Network Security (CSE350)
Jan-May 2023 at IIITD

Programming Assignment no. 2
Project Number - 0

By Group Number 2
Utkrisht Sikka (utkrisht19215@iiitd.ac.in)
Tanya Gupta (tanya19119@iiitd.ac.in)

Encryption

- DES_encryption(K,P):
  - Takes in the 64 bit master key K and 64 bit plaintext P as input.
  - It in turn calls the functions
    - key_gen(K) - generates the 16 48 bit subkeys
    - initial_permutation(P)
    - DES_round(c_i,k_i)
      - Simulates a round of the DES algo and in turn makes a call to the F_box function
      - Takes in a 64 bit c_i and the 48 bit round subkey k_i
      - This function is called 16 times
    - swap_32_bit(C) - performs the 32 bit swap of the resulting C from round 16
    - inverse_initial_permutation(C) - performs inverse initial permutation of the resultant C from the 32 bit swap.

Decryption

- DES_decryption(K,P):
  - Takes in the 64 bit master key K and 64 bit plaintext P as input.
  - It in turn calls the functions
    - key_gen(K) - generates the 16 48 bit subkeys
    - reverse the list of 16 keys
    - initial_permutation(P)
    - DES_round(c_i,k_i)
      - Simulates a round of the DES algo and in turn makes a call to the F_box function
      - Takes in a 64 bit c_i and the 48 bit round subkey k_i
      - This function is called 16 times
    - swap_32_bit(C) - performs the 32 bit swap of the resulting C from round 16
    - inverse_initial_permutation(C) - performs inverse initial permutation of the resultant C from the 32 bit swap.

Sample Input Output 1

Key = 0000111100010101011100011100100101000111110110011111010000101100 1

```
Plaintext:  0x2468ace 0xeca86420
After encryption
C after initial_permutation:  0x5a005a00 0x3cf03c0f
C after round  1 :  0x3cf03c0f 0xbad22845
C after round  2 :  0xbad22845 0x99e9b723
C after round  3 :  0x99e9b723 0xbae3b9e
C after round  4 :  0xbae3b9e 0x42415649
C after round  5 :  0x42415649 0x18b3fa41
C after round  6 :  0x18b3fa41 0x9616fe23
C after round  7 :  0x9616fe23 0x67117cf2
C after round  8 :  0x67117cf2 0xc11bfc09
C after round  9 :  0xc11bfc09 0x887fbc6c
C after round  10 :  0x887fbc6c 0x600f7e8b
C after round  11 :  0x600f7e8b 0xf596506e
C after round  12 :  0xf596506e 0x738538b8
C after round  13 :  0x738538b8 0xc6a62c4e
C after round  14 :  0xc6a62c4e 0x56b0bd75
C after round  15 :  0x56b0bd75 0x75e8fd8f
C after round  16 :  0x75e8fd8f 0x25896490
C after 32 bit swap:  0x25896490 0x75e8fd8f
C after inverse_initial_permutation:  0xda02ce3a 0x89ecac3b
final C:  0xda02ce3a 0x89ecac3b
```

original plaintext

Output of 1st encryption round

Output of 14th encryption round

```
After decryption
P2 after initial_permutation:  0x25896490 0x75e8fd8f
P2 after round  1 :  0x75e8fd8f 0x56b0bd75
P2 after round  2 :  0x56b0bd75 0xc6a62c4e
P2 after round  3 :  0xc6a62c4e 0x738538b8
P2 after round  4 :  0x738538b8 0xf596506e
P2 after round  5 :  0xf596506e 0x600f7e8b
P2 after round  6 :  0x600f7e8b 0x887fbc6c
P2 after round  7 :  0x887fbc6c 0xc11bfc09
P2 after round  8 :  0xc11bfc09 0x67117cf2
P2 after round  9 :  0x67117cf2 0x9616fe23
P2 after round  10 :  0x9616fe23 0x18b3fa41
P2 after round  11 :  0x18b3fa41 0x42415649
P2 after round  12 :  0x42415649 0xbae3b9e
P2 after round  13 :  0xbae3b9e 0x99e9b723
P2 after round  14 :  0x99e9b723 0xbad22845
P2 after round  15 :  0xbad22845 0x3cf03c0f
P2 after round  16 :  0x3cf03c0f 0x5a005a00
P2 after 32 bit swap:  0x5a005a00 0x3cf03c0f
P2 after inverse_initial_permutation:  0x2468ace 0xeca86420
```

Output after 2nd decryption round

Output after 15th decryption round

ciphertext after decryption

Sample Input Output 2

Key = 0111001000110110100010101101011111011000111100001101100001001000 1

```
Plaintext:  0x8172abe1 0x1b1c1c12
After encryption
C after initial_permutation:  0xaf2601d 0xd0e7496
C after round  1 :  0xd0e7496 0xe2de1b9
C after round  2 :  0xe2de1b9 0xb78e1533
C after round  3 :  0xb78e1533 0xe36d86ab
C after round  4 :  0xe36d86ab 0x4e77ba7f
C after round  5 :  0x4e77ba7f 0x768297f1
C after round  6 :  0x768297f1 0xdb05c8be
C after round  7 :  0xdb05c8be 0xf7064566
C after round  8 :  0xf7064566 0x4a58c712
C after round  9 :  0x4a58c712 0xf4ed7f1
C after round  10 :  0xf4ed7f1 0x7cc5e2b2
C after round  11 :  0x7cc5e2b2 0x57b918c1
C after round  12 :  0x57b918c1 0xc9455767
C after round  13 :  0xc9455767 0xb1d7ae46
C after round  14 :  0xb1d7ae46 0xda742580
C after round  15 :  0xda742580 0x6fe5d0de
C after round  16 :  0x6fe5d0de 0x3f0cd194
C after 32 bit swap:  0x3f0cd194 0x6fe5d0de
C after inverse_initial_permutation:  0xe4c2f3d2 0x4fe0ae2f
final C:  0xe4c2f3d2 0x4fe0ae2f
```

original plaintext

Output of 1st encryption round

Output of 14th encryption round

```
After decryption
P2 after initial_permutation:  0x3f0cd194 0x6fe5d0de
P2 after round  1 :  0x6fe5d0de 0xda742580
P2 after round  2 :  0xda742580 0xb1d7ae46
P2 after round  3 :  0xb1d7ae46 0xc9455767
P2 after round  4 :  0xc9455767 0x57b918c1
P2 after round  5 :  0x57b918c1 0x7cc5e2b2
P2 after round  6 :  0x7cc5e2b2 0xf4ed7f1
P2 after round  7 :  0xf4ed7f1 0x4a58c712
P2 after round  8 :  0x4a58c712 0xf7064566
P2 after round  9 :  0xf7064566 0xdb05c8be
P2 after round  10 :  0xdb05c8be 0x768297f1
P2 after round  11 :  0x768297f1 0x4e77ba7f
P2 after round  12 :  0x4e77ba7f 0xe36d86ab
P2 after round  13 :  0xe36d86ab 0xb78e1533
P2 after round  14 :  0xb78e1533 0xe2de1b9
P2 after round  15 :  0xe2de1b9 0xd0e7496
P2 after round  16 :  0xd0e7496 0xaf2601d
P2 after 32 bit swap:  0xaf2601d 0xd0e7496
P2 after inverse_initial_permutation:  0x8172abe1 0x1b1c1c12
```

Output after 2nd decryption round

Output after 15th decryption round

ciphertext after decryption