Design and Implementation of a DES Encryption

Student Details:

- Pranjal Bharti, 2021080
- Daksh Bhasin, 201035

Introduction & Objectives

What is DES?

- A symmetric-key block cipher operating on 64-bit blocks
- Uses a 64-bit key (56 effective bits)

Project Objectives:

- Implement DES from scratch (no external libraries)
- Capture intermediate round states during encryption and decryption
- Verify:
  - (a) Decryption recovers the original plaintext
  - (b) 1st encryption round equals 15th decryption round (after swapping halves)
  - (c) 14th encryption round equals 2nd decryption round (after swapping halves)

System Overview & Data Representation

DES Process Overview:

- Initial Permutation (IP) → 16 Feistel Rounds → Final Permutation (IP^{-1})

Key Scheduling:

- PC-1: Reduces 64-bit key to 56 bits
- Left shifts and PC-2: Generate 16 round keys (48 bits each)

Data Representation:

- Plaintext, ciphertext, and keys are in hexadecimal
- 16 hex characters represent 64 bits (4 bits per character)

Detailed System Design

Encryption Flow:

Apply IP, split into L and R halves

Execute 16 Feistel rounds: Expand, XOR with round key, S-box substitution, and permutation

Final swap and apply IP^{-1} to produce ciphertext

Decryption Flow:

Mirror encryption steps using round keys in reverse order

Ensure the reversibility of the process

Intermediate State Capture:

Record state after each round in both encryption and decryption

Intermediate Round Verification

Verification (b):

Compare 1st encryption round state with 15th decryption round state

Note: Due to the Feistel structure, swap decryption state halves before comparing

Verification (c):

Compare 14th encryption round state with 2nd decryption round state

Note: Again, swap halves of the decryption round state for an accurate match

Implementation Challenges

Bit-Level Operations:

- Implementing correct permutations, shifts, and XOR operations

Intermediate State Handling:

- Capturing and managing 64-bit states across rounds
- Adjusting for the “mirrored” nature of decryption outputs

Testing and Validation:

- Use of standard hexadecimal test vectors (e.g., "0123456789ABCDEF", "0000000000000000")
- Debugging and ensuring correctness through intermediate verifications

Results & Conclusions

Verification Success:

- Decrypted output matches the original plaintext
- 1st encryption round equals 15th decryption round (post-swap)
- 14th encryption round equals 2nd decryption round (post-swap)

Conclusions:

- Successful implementation of DES from scratch
- Validation of DES properties and intermediate round verifications
- Enhanced understanding of symmetric-key cryptography and Feistel networks

```
Test Pair 1:
Key:       133457799BBCDFF1
Plaintext: 0123456789ABCDEF
================================
Ciphertext: 85E813540F0AB405
Decrypted:  0123456789ABCDEF
Verification (a): SUCCESS - Decrypted text matches the original plaintext.

1st Encryption Round:          F0AAF0AAEF4A6544
15th Decryption Round (swapped): F0AAF0AAEF4A6544
Verification (b): SUCCESS - 1st encryption round equals 15th decryption round (after swapping).

14th Encryption Round:         18C3155AC28C960D
2nd Decryption Round (swapped):  18C3155AC28C960D
Verification (c): SUCCESS - 14th encryption round equals 2nd decryption round (after swapping).

================================
Test Pair 2:
Key:       AABB09182736CCDD
Plaintext: 1234567890ABCDEF
================================
Ciphertext: 2482286C96BBD75F
Decrypted:  1234567890ABCDEF
Verification (a): SUCCESS - Decrypted text matches the original plaintext.

1st Encryption Round:          F0AAE8A5116BA133
15th Decryption Round (swapped): F0AAE8A5116BA133
Verification (b): SUCCESS - 1st encryption round equals 15th decryption round (after swapping).

14th Encryption Round:         E884876803AADF6C
2nd Decryption Round (swapped):  E884876803AADF6C
Verification (c): SUCCESS - 14th encryption round equals 2nd decryption round (after swapping).

================================
Test Pair 3:
Key:       FFFFFFFFFFFFFFFF
Plaintext: 0000000000000000
================================
Ciphertext: CAAAAF4DEAF1DBAE
Decrypted:  0000000000000000
Verification (a): SUCCESS - Decrypted text matches the original plaintext.

1st Encryption Round:          0000000038DBF9CB
15th Decryption Round (swapped): 0000000038DBF9CB
Verification (b): SUCCESS - 1st encryption round equals 15th decryption round (after swapping).

14th Encryption Round:         044D9D35472AC861
2nd Decryption Round (swapped):  044D9D35472AC861
Verification (c): SUCCESS - 14th encryption round equals 2nd decryption round (after swapping).
```


thank
you