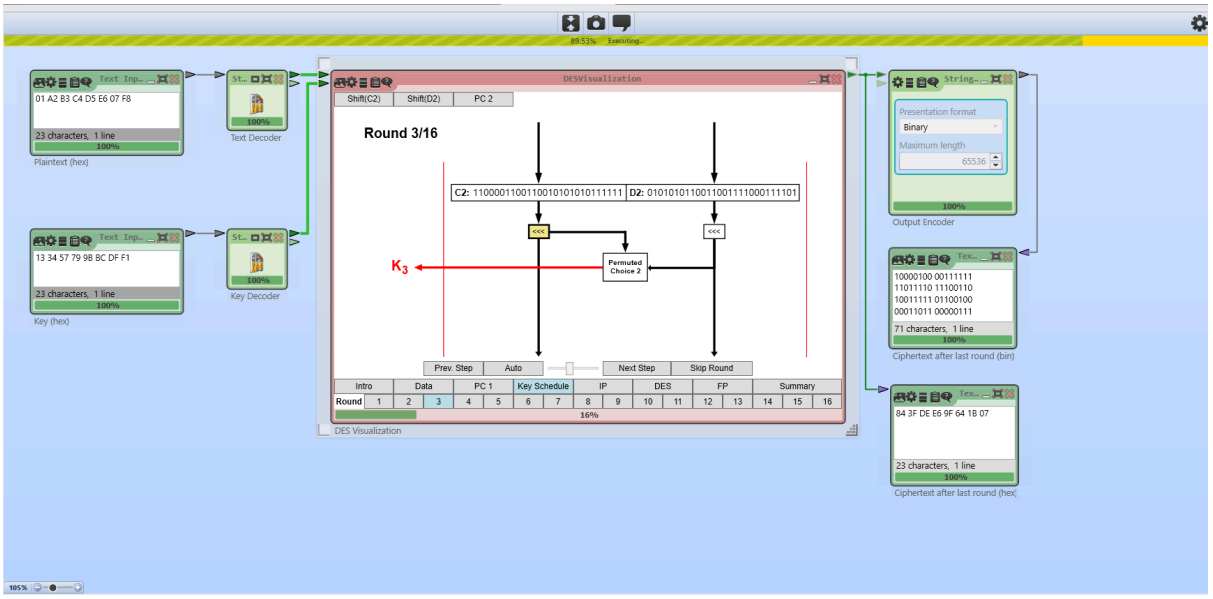

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Round 2/16
C1: 1110000110011001010101011111
D1: 1010101011001100111100011110
<<<
<<<
Permuted Choice 2
K2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
14%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

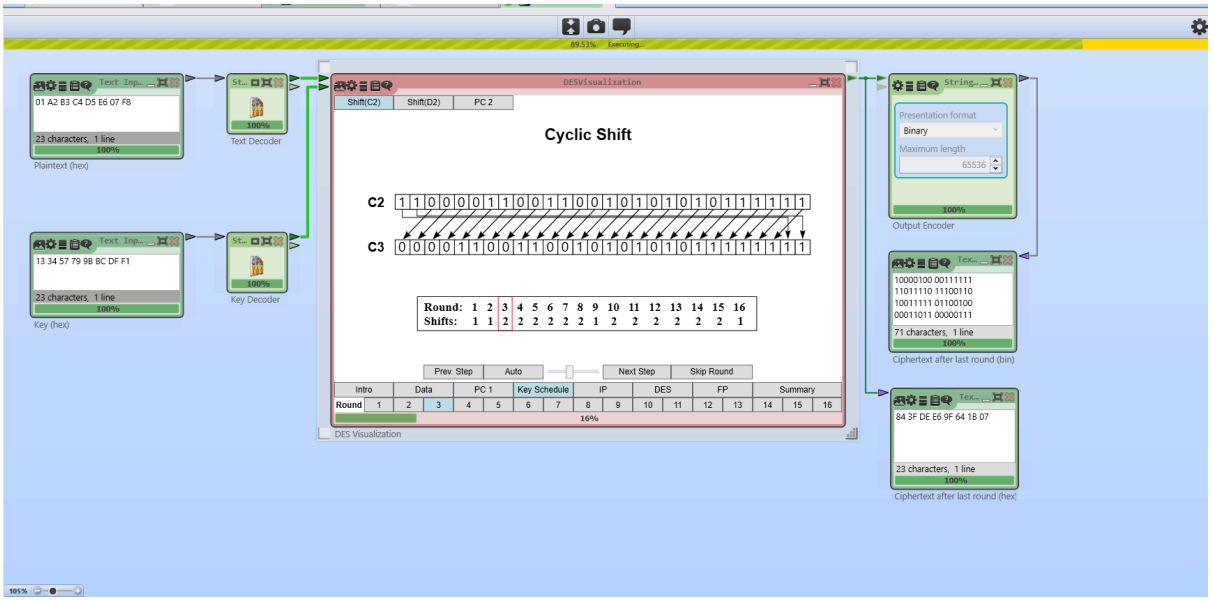

01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C1)
Shift(D1)
PC 2
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
14%
DES Visualization
Output Encoder
Ciphertext after last round (bin)
71 characters, 1 line
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

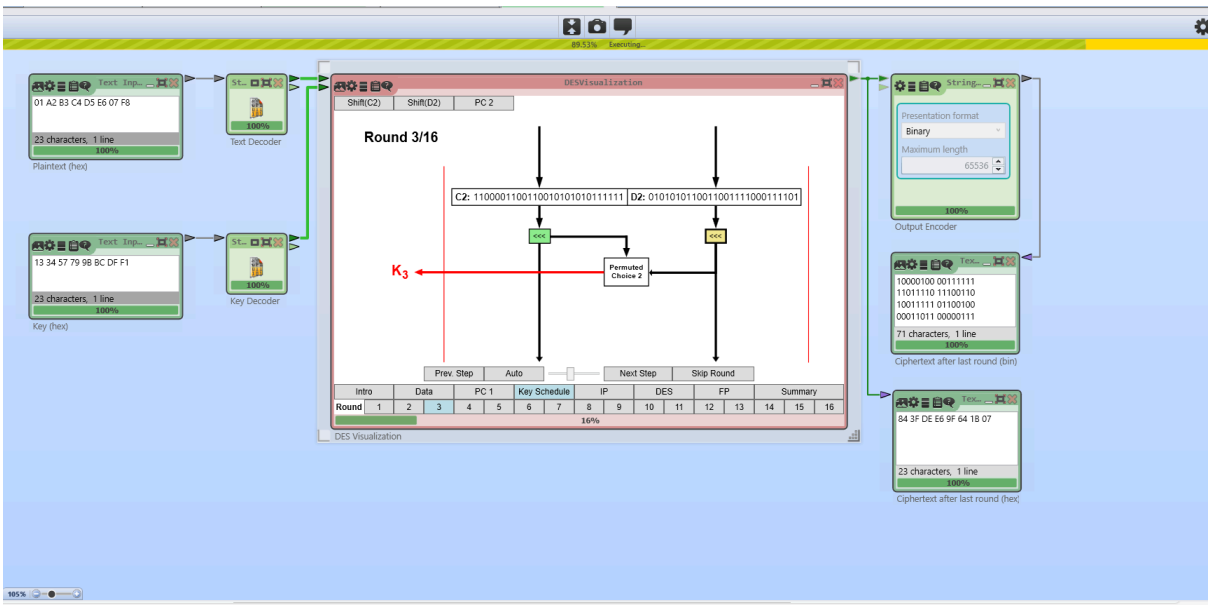

Round 2/16
C1: 1110000110011001010101011111
D1: 1010101011001100111100011110
<<<
Permuted Choice 2
K2
Prev. Step
Auto
Next Step
Skip Round
14%
DES Visualization

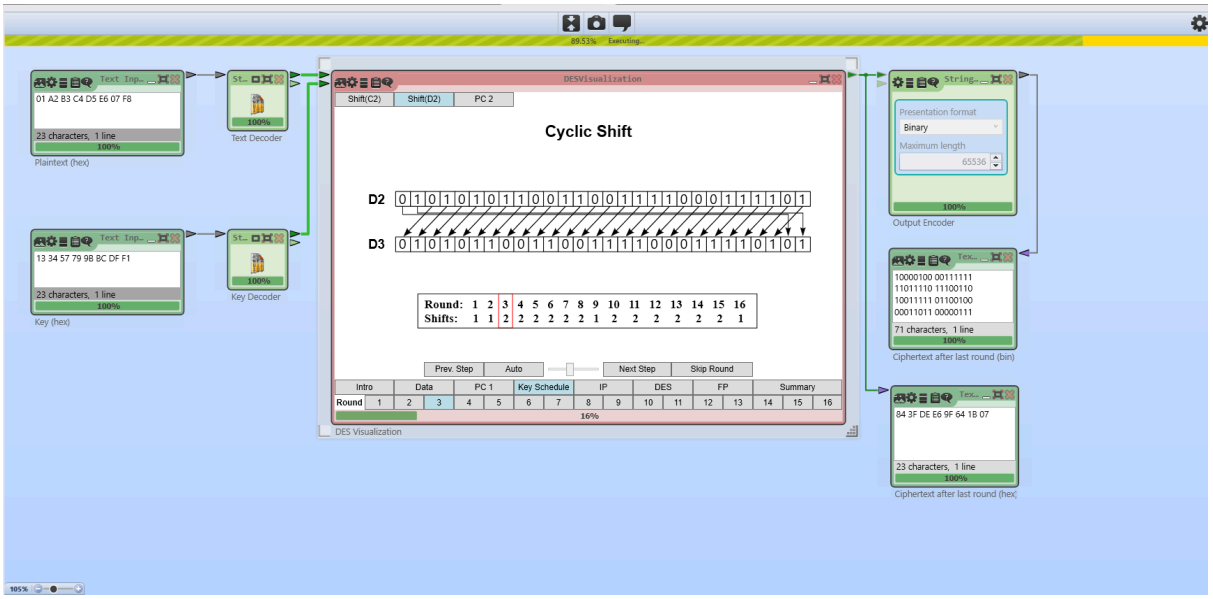

Round
Round Key
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
14%
DES Visualization

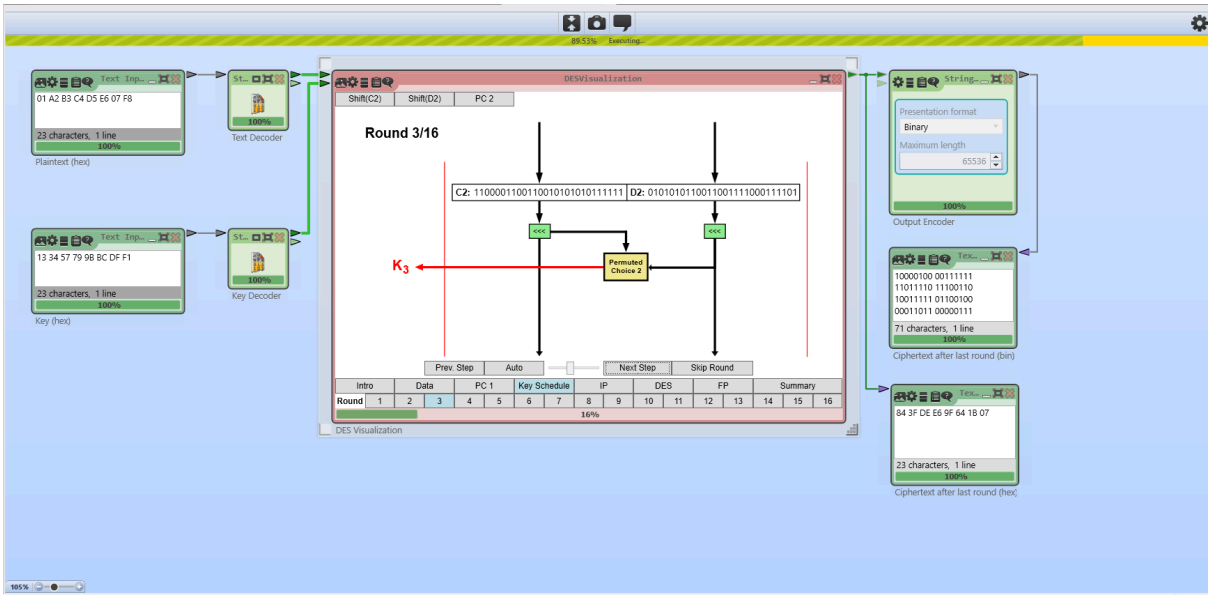
Round 3:

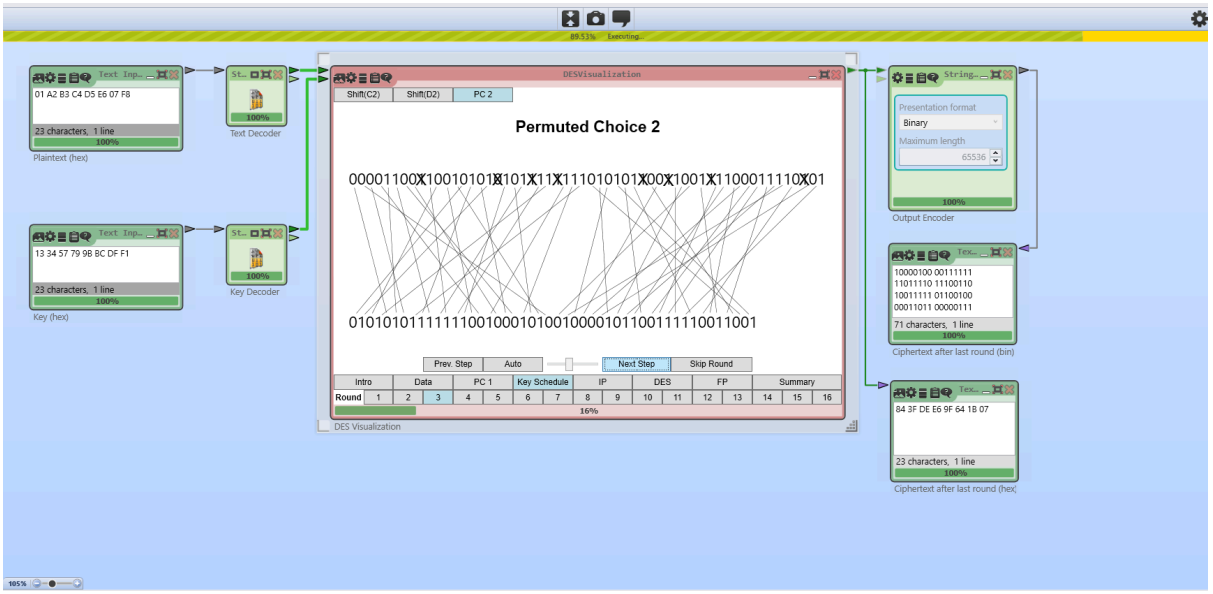

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Round 3/16
C2: 1100001100110010101010111111
D2: 0101010110011001111000111101
<<<
<<<
K3
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

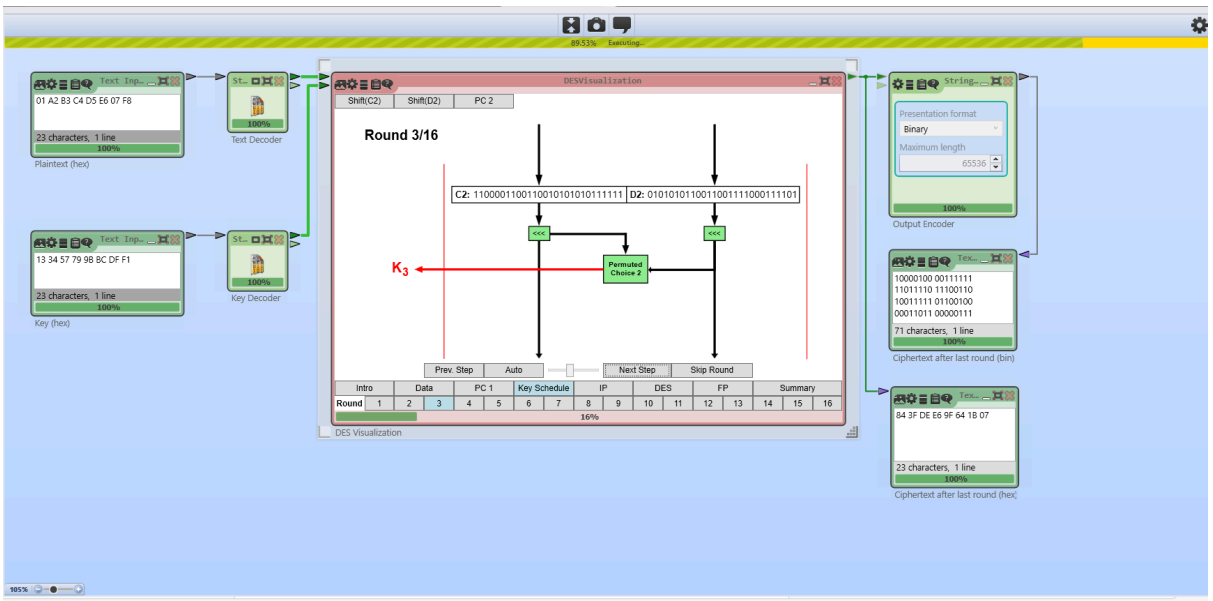

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Cyclic Shift
C2 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1
C3 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

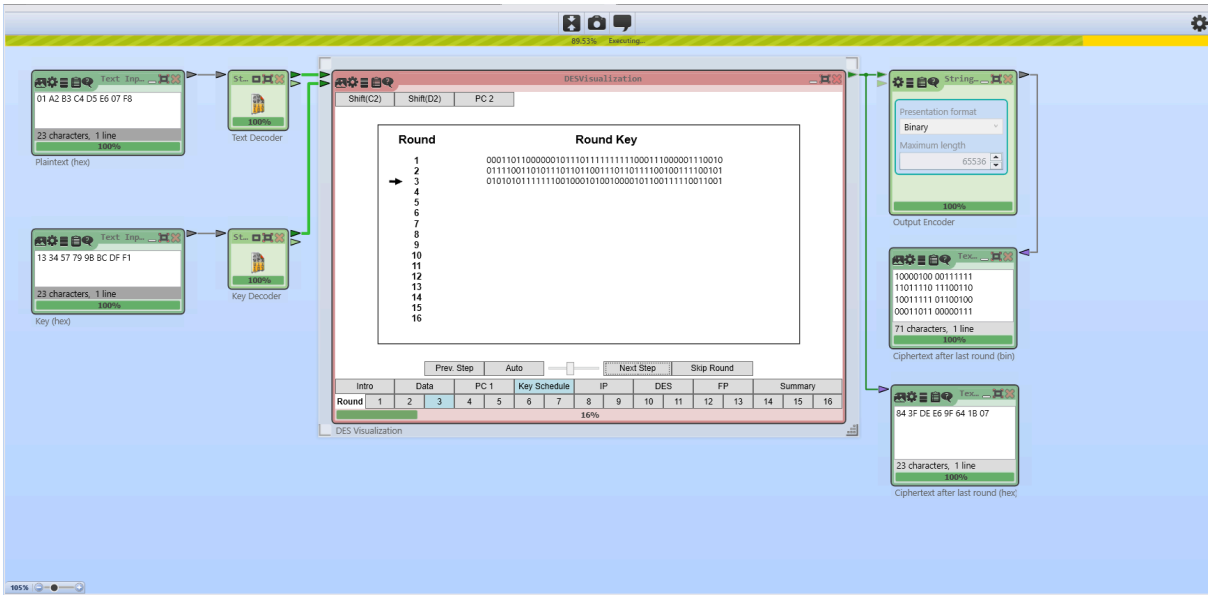

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Round 3/16
C2: 1100001100110010101010111111
D2: 0101010110011001111000111101
<<<
<<<
K3
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Cyclic Shift
D2 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1
D3 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

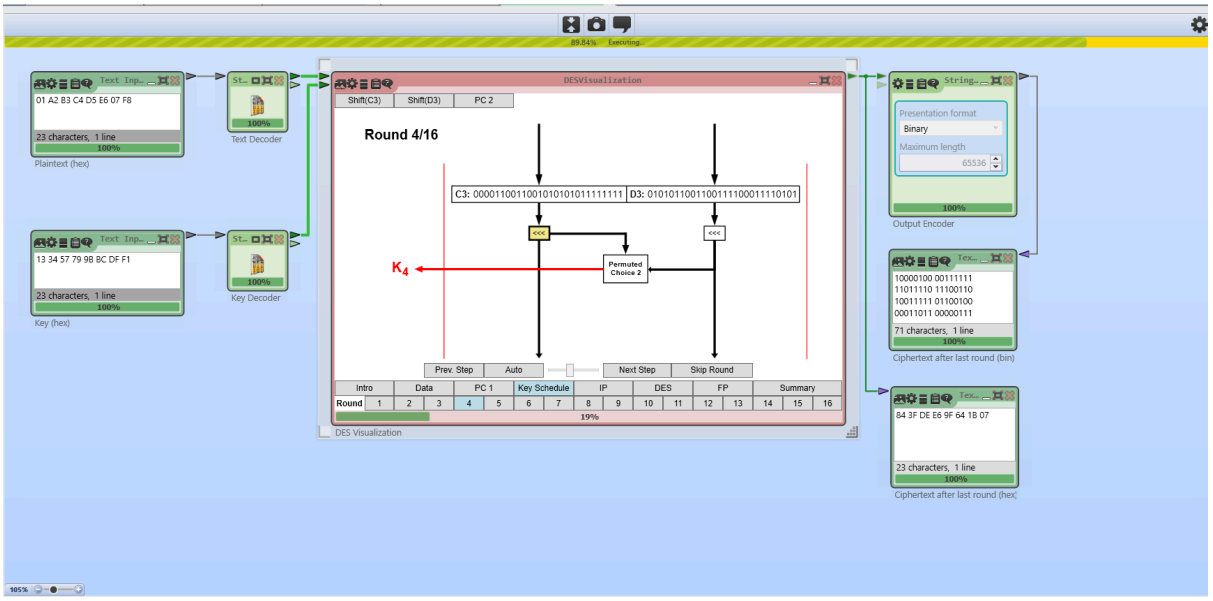

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Round 3/16
C2: 1100001100110010101010111111
D2: 0101010110011001111000111101
<<<
<<<
K3
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

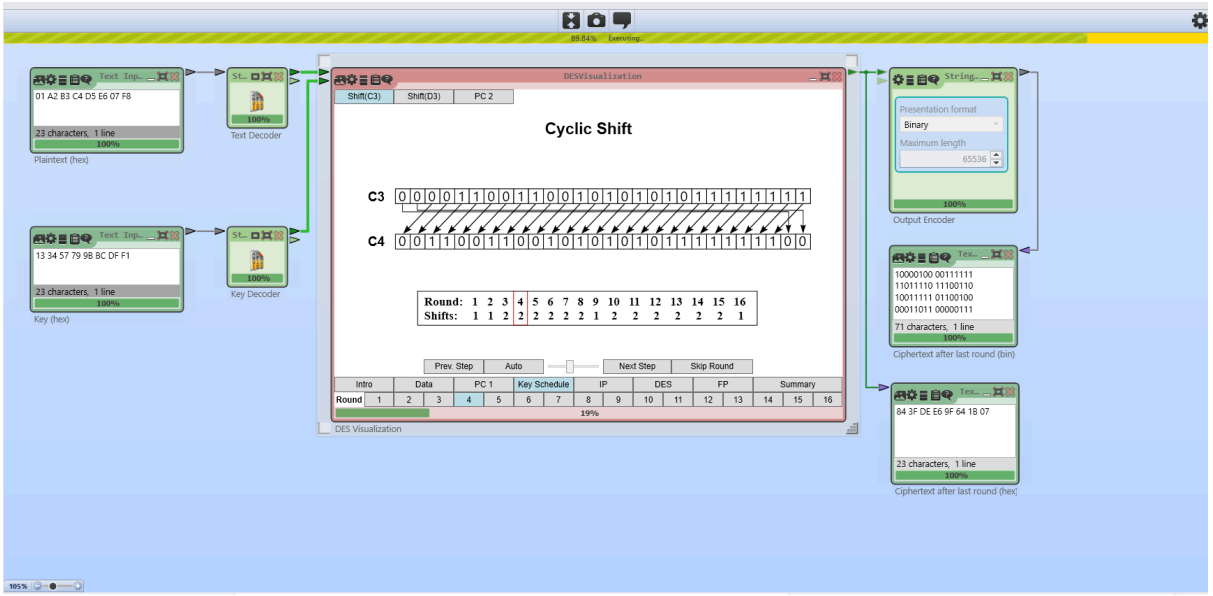

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Permuted Choice 2
00001100X10010101X101X11X111010101X00X1001X1100011110X01
0101010111111100100010100100001011001111100 11001
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
16%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

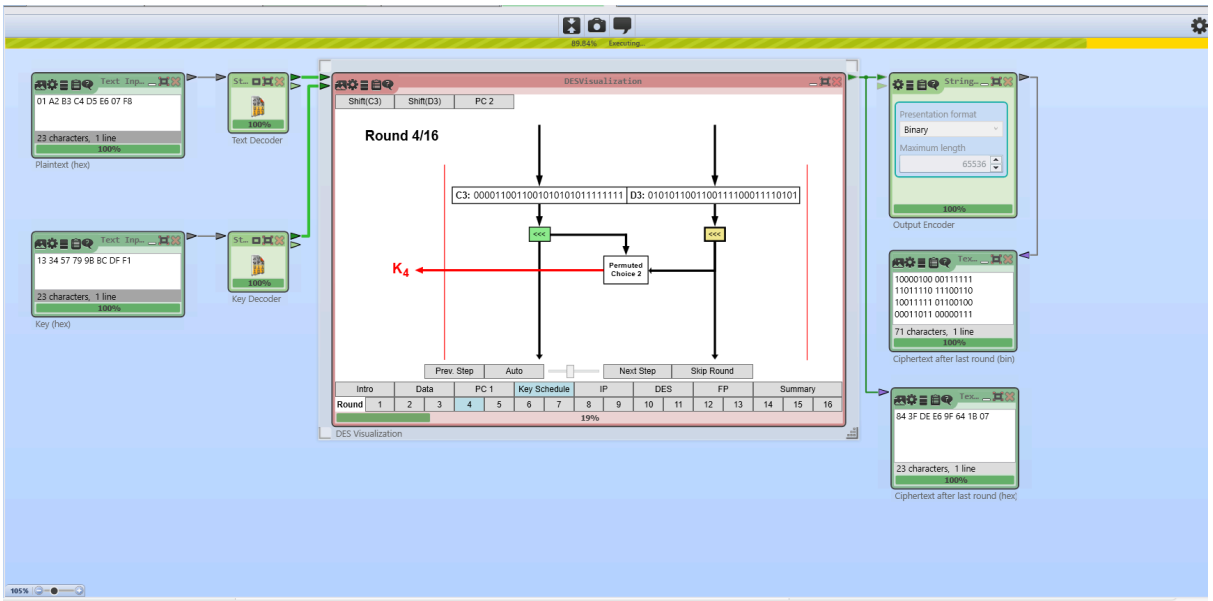

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Key (hex)
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Round 3/16
C2: 1100001100110010101010111111
D2: 0101010110011001111000111101
<<<
Permuted Choice 2
K3
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
16%
DES Visualization
Output Encoder
Presentation format
Binary
Maximum length
65536
Ciphertext after last round (bin)
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (hex)
84 3F DE E6 9F 64 1B 07

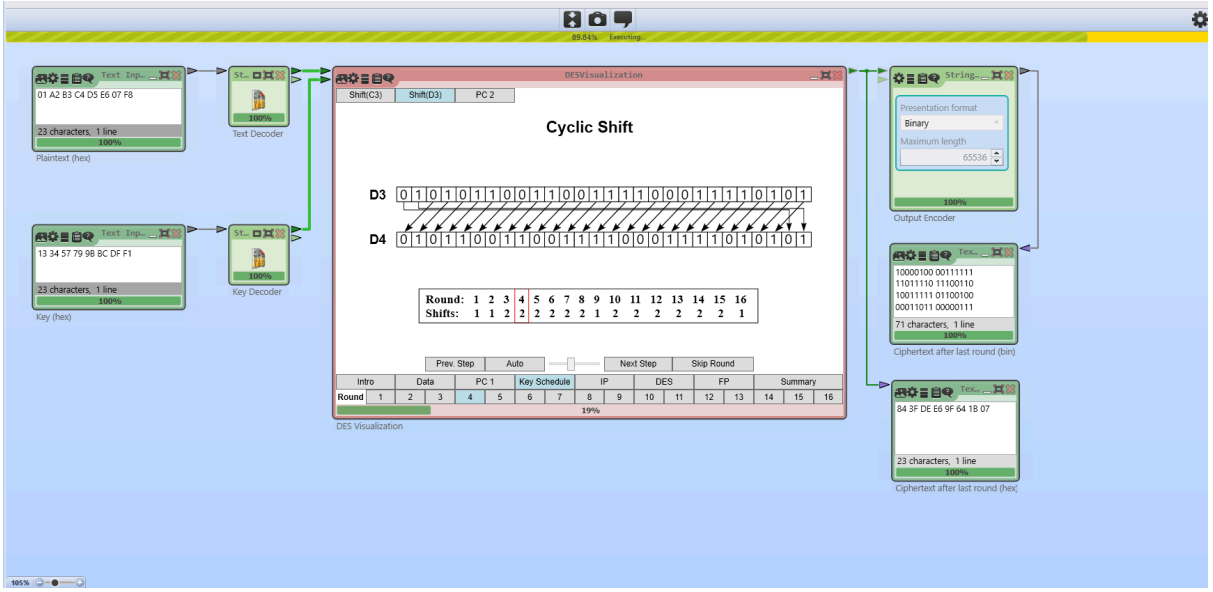

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Key (hex)
Key Decoder
DESVisualization
Shift(C2)
Shift(D2)
PC 2
Round
Round Key
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
0001101100000010111011111111110001110000011110010
0111100110101101101100111101111001001111001 01
0101010111111100100010100100001011001111100 11001
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
16%
DES Visualization
Output Encoder
Presentation format
Binary
Maximum length
65536
Ciphertext after last round (bin)
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (hex)
84 3F DE E6 9F 64 1B 07

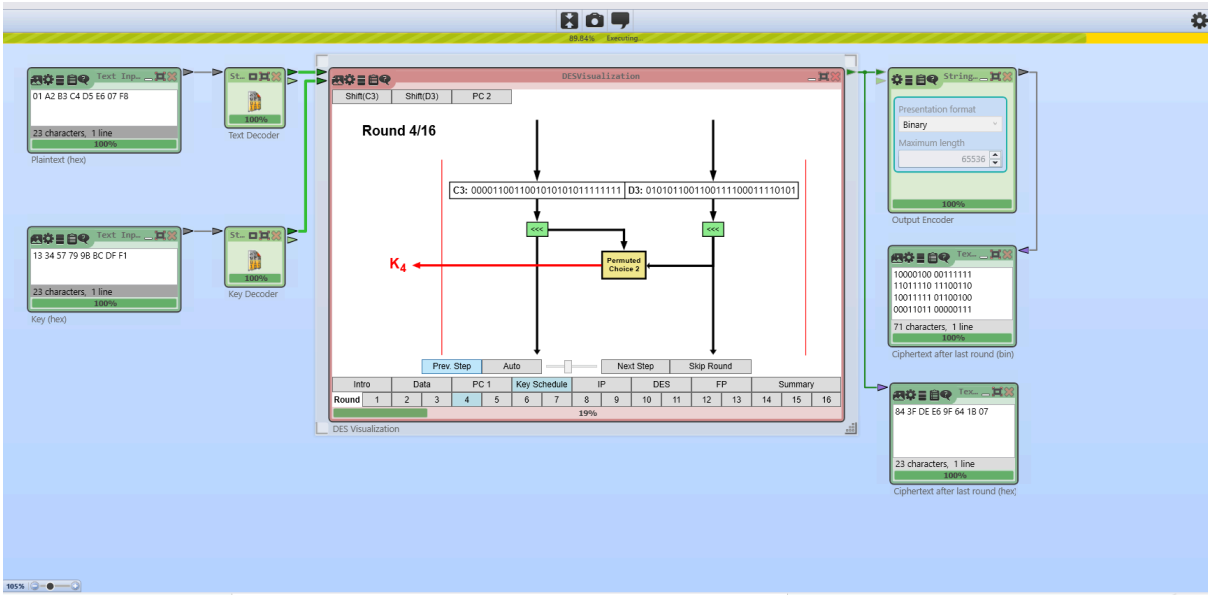
Round 4:

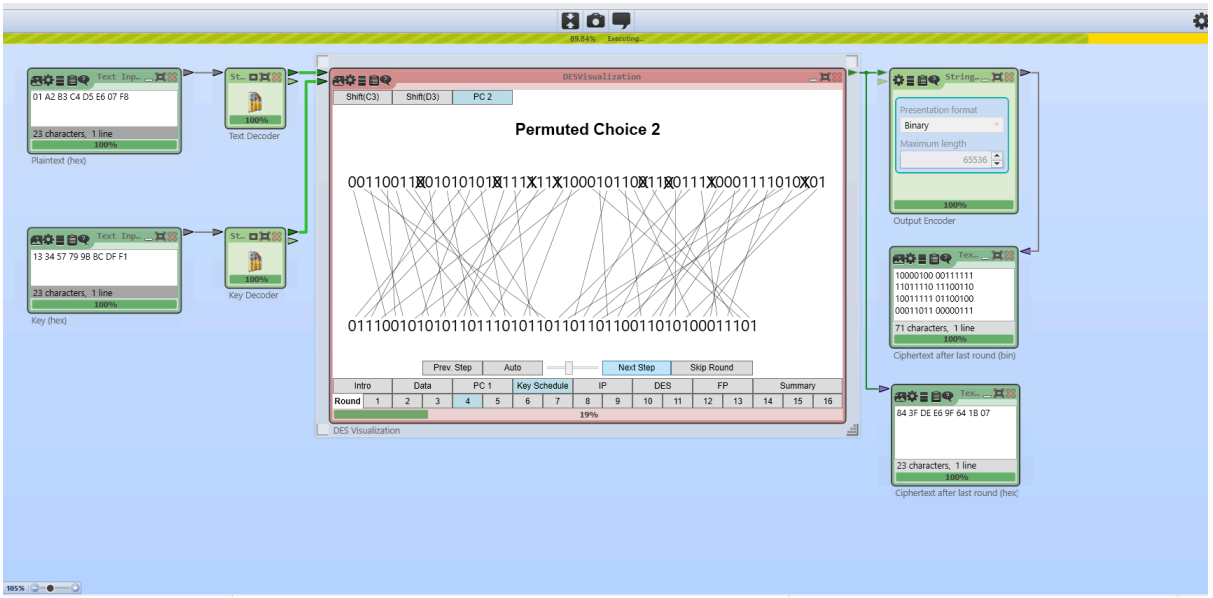

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Round 4/16
C3: 0000110011001010101011111111
D3: 0101011001100111100011110101
<<<
<<<
K4
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

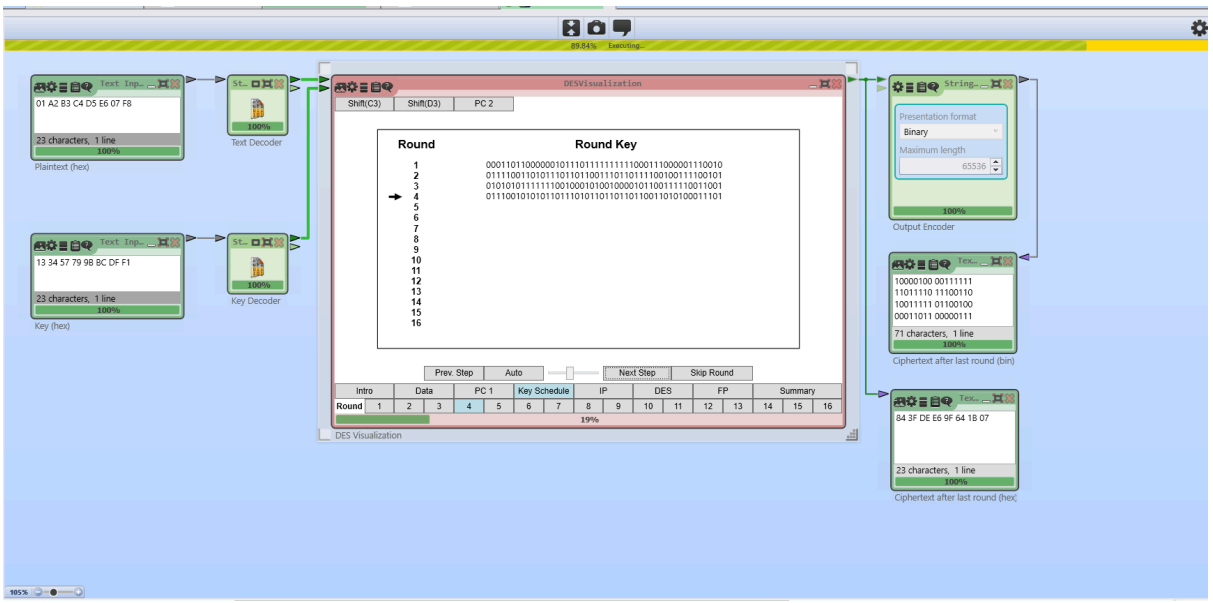

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Cyclic Shift
C3
0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
C4
0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 0 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Round 4/16
C3: 0000110011001010101011111111
D3: 0101011001100111100011110101
<<<
<<<
K4
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

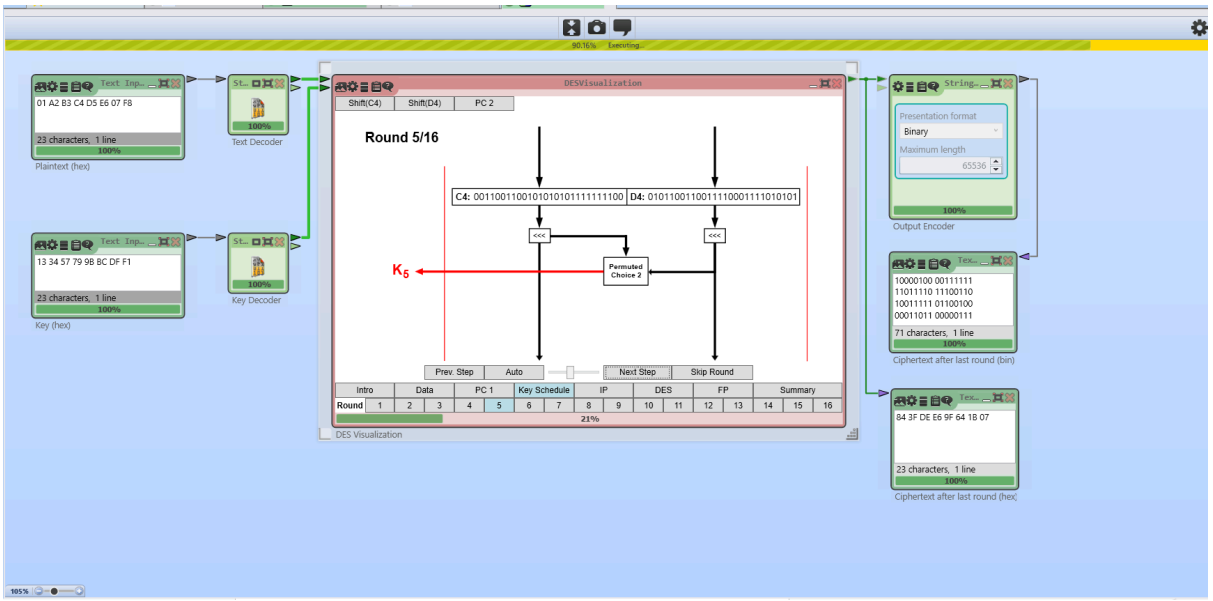

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Cyclic Shift
D3 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1
D4 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

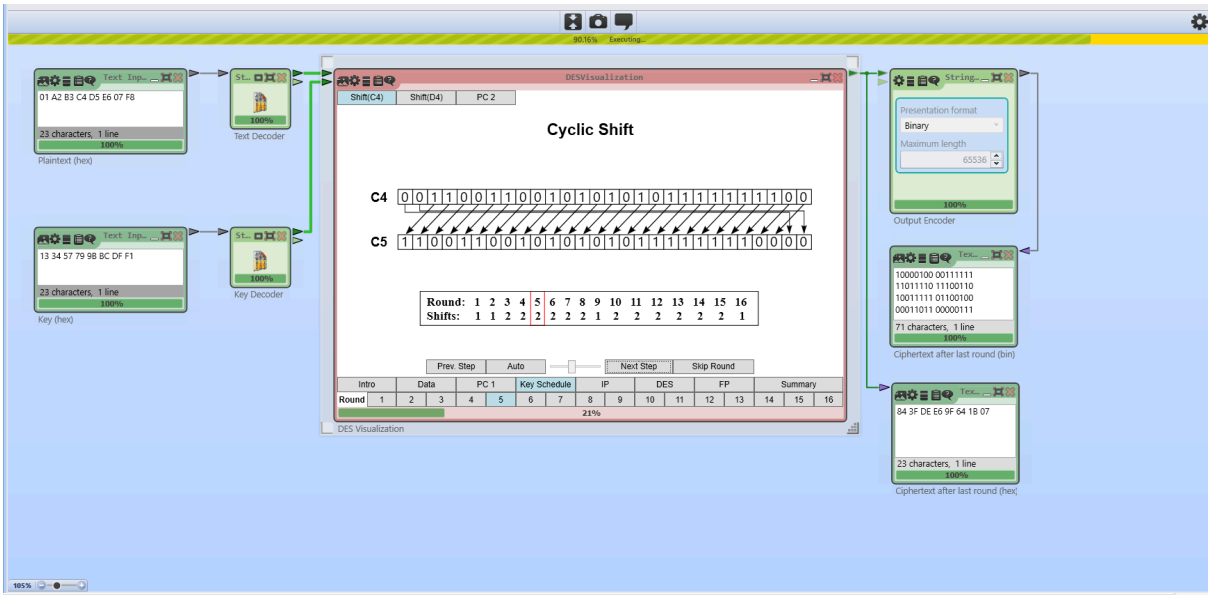

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Round 4/16
C3: 0000110011001010101011111111
D3: 0101011001100111100011110101
<<<
<<<
K4
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

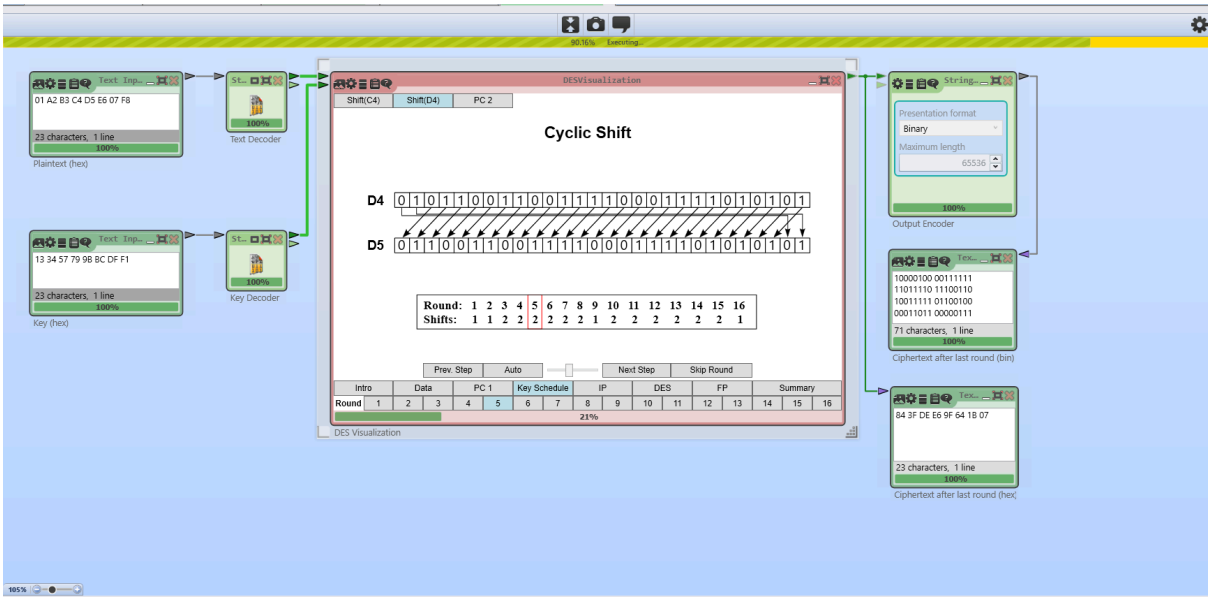

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Permuted Choice 2
0011001 1X01010101X111X11X10001011 0X11X0111X0001111010X01
0111001010101101110101101101101100110101000 11101
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C3)
Shift(D3)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011110010
2 0111100110101110110110011110110111100100011110010 1
3 0101010111111001000101010000101100111110011001
4 0111001010101101110101101101101100110101000111 01
5
6
7
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
19%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

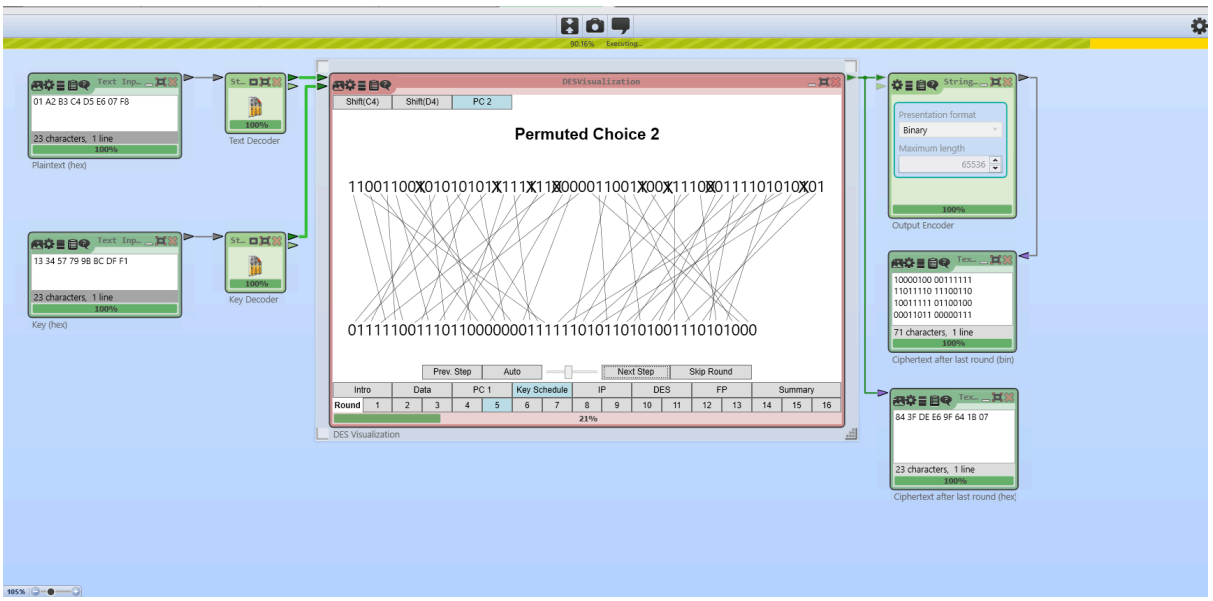
Round 5:

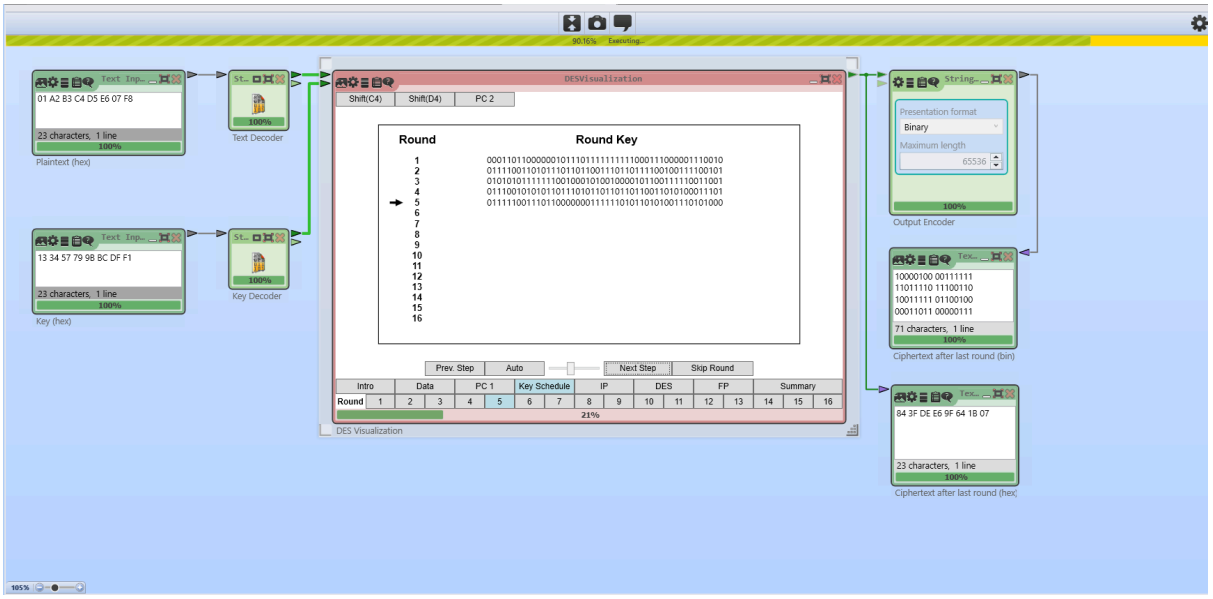

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C4)
Shift(D4)
PC 2
Round 5/16
C4: 0011001100101010101111111100
D4: 0101100110011110001111010101
<<<
<<<
Permuted Choice 2
K5
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
21%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%



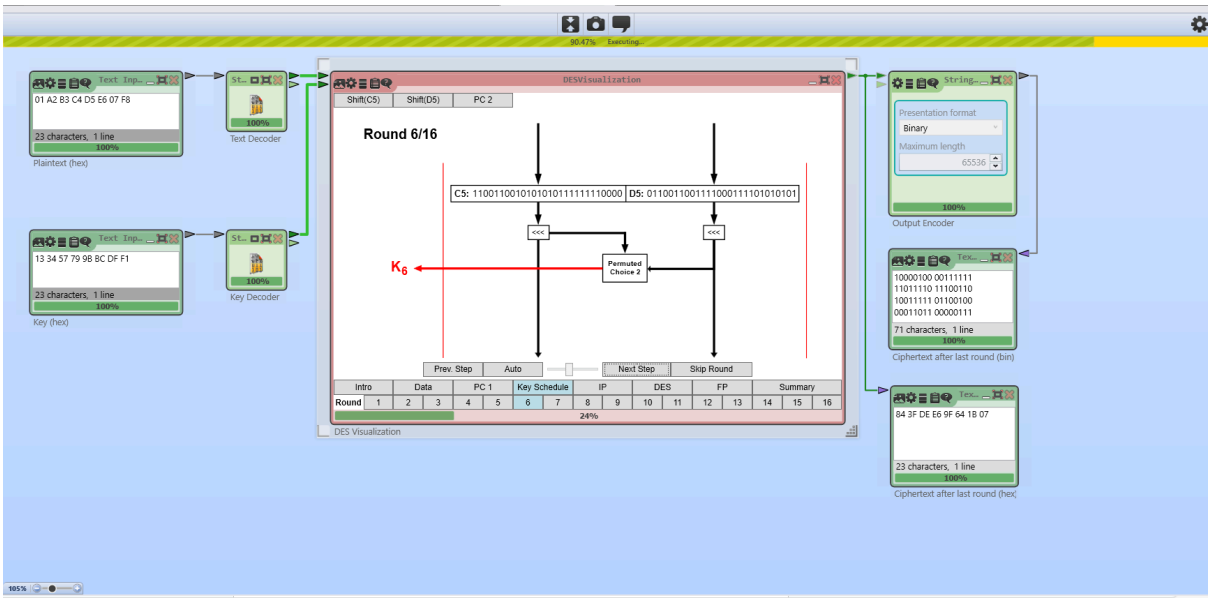


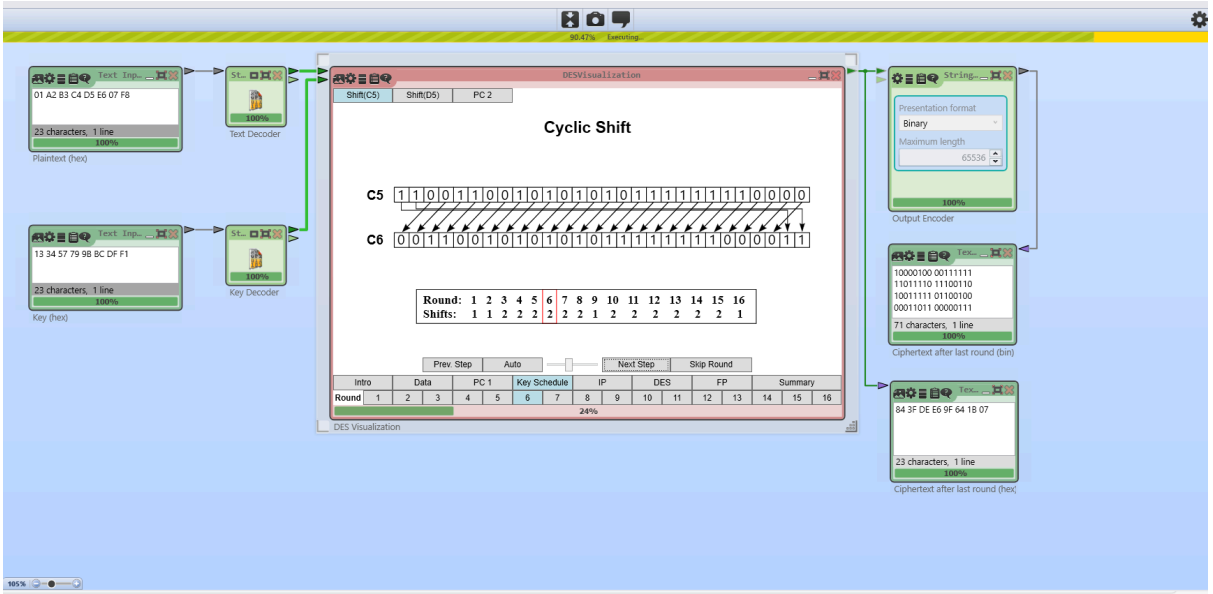
Permutation choice 2:

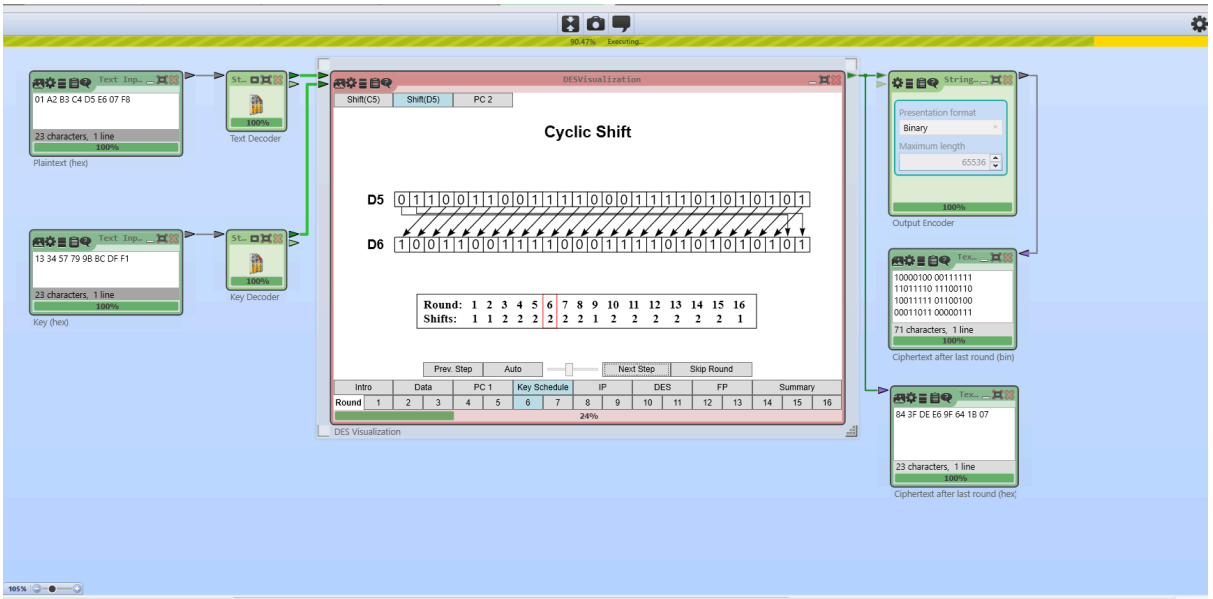


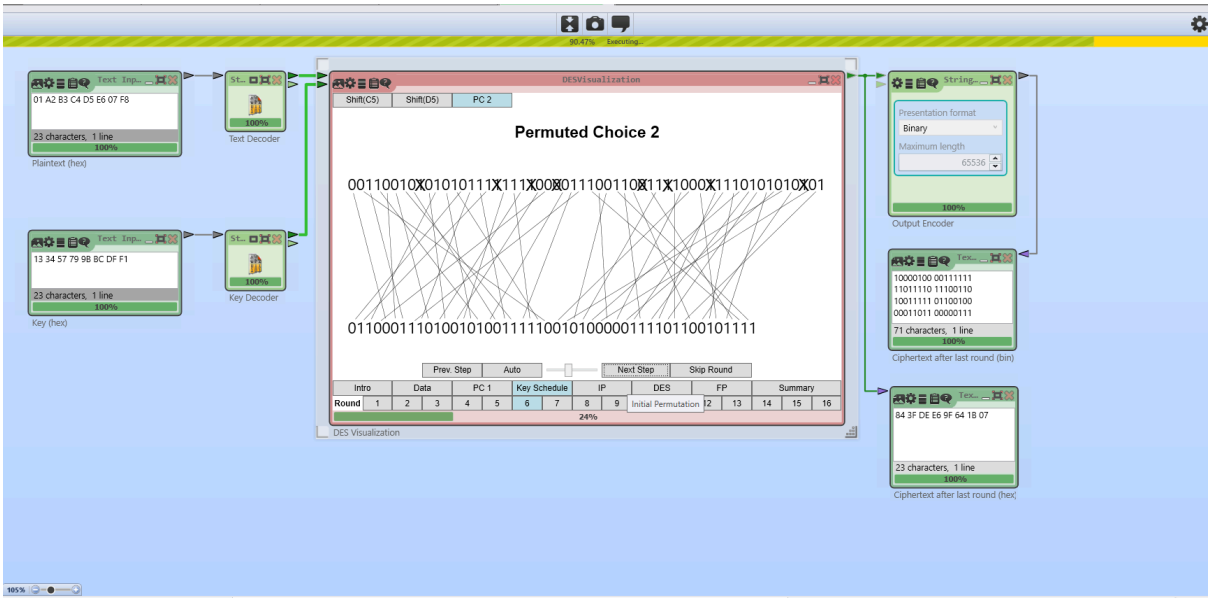

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C4)
Shift(D4)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011100 10
2 0111100110101110110110011011011110010011110010 1
3 0101010111111110010010100100001011001111100110 01
4 0111001010101101110101101101101100110101001110 1
5 0111110011101100000001111110101101001110101000
6
7
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
21%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

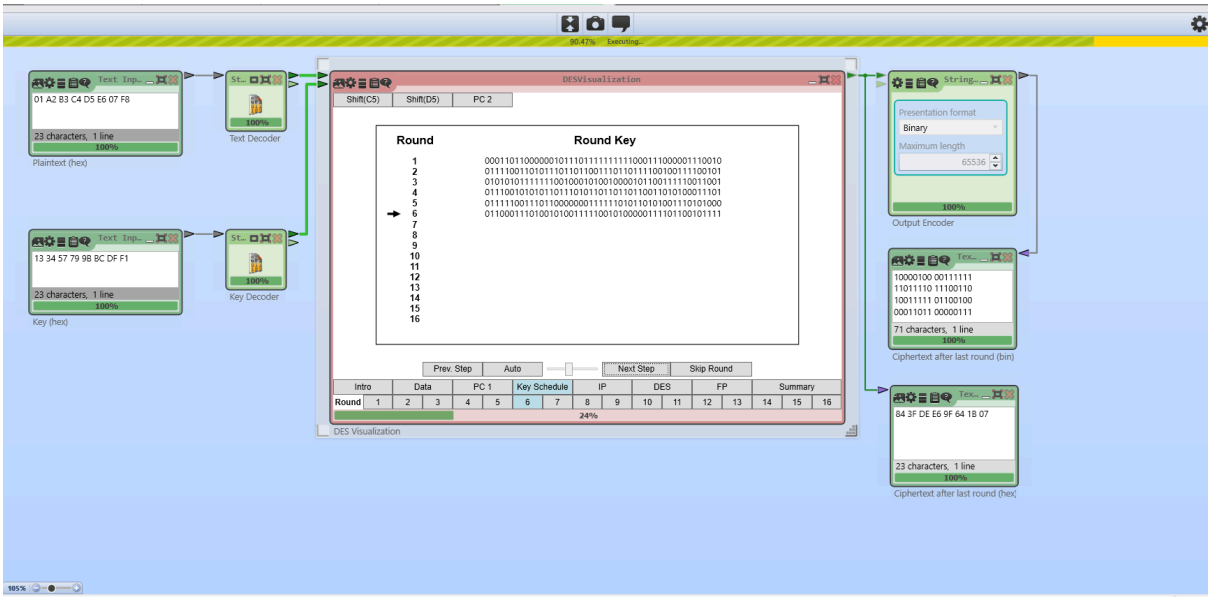
Round 6:


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C5)
Shift(D5)
PC 2
Round 6/16
C5: 1100110010101010111111110000
D5: 0110011001111000111101010101
<<<
<<<
Permuted Choice 2
K6
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
24%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

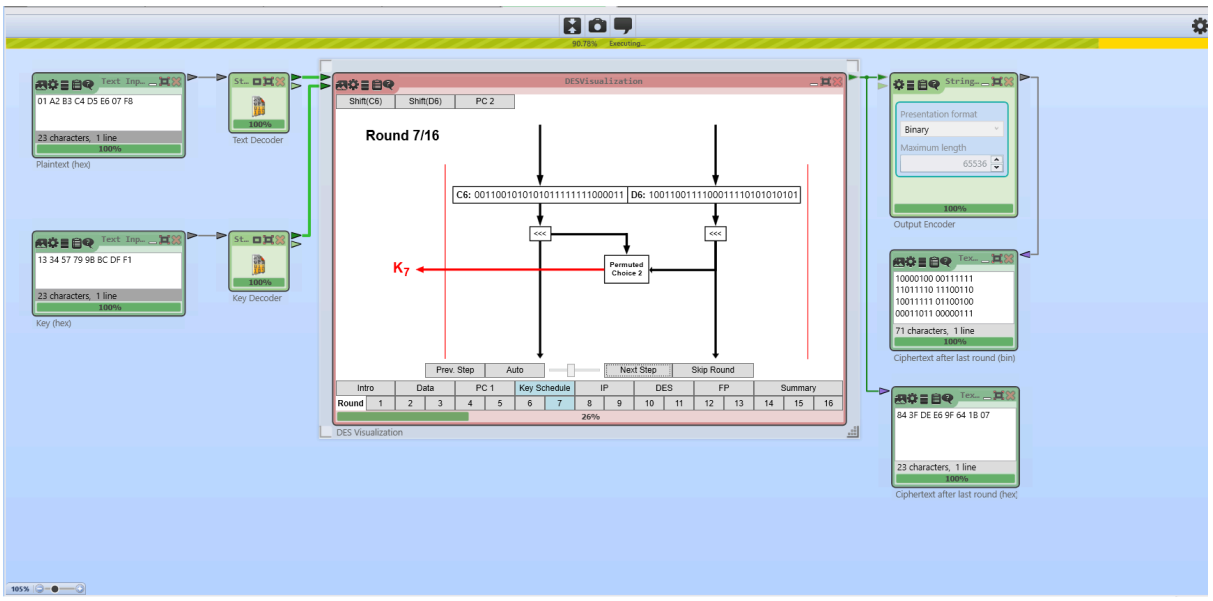

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Text Decoder
St...
100%
Key Decoder
DESVisualization
Shift(C5)
Shift(D5)
PC 2
Cyclic Shift
C5 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0
C6 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
24%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Text Decoder
St...
100%
Key Decoder
DESVisualization
Shift(C5)
Shift(D5)
PC 2
Cyclic Shift
D5 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1
D6 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
24%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

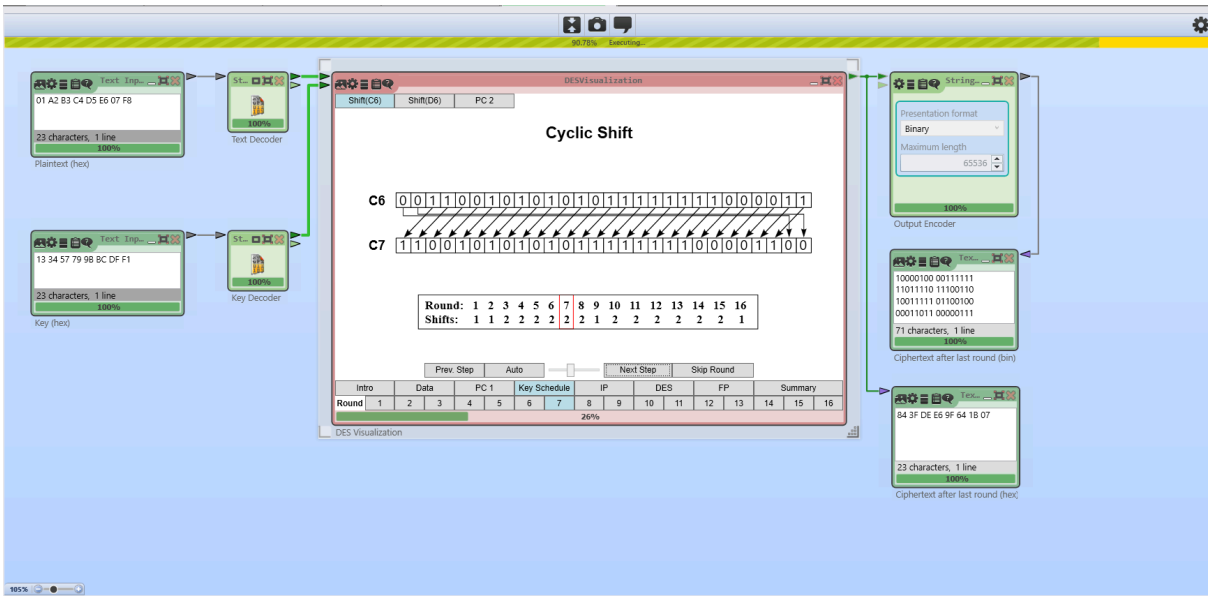

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Text Decoder
St...
100%
Key Decoder
DESVisualization
Shift(C5)
Shift(D5)
PC 2
Permuted Choice 2
0011001 0X0101011 1X111X00X0111001 10X111X1000X1110101010X01
0110001110100101001111100101000001111011001011 11
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 Initial Permutation 12 13 14 15 16
24%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C5)
Shift(D5)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011100010
2 0111001101011101101100111011011110010011110010 1
3 0101010111111100100010100100001011001111100110 01
4 0111001010101101110101101101101100110010100011101
5 0111110011101100000001111110101101001110101000
6 0110001110100101001111100101000001111011001011 11
7
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
24%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

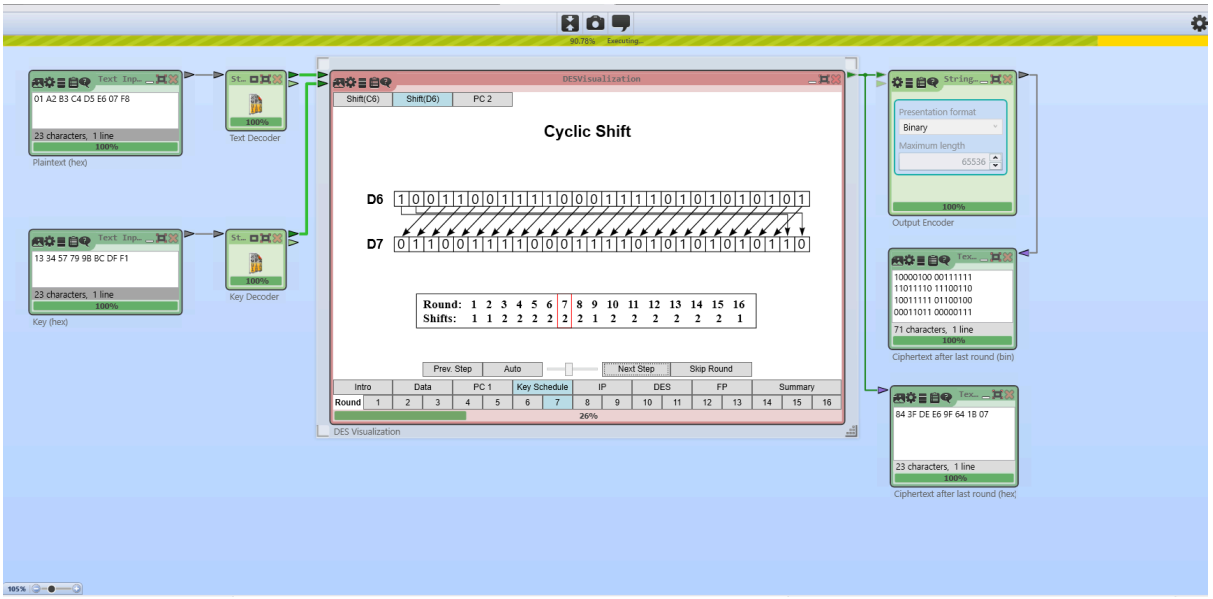
Round 7:

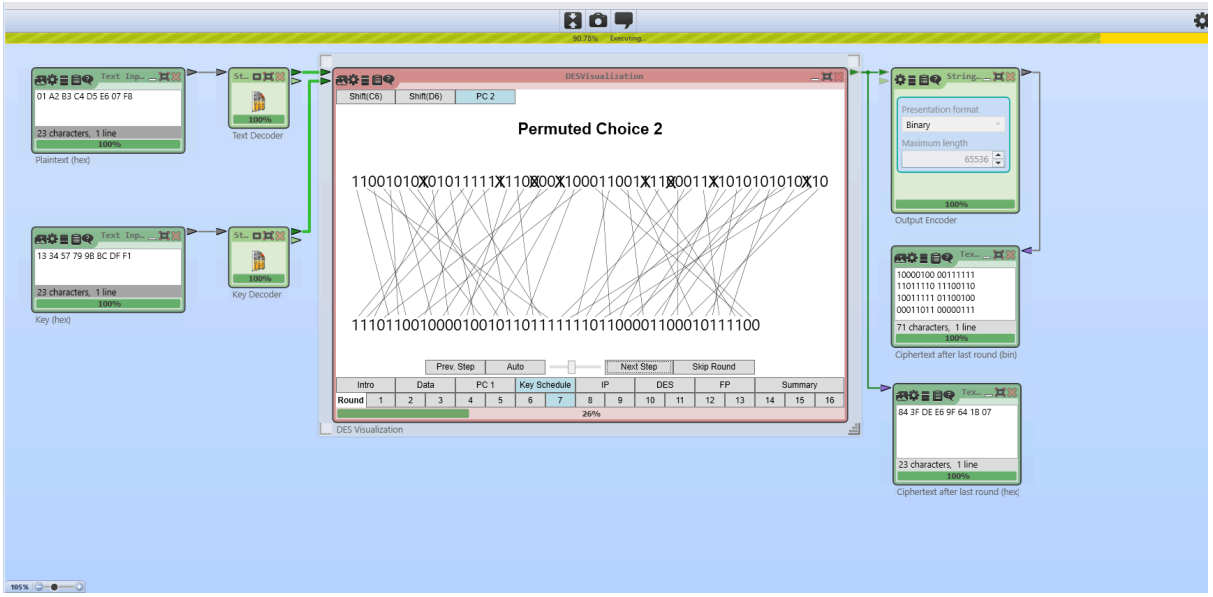


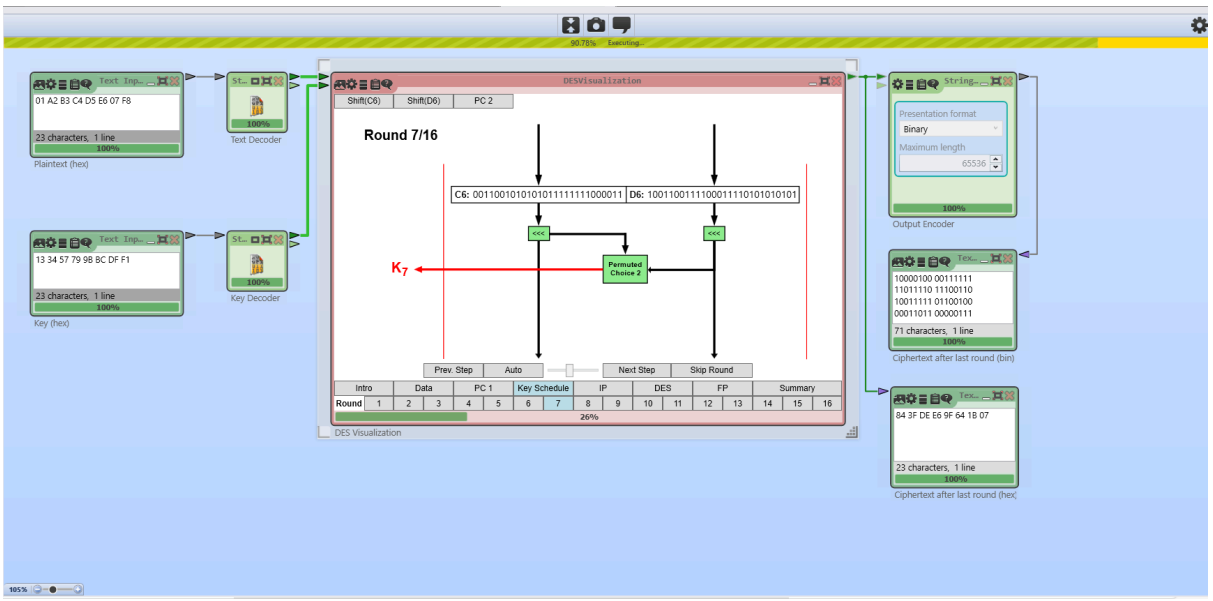
Cyclic shift of c6:

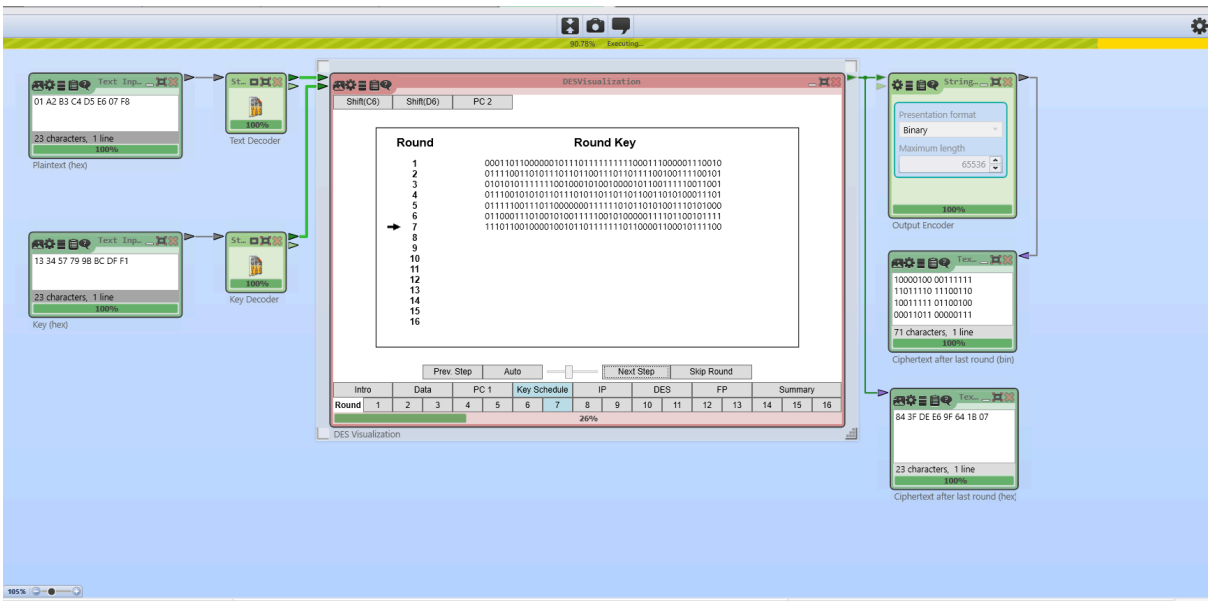


Cyclic shift of d6:

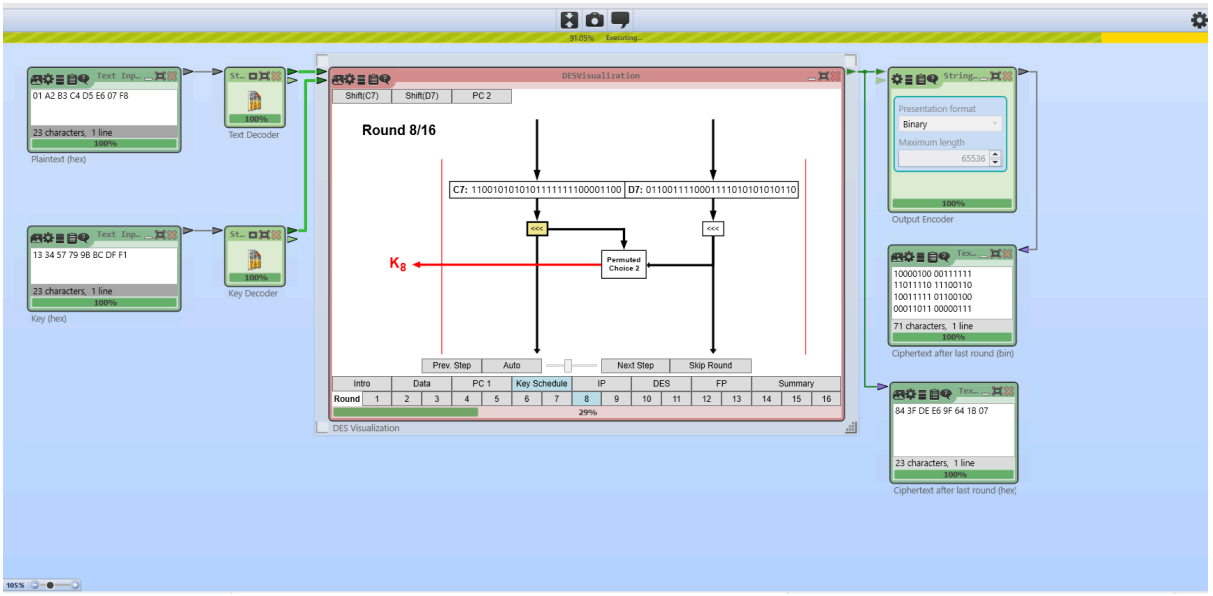

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C6)
Shift(D6)
PC 2
Cyclic Shift
D6 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1
D7 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
26%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

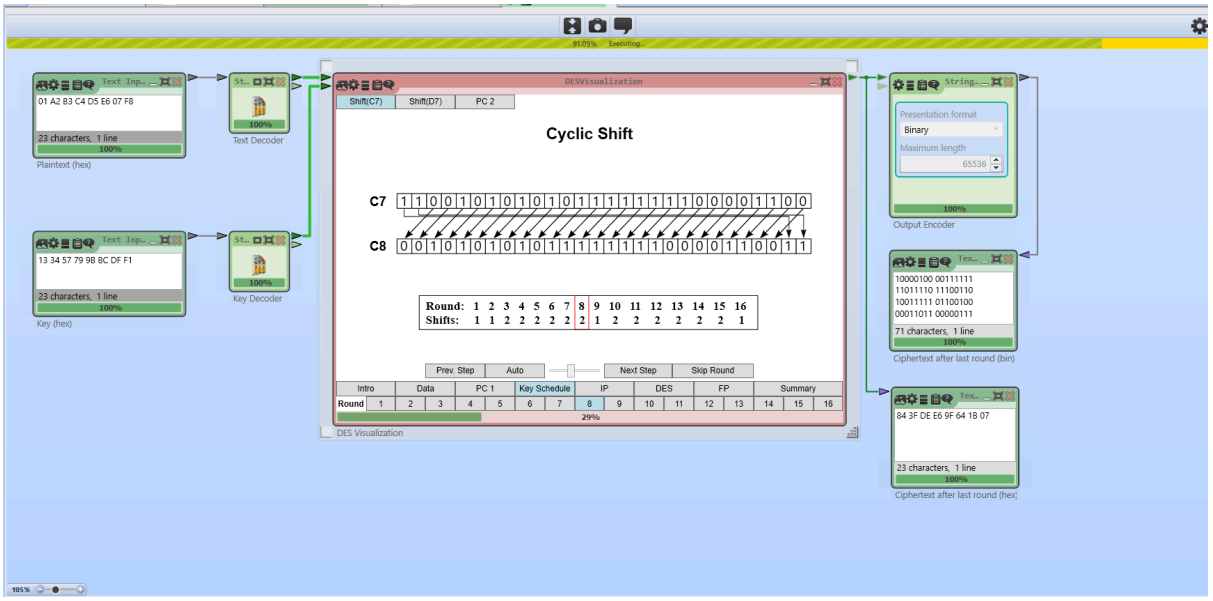

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C6)
Shift(D6)
PC 2
Permuted Choice 2
11001010X01011111X1100X00X100011001X11X00011X1010101010X10
11101100100001001011011111110110000110001011110 0
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
26%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

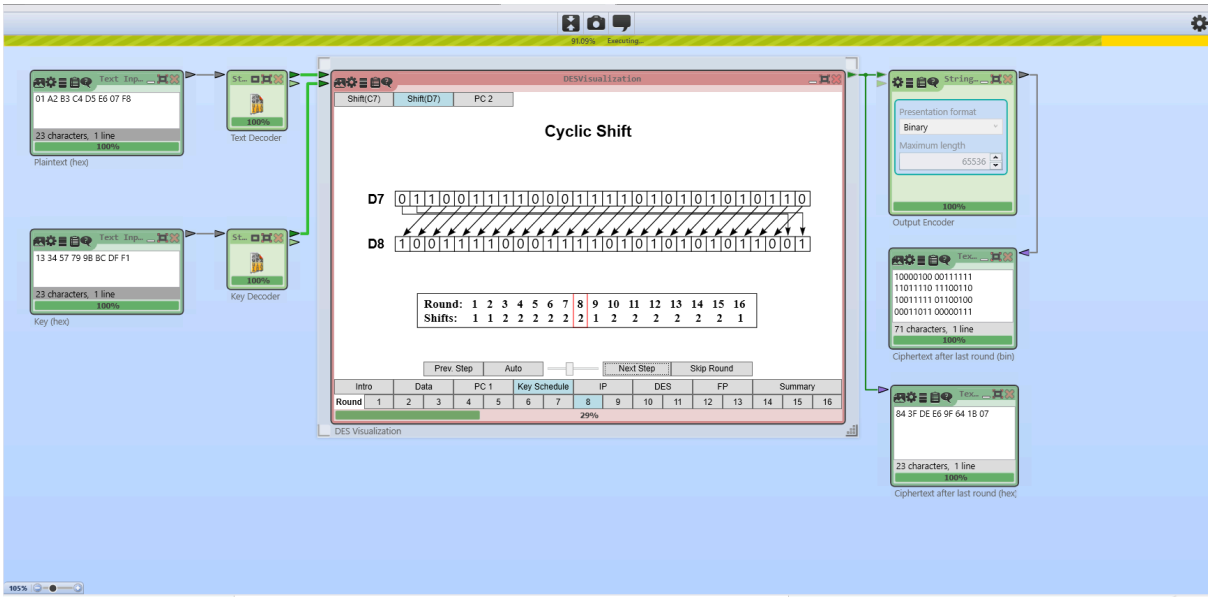

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C6)
Shift(D6)
PC 2
Round 7/16
C6: 0011001010101011111111000011
D6: 1001100111100011110101010101
<<<
<<<
Permuted Choice 2
K7
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
26%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C6)
Shift(D6)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011100010
2 0111001101011101101100111011111001001111001
3 0101010111111001000101001000010110011111001001
4 0111001010101101110101101101101101001101010001101
5 0111110011101100000001111110101101001110101000
6 0110001110100101001111100101000001111011001011
7 1110110010000100101101111111101100001100011100
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
26%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

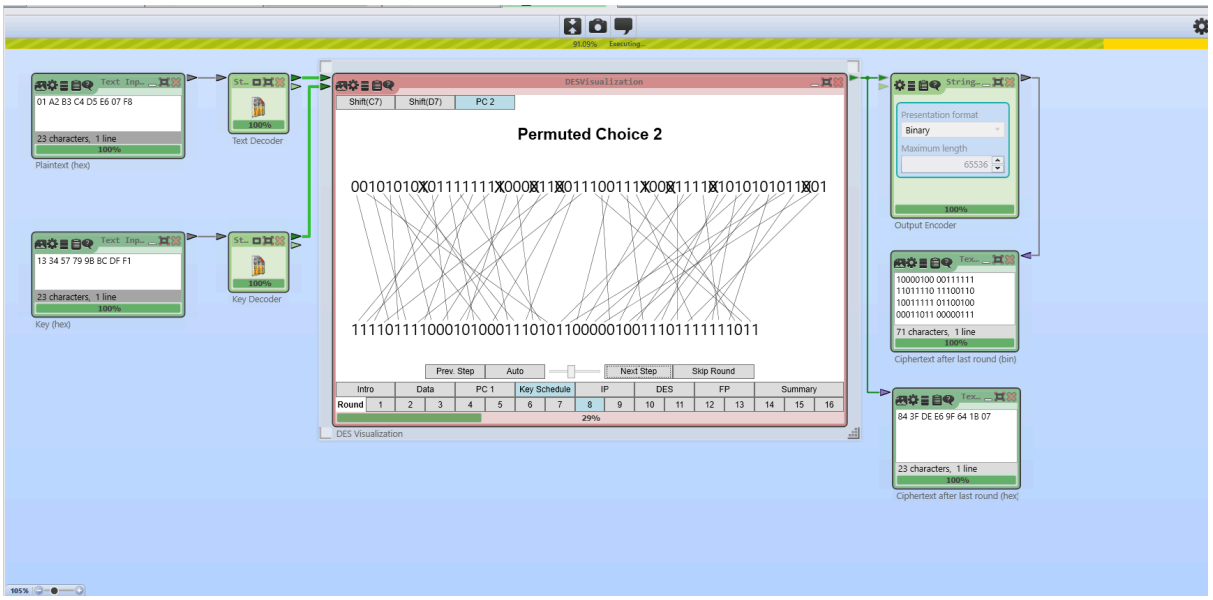
Round 8:

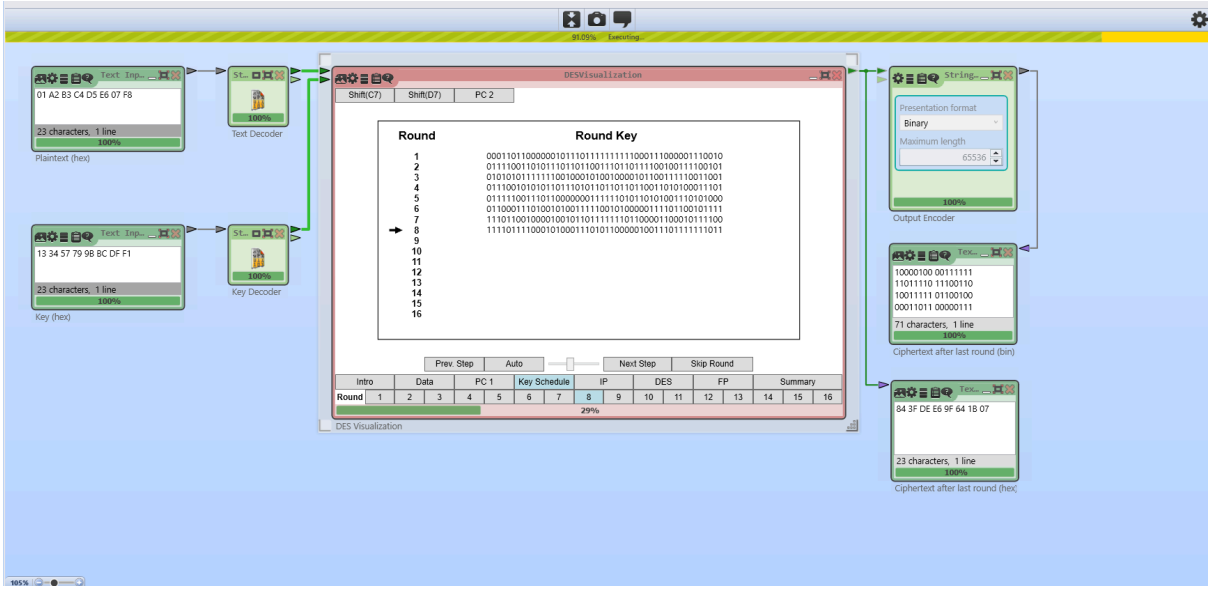

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C7)
Shift(D7)
PC 2
Round 8/16
C7: 1100101010101111111100001100
D7: 0110011110001111010101010110
<<<
<<<
K8
Permuted Choice 2
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
29%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)



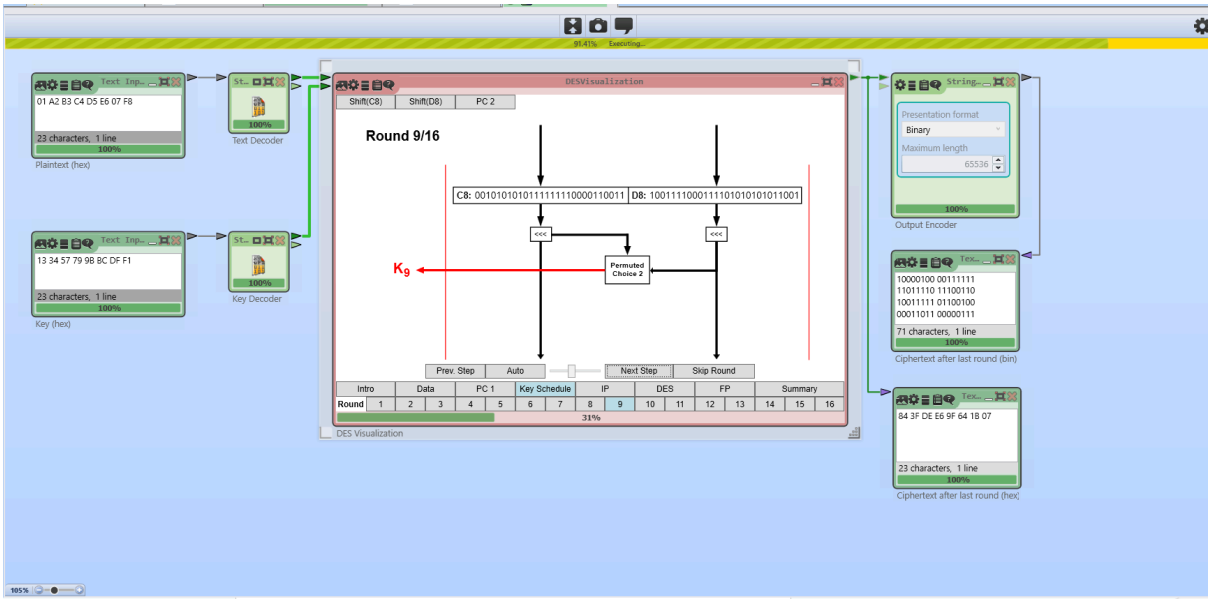


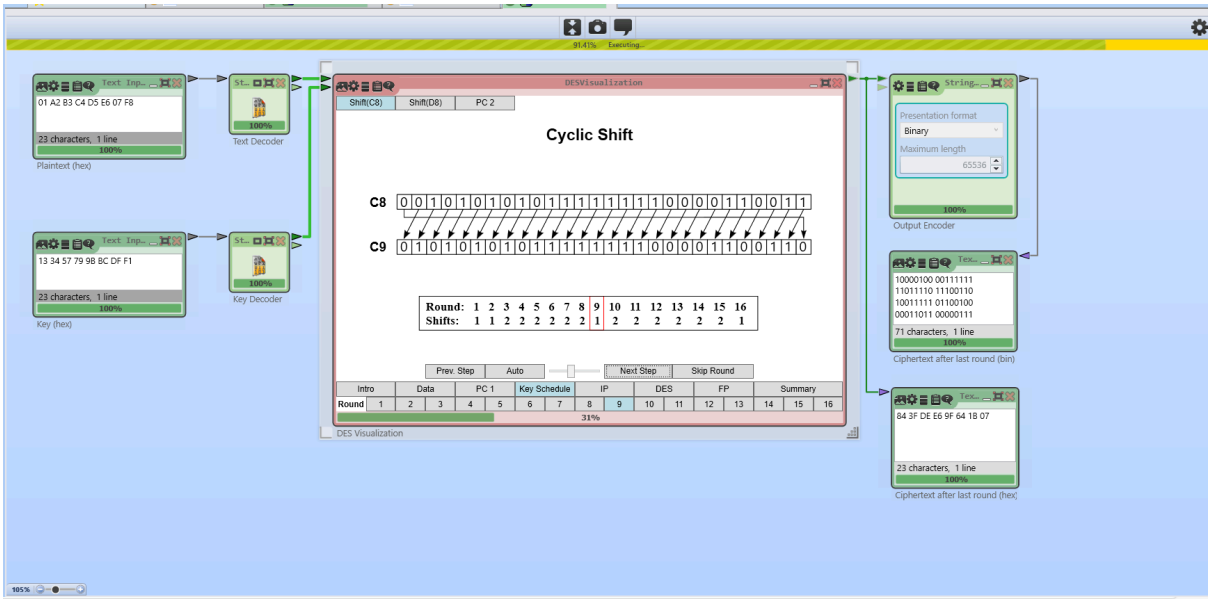
Permutation choice 2:

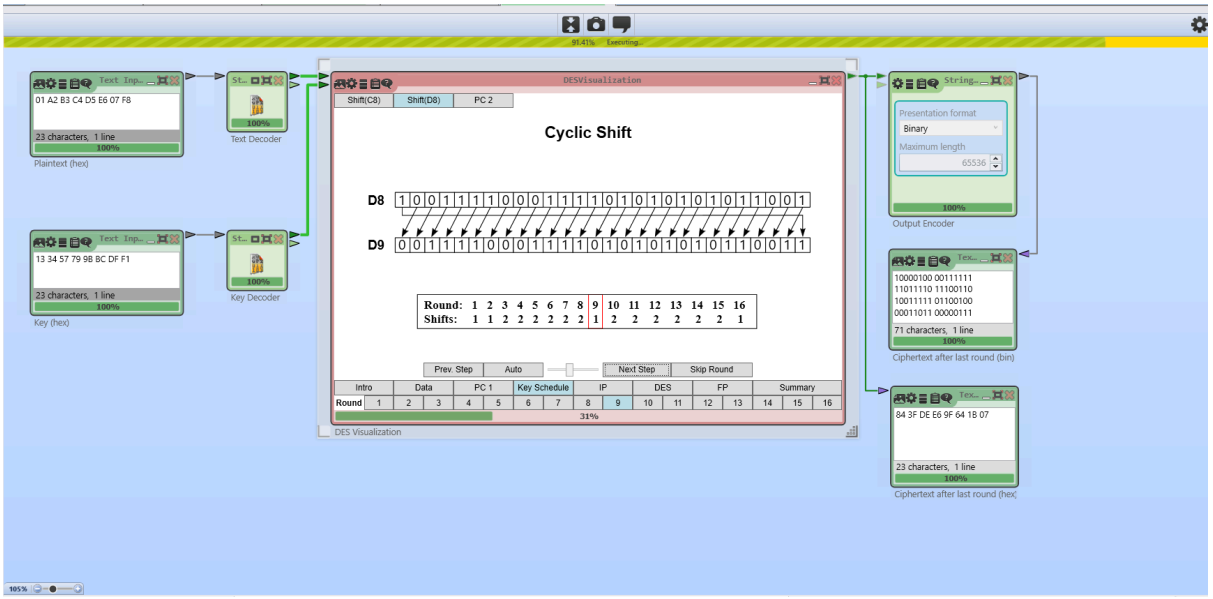


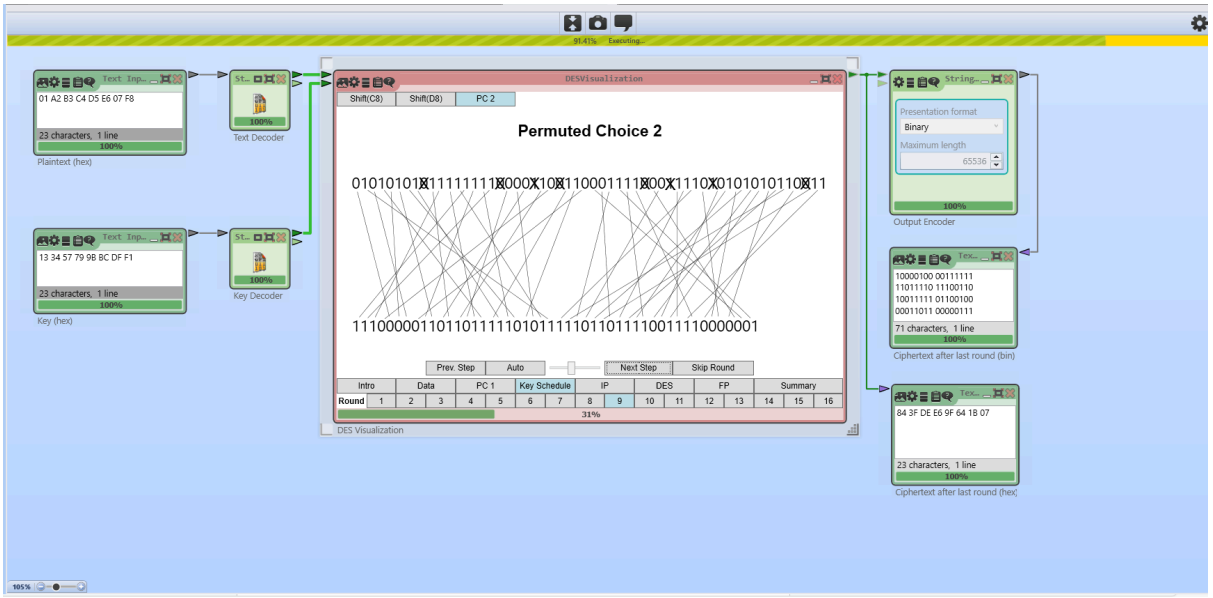

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C7)
Shift(D7)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000111001 0
2 0111100110101110110110011101110111100100111100101
3 0101010111111110010010100100001011001111100110 01
4 0111001010101101110101101101101101100110101001 1101
5 0111110011101100000001111110101101101001110101000
6 0110001110100101001111100101000001111101100101111
7 1110110010000100101101111111101100001100010111100
8 1111011110001010001110101100000100111011111111011
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
29%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

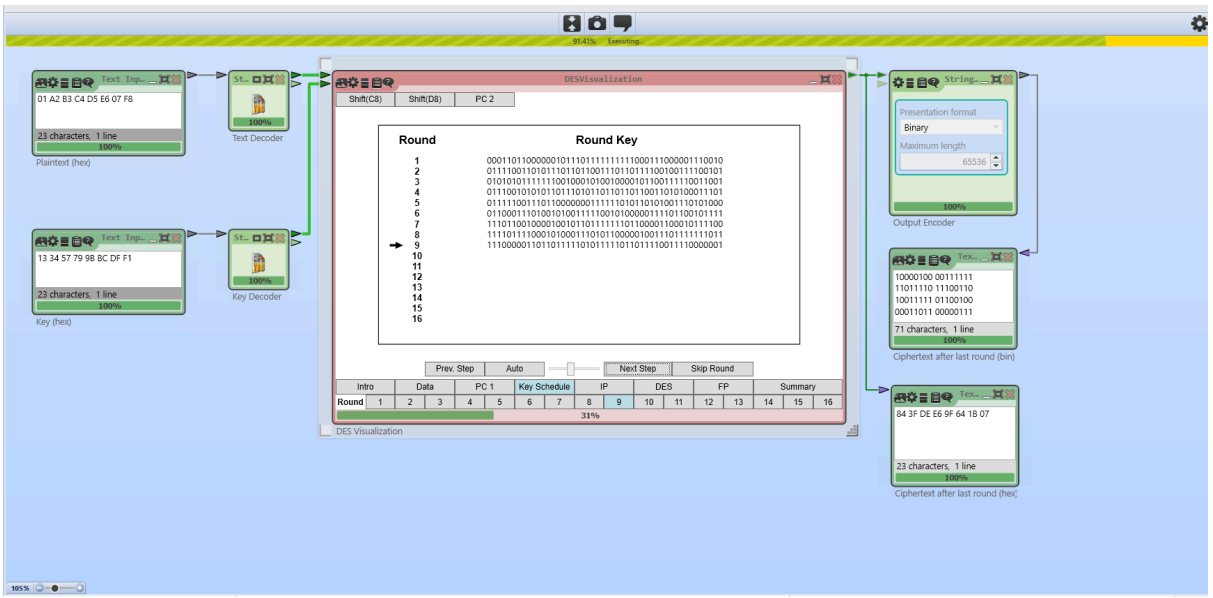
Round 9:


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C8)
Shift(D8)
PC 2
Round 9/16
C8: 0010101010111111110000110011
D8: 1001111000111101010101011001
<<<
<<<
Permuted Choice 2
K9
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
31%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

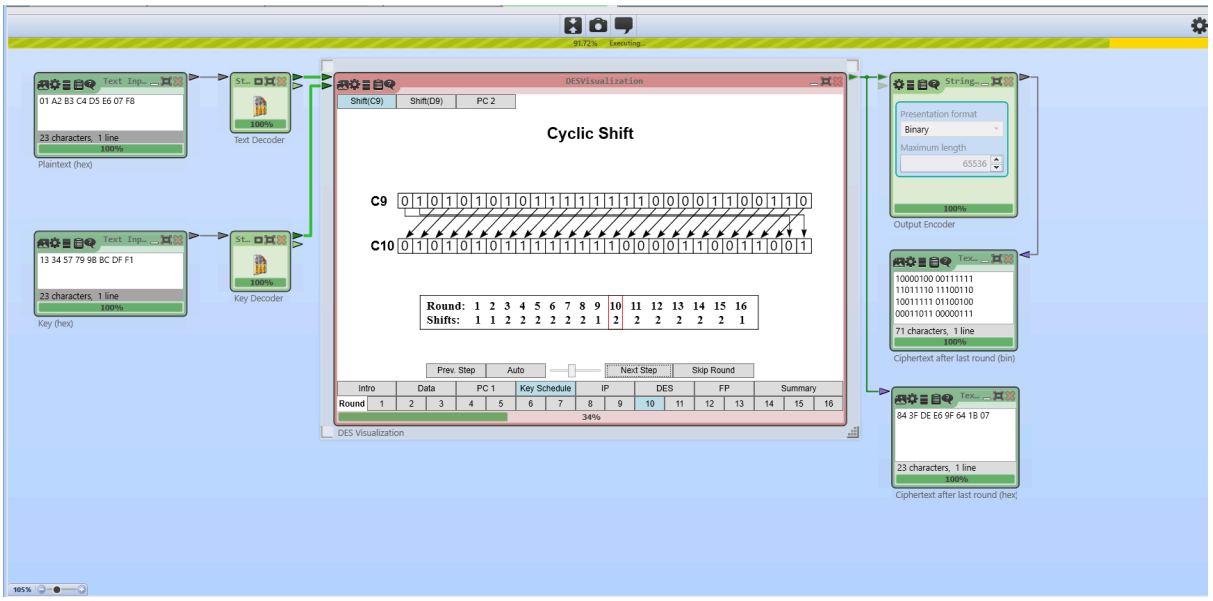

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C8)
Shift(D8)
PC 2
Cyclic Shift
C8 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1
C9 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
31%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

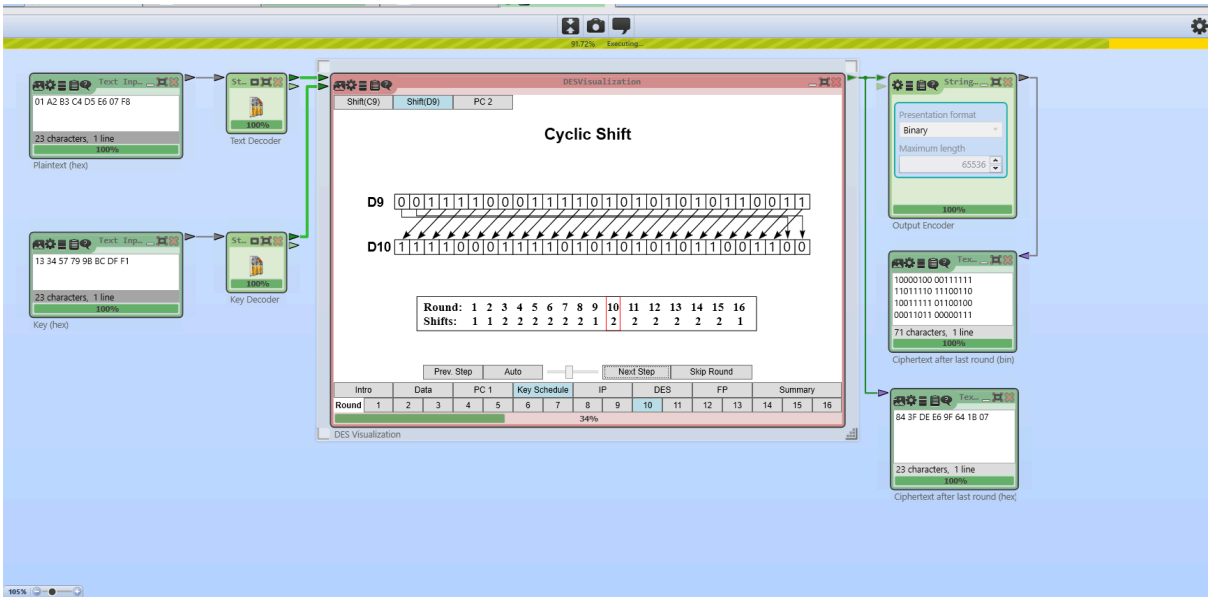

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C8)
Shift(D8)
PC 2
Cyclic Shift
D8 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1
D9 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
31%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

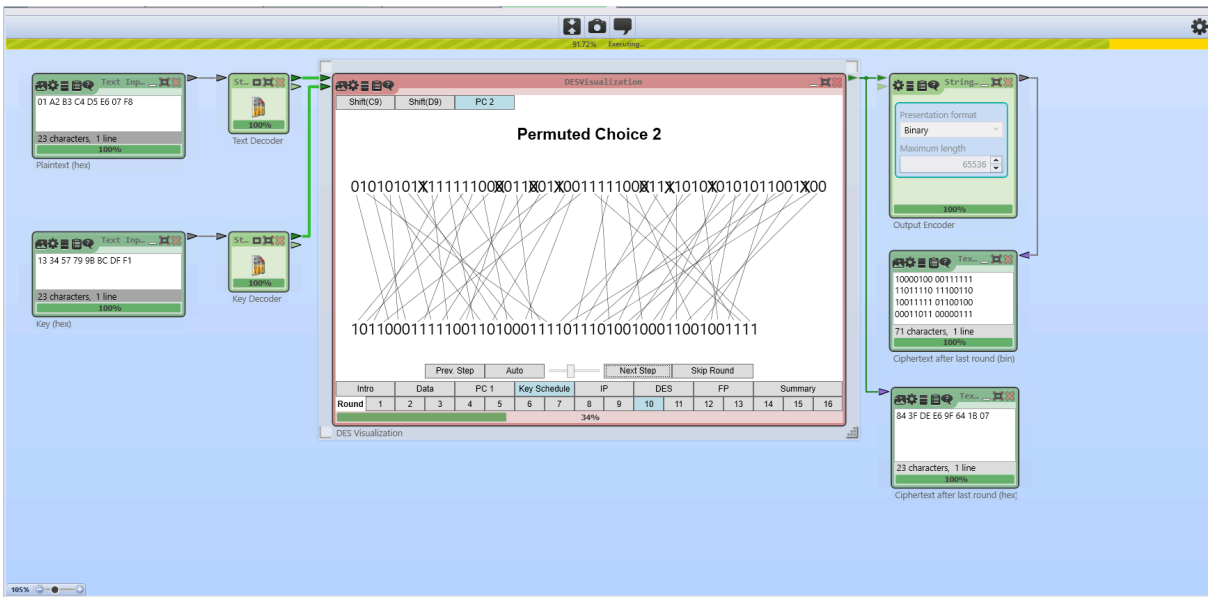

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C8)
Shift(D8)
PC 2
Permuted Choice 2
01010101X11111111X000X10X1100011111X00X1110X0101010110X11
11100000110110111110101111101101111001111000001
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
31%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

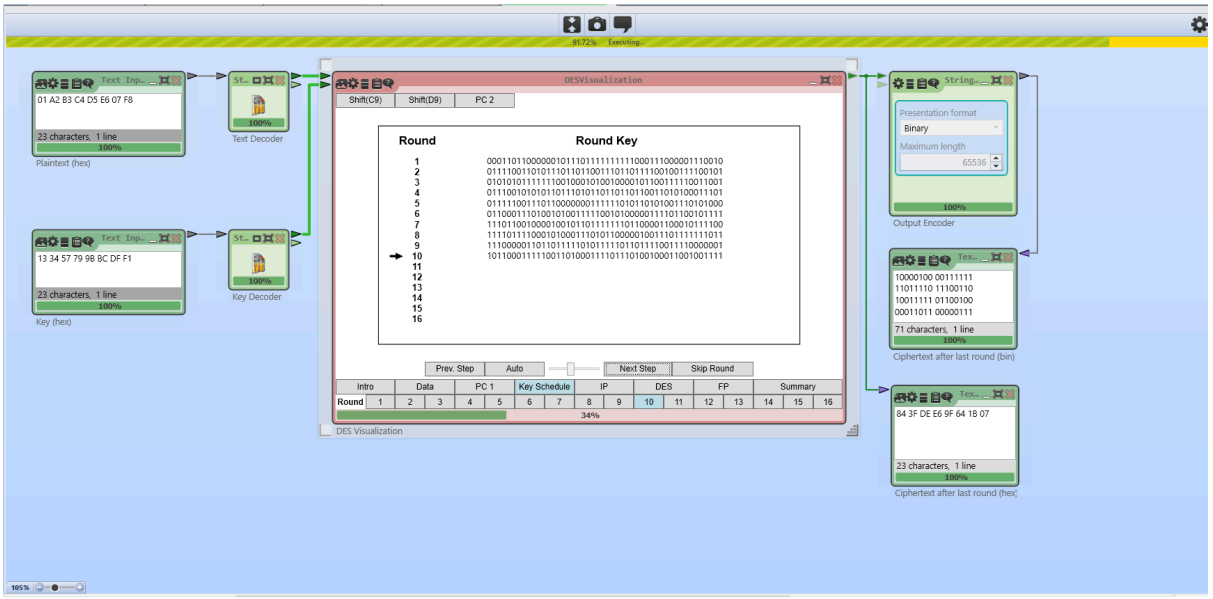

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C8)
Shift(D8)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011110010
2 0111100110101110110110011011011111001110011100101
3 0101010111111001000101001000010110011111001101
4 0111001010101101110101101101101101101101001101
5 0111100111011000000011111010110101001110101000
6 0110001110100101001111100101000001111011001011111
7 1110110010000100101101111111101100001100010111100
8 1111011110001010001110101101000001001110111111011
9 1110000001101101111010111110111011110011100000001
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
31%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

Round 10:

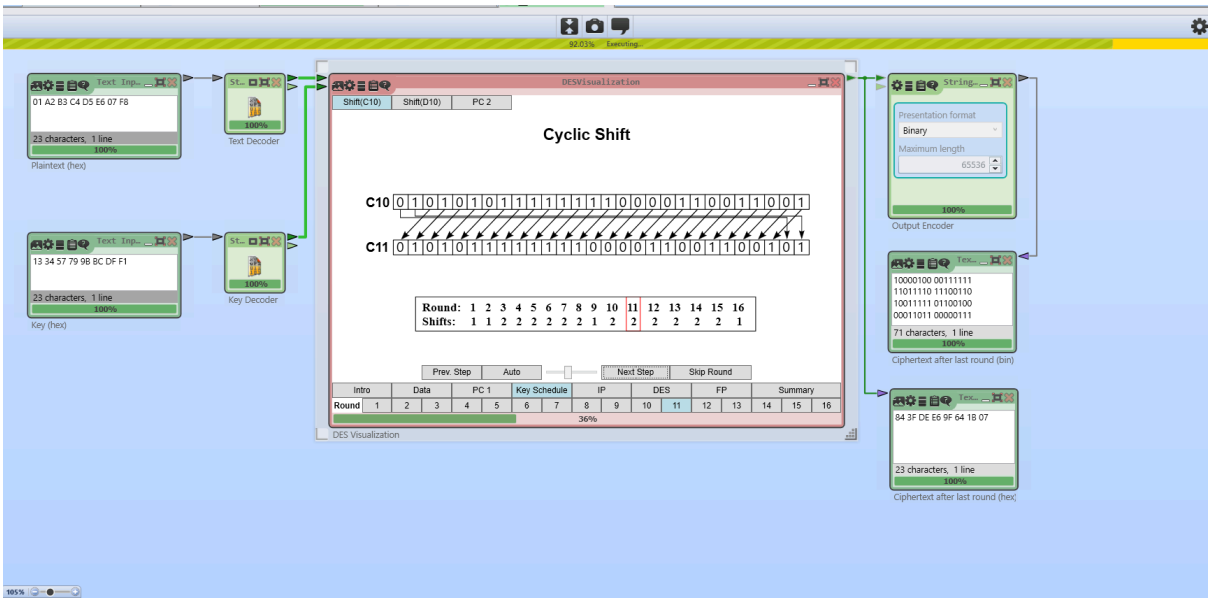

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C9)
Shift(D9)
PC 2
Cyclic Shift
C9 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0
C10 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
34%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

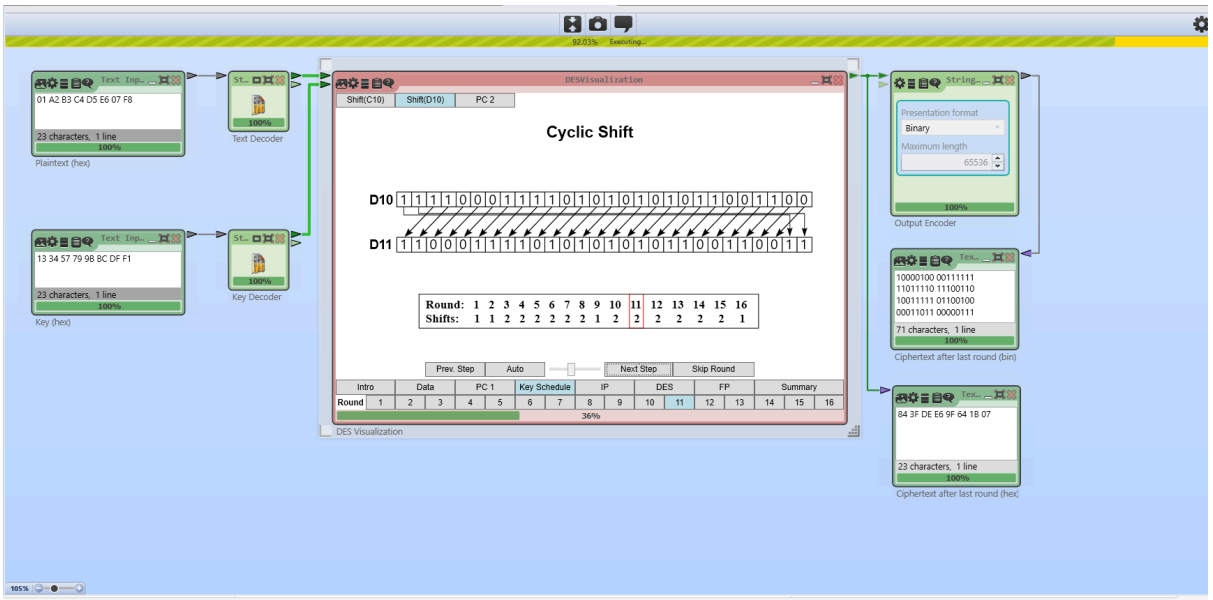

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C9)
Shift(D9)
PC 2
Cyclic Shift
D9 0 0 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1
D10 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
34%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

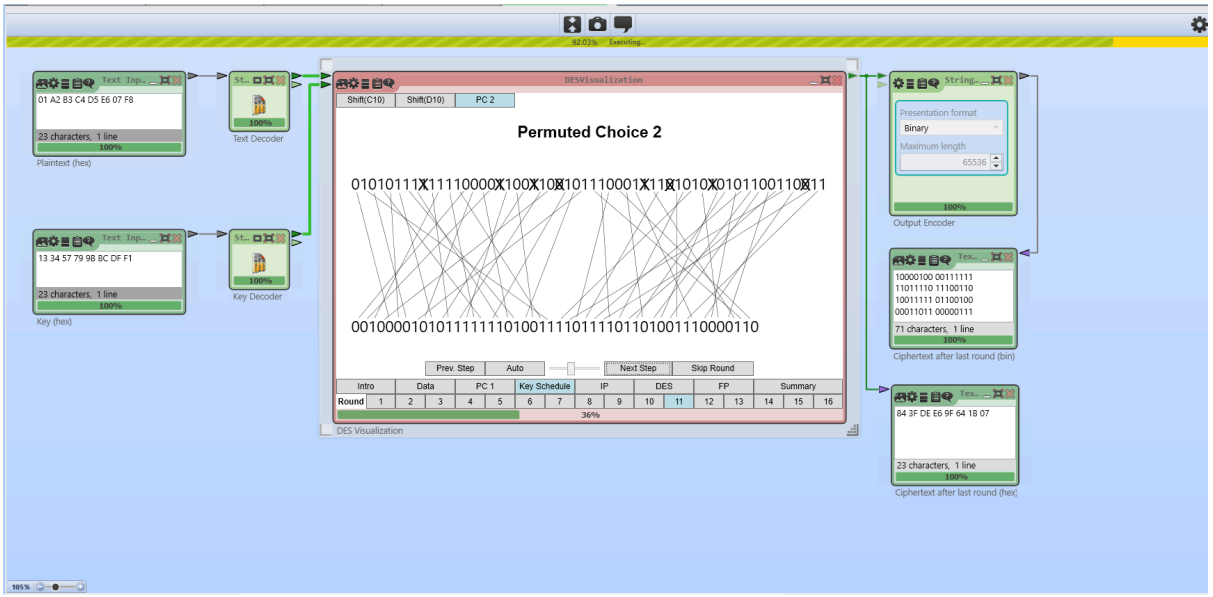

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C9)
Shift(D9)
PC 2
Permuted Choice 2
01010101X1111110X0011X01X0011110X11X1010X0101011001X00
10110001111100110100011110111010010001100100111
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
34%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

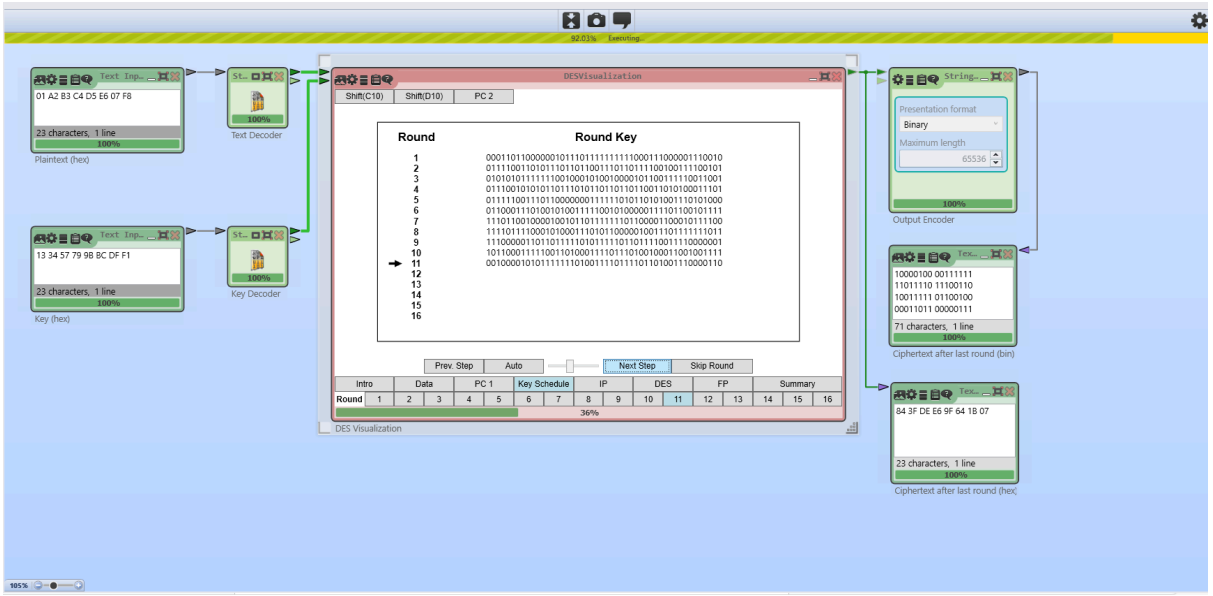

01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C9)
Shift(D9)
PC 2
Round
Round Key
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
34%
DES Visualization
Presentation format
Binary
Maximum length
65536
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

Round 11:

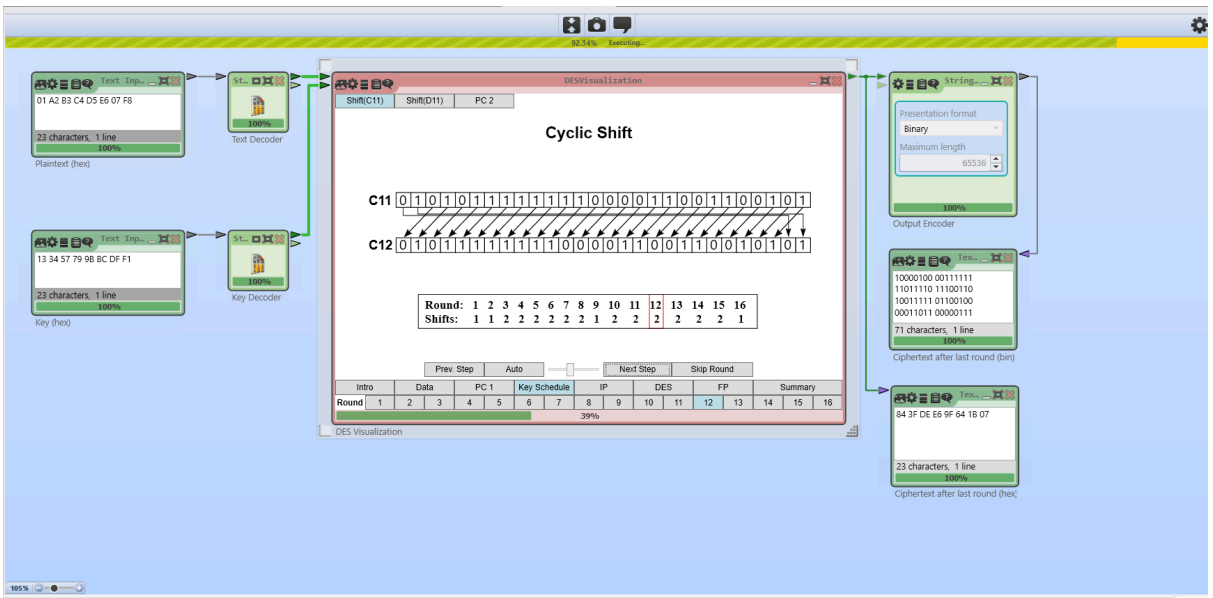

01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C10)
Shift(D10)
PC 2
Cyclic Shift
C10 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1
C11 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
36%
DES Visualization
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

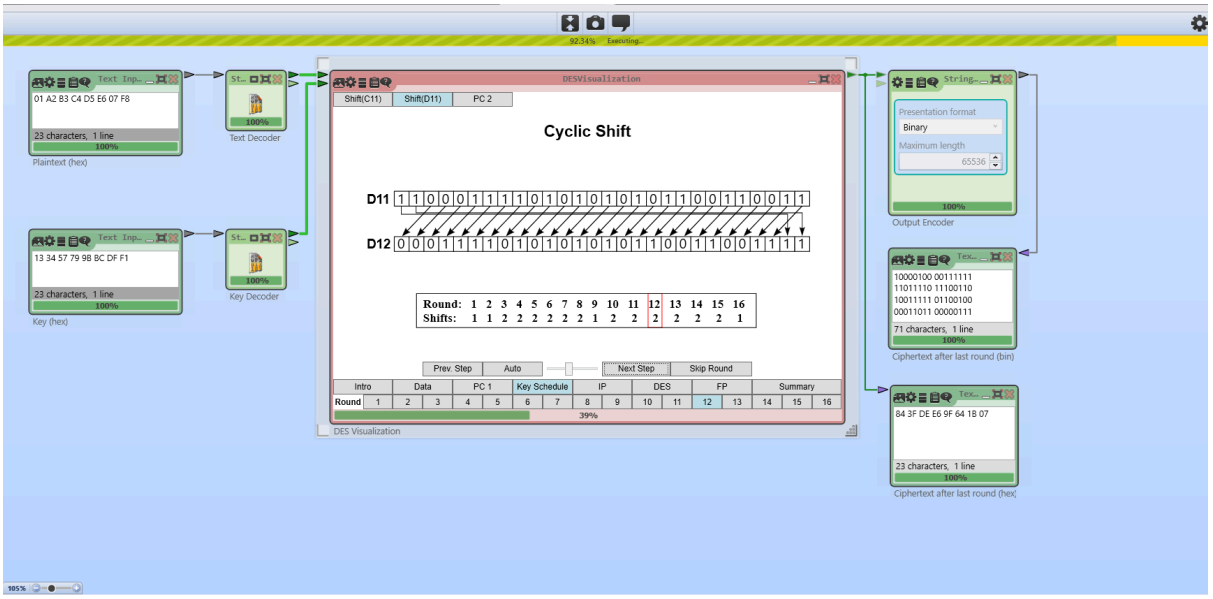

01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Shift(C10)
Shift(D10)
PC 2
Cyclic Shift
D10 1 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0
D11 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
36%
DES Visualization
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

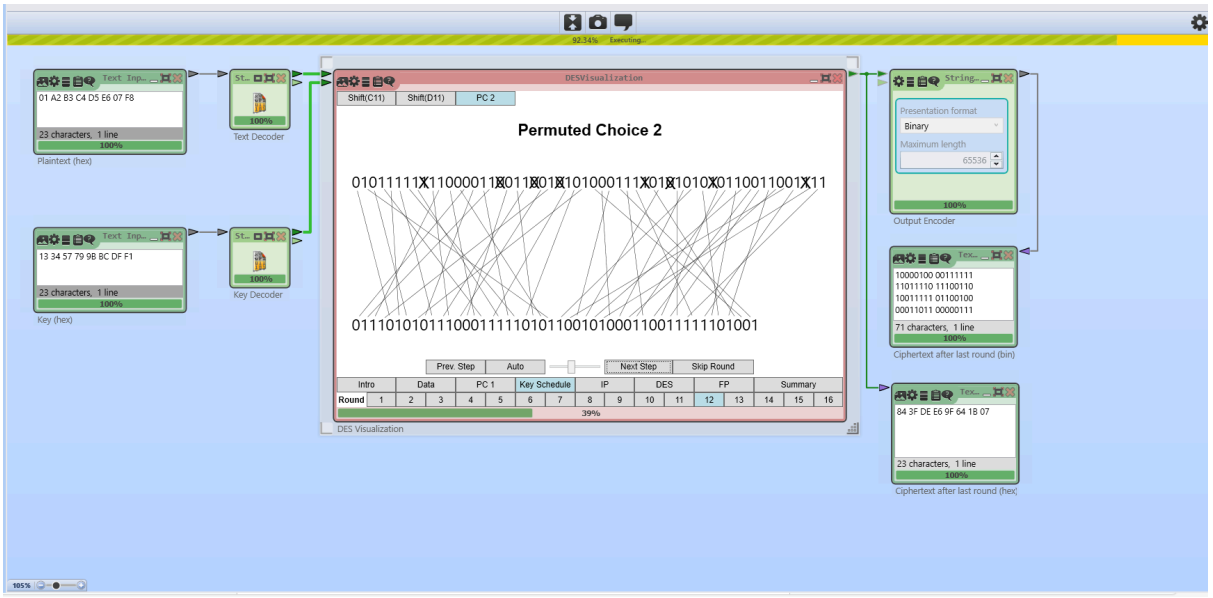

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C10)
Shift(D10)
PC 2
Permuted Choice 2
01010111X11110000X100X10X101110001X11X1010X01011001100X11
0010000101011111110100111101111011010011100001 10
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
36%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

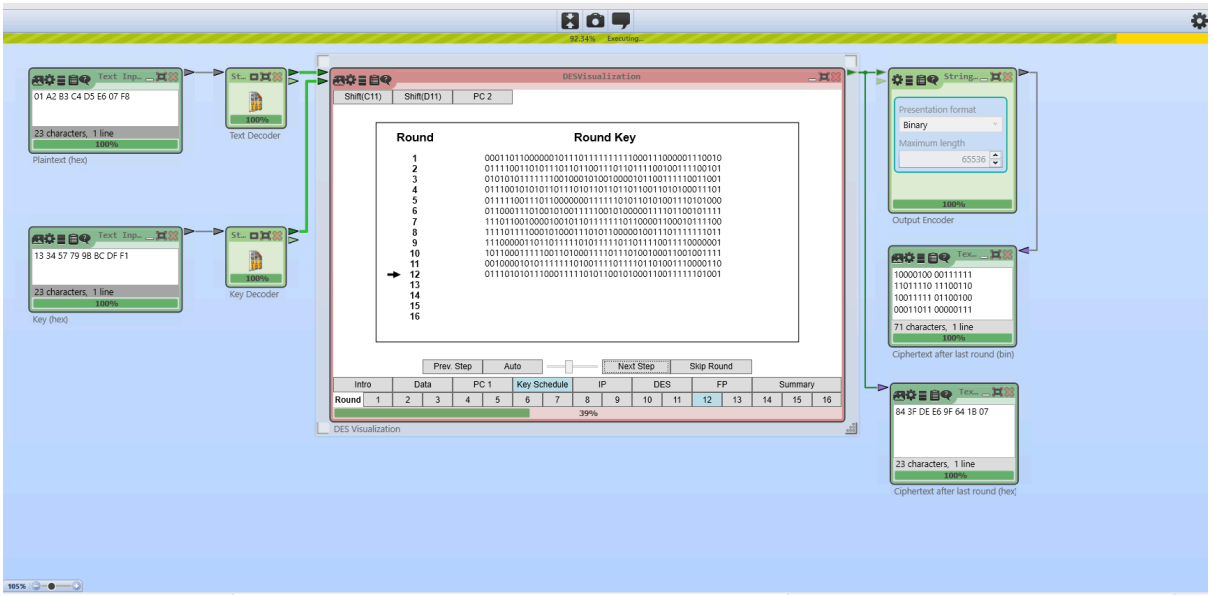

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C10)
Shift(D10)
PC 2
Round
Round Key
1 0001101100000010111011111111110001100000111 0010
2 0111100110101110110110011101101111001001110010 1
3 0101010111111100100010100000010110011111001 1001
4 0111001010101110110101101101101100110101000111 01
5 0111110011101100000001111110101101001110101000
6 0110001110100101001111100101000001111011001011 11
7 1110110100001001011011111110110000110001011110 0
8 1111011110001010001110101100000100111011111111 011
9 1110000011011111101011111011011110011110000001
10 1011000111110011010001111101101001000110010011 11
11 0010000101011111110100111101111011010011100001 10
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
36%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

Round 12:

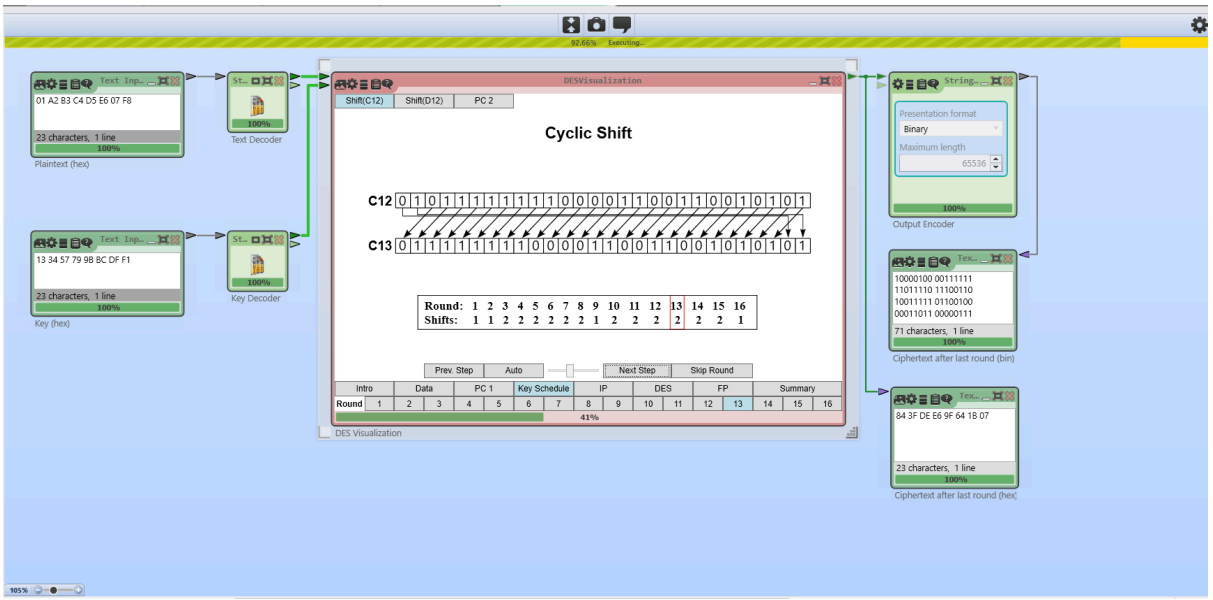

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C11)
Shift(D11)
PC 2
Cyclic Shift
C11 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1
C12 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
39%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

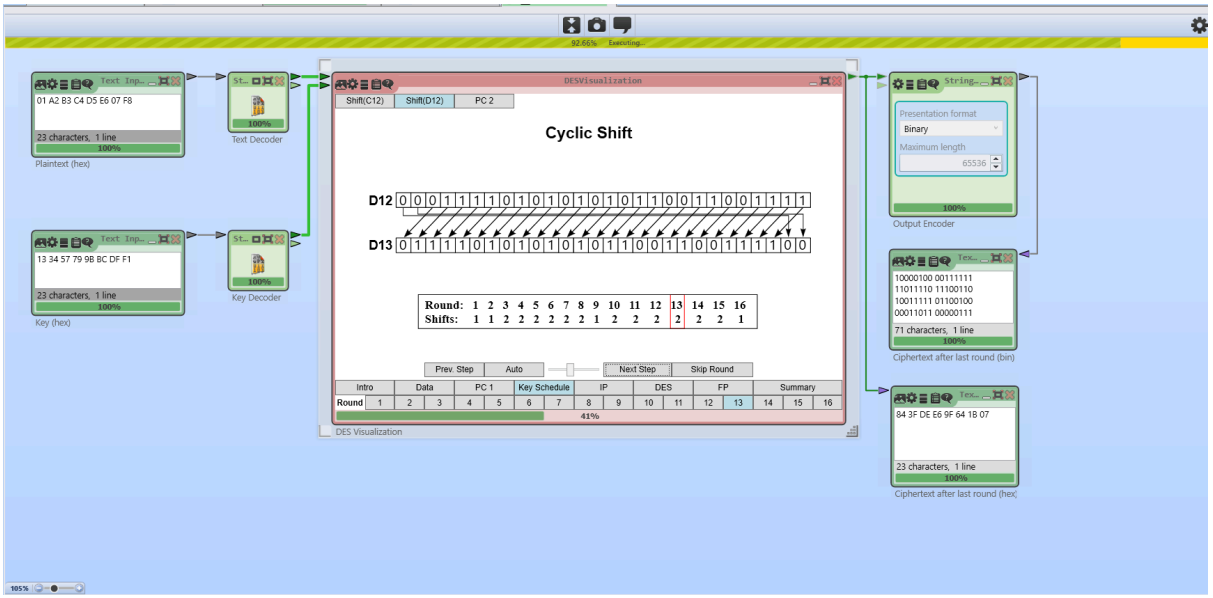

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C11)
Shift(D11)
PC 2
Cyclic Shift
D11 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1
D12 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
39%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

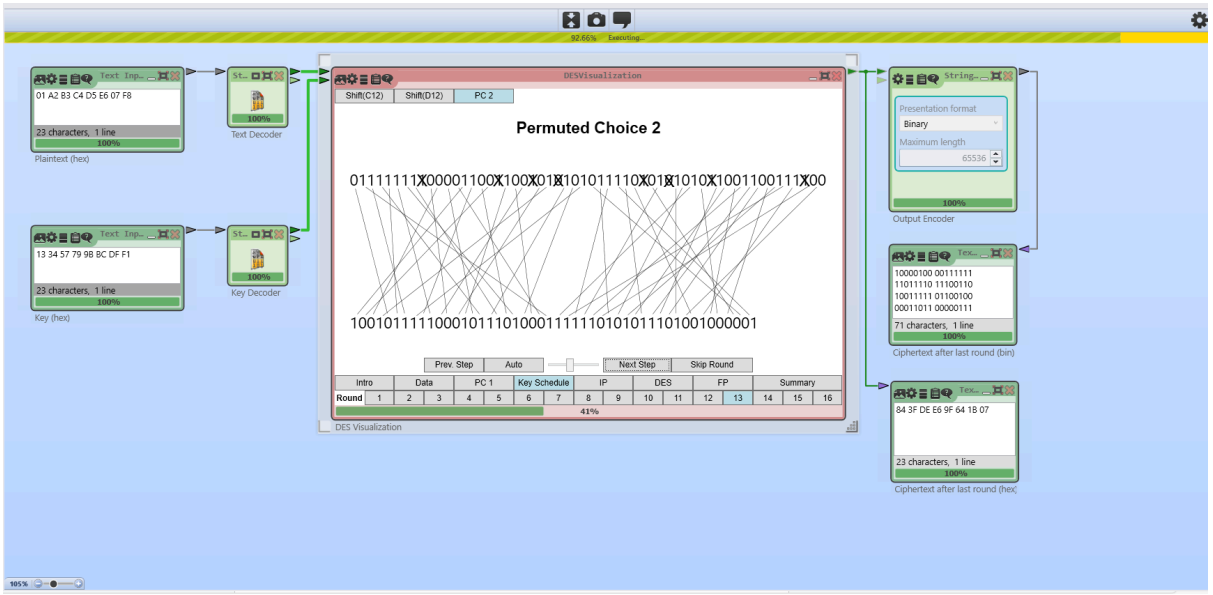

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C11)
Shift(D11)
PC 2
Permuted Choice 2
01011111X11000011X011X01X101000111X01X1010X0110011001X11
011101010111000111110101100101000110011111101001
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
39%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

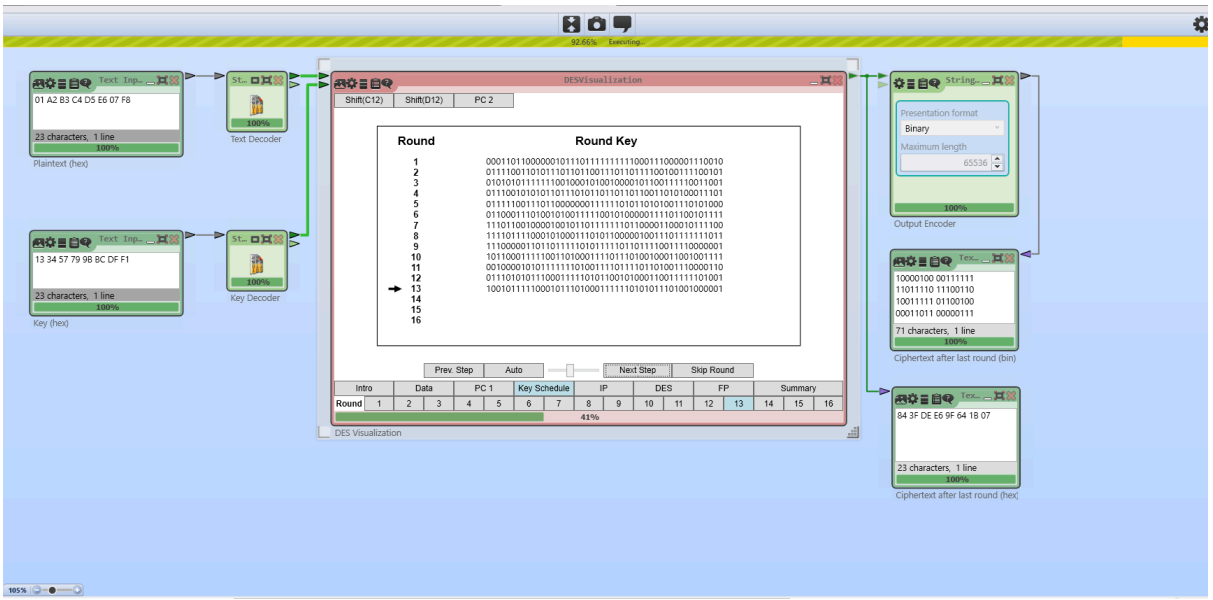

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C11)
Shift(D11)
PC 2
Round
Round Key
1 0001101100000010110111111111110001110000011100010
2 0111100110101110110110011001111011011110010011100101
3 0101010111111001000101001000010110011111001001
4 0111001010101101110101101101101101101001010100011101
5 0111110011101100000000111111010110101001110101000
6 0110001110100101001011110010100000111101100101111
7 1110110010000100101101111111101100001100001011100
8 1111011100010100011101011100000010011101111111011
9 1110000011101011111101011111101101111001111000001
10 1011000111110011010001111011110100100011001001111
11 0010000101011111110100111101110110100111000110
12 0111010101110001111101011001010001100111111001
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
39%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

Round 13:

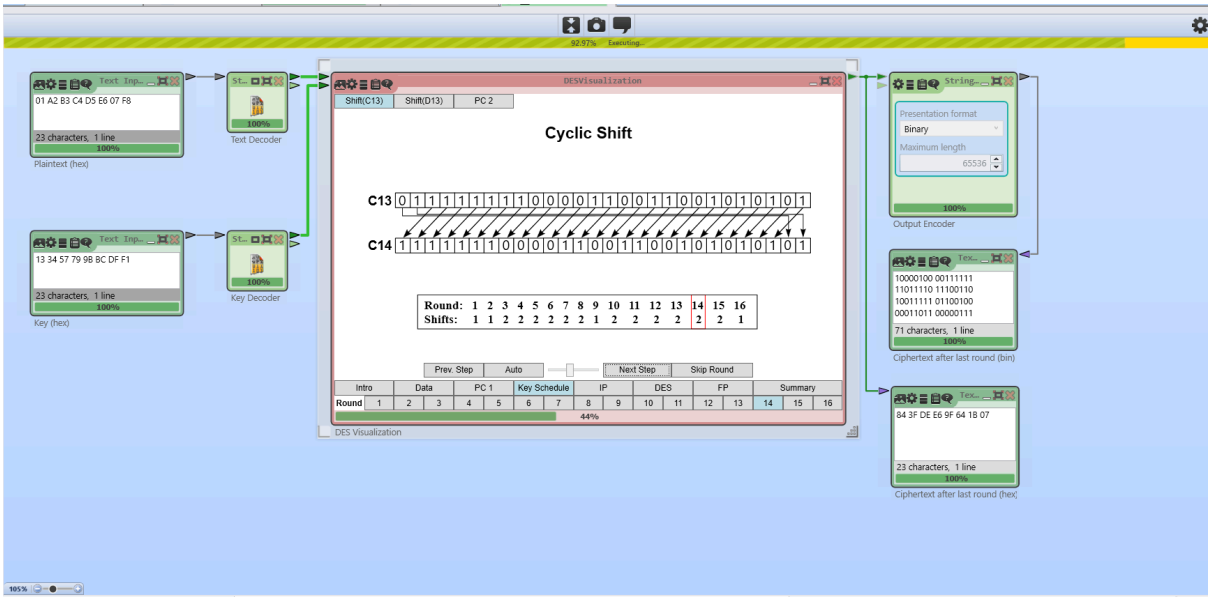

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C12)
Shift(D12)
PC 2
Cyclic Shift
C12 0 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1
C13 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
41%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

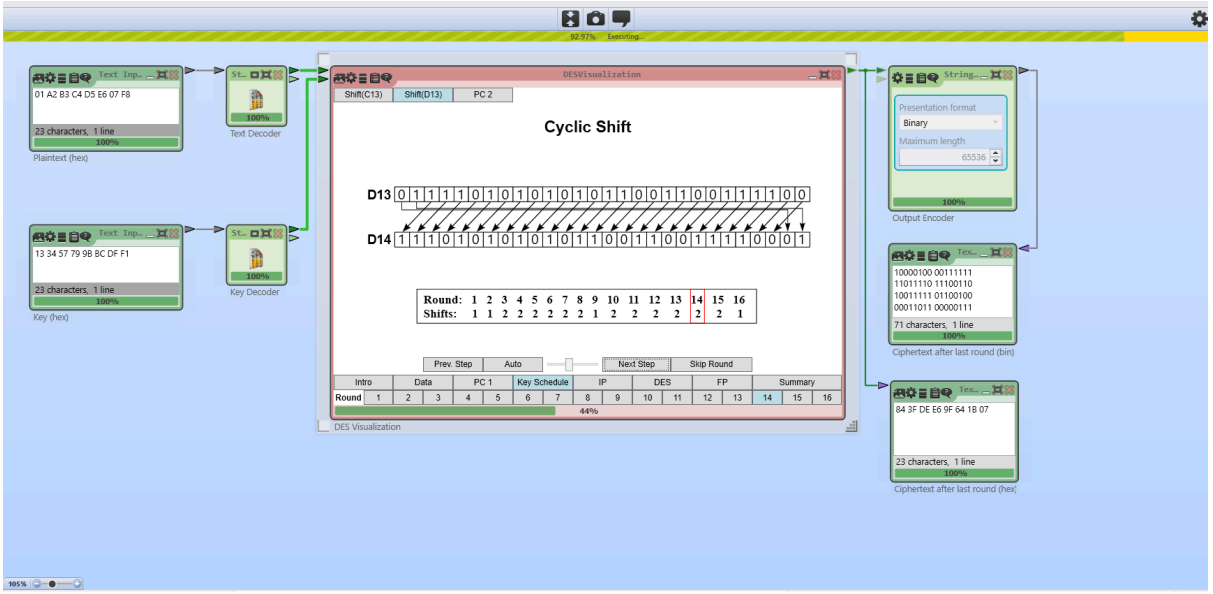

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C12)
Shift(D12)
PC 2
Cyclic Shift
D12 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1
D13 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 0 0
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
41%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

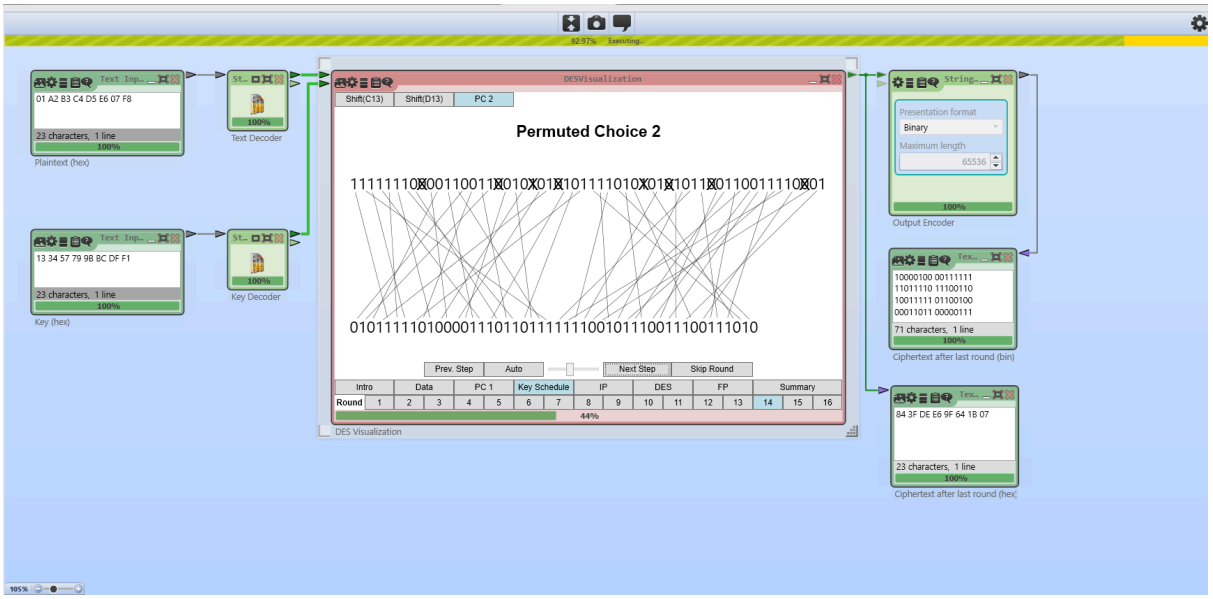

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C12)
Shift(D12)
PC 2
Permuted Choice 2
01111111X00001100X100X01X10101111 0X01X1010X1001100111X00
1001011111000101110100011111101010111010010000 01
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
41%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

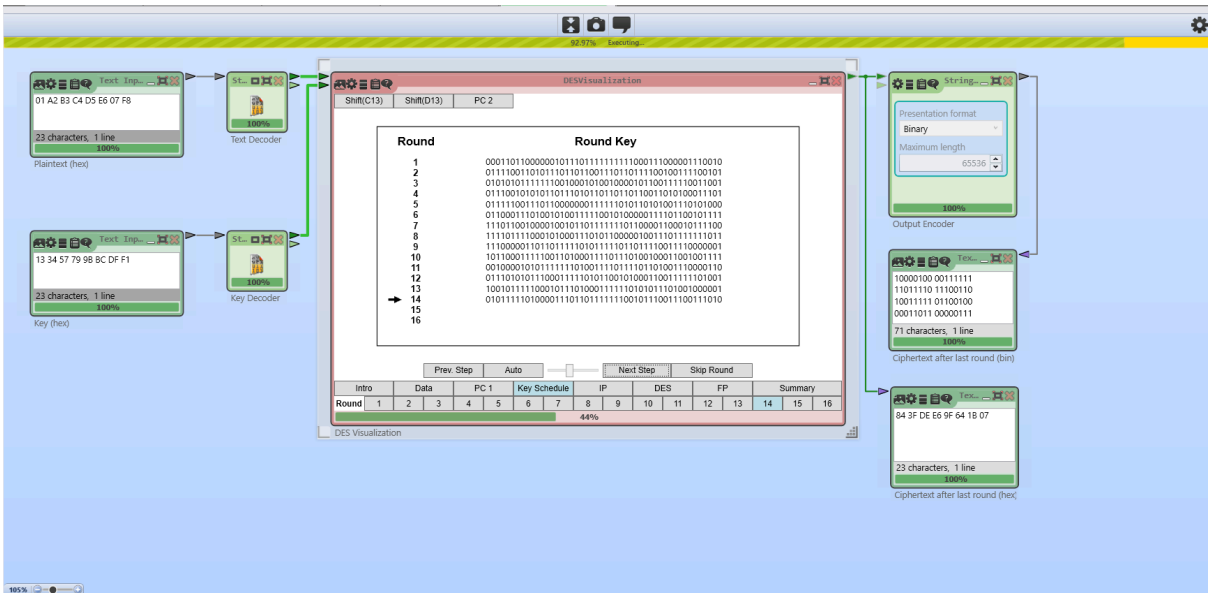

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C12)
Shift(D12)
PC 2
Round
Round Key
1 0001101100000001011101111111111000111000001110010
2 0111100110101111011011001111011011111001001111100101
3 0101010111111100100010100100001011001111110011001
4 0111001010101101110101101101101101101001101010001101
5 0111100111011000000011111101101101010011101010001000
6 0110001110100101001111100101000001111011001011111
7 1110110010000100101011111111101100001100010111100
8 1111011110001010001110101100000100111011111111011
9 1110000010110111110101111101011110110111001111000001
10 1011000111110011010001111101110100100011001001111
11 0010000101011111110100111101111101101001110000110
12 0111010101110001111101011001010001001111111101001
13 1001011111000101110100011111101010111010010000001
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
41%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

Round 14:

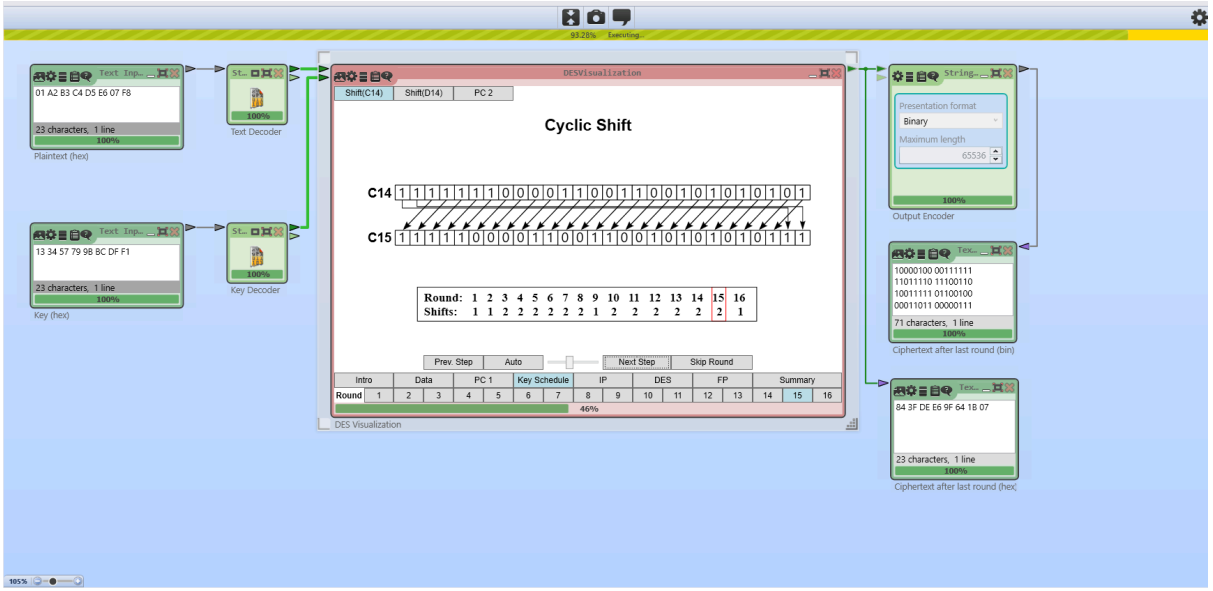

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Shift(C13)
Shift(D13)
PC 2
Cyclic Shift
C13 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1
C14 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
44%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

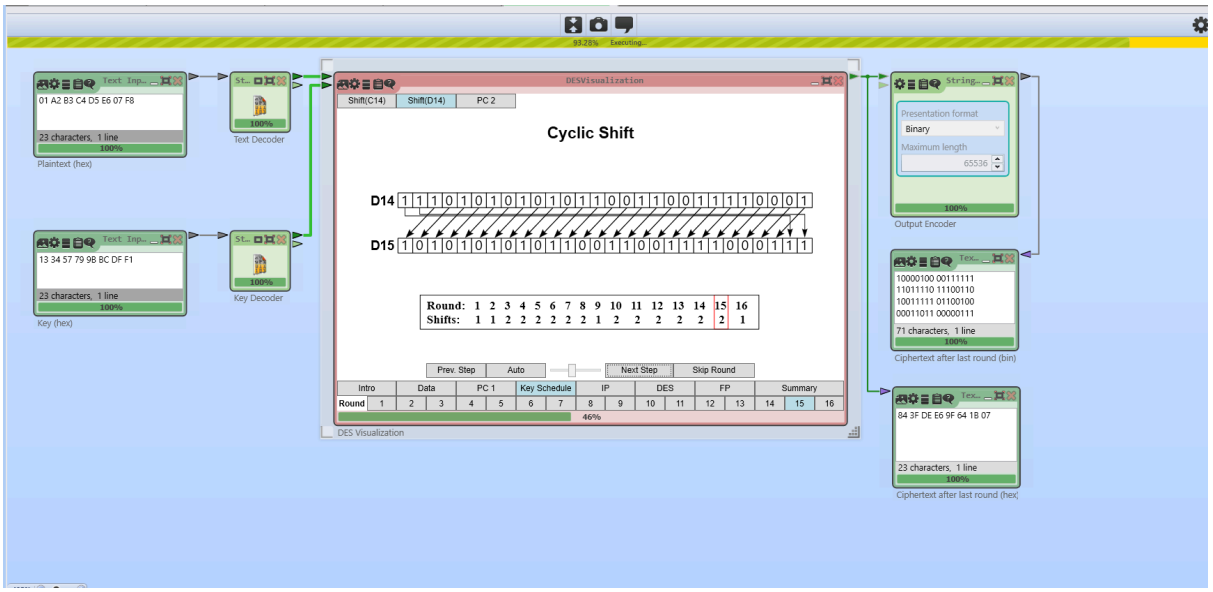

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C13)
Shift(D13)
PC 2
Cyclic Shift
D13 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0
D14 1 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
44%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

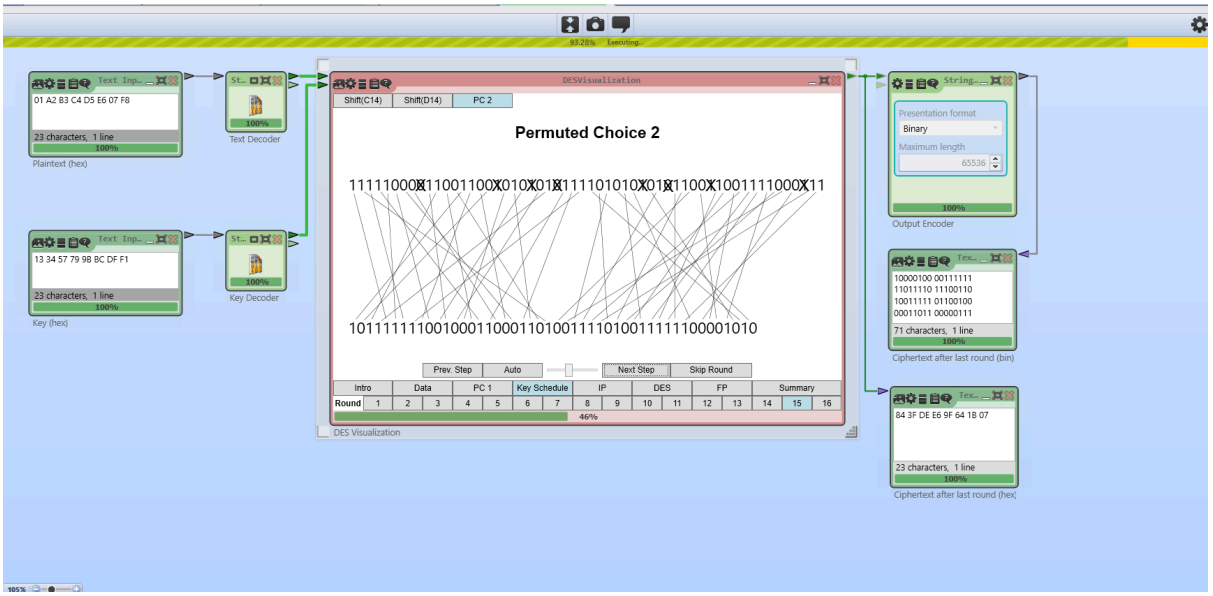

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C13)
Shift(D13)
PC 2
Permuted Choice 2
11111110X00110011X010X01X101111010X01X1011X0110011110X01
0101111101000011101101111111001011100111001110 10
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
44%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

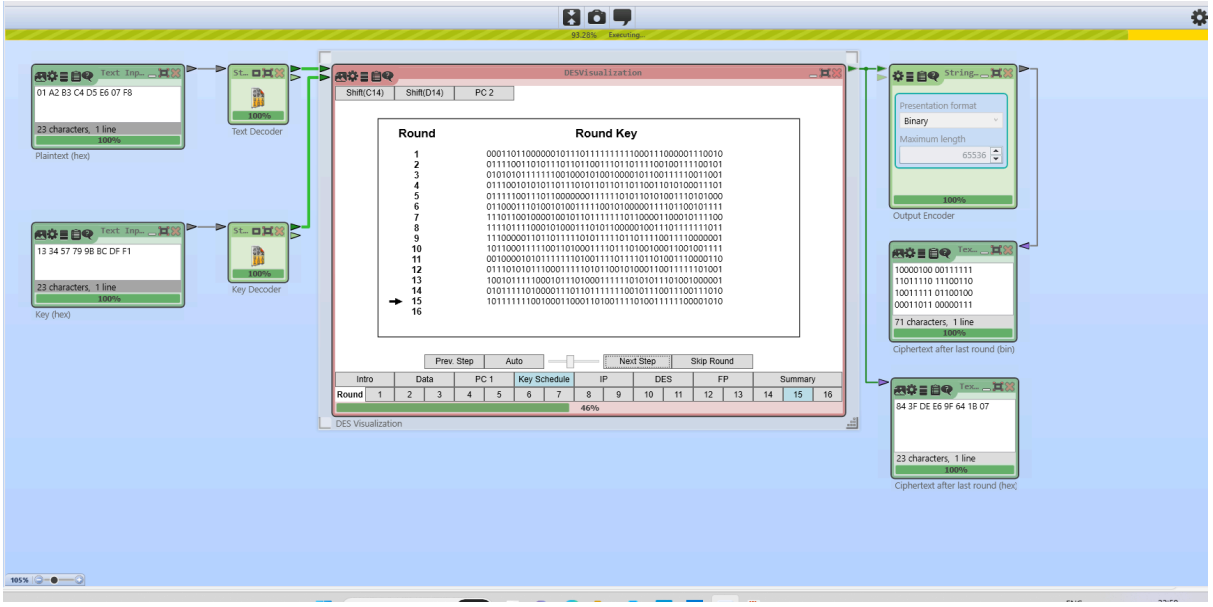

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C13)
Shift(D13)
PC 2
Round
Round Key
1 0001101100000010111011111111110001110000011110010
2 0111100111011110110110011011101101111100100111100101
3 0101010111111001000101001000010110011111001 1001
4 0111001010110111101011011011011011001101010011101
5 0111111001110110000000111111011011010110110110101000
6 0110001110100101001111100101000001111011001011111
7 1110110010000100101101111111101100001100010111100
8 1111011110001010001110101100000100110111111111011
9 1110000011011011110101111101101111001111000001
10 1011000111110011010001111011110100100011001001111
11 0010000101011111110100011110111101101001110000110
12 0111010101110001111010101001010001001111111001
13 1001011111100010111010001111111010101110100100001
14 0101111101000011101101111111100101110011100111010
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
44%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

Round 15:

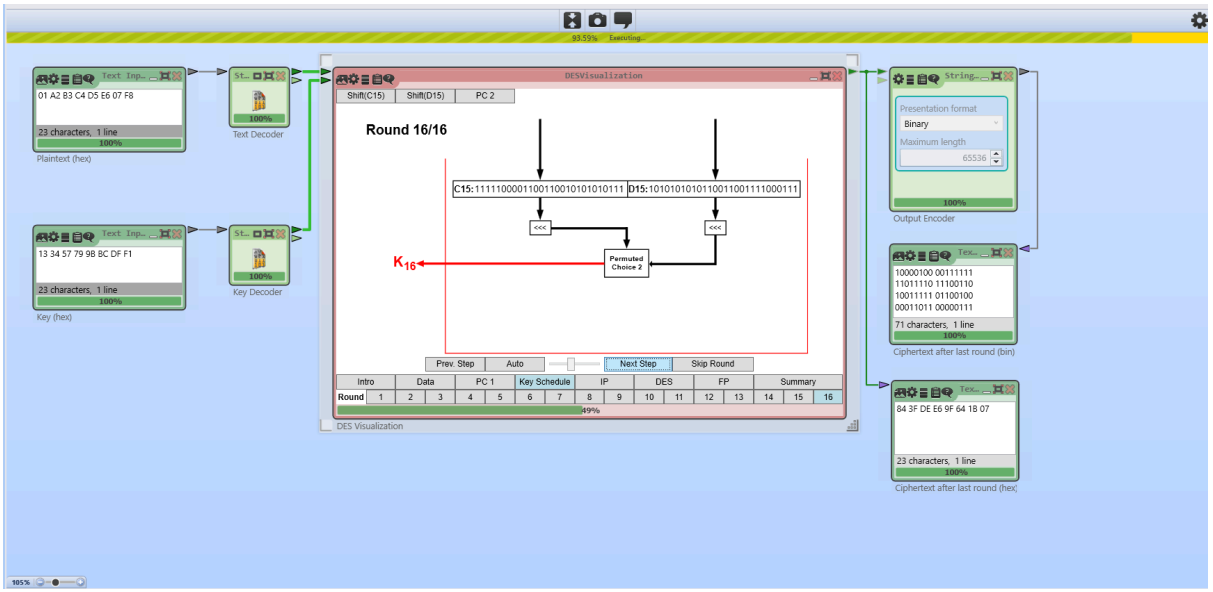

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C14)
Shift(D14)
PC 2
Cyclic Shift
C14 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 0 1
C15 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
46%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

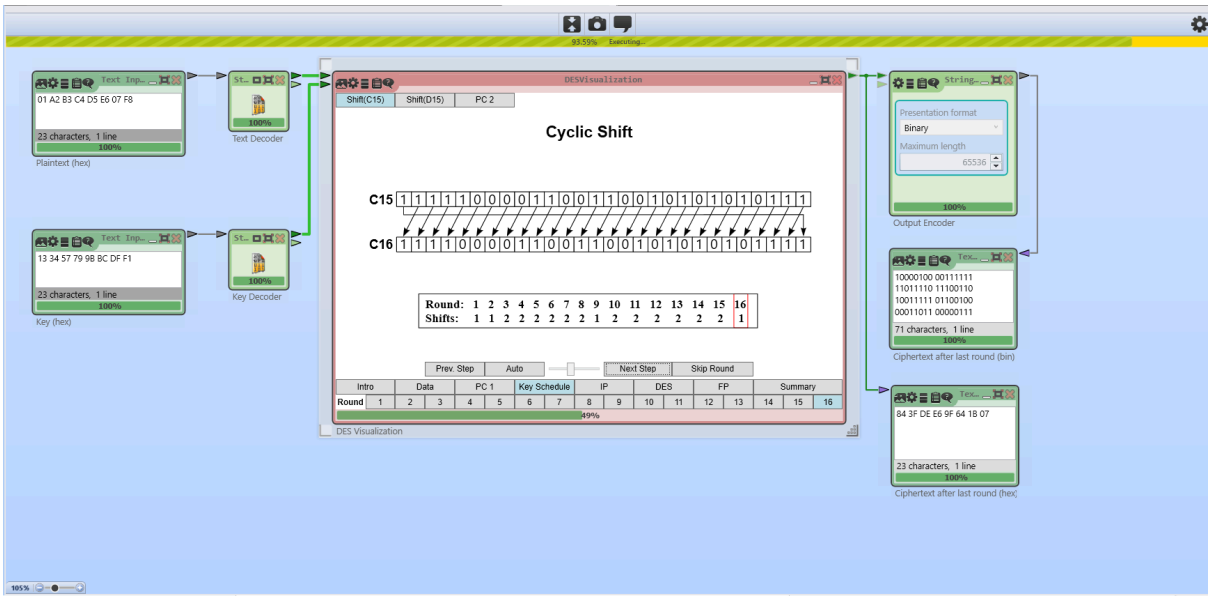

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C14)
Shift(D14)
PC 2
Cyclic Shift
D14 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1
D15 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
46%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

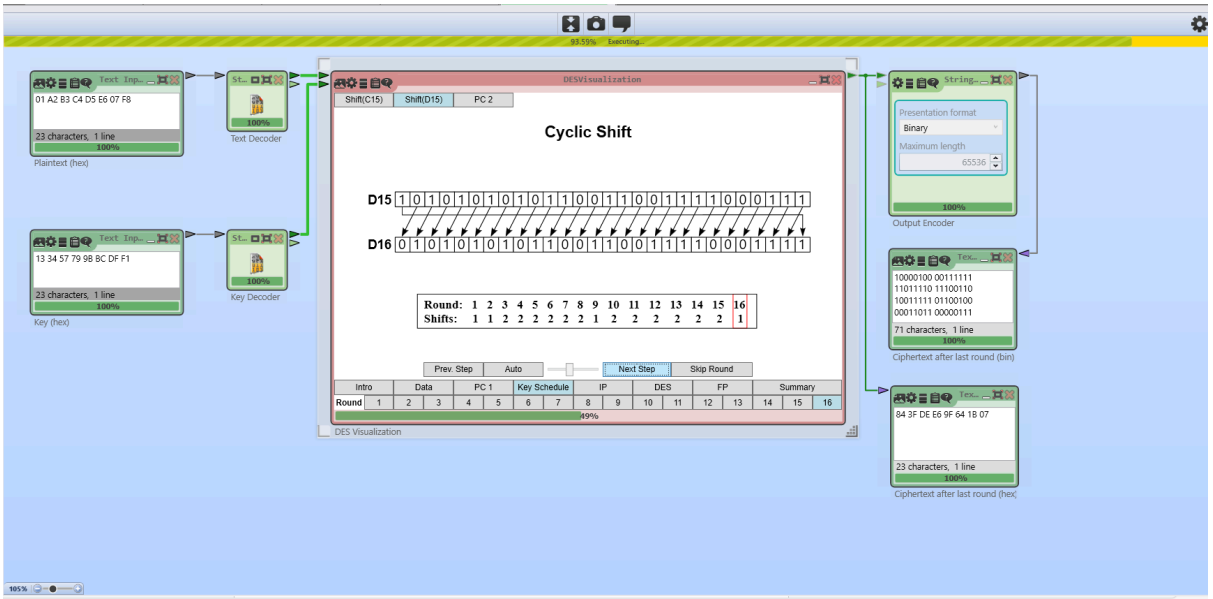

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C14)
Shift(D14)
PC 2
Permuted Choice 2
11111000X11001100X010X01X1111010 10X01X1100X1001111000X11
1011111110010001100011010011110100111111000010 10
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
46%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

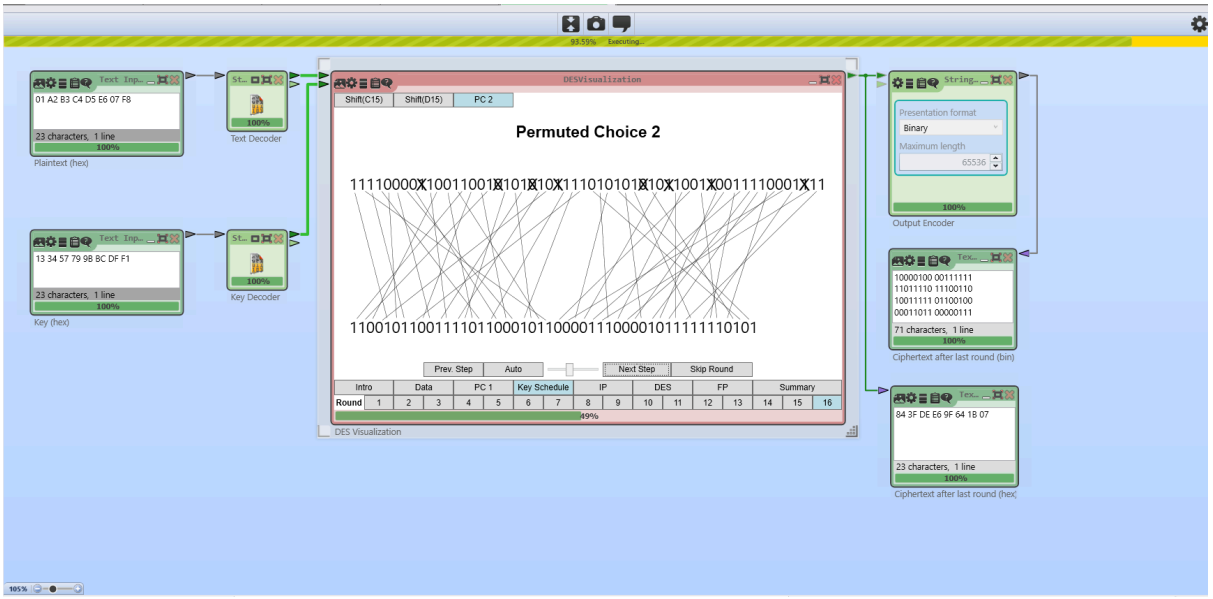

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C14)
Shift(D14)
PC 2
Round
Round Key
1 0001101100000010111011111111111000111000001110010
2 0111100110101110110110011101101111001001111001101
3 0101010111111110010010100100001011001111100011001
4 0111001010101101110101101101101100110110100001101
5 0111100111011000000011111101101101001110101000
6 0110001110100101001111100101000001111011001011
7 1110110010000100101101111111101100001100010111100
8 1111011110001010001110101100000100111011111111011
9 1110000011010111110101111101101101100111100000001
10 1011000111110011010001111101101001000110011011111
11 0010000101011111110010111111101101100111000110
12 0111010101110001111101010110010100011001111110100
13 1001011111000101110100111111010101110100100001
14 0101111101000011101101111111001011100111001110
15 1011111110010001100011010011110100111111000010
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
46%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

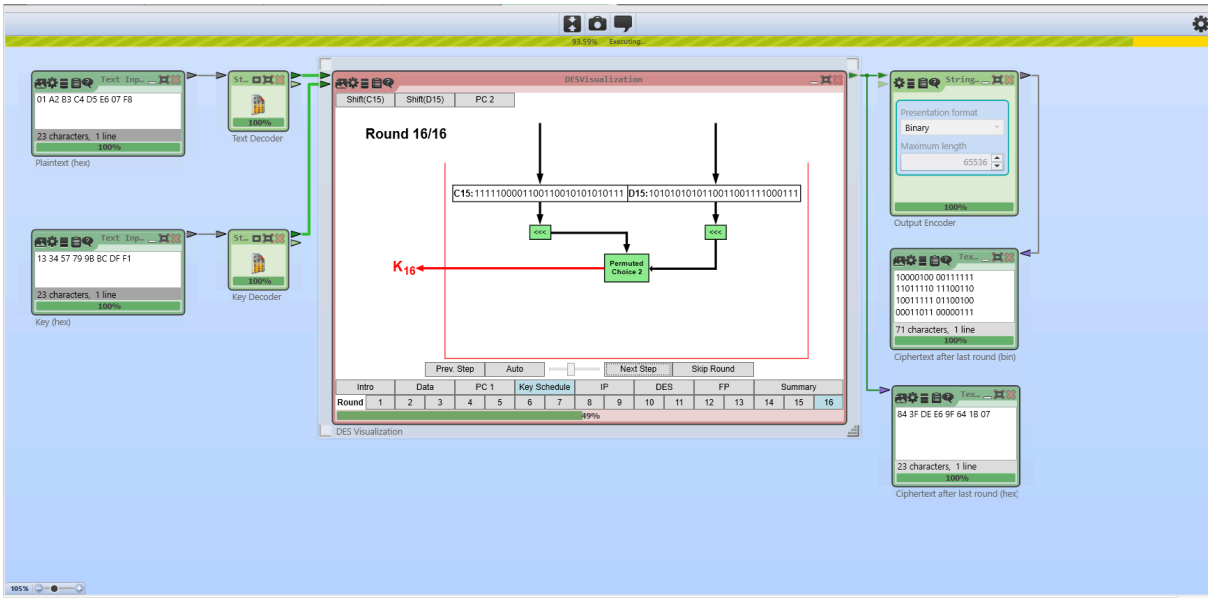
Round 16:

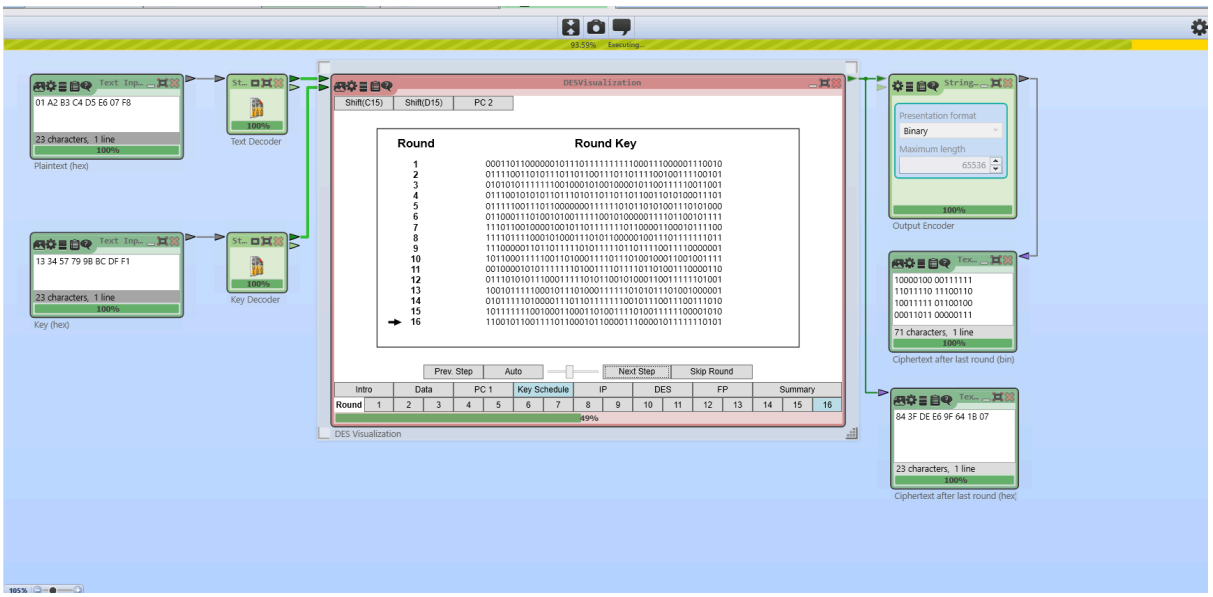

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Round 16/16
C15: 1111100001100110010101010111
D15: 1010101010110011001111000111
<<<
<<<
Permuted Choice 2
K16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

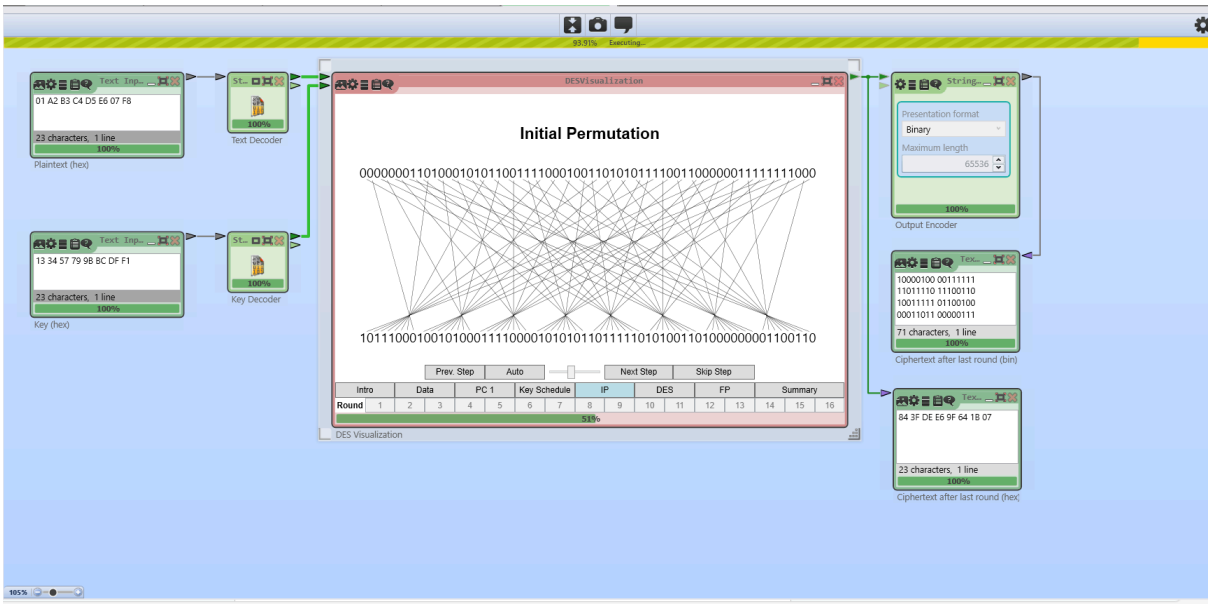

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Cyclic Shift
C15 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1
C16 1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Cyclic Shift
D15 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1
D16 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1
Round: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Shifts: 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

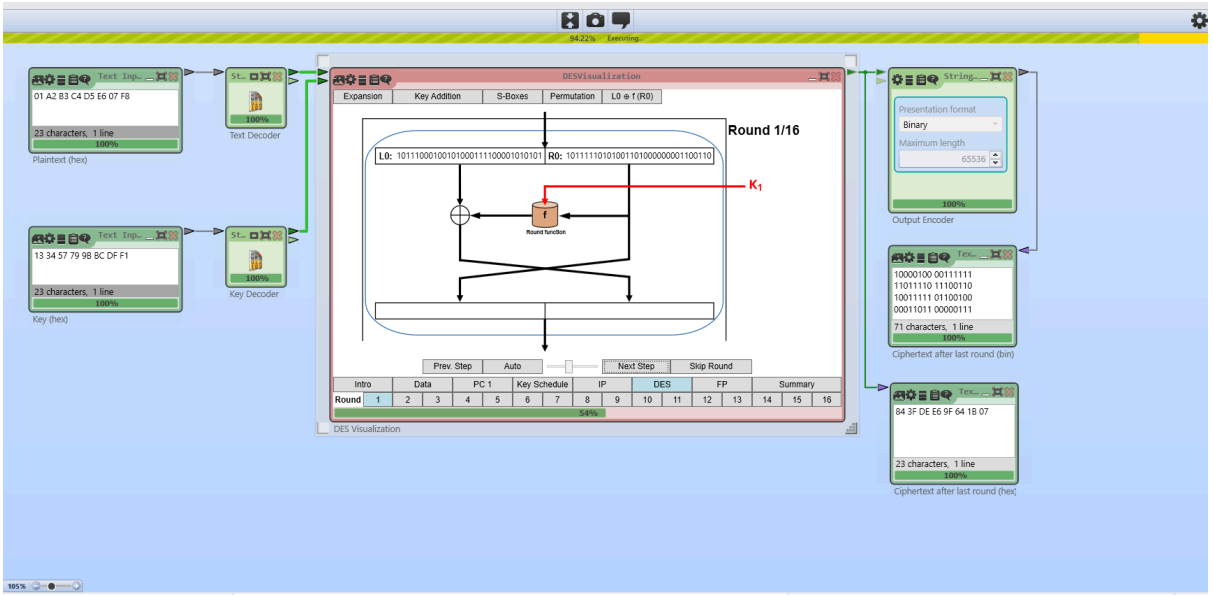

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Permuted Choice 2
11110000X10011001X101X10X11101010 1X10X1001X0011110001X11
11001011001111011000101100001110000101111110101
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

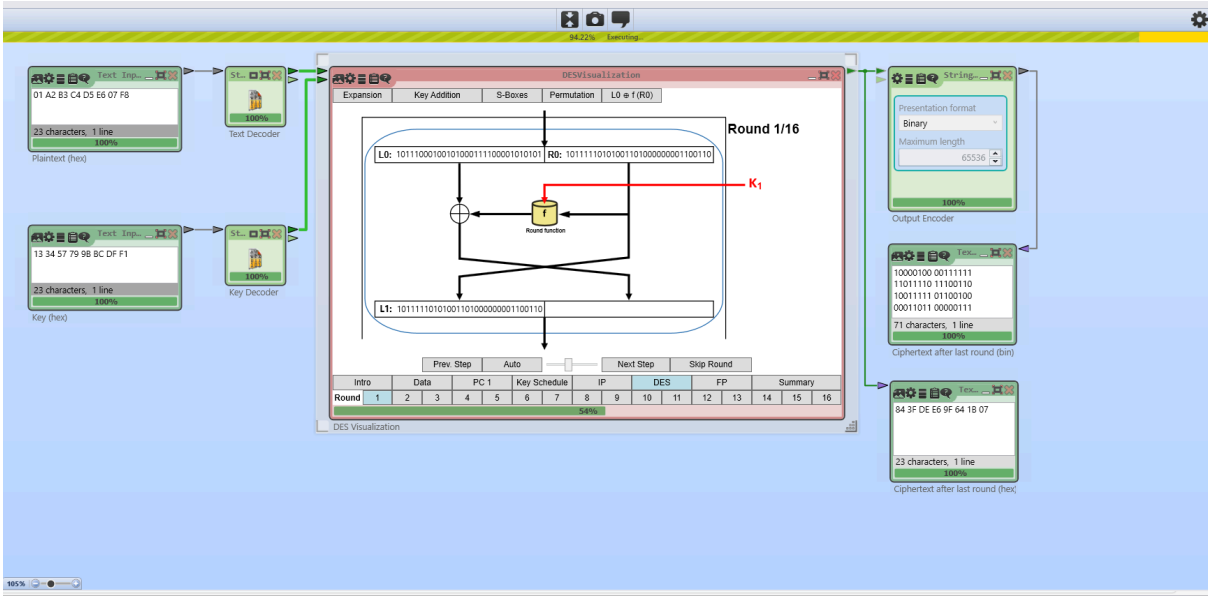

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Round 16/16
C15: 1111100001100110010101010111
D15: 1010101010110011001111000111
<<<
<<<
Permuted Choice 2
K16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

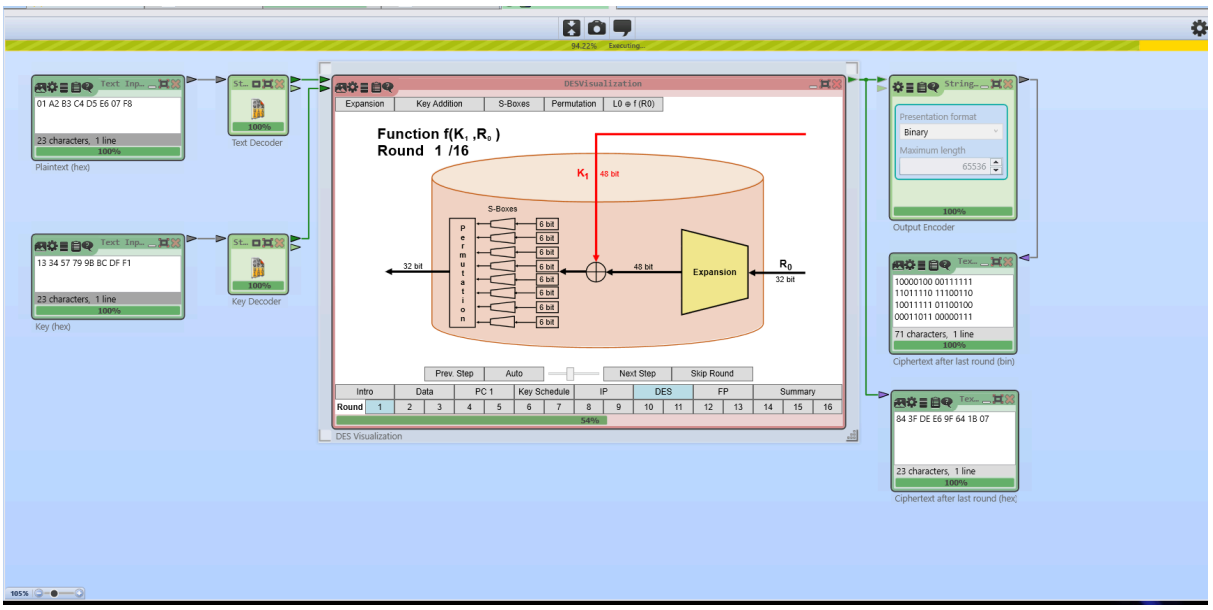

93.55% Executing...
Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Shift(C15)
Shift(D15)
PC 2
Round
Round Key
1 0001101000000101101111111111000111000001110010
2 0111001101011101101100111001101101111001001110010 1
3 0101101111111001000101001000101100111110011001
4 0111001010101101110101101101101100110101000111101
5 0111110011101100000000111111010110101001110101000
6 0110001110100101001111100101000001111011001011 1
7 1110110010000100101101111111101100001100010111100
8 1111011110001010001110101100000100111011111111011
9 1110000011011111101011111101101111001111000001
10 1011000111110011010001111011101001000110010011 11
11 0010000101011111101001111011110110100110000110
12 0111010101110001111101011001010001100111111001
13 1001011111000101110100011111101010111010010000 01
14 0101111101000011101101111111000101110011100111010
15 1011111110010001100010101001111010011111100001010
16 1100101100111101100010110000111000010111111101 01
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
49%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

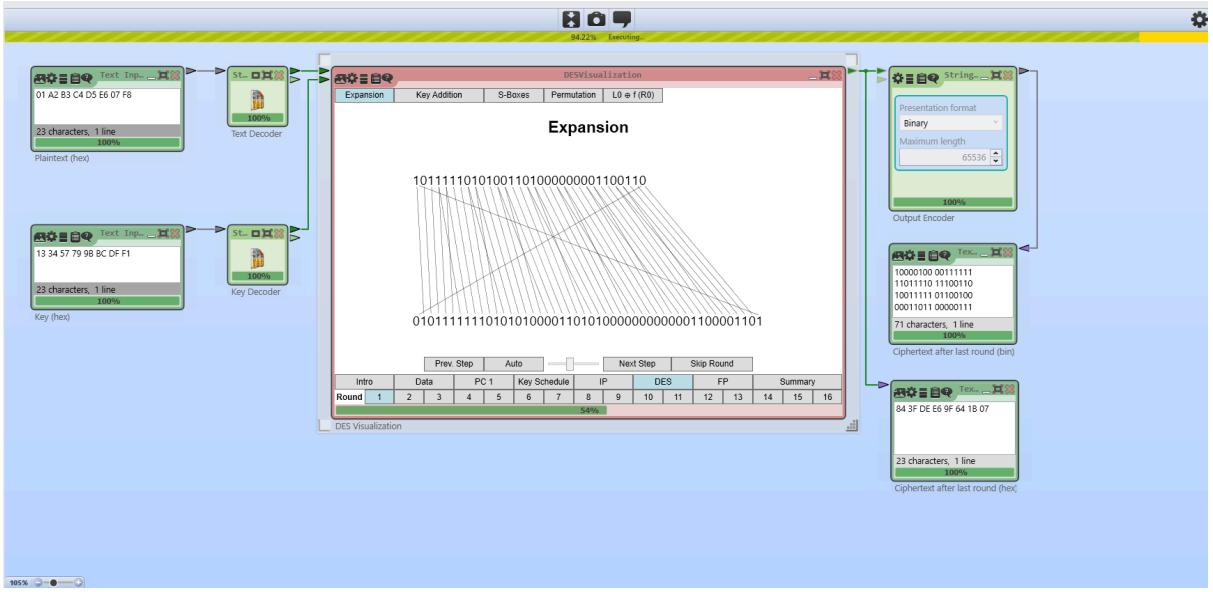

93.91% Executing...
Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Initial Permutation
0000000110100010101100111100010011010101111001100000011111111000
1011100010010100011110000101101101111101010011010000000011001 10
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
51%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

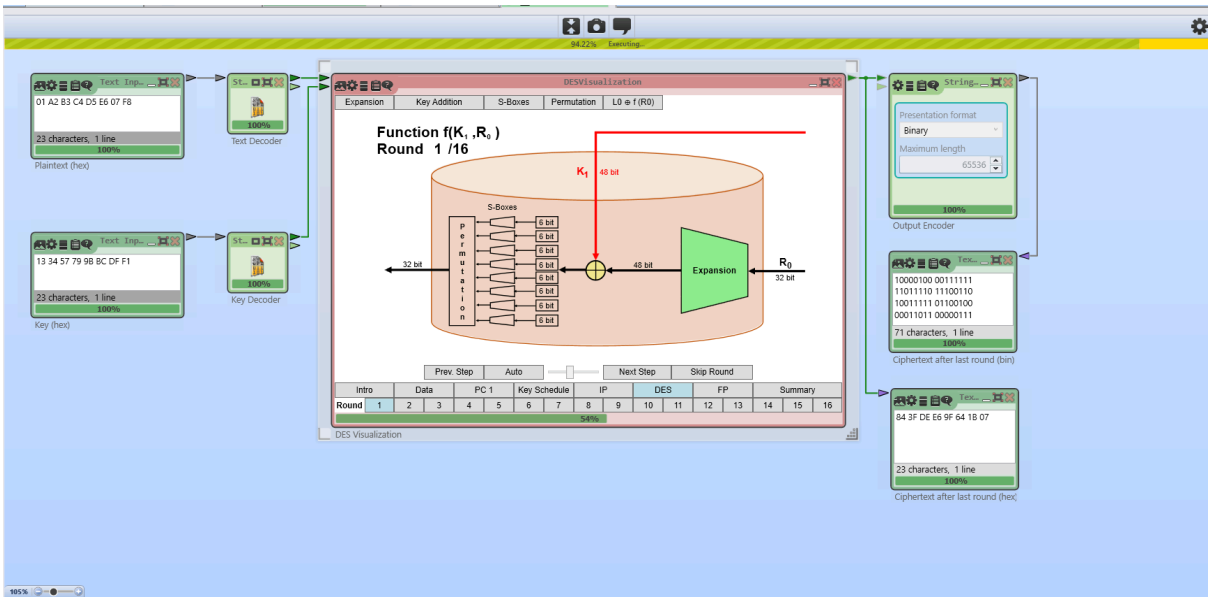
Encryption:

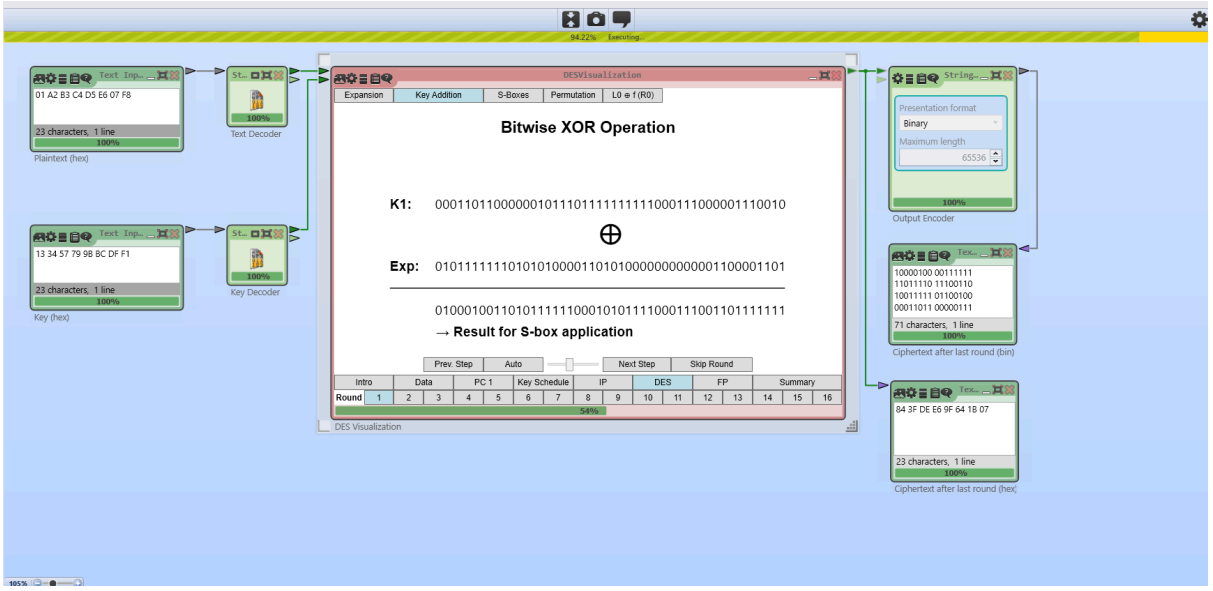

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Round 1/16
L0: 10111000100101000111100001010101
R0: 10111110101001101000000001100110
K1
f
Round function
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

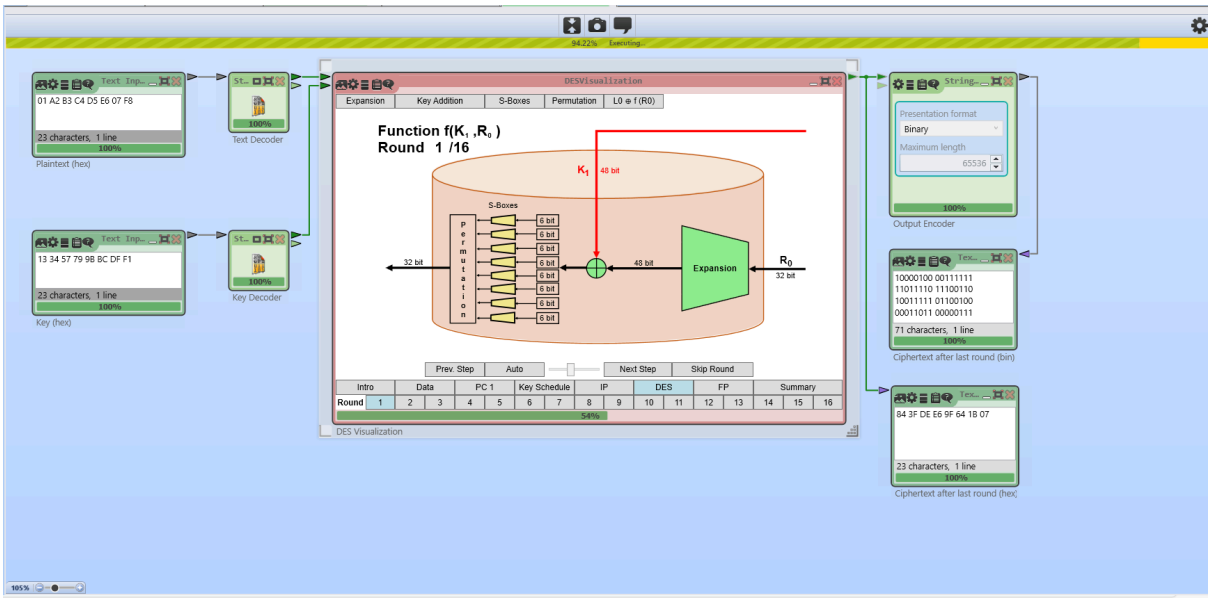

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Round 1/16
L0: 10111000100101000111100001010101
R0: 10111110101001101000000001100110
K1
f
Round function
L1: 10111110101001101000000001100110
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

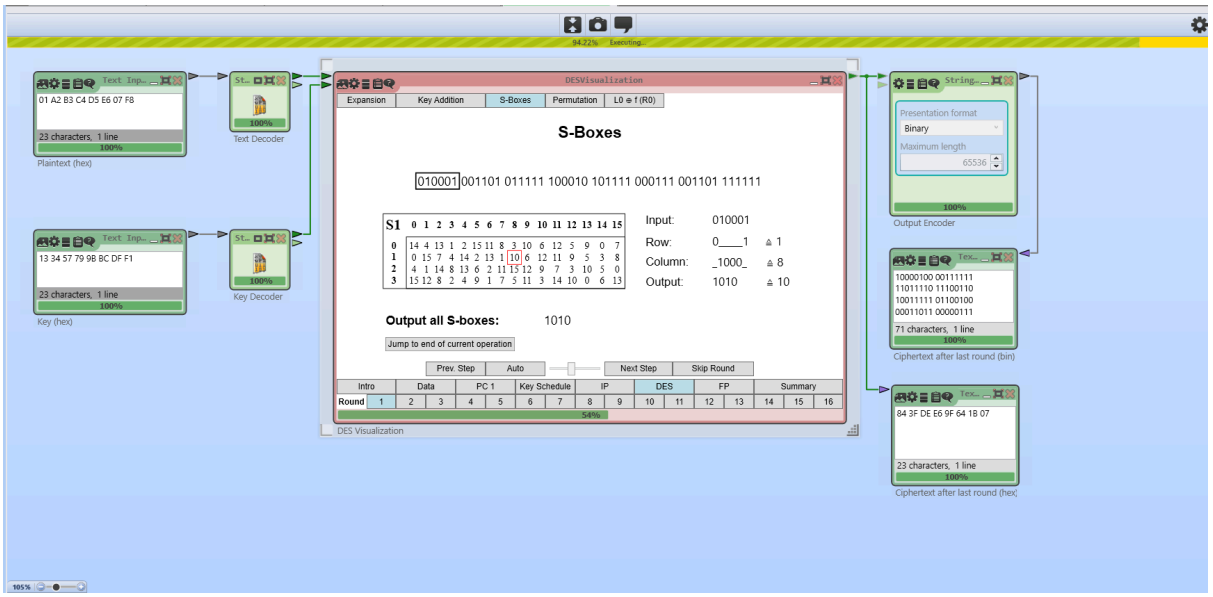

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Function f(K1 ,R0)
Round 1 /16
K1
48 bit
S-Boxes
Permutation
6 bit
32 bit
48 bit
Expansion
R0
32 bit
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

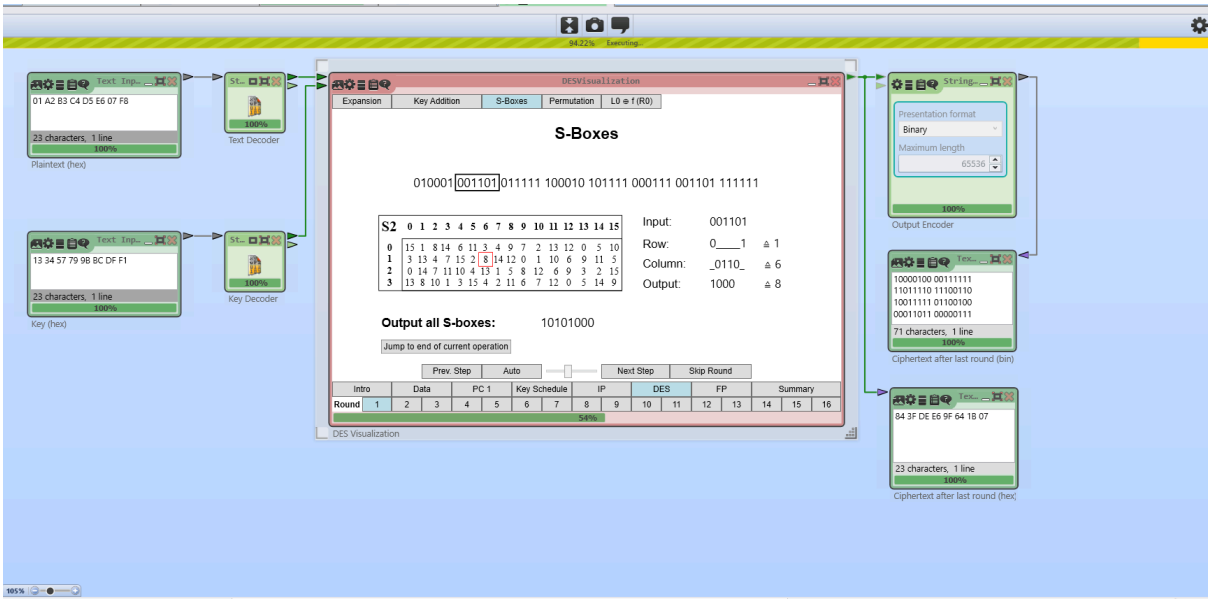

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Expansion
101111101010011010000000011001 10
0101111111010101000011010100000000000011000011 01
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

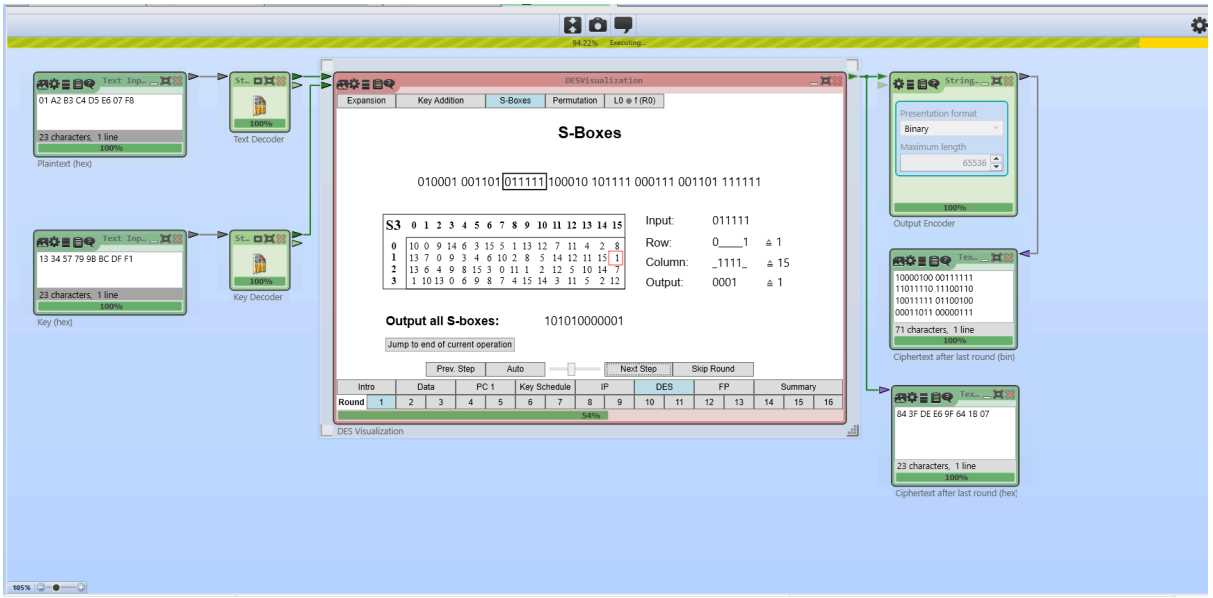

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Function f(K1 ,R0)
Round 1 /16
K1
48 bit
S-Boxes
Permutation
6 bit
32 bit
48 bit
Expansion
R0
32 bit
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

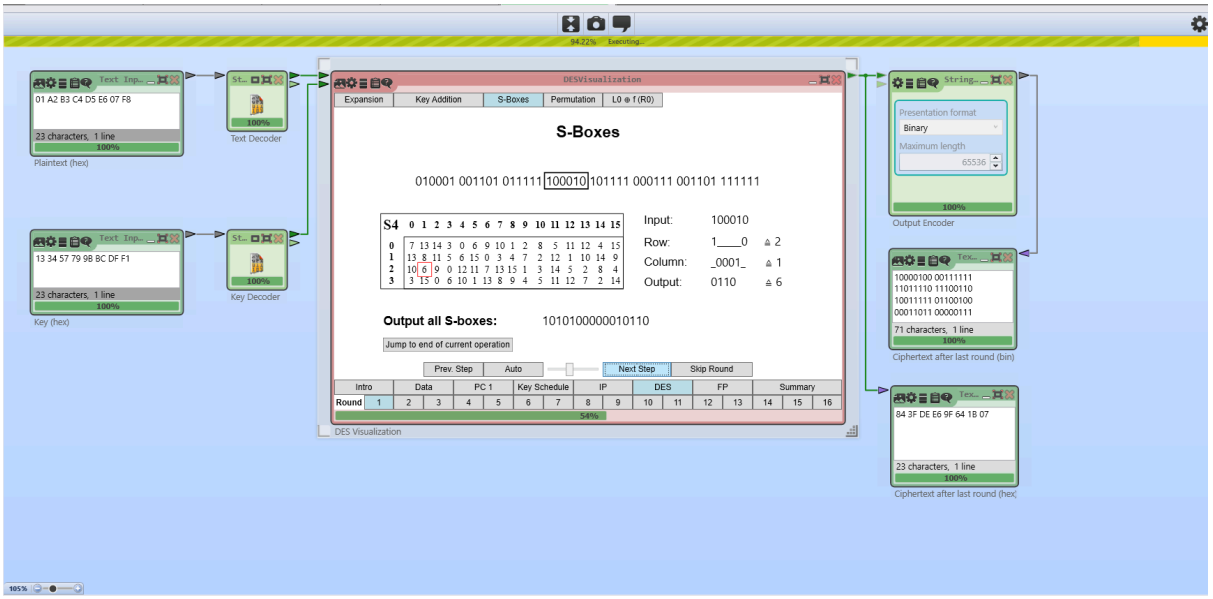

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Bitwise XOR Operation
K1: 000110110000001011101111111111000111000001110010
⊕
Exp: 010111111101010100001101010000000000001100001101
010001001101011111100010101111000111001101111111
→ Result for S-box application
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

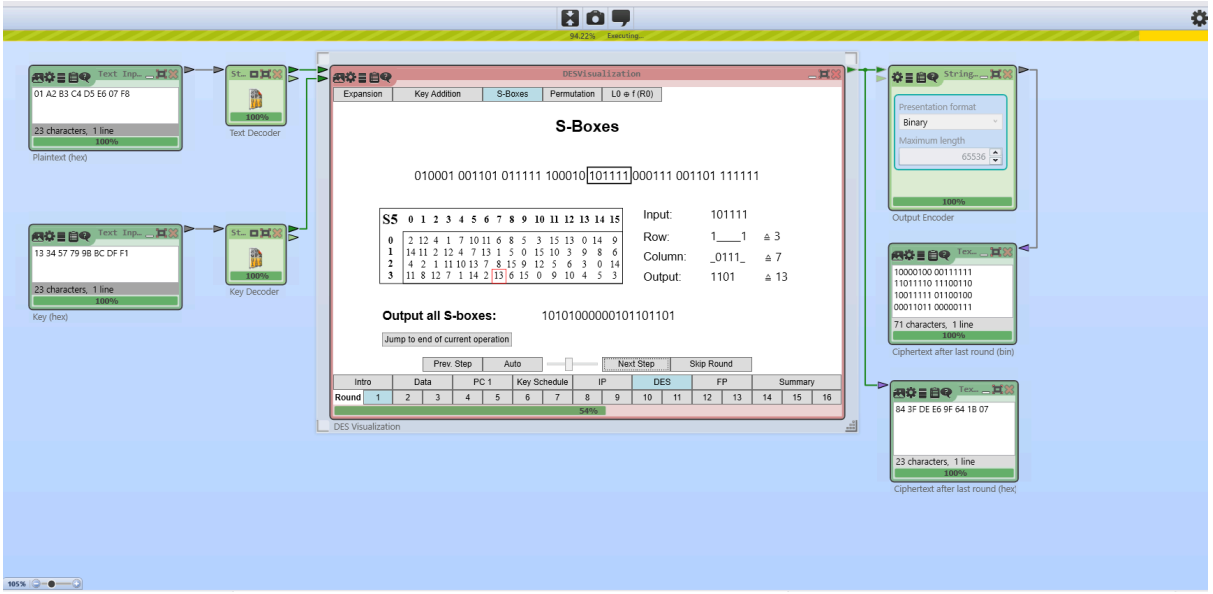

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Function f(K1 ,R0)
Round 1 /16
K1
48 bit
S-Boxes
6 bit
32 bit
48 bit
Expansion
R0
32 bit
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

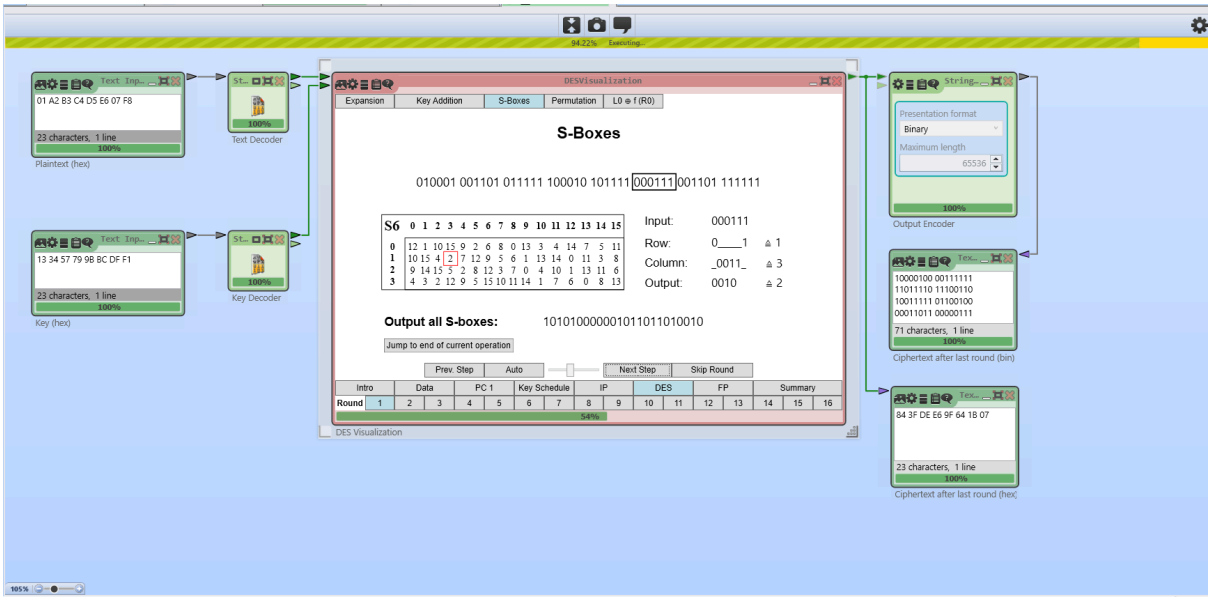

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
1 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
2 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
3 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13
Input: 010001
Row: 0____1 ≙ 1
Column: _1000_ ≙ 8
Output: 1010 ≙ 10
Output all S-boxes: 1010
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

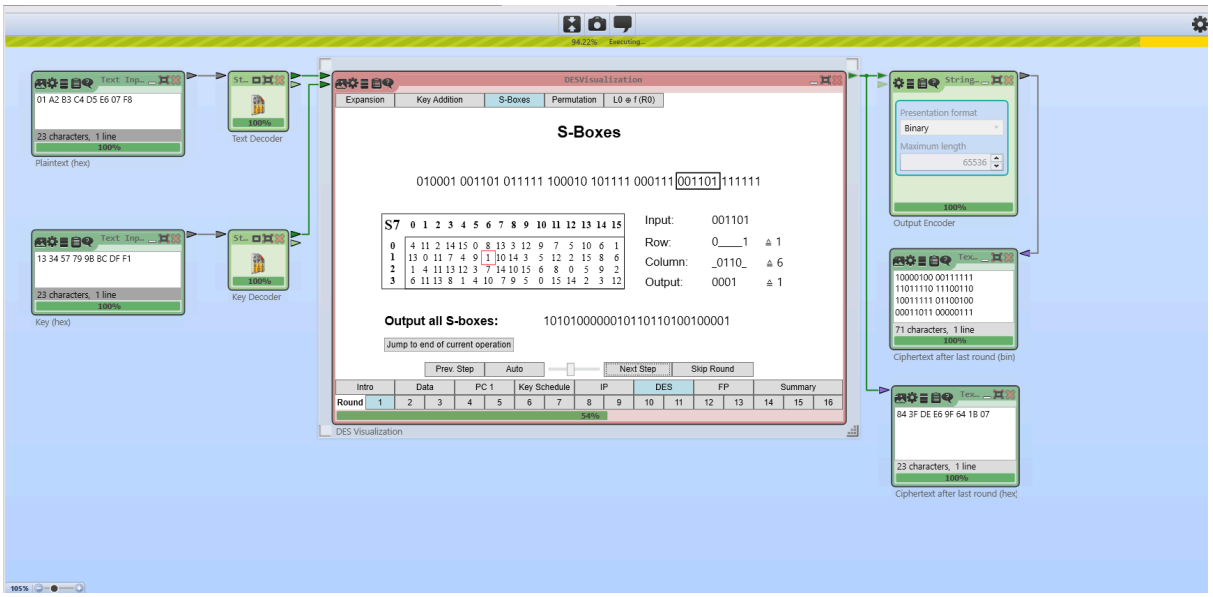

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S2 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
1 3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5
2 0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15
3 13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9
Input: 001101
Row: 0____1 ≙ 1
Column: _0110_ ≙ 6
Output: 1000 ≙ 8
Output all S-boxes: 10101000
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

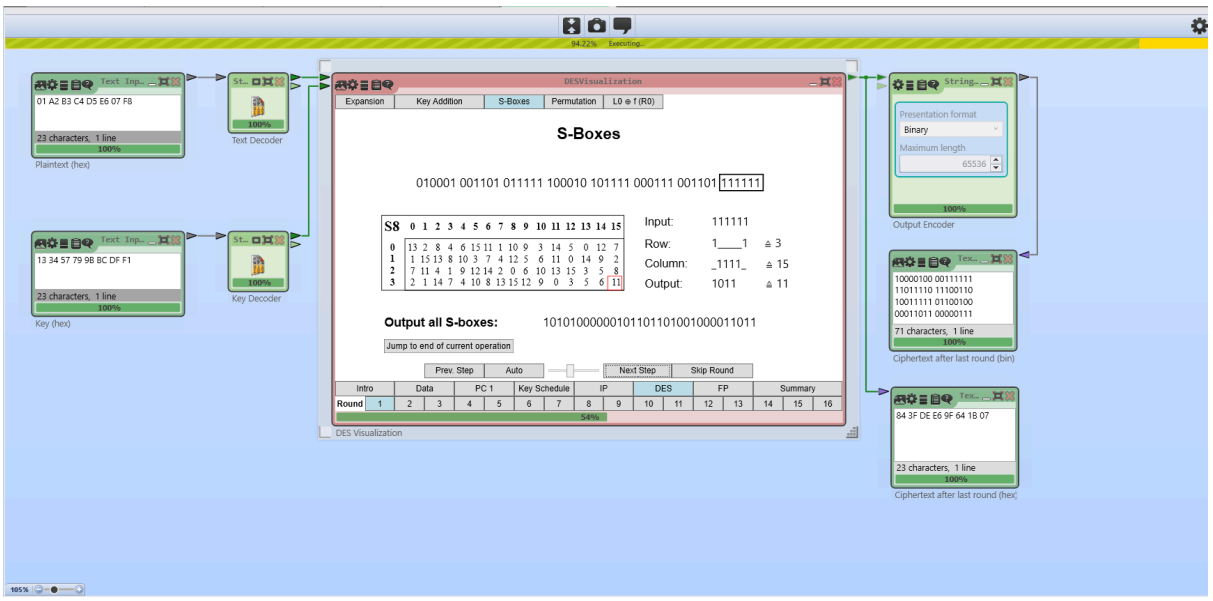

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S3 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
1 13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1
2 13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
3 1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12
Input: 011111
Row: 0____1 ≙ 1
Column: _1111_ ≙ 15
Output: 0001 ≙ 1
Output all S-boxes: 101010000001
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

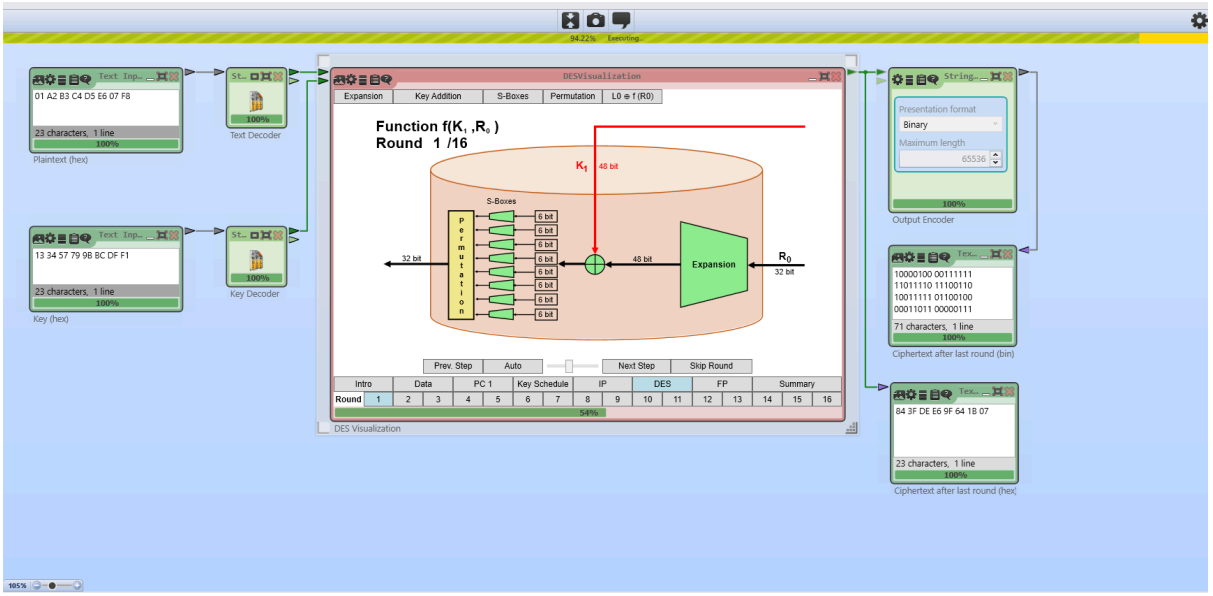

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S4 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
1 13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
2 10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
3 3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14
Input: 100010
Row: 1____0 ≙ 2
Column: _0001_ ≙ 1
Output: 0110 ≙ 6
Output all S-boxes: 1010100000010110
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)

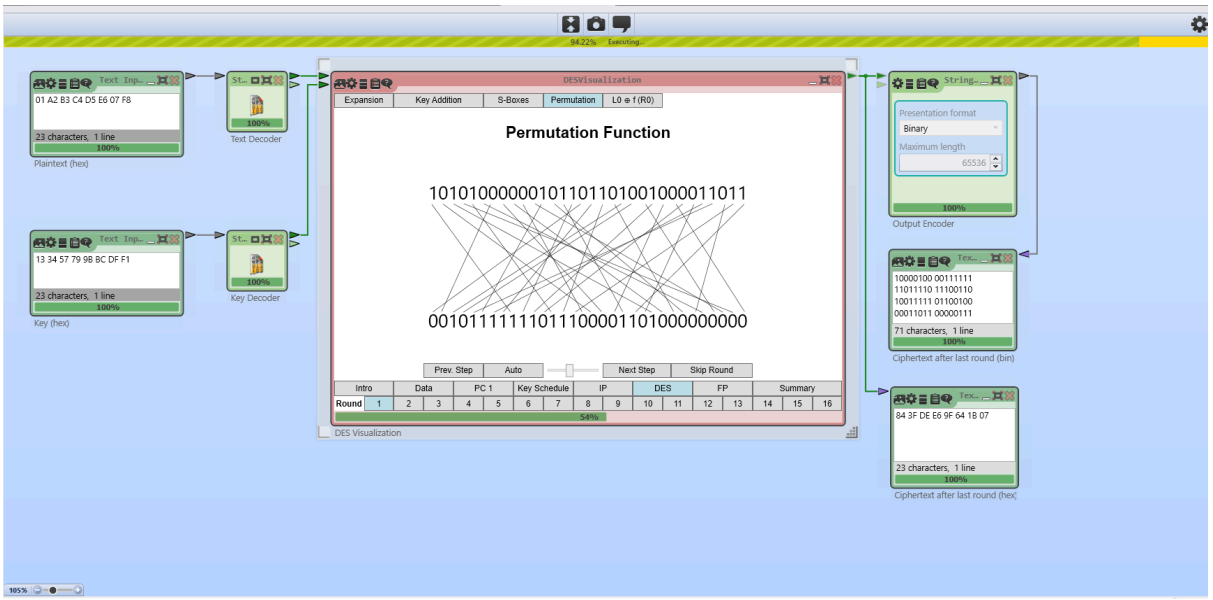

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S5 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9
1 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6
2 4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14
3 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3
Input: 101111
Row: 1____1 ≙ 3
Column: _0111_ ≙ 7
Output: 1101 ≙ 13
Output all S-boxes: 10101000000101101101
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

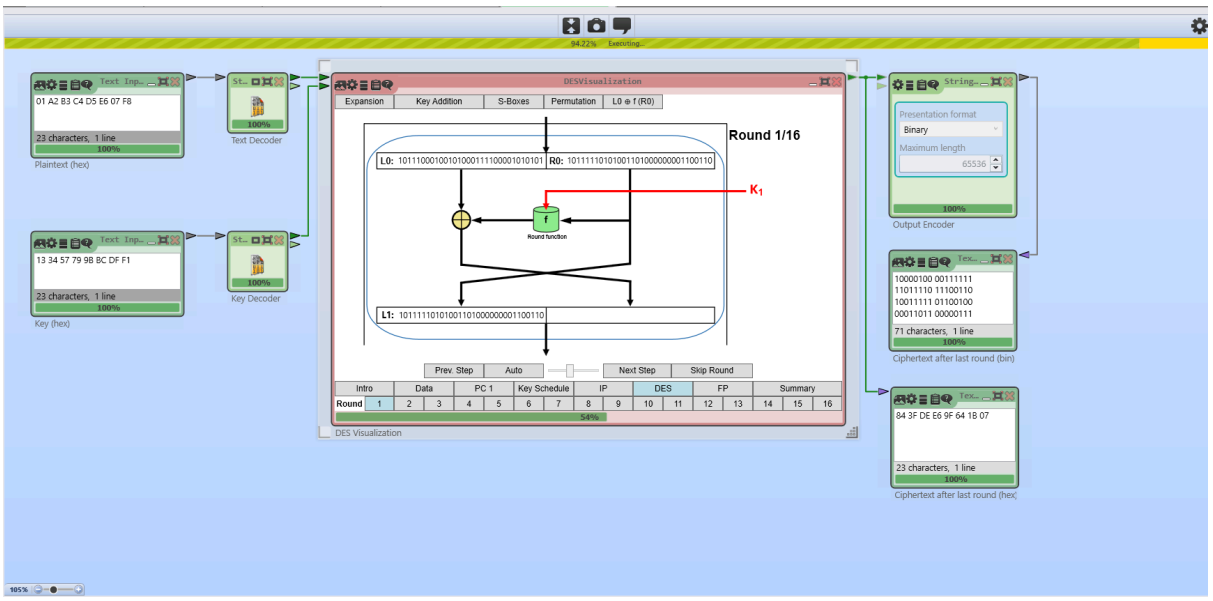

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S6 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
1 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
2 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
3 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13
Input: 000111
Row: 0____1 ≙ 1
Column: _0011_ ≙ 3
Output: 0010 ≙ 2
Output all S-boxes: 10101000000101101101010010
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

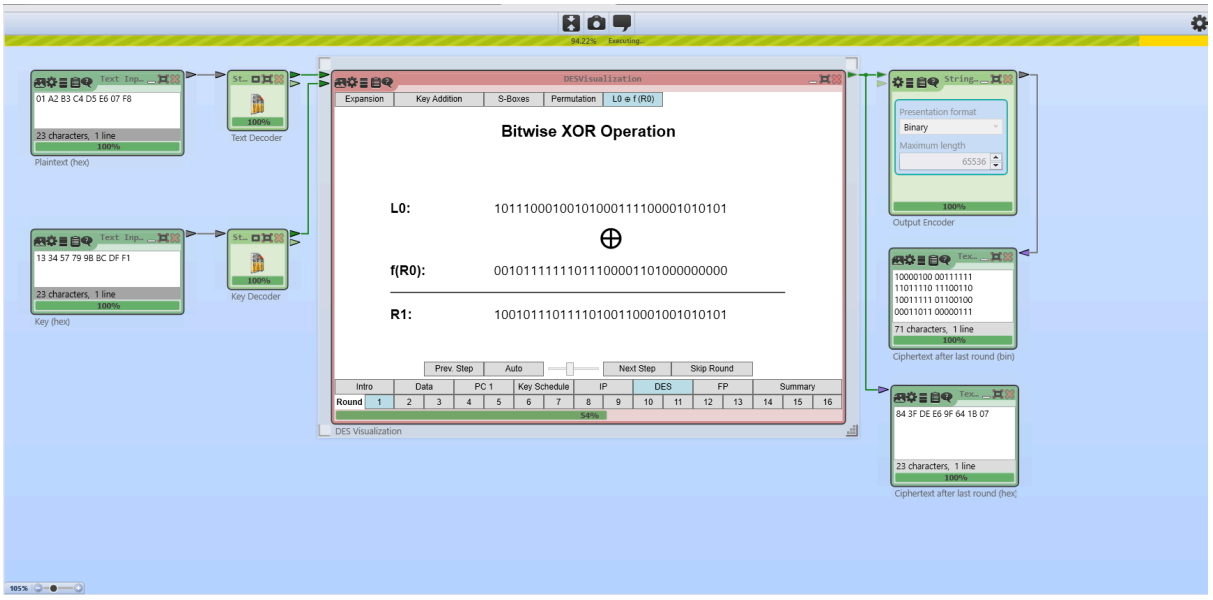

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
St...
100%
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
St...
100%
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S7 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
1 13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6
2 1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
3 6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12
Input: 001101
Row: 0____1 ≙ 1
Column: _0110_ ≙ 6
Output: 0001 ≙ 1
Output all S-boxes: 10101000000101101101000100001
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

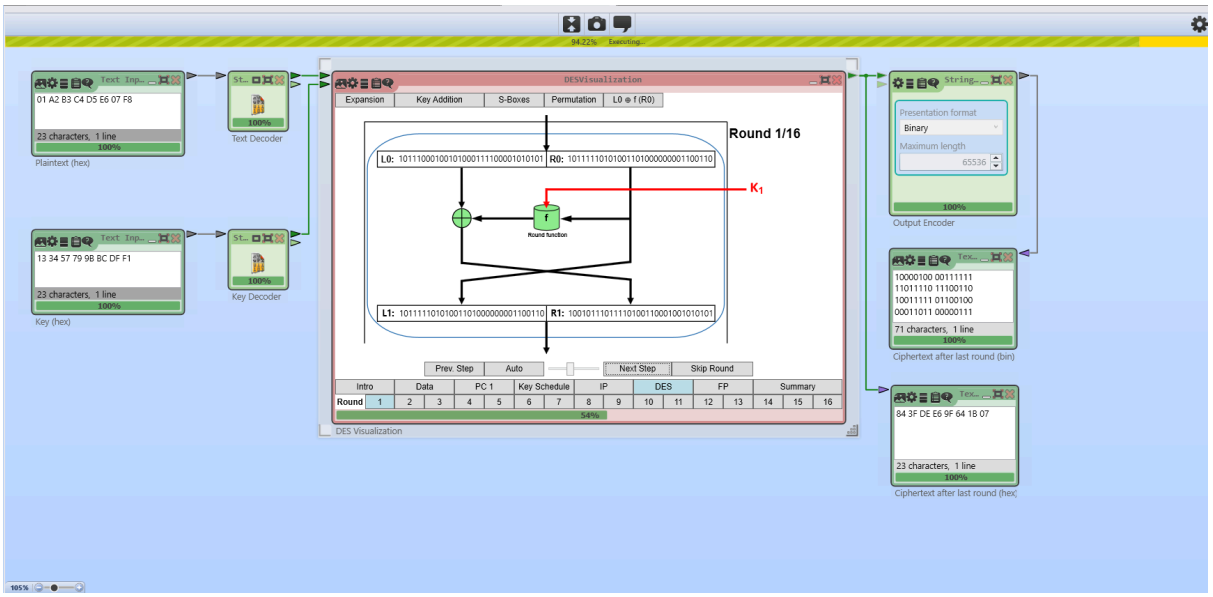

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
S-Boxes
010001 001101 011111 100010 101111 000111 001101 111111
S8 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
1 1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2
2 7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
3 2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11
Input: 111111
Row: 1____1 ≙ 3
Column: _1111_ ≙ 15
Output: 1011 ≙ 11
Output all S-boxes: 10101000000101101101001000011011
Jump to end of current operation
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

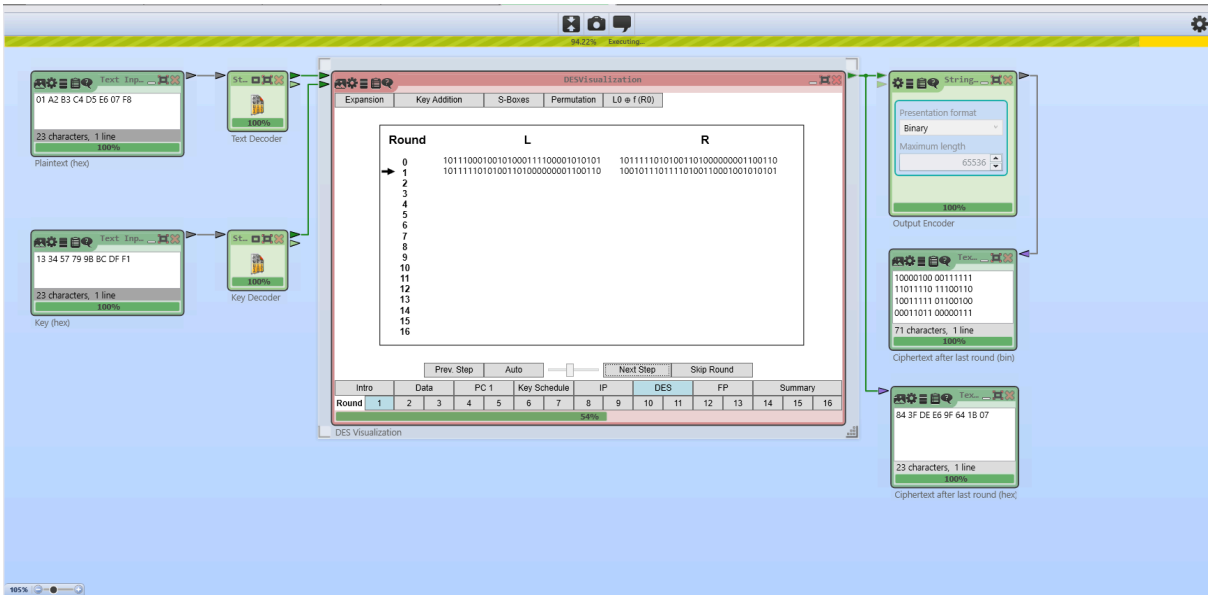

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Function f(K1 ,R0)
Round 1 /16
K1
48 bit
S-Boxes
6 bit
32 bit
48 bit
Expansion
R0
32 bit
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

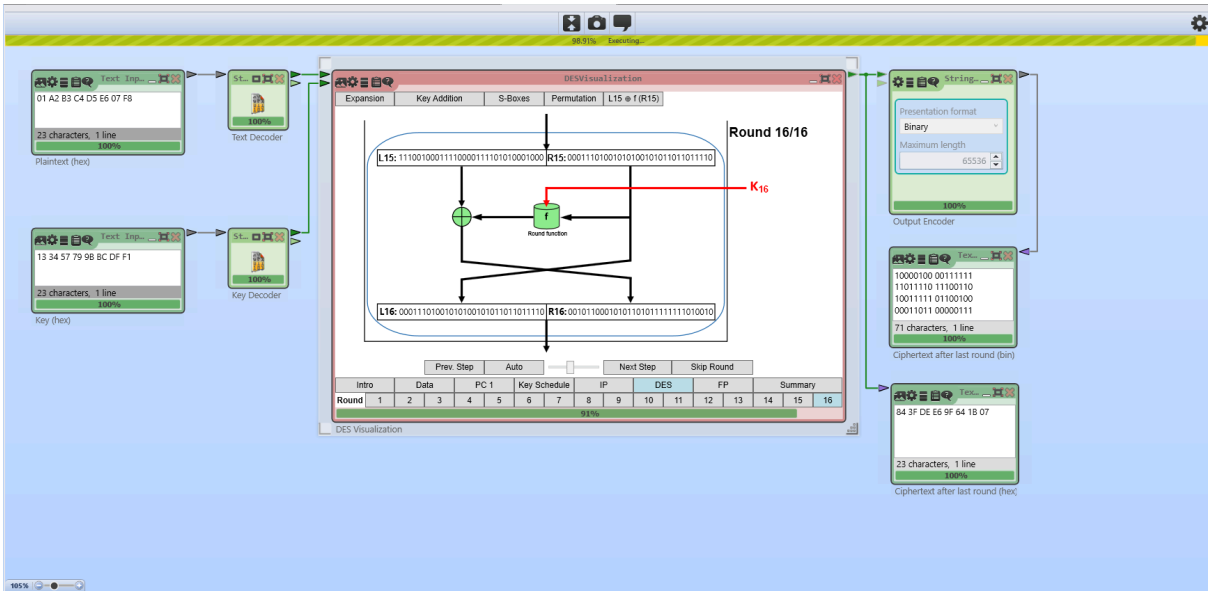

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Permutation Function
1010100000010110110100100001101 1
0010111111101110000110100000000
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
Ciphertext after last round (hex)

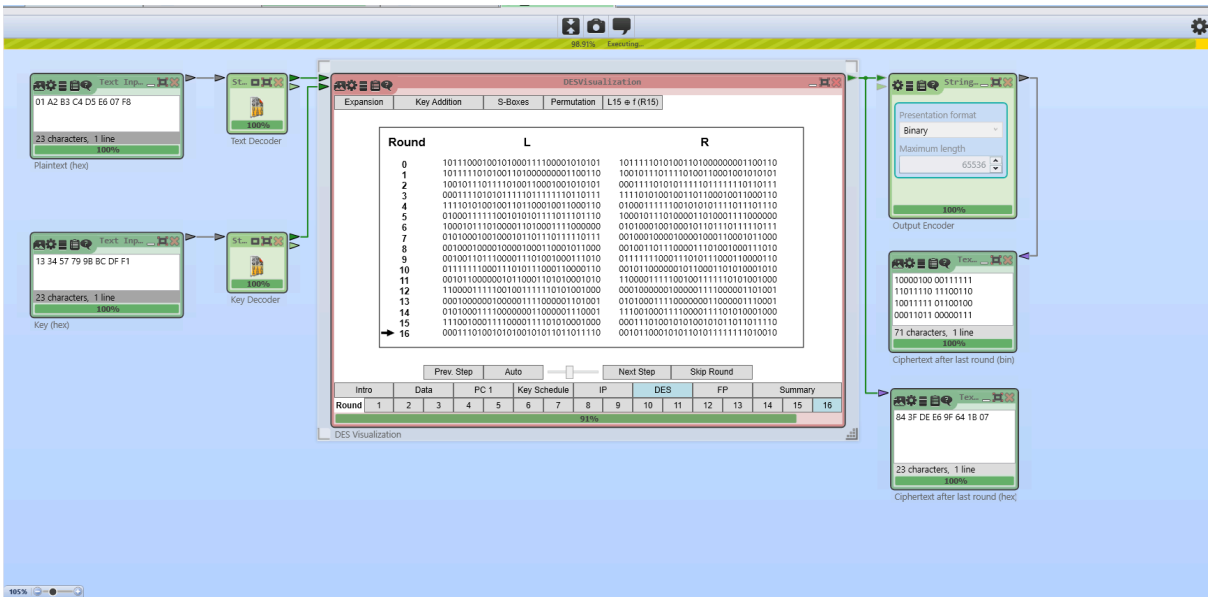

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Round 1/16
L0: 10111000100101000111100001010101
R0: 10111110101001101000000001100110
K1
f
Round function
L1: 10111110101001101000000001100110
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

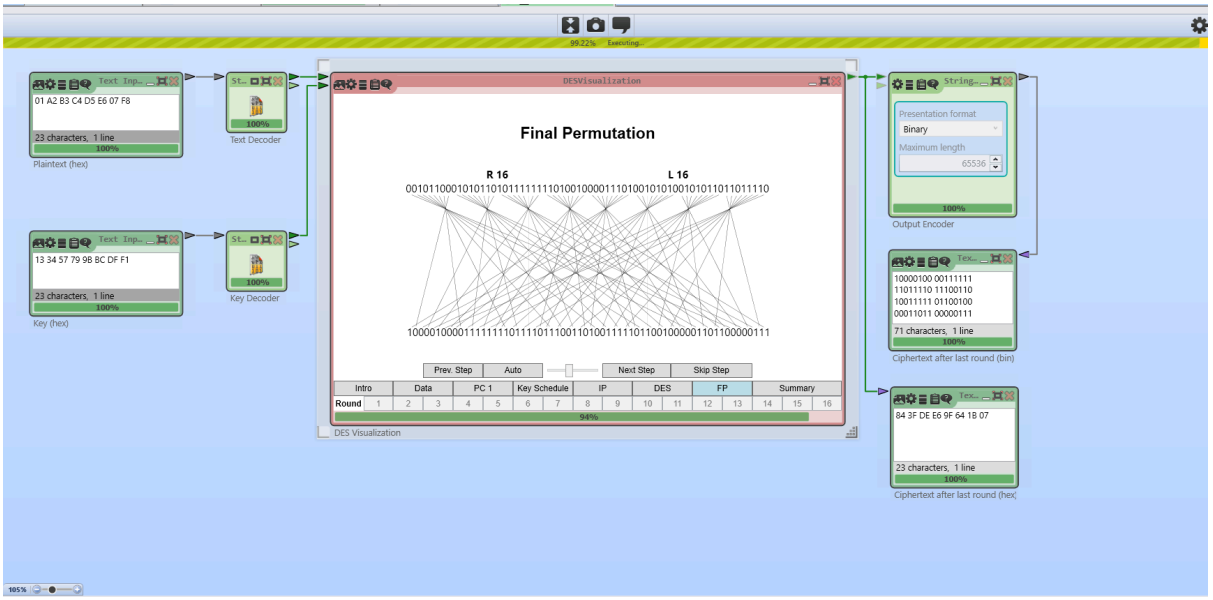

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Bitwise XOR Operation
L0:
10111000100101000111100001010101
⊕
f(R0):
00101111111011100001101000000000
R1:
10010111011110100110001001010101
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

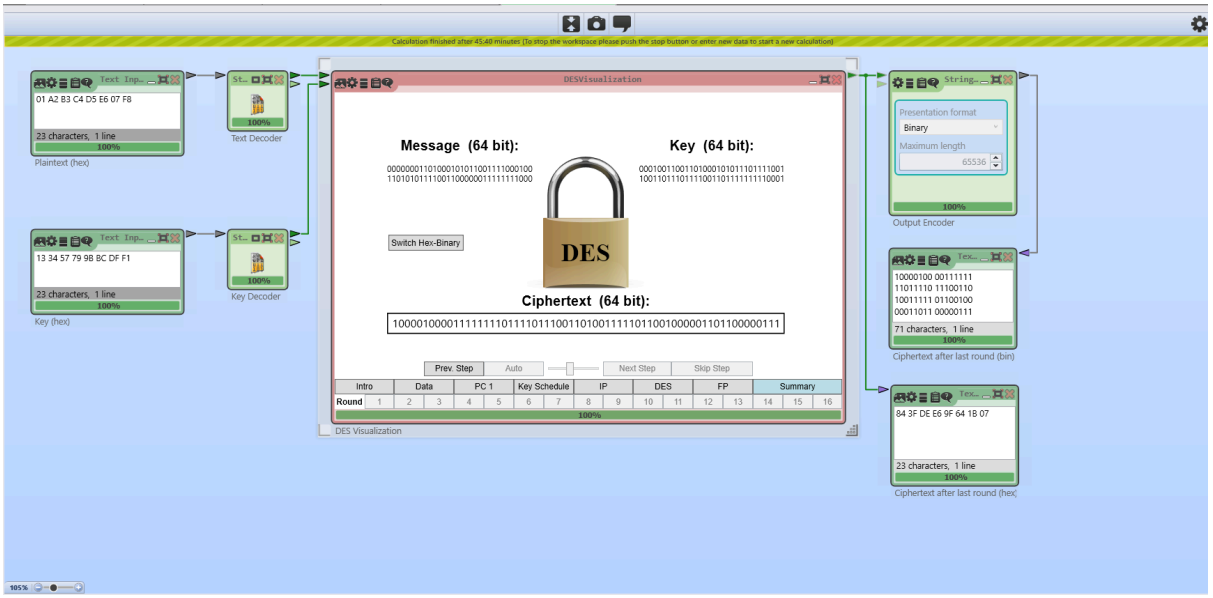

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Round 1/16
L0: 10111000100101000111100001010101
R0: 10111110101001101000000001100110
K1
f
Round function
L1: 10111110101001101000000001100110
R1: 10010111011110100110001001010101
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

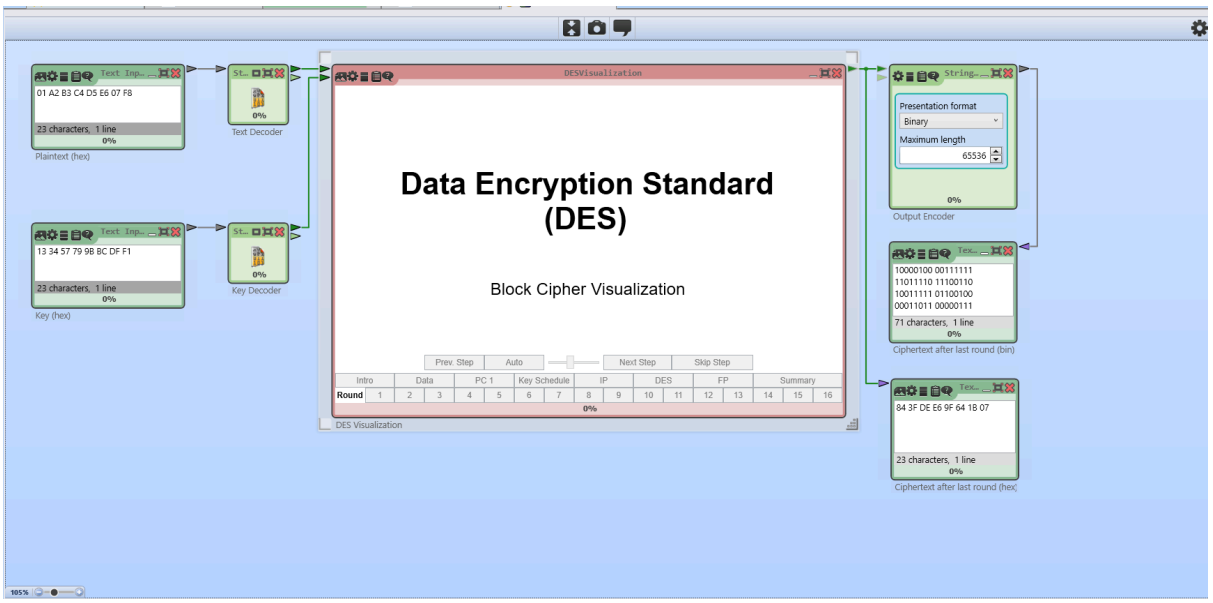

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L0 ⊕ f (R0)
Round
L
R
0 1011100010010100011110000101010 1011111010100110100000000110011 0
1 1011111010100110100000000110011 0 1001011110111101001100010101010 1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
54%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L15 ⊕ f (R15)
Round 16/16
L15: 1110010001111000011110101001000 R15: 0001110100101001010110111011110
K16
f
Round function
L16: 0001110100101001010110111011110 R16: 0010110001010110101111111010010
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
91%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%


Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Expansion
Key Addition
S-Boxes
Permutation
L15 ⊕ f (R15)
Round
L
R
0 1011100010010100011110000101010 1011111010100110100000000110011 0
1 1011111010100110100000000110011 0 1001011110111101001100010101010 1
2 1001011110111101001100010101010 1 0001111010101111101111111101011 1
3 0001111010101111101111111101011 1 1111010100100110110000100100011 0
4 1111010100100110110001001100011 0 0100011111100101010111111011110
5 0100011111100101010111111011110 1000100111010000110100011110000 0
6 1000101110100011010000111100000 0 0101000100100010101101111110111
7 0101000100100010101101111110111 1 0010000100001000010001100101100 0
8 0010000100001000010001100101100 0 0010011011110000111010010001101 0
9 0010011011110000111010010001101 0 0111111100011101011100010000110
10 0111111100011101011100010000110 0010110000000101100011010100101 0
11 0010110000000101100011010100101 0 1100001111100100111111010100100 0
12 1100001111100100111111010100100 0 0001000000100000111100000011010 1
13 0001000000100000111100000011010 1 0101000111100000000110000011000 1
14 0101000111100000000110000011000 1 1110010001111000011110101001000 0
15 1110010001111000011110101001000 0 0001110100101010010101101011110
16 0001110100101010010101101011110 0 0010110001010110101111111101001 0
Prev. Step
Auto
Next Step
Skip Round
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
91%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

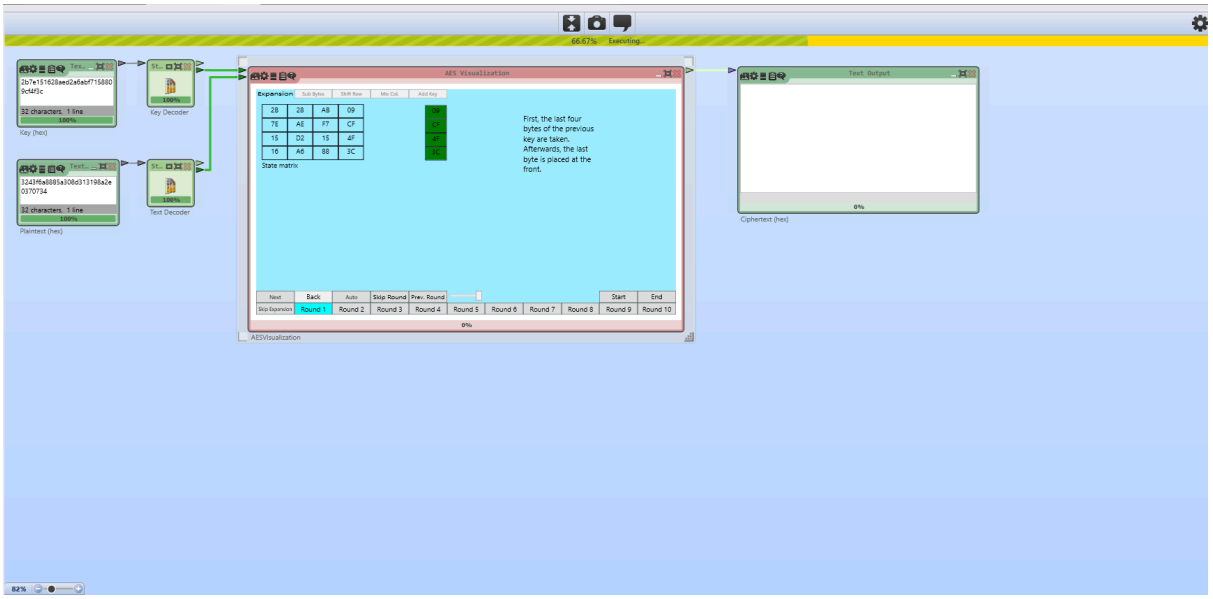

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Final Permutation
R 16
L 16
0010110001010110101111111101001000011101001010010101011011011110
1000010000111111110111101110011010011111011001000001101100000111
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
94%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

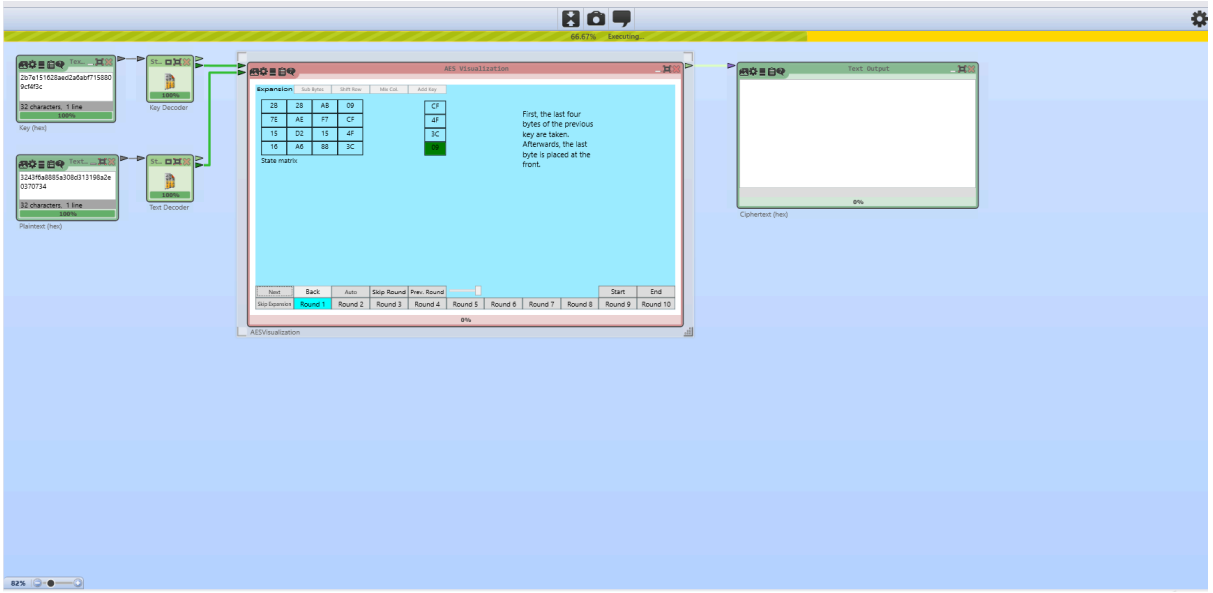

Calculation finished after 45.48 minutes (To stop the workspace please push the stop button or enter new data to start a new calculation)
Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
100%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
100%
Key (hex)
Key Decoder
DESVisualization
Message (64 bit):
0000000110100010101100111100010011101010111100110000001111111000
Key (64 bit):
0001001100110100010101101111001100110111011100110100010101111110001
Switch Hex-Binary
DES
Ciphertext (64 bit):
1000010000111111110111101110011010011111011001000001101100000111
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
100%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
100%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
100%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
100%
Ciphertext after last round (hex)
105%

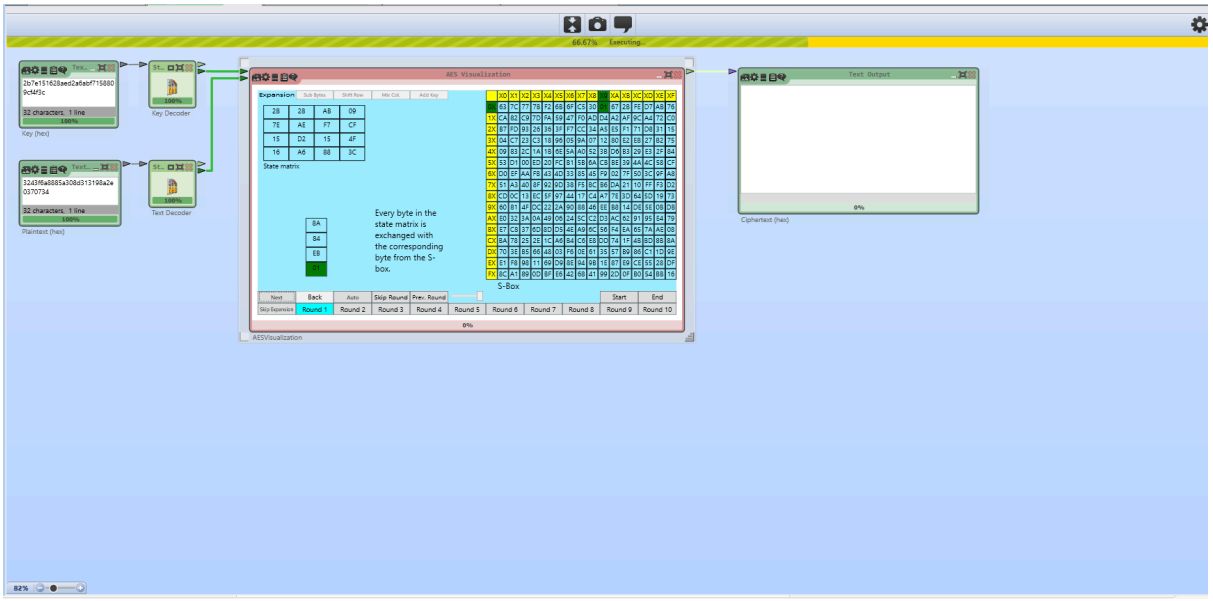

Text Inp...
01 A2 B3 C4 D5 E6 07 F8
23 characters, 1 line
0%
Plaintext (hex)
Text Decoder
Text Inp...
13 34 57 79 9B BC DF F1
23 characters, 1 line
0%
Key (hex)
Key Decoder
DESVisualization
Data Encryption Standard
(DES)
Block Cipher Visualization
Prev. Step
Auto
Next Step
Skip Step
Intro
Data
PC 1
Key Schedule
IP
DES
FP
Summary
Round
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
0%
DES Visualization
String...
Presentation format
Binary
Maximum length
65536
0%
Output Encoder
Tex...
10000100 00111111
11011110 11100110
10011111 01100100
00011011 00000111
71 characters, 1 line
0%
Ciphertext after last round (bin)
Tex...
84 3F DE E6 9F 64 1B 07
23 characters, 1 line
0%
Ciphertext after last round (hex)
105%

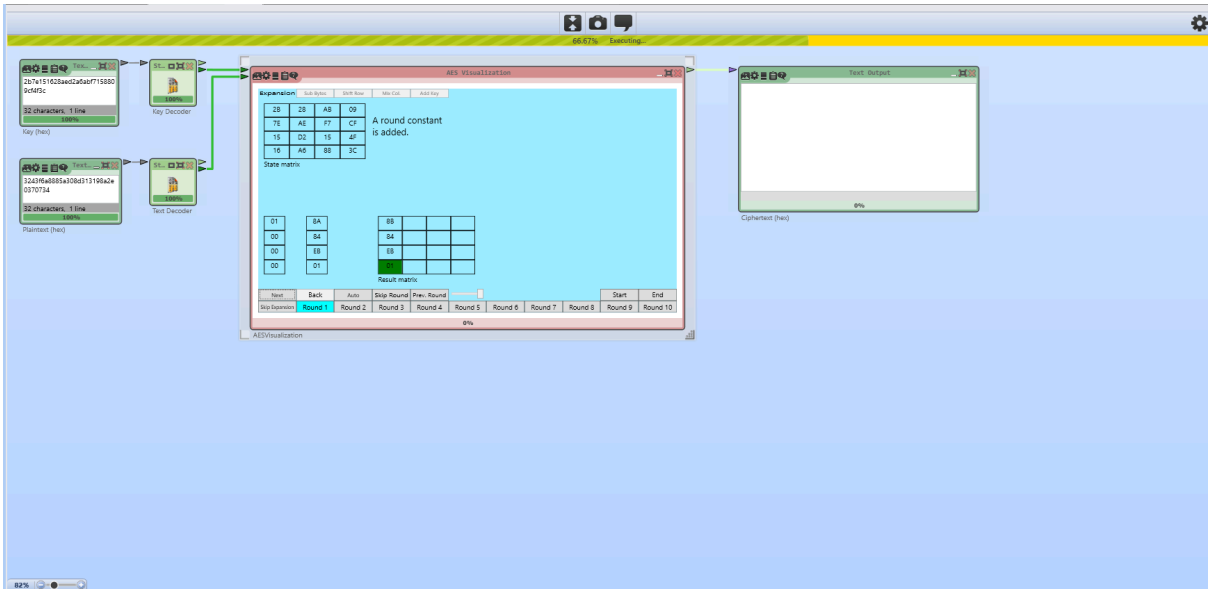
AES Encyprtion:

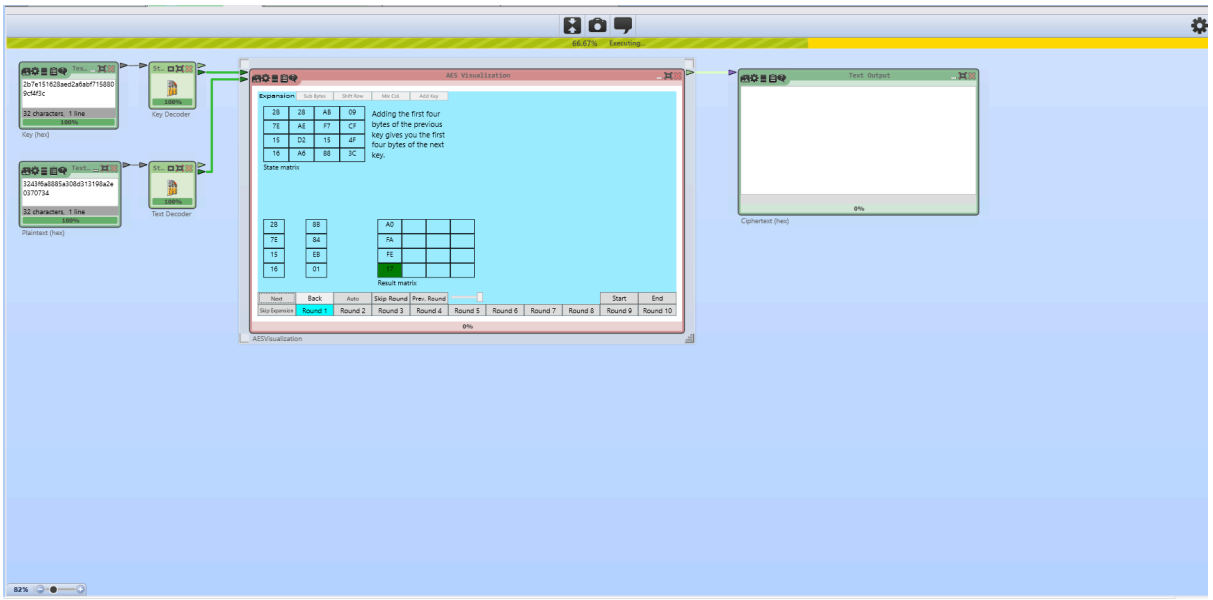
Expansion:

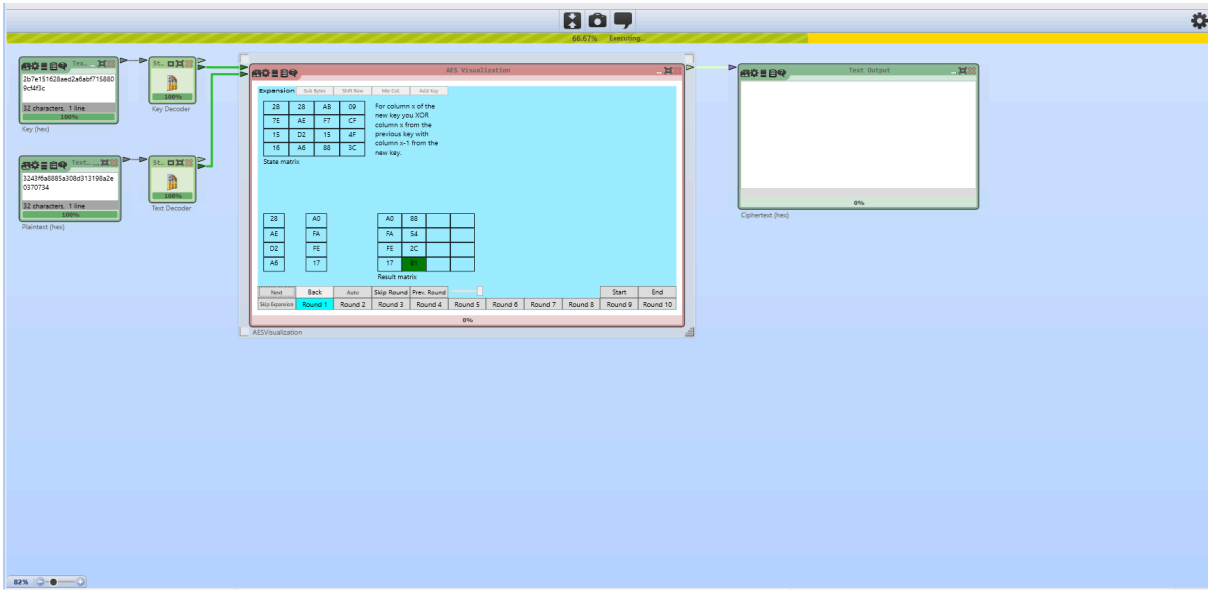


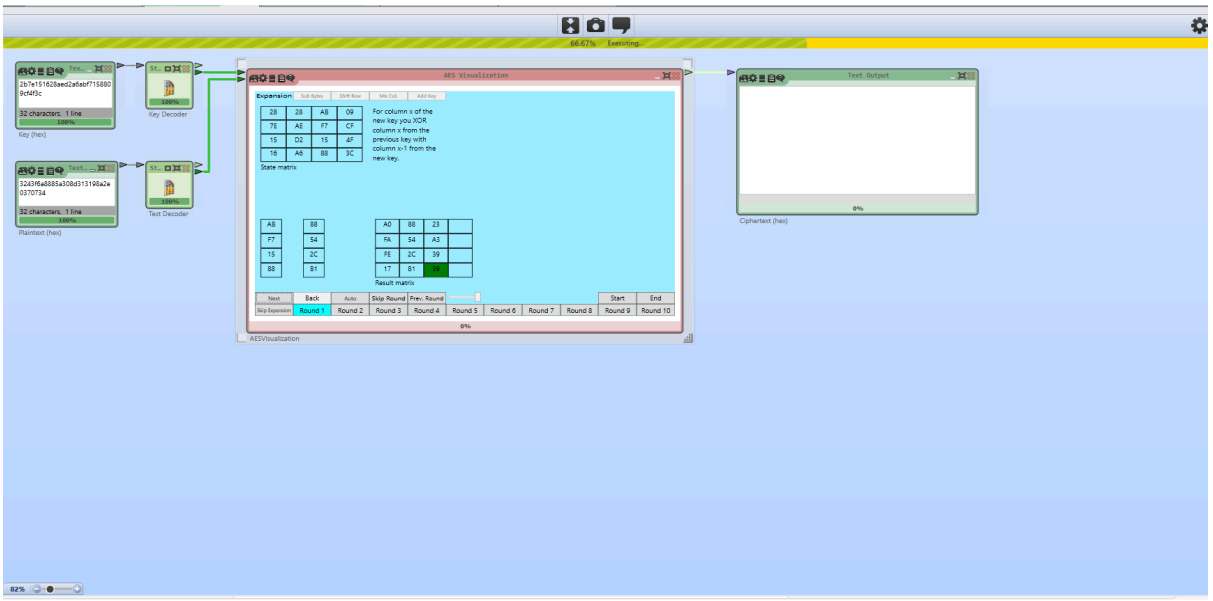


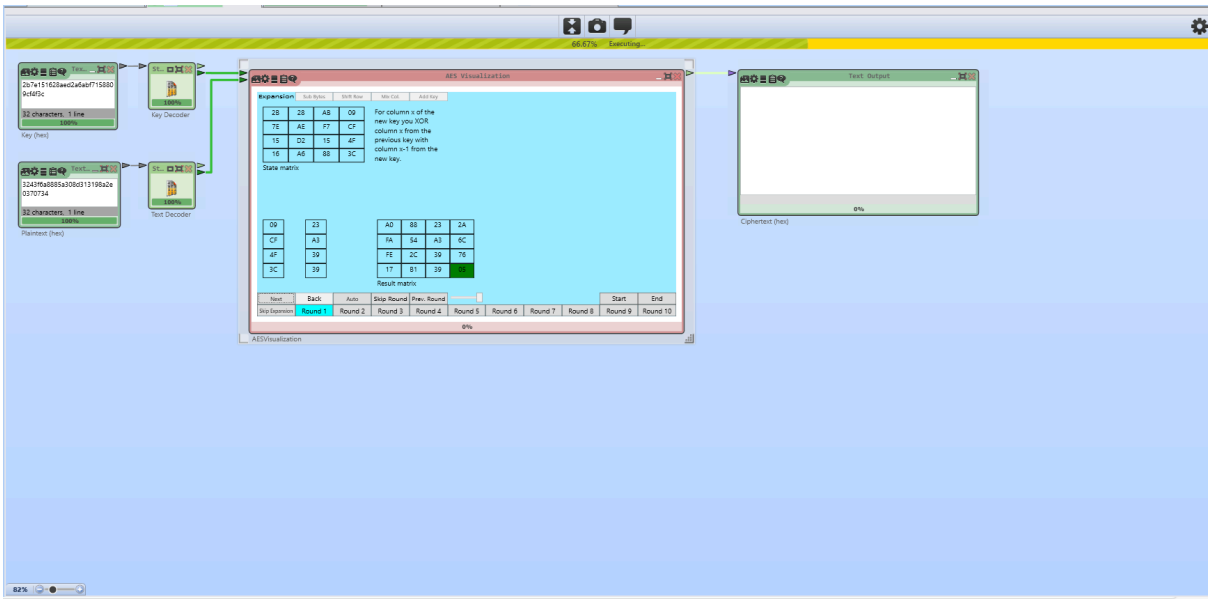

66.67% Executing...
2b7e151628aed2a6abf715880 9c4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
State matrix
Every byte in the state matrix is exchanged with the corresponding byte from the S-box.
S-Box
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%


66.67% Executing...
2b7e151628aed2a6abf715880 9c4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
State matrix
A round constant is added.
Result matrix
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%

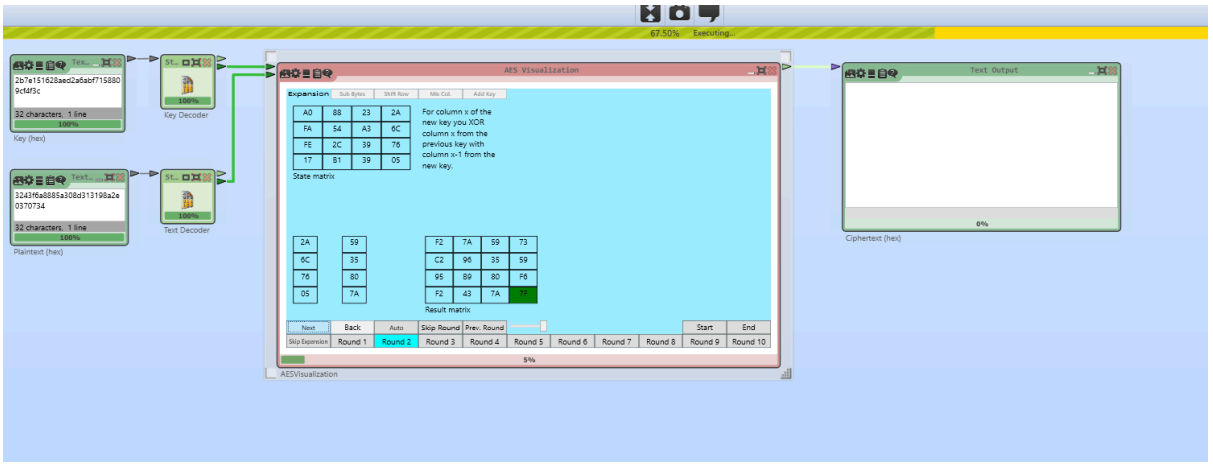

66.67% Executing...
2b7e151628aed2a6abf715880 9c4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
State matrix
Adding the first four bytes of the previous key gives you the first four bytes of the next key.
Result matrix
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%


66.67% Executing...
2b7e151628aed2a6abf715880 9cf4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
28 28 AB 09
7E AE F7 CF
15 D2 15 4F
16 A6 88 3C
State matrix
For column x of the new key you XOR column x from the previous key with column x-1 from the new key.
28 A0
AE FA
D2 FE
A6 17
A0 88
FA 54
FE 2C
17 81
Result matrix
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%

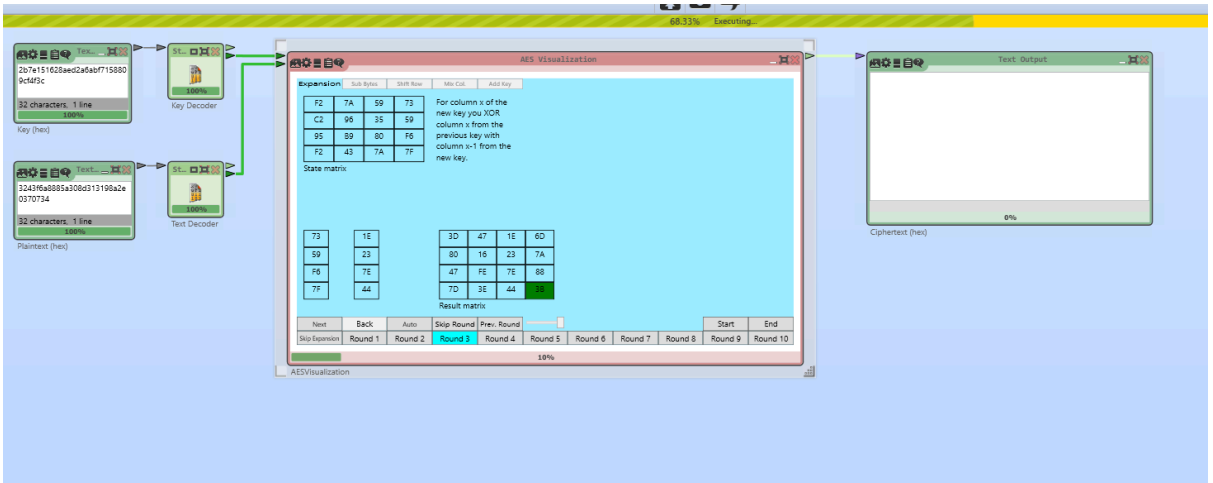

66.67% Executing...
2b7e151628aed2a6abf715880 9cf4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
28 28 AB 09
7E AE F7 CF
15 D2 15 4F
16 A6 88 3C
State matrix
For column x of the new key you XOR column x from the previous key with column x-1 from the new key.
AB 88
F7 54
15 2C
88 81
A0 88 23
FA 54 A3
FE 2C 39
17 81 39
Result matrix
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%


66.67% Executing...
2b7e151628aed2a6abf715880 9cf4f3c
32 characters, 1 line
100%
Key (hex)
Key Decoder
3243f6a8885a308d313198a2e 0370734
Plaintext (hex)
Text Decoder
AES Visualization
Expansion
Sub Bytes
Shift Row
Mix Col.
Add Key
28 28 AB 09
7E AE F7 CF
15 D2 15 4F
16 A6 88 3C
State matrix
For column x of the new key you XOR column x from the previous key with column x-1 from the new key.
09 23
CF A3
4F 39
3C 39
A0 88 23 2A
FA 54 A3 6C
FE 2C 39 76
17 81 39 09
Result matrix
Next
Back
Auto
Skip Round
Prev. Round
Start
End
Skip Expansion
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
0%
AESVisualization
Text Output
Ciphertext (hex)
82%

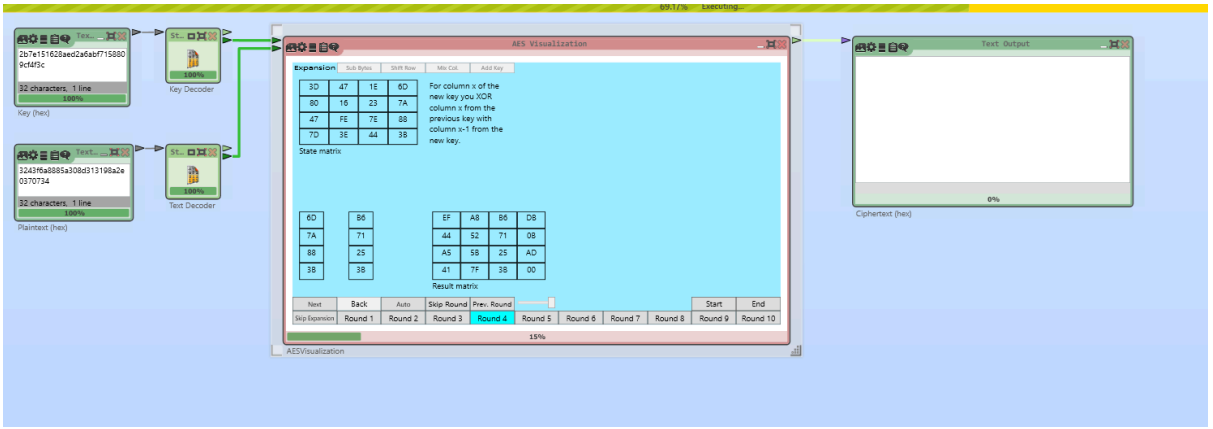
Round 2:



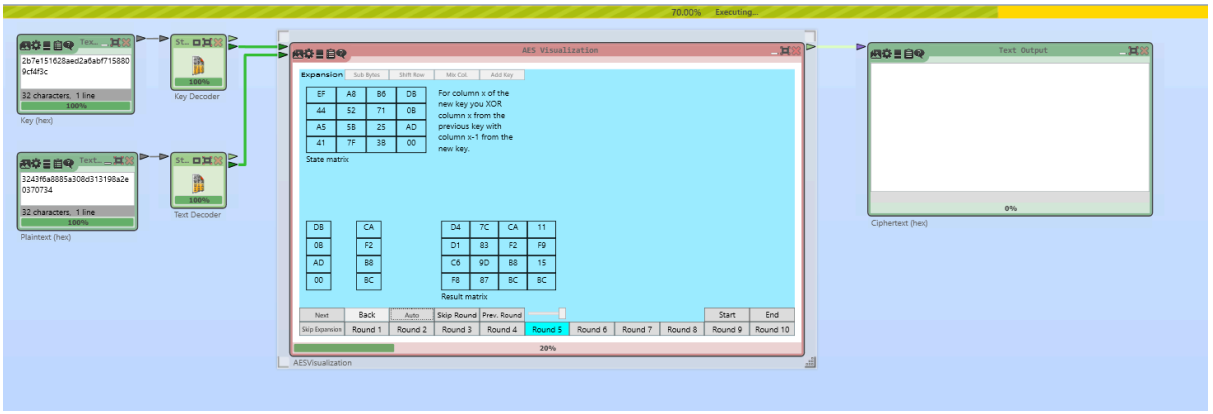
Round 3:



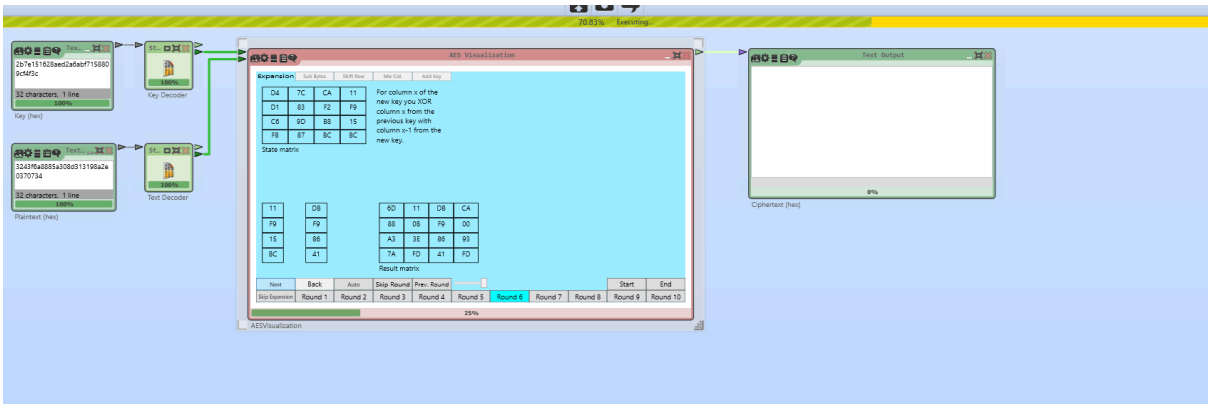
Round 4:



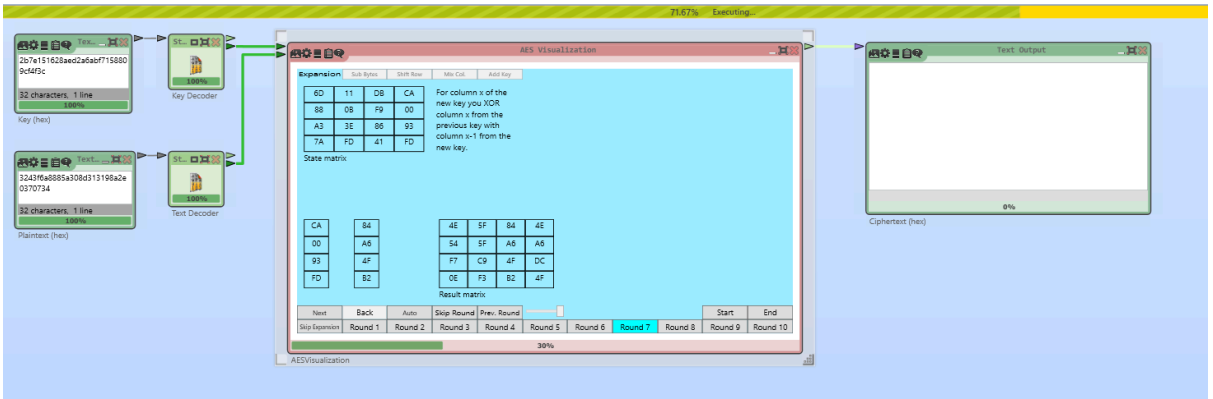
Round 5:



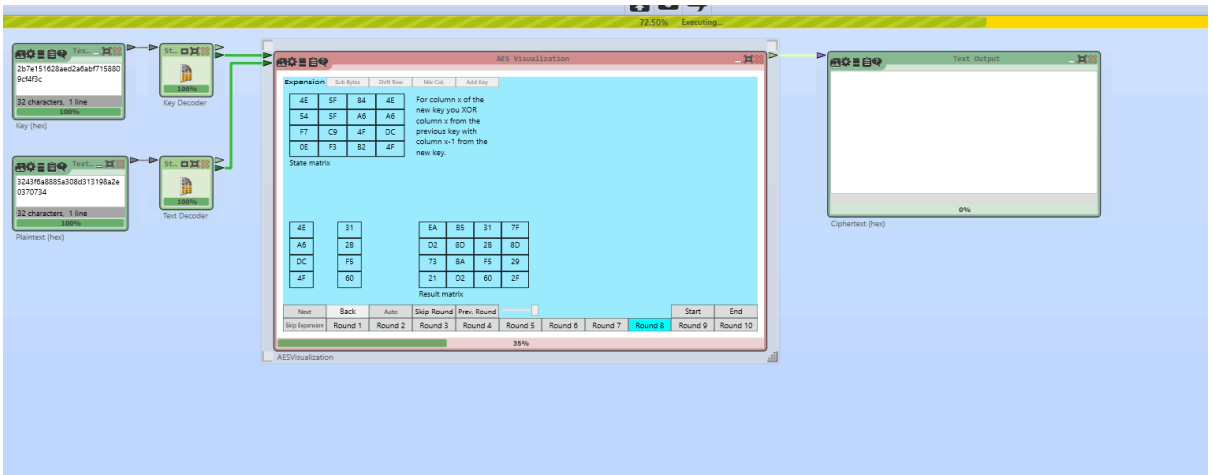
Round 6:



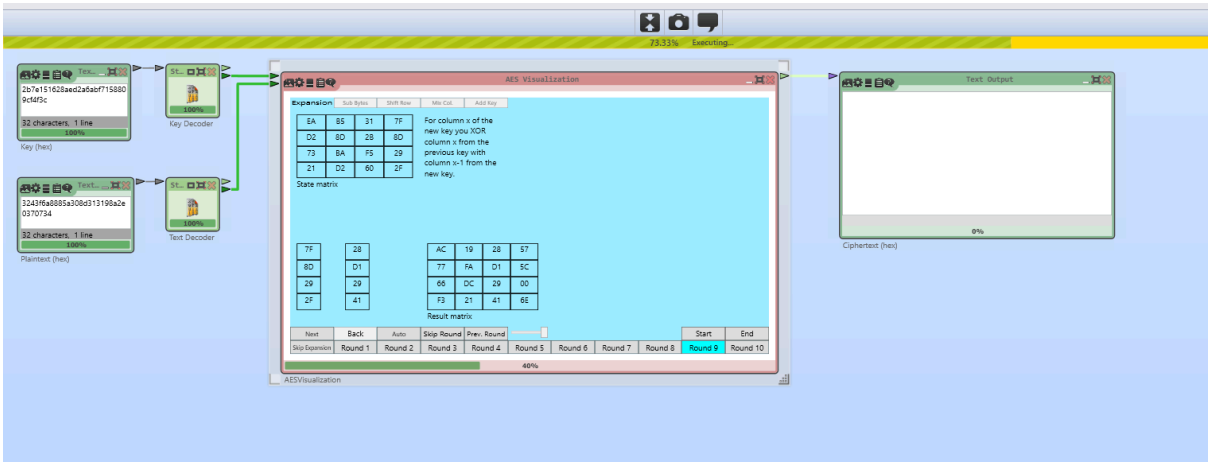
Round 7:

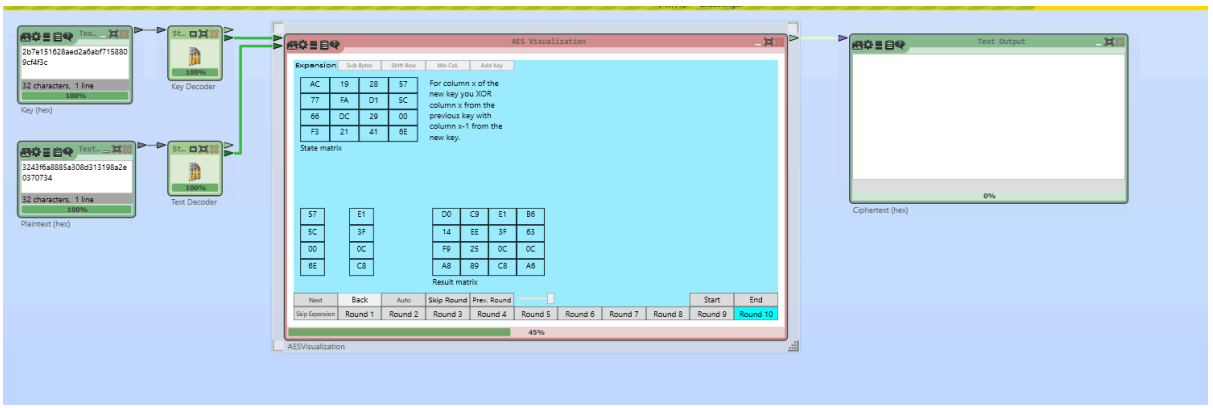


Round 8:



Round 9:

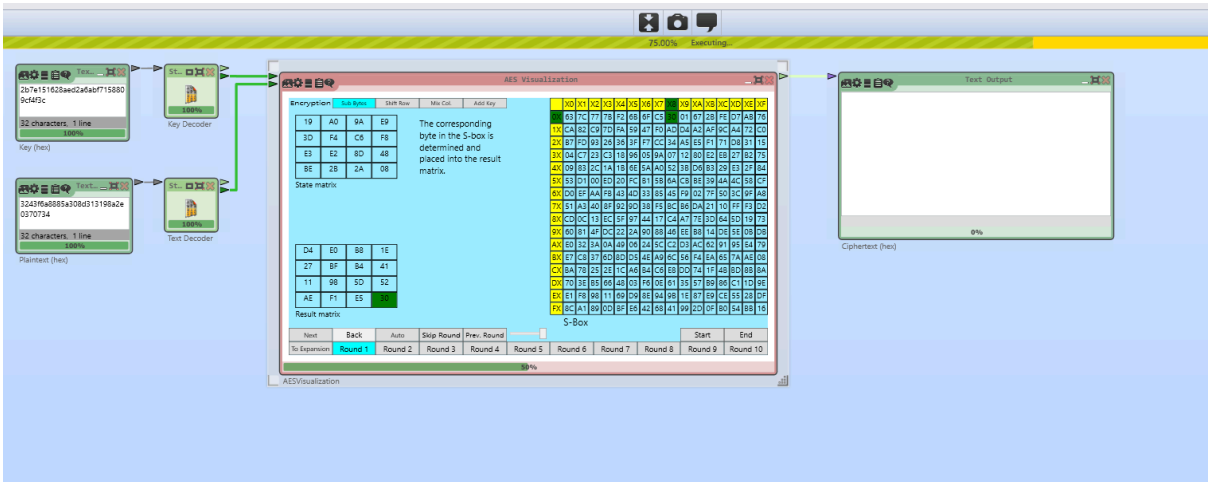




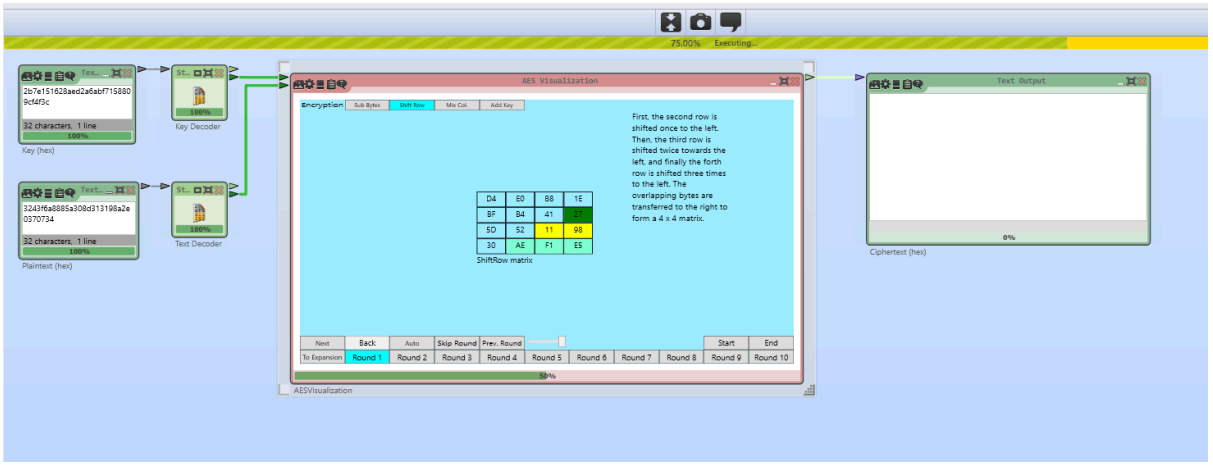
Encryption:

Round 1:

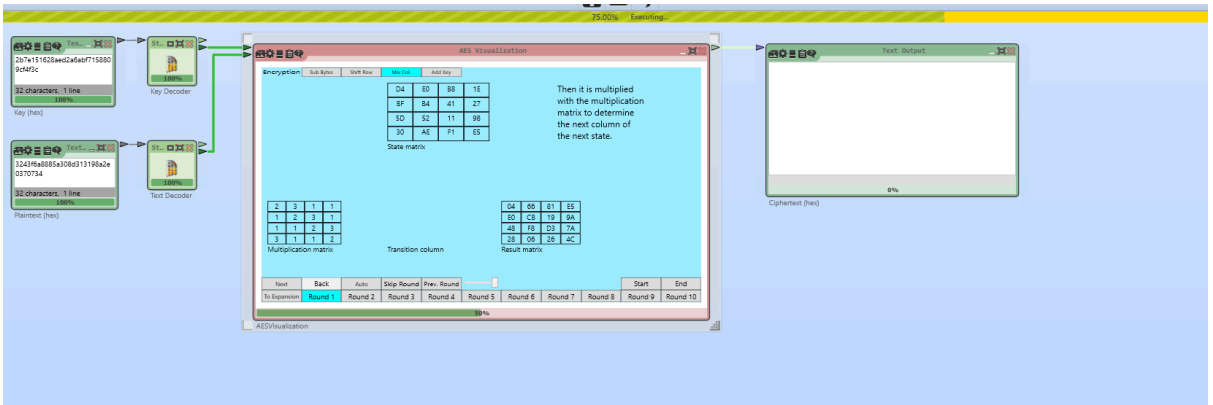
S-box:



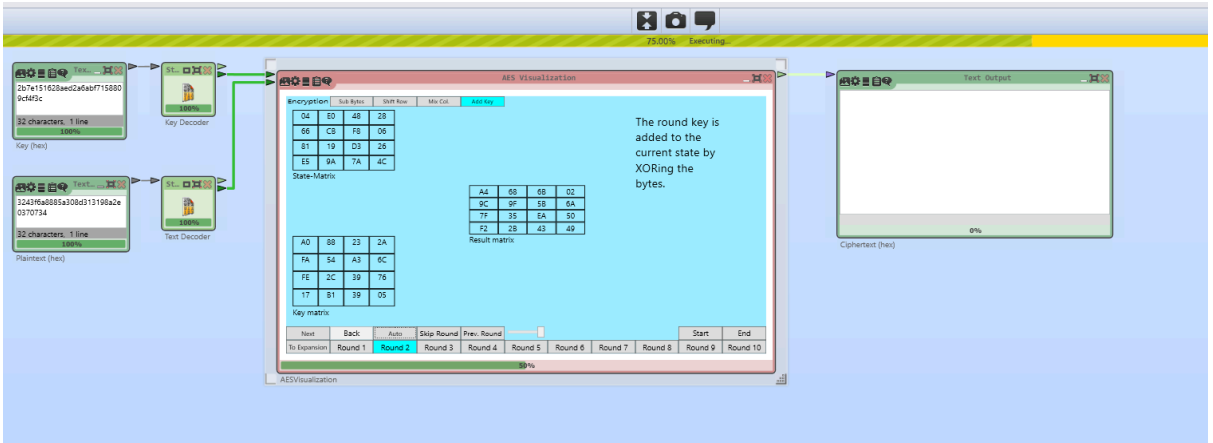
Shift row:



Mix Column:

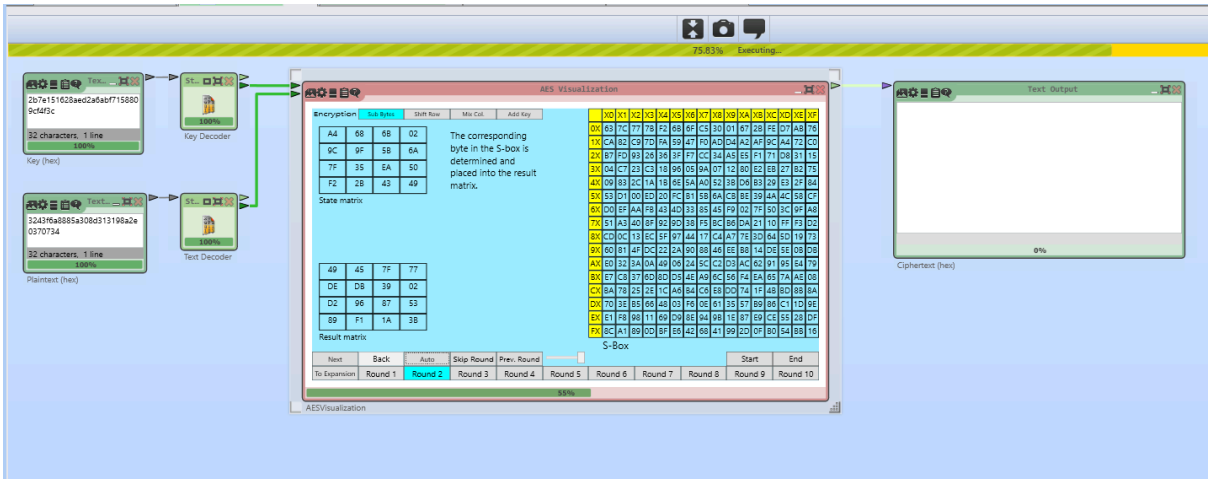


Add round key:

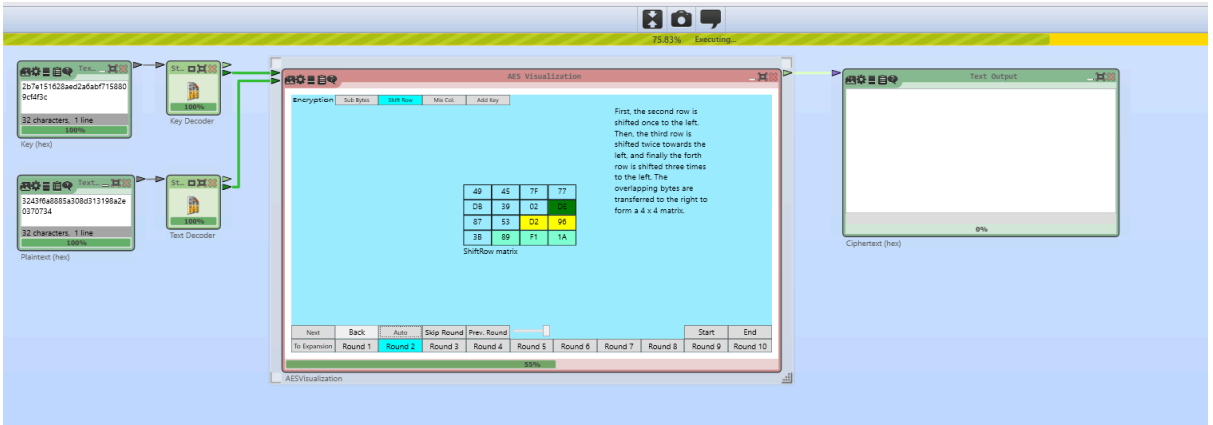


Round 2:

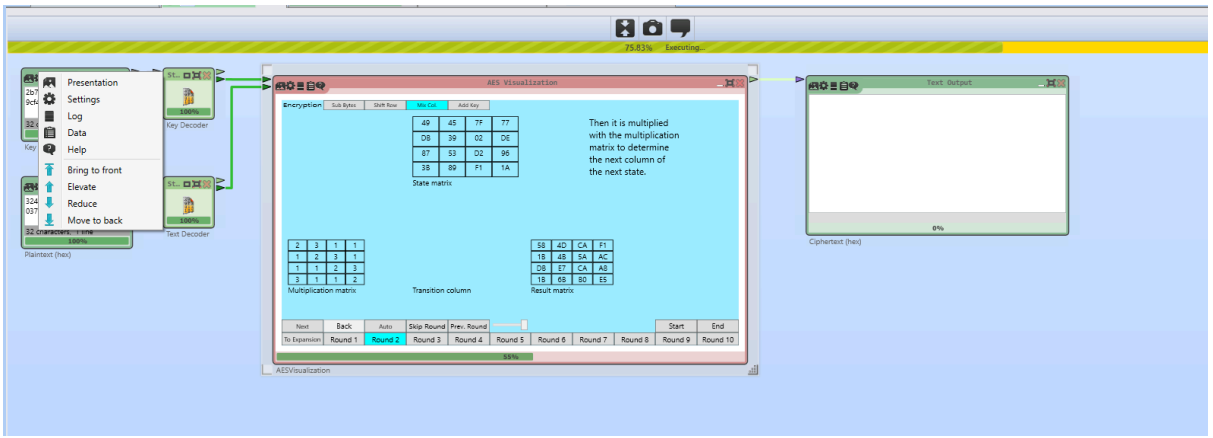
S-box:



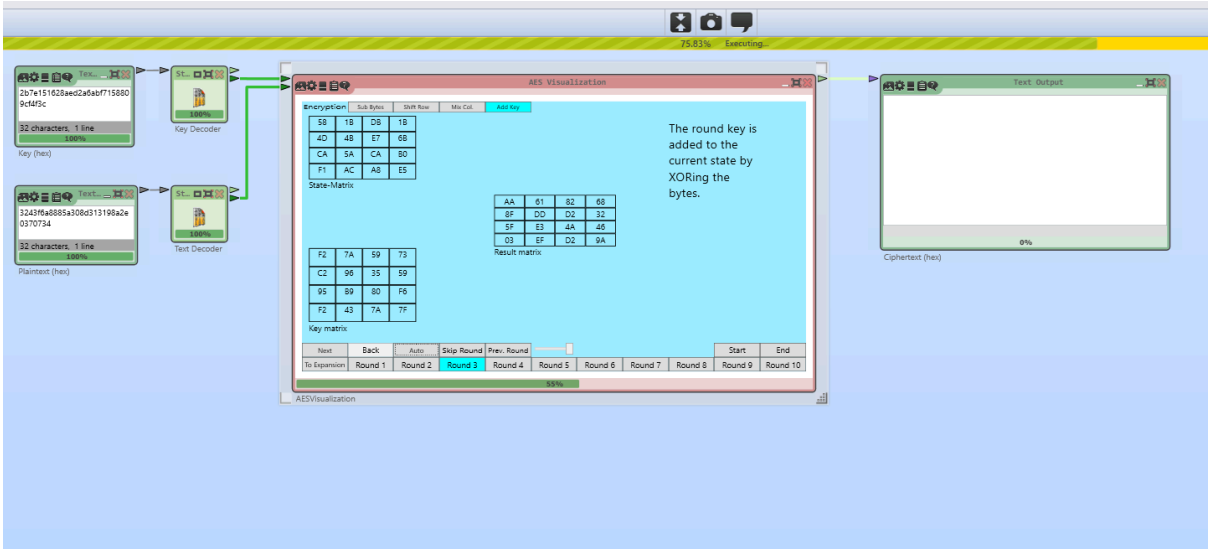
Shift row:



Mix column:

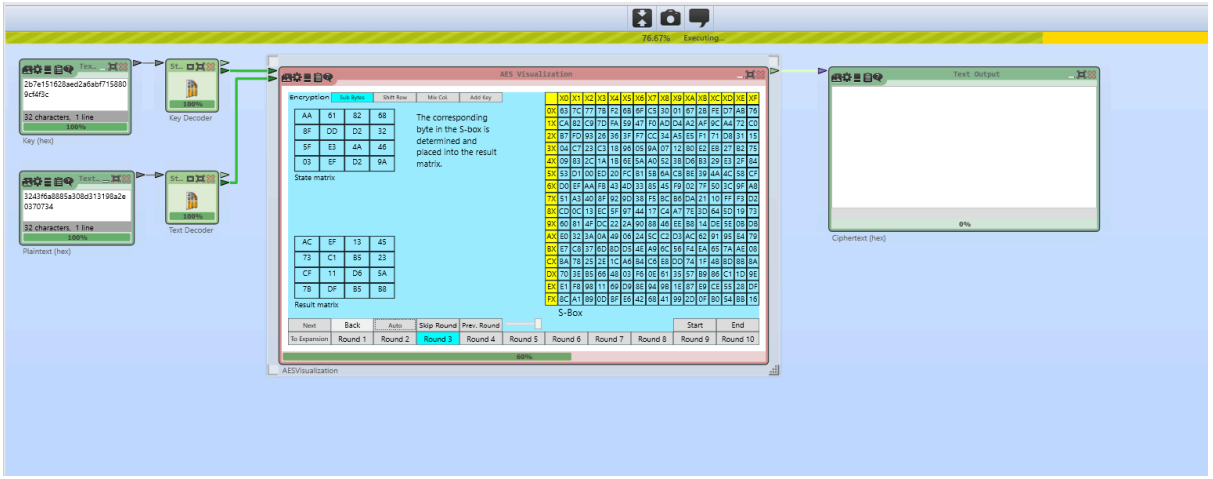


Add key:

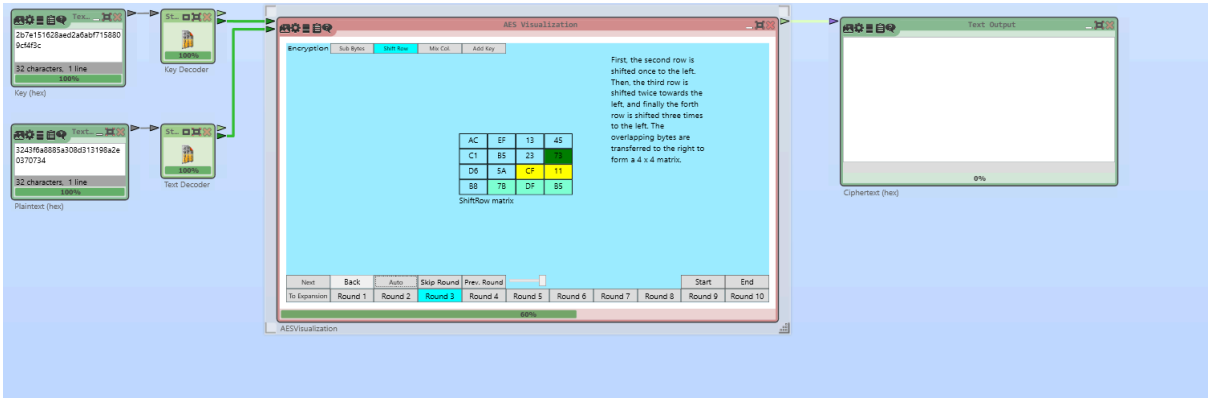


Round 3:

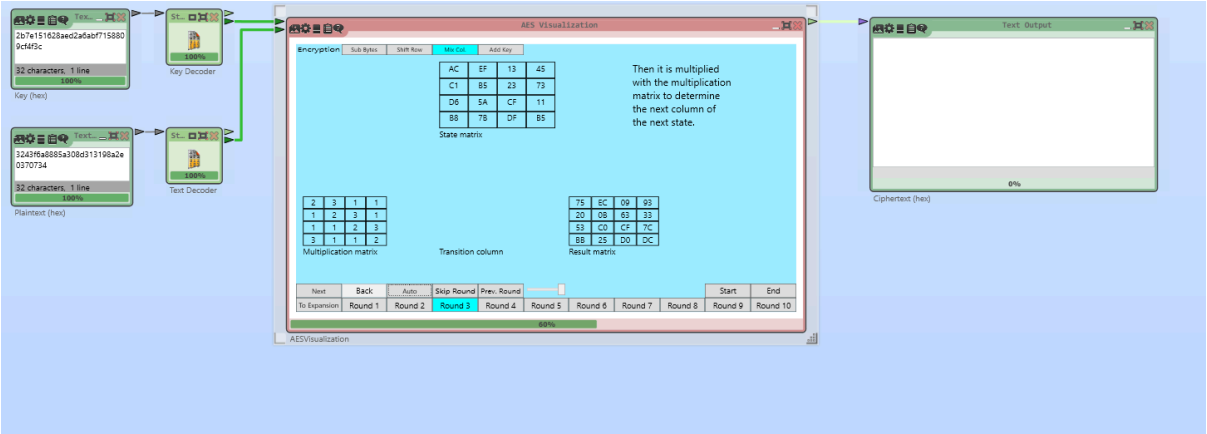
S-box



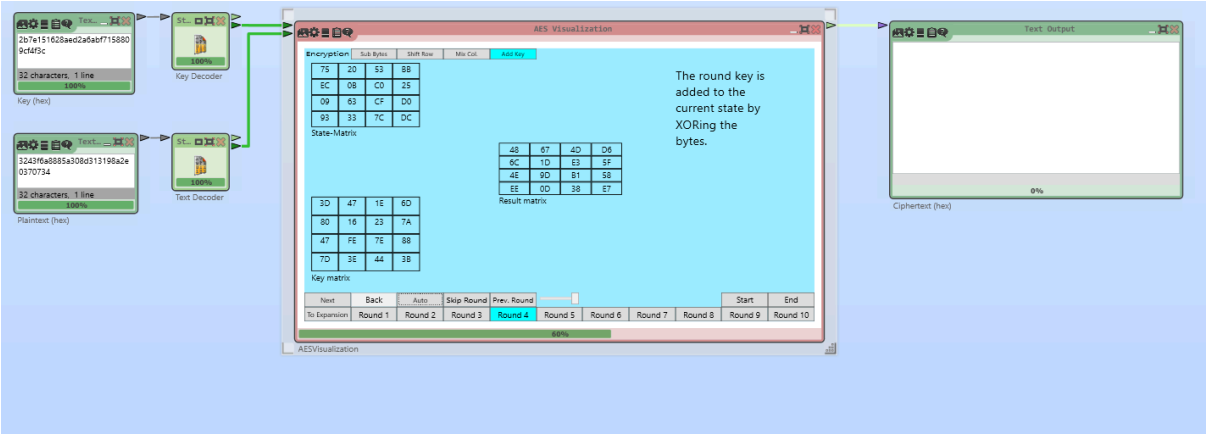
Shift row:



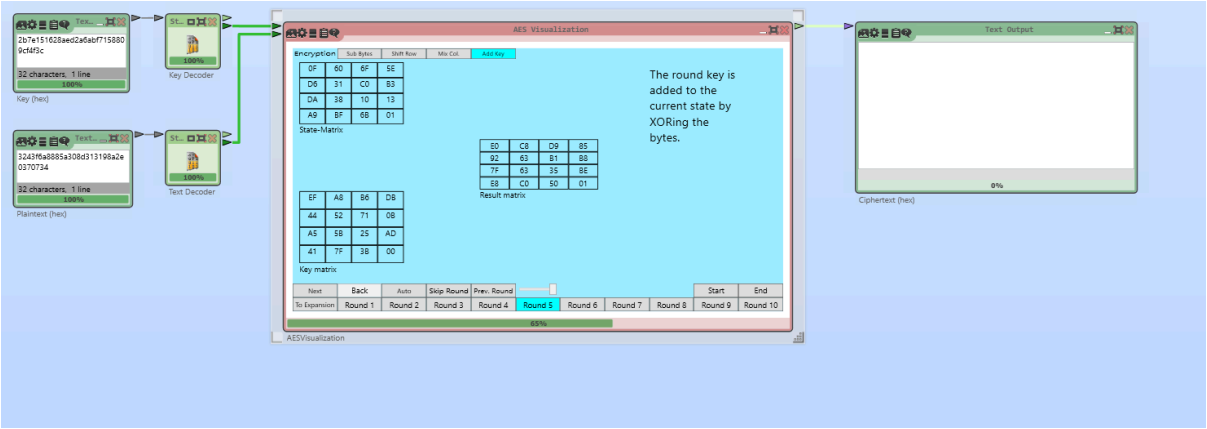
Mix column:



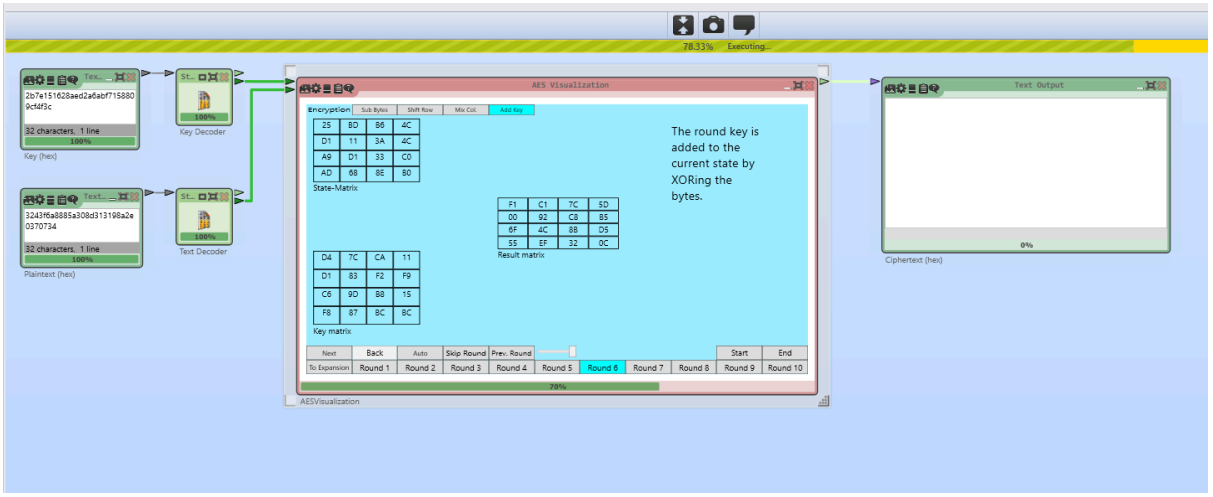
Add round key:



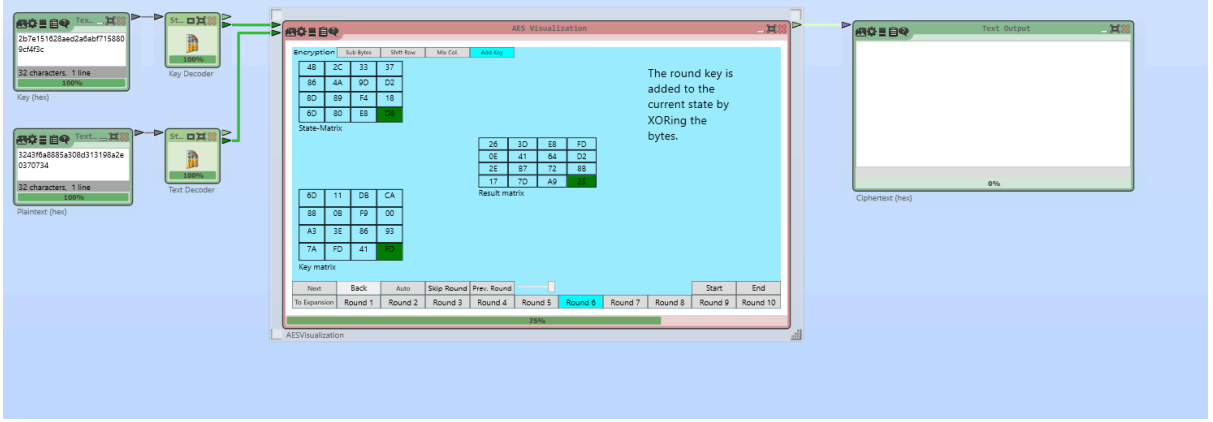
Round 4:



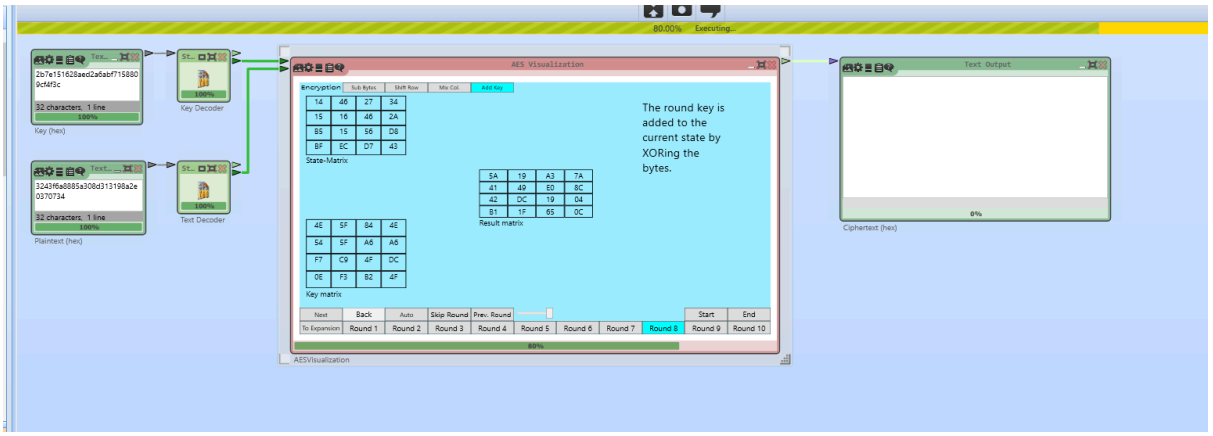
Round 5:



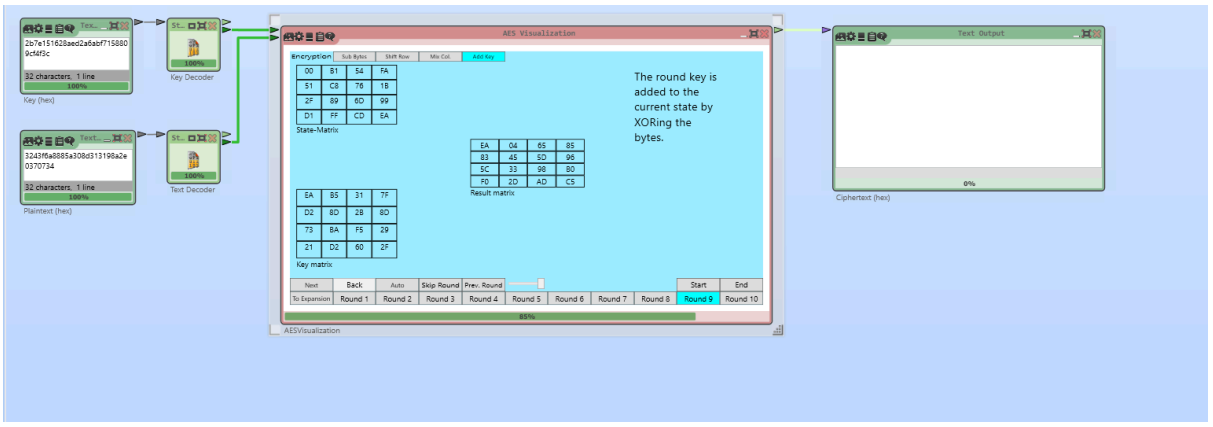
Round 6:



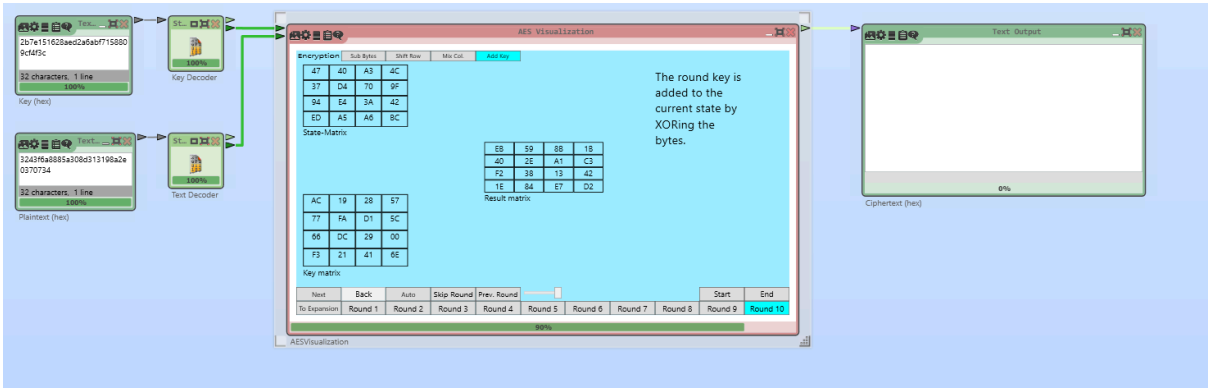
Round 7:



Round 8:

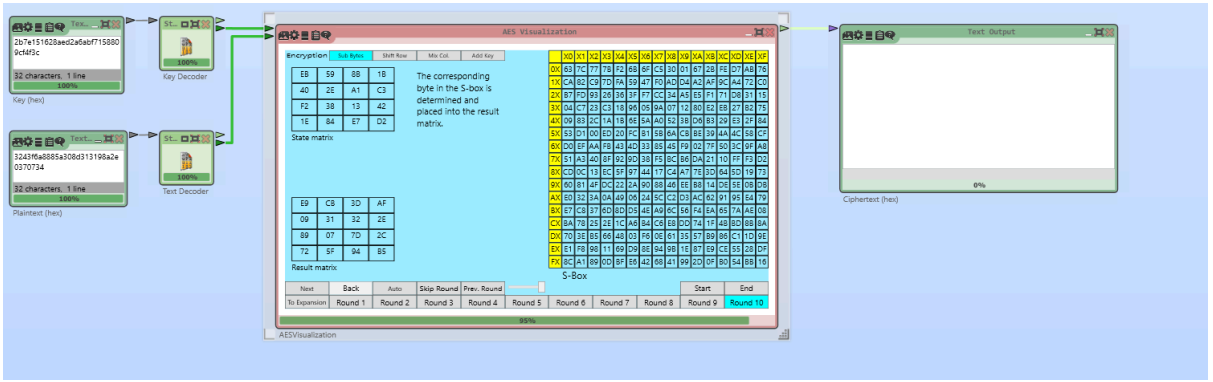


Round 9:

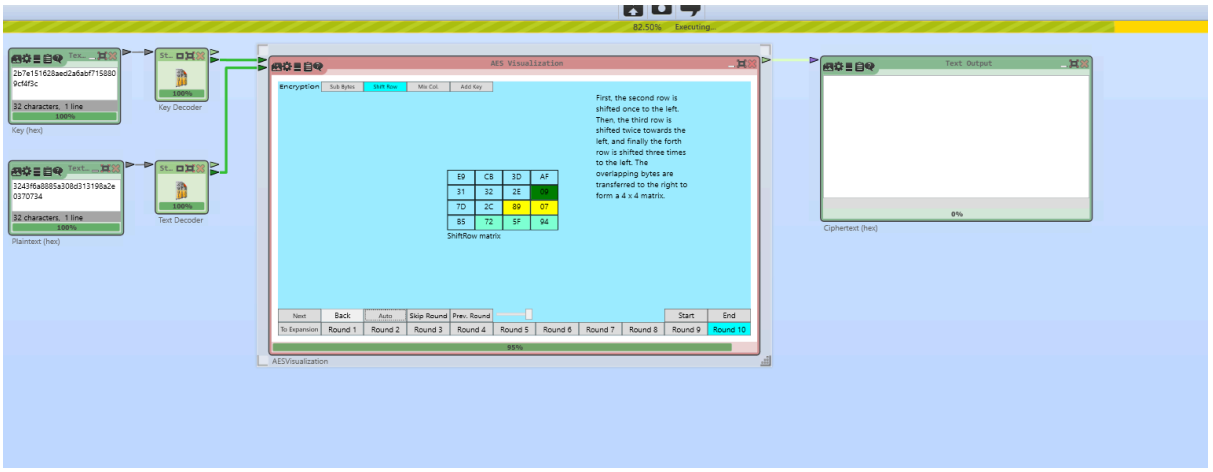


Round10:

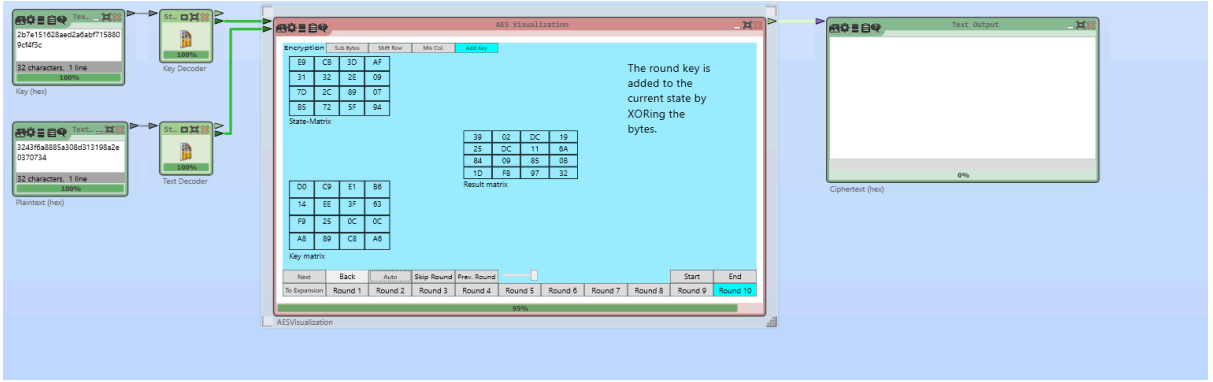
s-box:



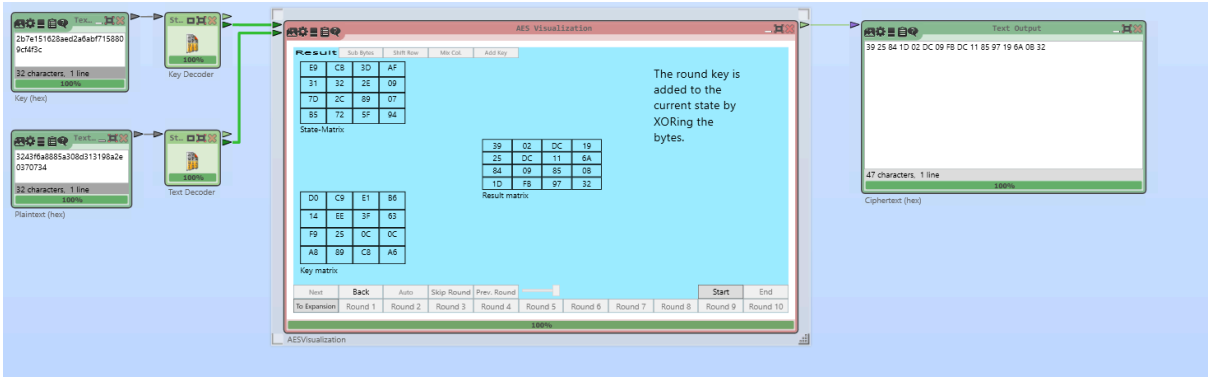
Shift row:



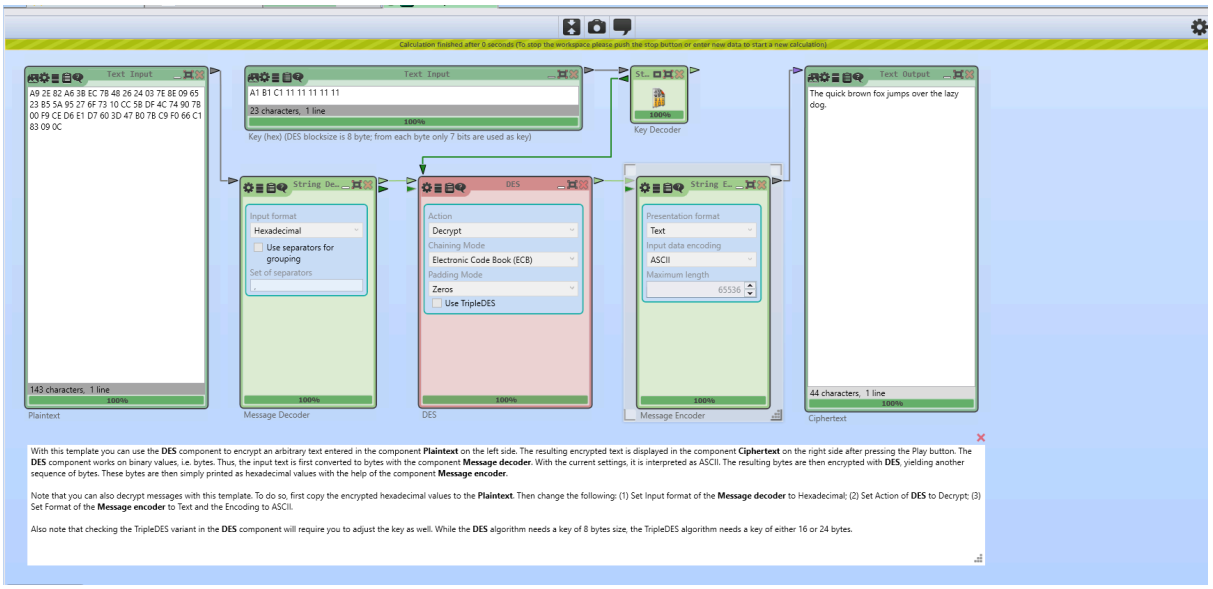
Add round key:

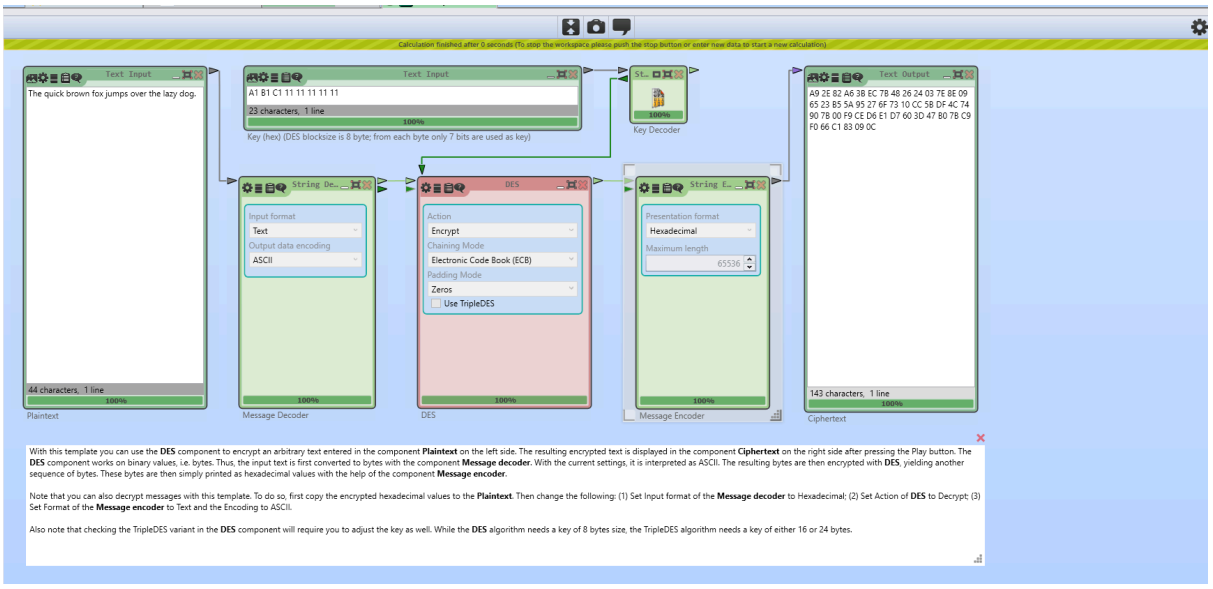


Cipher text:

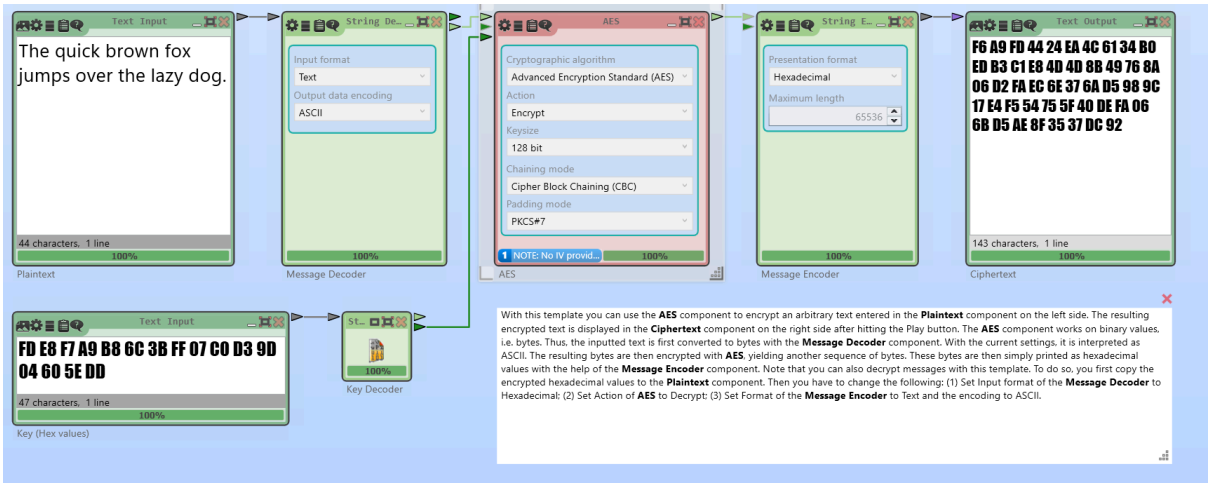


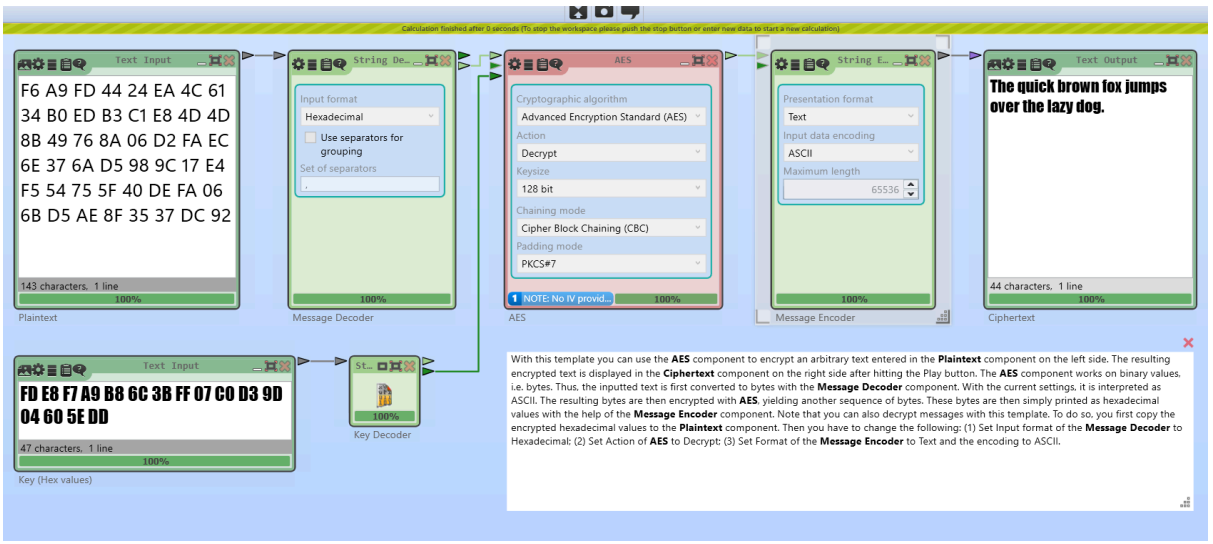
DES Decryption:





AES:




Calculation finished after 0 seconds (To stop the workspace please push the stop button or enter new data to start a new calculation).
Text Input
F6 A9 FD 44 24 EA 4C 61
34 B0 ED B3 C1 E8 4D 4D
8B 49 76 8A 06 D2 FA EC
6E 37 6A D5 98 9C 17 E4
F5 54 75 5F 40 DE FA 06
6B D5 AE 8F 35 37 DC 92
143 characters, 1 line
100%
Plaintext
String De...
Input format
Hexadecimal
Use separators for grouping
Set of separators
,
100%
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Cipher Block Chaining (CBC)
Padding mode
PKCS#7
1 NOTE: No IV provid...
100%
AES
String E...
Presentation format
Text
Input data encoding
ASCII
Maximum length
65536
100%
Message Encoder
Text Output
The quick brown fox jumps over the lazy dog.
44 characters, 1 line
100%
Ciphertext
Text Input
FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D
04 60 5E DD
47 characters, 1 line
100%
Key (Hex values)
St...
100%
Key Decoder
With this template you can use the AES component to encrypt an arbitrary text entered in the Plaintext component on the left side. The resulting encrypted text is displayed in the Ciphertext component on the right side after hitting the Play button. The AES component works on binary values, i.e. bytes. Thus, the inputted text is first converted to bytes with the Message Decoder component. With the current settings, it is interpreted as ASCII. The resulting bytes are then encrypted with AES, yielding another sequence of bytes. These bytes are then simply printed as hexadecimal values with the help of the Message Encoder component. Note that you can also decrypt messages with this template. To do so, you first copy the encrypted hexadecimal values to the Plaintext component. Then you have to change the following: (1) Set Input format of the Message Decoder to Hexadecimal; (2) Set Action of AES to Decrypt; (3) Set Format of the Message Encoder to Text and the encoding to ASCII.