cs7349-001c-1252-final

Garrett Gruss | **4/27/2025**

Installation

1. **Clone the repo**

```
git clone https://github.com/GarrettGruss/cs7349-001c-1252-final.git
cd cs7349-001c-1252-final
```

2. **Create venv with poetry**

```
poetry config virtualenvs.in-project true
```

3. **Install dependencies**

```
poetry install
```

4. **Activate the venv**

   - **Unix / macOS**

```
source .venv/bin/activate
```

   - **Windows (PowerShell)**

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
.\.venv\Scripts\Activate.ps1
```

Demos

DES demo

```
poetry run python -m cs7349_001c_1252_final.scripts.des_cipher
```

RSA demo

```
poetry run python -m cs7349_001c_1252_final.scripts.rsa_cipher
```

tests

```
poetry run pytest
```

To run tests in verbose mode (shows more detailed log messages).

```
poetry run pytest -v --log-cli-level=DEBUG
```

Project Report

Assignment: You are required to write a project report by solving the above problems. Describe your design clearly and your observations. Submit a copy of your code. Your grade will be based on the clarity and thoroughness of your report.

Problem 1. Modern Symmetric Cipher & Decipher Implementation

Assignment: Program to implement the DES or AES algorithm. You can choose either one based on your interest and use any programming language you like, such as C, C++, Java, and python. Directly using des or aes libraries receives 0 for this problem. Your program does not need to encode a plaintext exactly the same as the existing library function. But you need to specify in your report how you implement each component of the cipher/decipher in both text and code segments. And how many rounds? You can refer to the DES or AES algorithm designs in the lecture notes or some similar designs. Show that your encryption and decryption function work using example plaintexts.

1.1 Overview & Components

This script implements the DES cipher over 16 feistel rounds.

1. **cs7349_001c_1252_final.scripts.des_cipher.py** Contains the core functionality of the cipher
    - `bytes_to_bit_array` Converts a byte into 8 bits (big-endian).
    - `bit_array_to_bytes` Packs a bit list into bytes.
    - `permute` Applies a permutation table.
    - `left_shift` Performs a circular left shift by *n* bits.
    - `xor` Performs a bitwise XOR of two bit-vectors.
    - `generate_subkeys` Produces sixteen 48-bit round keys.
    - `sbox_substitution` Splits the 48-bit input into eight 6-bit blocks, looks up each in its S-box, and concatenates the eight 4-bit outputs.
    - `feistel` Performs E-Box expansions, XOR, S-Box substitution, and P-permutation.

- `process_block` Performs initial permutation, 16 rounds of Feistal, and final permutation
- `pad` Pads data.
- `des_encrypt` Performs the overall DES encryption process.
- `des_decrypt` Performs the overall DES decryption process.

2. **cs7349_001c_1252_final.config.des_constants.py**

- Contains the DES tables
- `INITIAL_PERMUTATION`
- `FINAL_PERMUTATION`
- `EXPANSION_PERMUTATION`
- `P_PERMUTATION`
- `PERMUTATION_CHOICE_1`
- `PERMUTATION_CHOICE_2`
- `S_BOXES`
- `SHIFT_SCHEDULE`

1.2 Overall Flow

The DES encryption algorithm pads the UTF-8 plaintext to the nearest 8-byte multiple with PKCS#5, then processes each 64-bit block using an initial permutation, sixteen rounds of the Feistel function, and finishes with a final permutation.

```
def des_encrypt(plaintext: str, key: bytes) -> str:
    if len(key) != 8:
        raise ValueError("Key must be 8 bytes long.")
    data = pad(plaintext.encode('utf-8'))
    subkeys = generate_subkeys(key)
    encrypted = b''
    for i in range(0, len(data), 8):
        encrypted += process_block(data[i:i+8], subkeys, encrypt=True)
    return encrypted.hex()
```

The eight-byte is transformed to a 64-bit list. Each round then uses the Feistel function and exchanges the halves. This process is performed for 16 rounds, and the final output halves are then exchanged, and a final permutation is performed.

```
def process_block(block: bytes, subkeys: List[List[int]], encrypt: bool = True) ->
bytes:
    bits = bytes_to_bit_array(block)
    permuted = permute(bits, INITIAL_PERMUTATION)
    logger.debug(f"Initial Permutation applied:
{bit_array_to_bytes(permuted).hex()}")

    left, right = permuted[:32], permuted[32:]
    keys = subkeys if encrypt else list(reversed(subkeys))

    for i, key in enumerate(keys, start=1):
```

```
        temp = right.copy()
        f_out = feistel(right, key)
        right = xor(left, f_out)
        left = temp
        logger.debug(f"Round {i:2d} L={bit_array_to_bytes(left).hex()} R=
{bit_array_to_bytes(right).hex()}")

    combined = right + left  # swap halves
    final_bits = permute(combined, FINAL_PERMUTATION)
    output = bit_array_to_bytes(final_bits)
    logger.debug(f"Final Permutation applied: {output.hex()}")
    return output
```

Decryption is similar, relying on the same logic but with the subkeys passed in reverse order.

1.3 Feistel Function

Each Feistel round applies a non-linear mixing of the 32-bit right half with a 48-bit subkey. The feistel function performs:

Each Feistel round uses a non-linear mixing of the 32-bit R side with a 48-bit subkey:

1. 32-bit to 48-bit expansion permutation (E-box) by duplicating and reordering according to the standard DES expansion table.
2. XOR the expanded bits with the related bit from round subkey.
3. S-box Substitution by splitting the The 48-bit result into eight 6-bit blocks; for block i, the first and last bits form a row index and the middle four form a column index into S_BOXES, yielding a 4-bit value each. The eight 4-bit outputs are concatenated to 32 bits. S-box Substitution by splitting the 48-bit Result into 8 6-bit blocks.
4. P-Permutation by permutation over 32-bit string to generate diffusion.

```
def feistel(right: List[int], subkey: List[int]) -> List[int]:
    expanded = permute(right, EXPANSION_PERMUTATION)
    logger.debug(f"Expanded R: {bit_array_to_bytes(expanded).hex()}")
    xored = xor(expanded, subkey)
    logger.debug(f"After XOR:   {bit_array_to_bytes(xored).hex()}")
    substituted = sbox_substitution(xored)
    logger.debug(f"After S-box: {bit_array_to_bytes(substituted).hex()}")
    return permute(substituted, P_PERMUTATION)
```

1.4 Key Schedule

The key schedule generates the sixteen 48-bit round keys that are utilized during the feistal functions. To generate the subkeys, the user key is permuted into a 64-bit array using the Permucation Choice 1. For the sixteen rounds, the halves are exchanged by the SHIFT_SCHEDULE[i-1] and a permutation of Permutation Choice 2.

```
def generate_subkeys(key_bytes: bytes) -> List[List[int]]:
    key_bits = bytes_to_bit_array(key_bytes)
    permuted = permute(key_bits, PERMUTATION_CHOICE_1)
    C, D = permuted[:28], permuted[28:]
    subkeys: List[List[int]] = []
    for i, shift in enumerate(SHIFT_SCHEDULE):
        C = left_shift(C, shift)
        D = left_shift(D, shift)
        combined = C + D
        subkey = permute(combined, PERMUTATION_CHOICE_2)
        logger.debug(f"Subkey {i+1:2d}: {bit_array_to_bytes(subkey).hex()}")
        subkeys.append(subkey)
    return subkeys
```

1.5 Code Example

The following main entry point can be used to verify the DES cipher. A key of `secr3t_k` and plain text of `Hello, DES!` is used. The log output shows the subkey generation, initial permutation, 16 rounds of Feistal (two log streams for each half), and the final permutation. The ciphertext is displayed, and the process repeated to decrypt the text. The log output details the internal logic being performed by the script.

```
if __name__ == "__main__":
    setup_logging()
    key = b"secr3t_k"
    sample = "Hello, DES!"
    cipher = des_encrypt(sample, key)
    logger.info(f"Encrypted: {cipher}")
    plain = des_decrypt(cipher, key)
    logger.info(f"Decrypted: {plain}")
```

Log Output

```
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  1:
80beee746913
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  2:
f0a6d6b68985
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  3:
74de36c207d3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  4:
e6b1765fa309
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  5:
aec677725548
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  6:
ef533a48b12e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  7:
ae93f9e47ca8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  8:
```

```
9f5a5b681a7b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  9:
3d4bdbeac530
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 10:
37719d894f0e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 11:
1f0dd5dc5290
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 12:
5f68bdd1426d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 13:
9fa5ac92ba88
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 14:
da0eafb03735
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 15:
f9ba2c3b2aa2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 16:
f1bcae0263e7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:88 DEBUG: Initial
Permutation applied: 9f00be12007e3d10
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0003fc1fa8a0
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
80bd126bc1b3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 42220bec
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  1
L=007e3d10 R=c7701a37
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: e0eba00f41af
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
104d76b9c82a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d8ee851c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  2
L=c7701a37 R=0bb78c7e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 057dafc583fc
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
71a39907842f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 0051e13d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  3
L=0bb78c7e R=48753697
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: a503aa9ad4ae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
43b2dcc577a7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 35446e17
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  4
L=48753697 R=1990d6c4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0f3ca16ad608
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
```

```
a1fad6188340
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d595191d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  5
L=1990d6c4 R=f6f5cfa5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: fad7abe5fd0b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
158491ad4c25
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 7cd4e3ae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  6
L=f6f5cfa5 R=14bf6177
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a95feb02bae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
240607545706
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: efb5f464
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  7
L=14bf6177 R=13691819
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a6b528f00f2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
153109e71a89
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 7096ab3a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  8
L=13691819 R=0bddd6f5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 857efbead7aa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
b8352000129a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: bdca2a00
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  9
L=0bddd6f5 R=03805bcb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 807c002f7e56
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
b70d9da63158
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 15ce13b5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 10
L=03805bcb R=29bcab86
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 153df9557c0c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
0a302c892e9c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 48a72d5c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 11
L=29bcab86 R=99d8ea67
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
```

```
R: cf3ef175430f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
90564ca40162
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: e4c91cbb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 12
L=99d8ea67 R=933f24df
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ca69fe9096ff
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
55cc52022c77
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: c5422e90
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 13
L=933f24df R=8b392afe
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 4569f29557fd
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
9f675d2560c8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 26fe4406
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 14
L=8b392afe R=d77837a3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: eaebf01afd07
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
1351dc21d7a5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d794731e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 15
L=d77837a3 R=e59fdb4c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 70bcffef6a59
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
810051ed09be
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 49d440d8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 16
L=e59fdb4c R=d965e6a2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:103 DEBUG: Final
Permutation applied: f82db66a6895deed
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:88 DEBUG: Initial
Permutation applied: 0302f9ff00040002
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 000008000004
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
80bee6746917
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 42508fbb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  1
L=00040002 R=5c2155f6
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 2f8102aabfac
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
```

```
df27d41c3629
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: e818cf54
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  2
L=5c2155f6 R=17b8a26a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0afdf1504354
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
7e23c7924487
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 8ea51fc8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  3
L=17b8a26a R=a49964eb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: d094f2b09757
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
362584ef345e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: de7e4ee7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  4
L=a49964eb R=43473e15
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: a06a0e9fc0aa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
0eac79ed95e2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: f44c40cb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  5
L=43473e15 R=ac0efeb8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 55805d7fd5f1
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
bad3673764df
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: b466da32
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  6
L=ac0efeb8 R=70a02803
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ba1500150006
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
1486f9f17cae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 76bc0ef2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  7
L=70a02803 R=fa3c69e7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ff41f8353f0f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
601ba35d2574
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 530fad5a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  8
L=fa3c69e7 R=abf2d8c9
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
```

```
R: d57fa56f1653
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
e8347e85d363
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: ad24b311
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  9
L=abf2d8c9 R=d9941373
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ef3ca80a6ba7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
d84d358324a9
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 782540c4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 10
L=d9941373 R=2bee4aee
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 157f5c25575c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
0a7289f905cc
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 4136e0cb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 11
L=2bee4aee R=d4c2cbf6
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 6a9605657fad
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
35feb8b43dc0
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d5a52ffd
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 12
L=d4c2cbf6 R=b15eb751
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: da2afd5aeaa3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
458f51c8502b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: ac24944a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 13
L=b15eb751 R=fd58d9ea
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 7faaf16f3f55
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
a5a45edf0860
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 402f9767
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 14
L=fd58d9ea R=102c0b3d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a01580569fa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
73bb743e4358
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 05831f15
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 15
```

```
L=102c0b3d R=4f38b0d2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 25e9f15a16a4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
d4555f587543
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 3459f25f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 16
L=4f38b0d2 R=bf1b01cf
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:103 DEBUG: Final
Permutation applied: d5d3c1f17a68834b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:144 INFO: Encrypted:
f82db66a6895deedd5d3c1f17a68834b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  1:
80beee746913
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  2:
f0a6d6b68985
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  3:
74de36c207d3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  4:
e6b1765fa309
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  5:
aec677725548
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  6:
ef533a48b12e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  7:
ae93f9e47ca8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  8:
9f5a5b681a7b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey  9:
3d4bdbeac530
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 10:
37719d894f0e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 11:
1f0dd5dc5290
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 12:
5f68bdd1426d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 13:
9fa5ac92ba88
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 14:
da0eafb03735
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 15:
f9ba2c3b2aa2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:58 DEBUG: Subkey 16:
f1bcae0263e7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:88 DEBUG: Initial
Permutation applied: d965e6a2e59fdb4c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 70bcffef6a59
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
810051ed09be
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 49d440d8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  1
```

```
L=e59fdb4c R=d77837a3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: eaebf01afd07
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
1351dc21d7a5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d794731e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  2
L=d77837a3 R=8b392afe
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 4569f29557fd
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
9f675d2560c8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 26fe4406
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  3
L=8b392afe R=933f24df
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ca69fe9096ff
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
55cc52022c77
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: c5422e90
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  4
L=933f24df R=99d8ea67
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: cf3ef175430f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
90564ca40162
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: e4c91cbb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  5
L=99d8ea67 R=29bcab86
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 153df9557c0c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
0a302c892e9c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 48a72d5c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  6
L=29bcab86 R=03805bcb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 807c002f7e56
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
b70d9da63158
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 15ce13b5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  7
L=03805bcb R=0bddd6f5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 857efbead7aa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
b8352000129a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
```

```
box: bdca2a00
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  8
L=0bddd6f5 R=13691819
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a6b528f00f2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
153109e71a89
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 7096ab3a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  9
L=13691819 R=14bf6177
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a95feb02bae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
240607545706
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: efb5f464
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 10
L=14bf6177 R=f6f5cfa5
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: fad7abe5fd0b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
158491ad4c25
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 7cd4e3ae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 11
L=f6f5cfa5 R=1990d6c4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0f3ca16ad608
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
a1fad6188340
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d595191d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 12
L=1990d6c4 R=48753697
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: a503aa9ad4ae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
43b2dcc577a7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 35446e17
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 13
L=48753697 R=0bb78c7e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 057dafc583fc
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
71a39907842f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 0051e13d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 14
L=0bb78c7e R=c7701a37
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: e0eba00f41af
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
```

```
104d76b9c82a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: d8ee851c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 15
L=c7701a37 R=007e3d10
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0003fc1fa8a0
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
80bd126bc1b3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 42220bec
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 16
L=007e3d10 R=9f00be12
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:103 DEBUG: Final
Permutation applied: 48656c6c6f2c2044
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:88 DEBUG: Initial
Permutation applied: bf1b01cf4f38b0d2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 25e9f15a16a4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
d4555f587543
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 3459f25f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  1
L=4f38b0d2 R=102c0b3d
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 8a01580569fa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
73bb743e4358
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 05831f15
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  2
L=102c0b3d R=fd58d9ea
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 7faaf16f3f55
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
a5a45edf0860
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 402f9767
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  3
L=fd58d9ea R=b15eb751
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: da2afd5aeaa3
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
458f51c8502b
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: ac24944a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  4
L=b15eb751 R=d4c2cbf6
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 6a9605657fad
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
35feb8b43dc0
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
```

```
box: d5a52ffd
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  5
L=d4c2cbf6 R=2bee4aee
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 157f5c25575c
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
0a7289f905cc
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 4136e0cb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  6
L=2bee4aee R=d9941373
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ef3ca80a6ba7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
d84d358324a9
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 782540c4
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  7
L=d9941373 R=abf2d8c9
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: d57fa56f1653
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
e8347e85d363
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: ad24b311
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  8
L=abf2d8c9 R=fa3c69e7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ff41f8353f0f
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
601ba35d2574
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 530fad5a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round  9
L=fa3c69e7 R=70a02803
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: ba1500150006
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
1486f9f17cae
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 76bc0ef2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 10
L=70a02803 R=ac0efeb8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 55805d7fd5f1
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
bad3673764df
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: b466da32
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 11
L=ac0efeb8 R=43473e15
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: a06a0e9fc0aa
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
```

```
0eac79ed95e2
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: f44c40cb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 12
L=43473e15 R=a49964eb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: d094f2b09757
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
362584ef345e
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: de7e4ee7
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 13
L=a49964eb R=17b8a26a
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 0afdf1504354
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
7e23c7924487
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 8ea51fc8
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 14
L=17b8a26a R=5c2155f6
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 2f8102aabfac
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
df27d41c3629
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: e818cf54
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 15
L=5c2155f6 R=00040002
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:77 DEBUG: Expanded
R: 000008000004
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:79 DEBUG: After XOR:
80bee6746917
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:81 DEBUG: After S-
box: 42508fbb
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:98 DEBUG: Round 16
L=00040002 R=0302f9ff
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:103 DEBUG: Final
Permutation applied: 4553210505050505
2025-04-27 20:55:36 cs7349_001c_1252_final.scripts.des_cipher:146 INFO: Decrypted:
Hello, DES!
```

Problem 2. RSA Crypto System

Assignment

1. Write a prime number check program to check any input number to be whether a prime number.
2. Find the 10th and the 19th prime numbers p and q between 1000 and 10000 to build an RSA crypto system. Write down the public key PU = {e, n} and the private key PR = {d, p, q}.
3. Program to implement the encipher and decipher. Test your RSA crypto system by encrypting and decrypting a message “rsa” (Map each letter to 0 - 25).

4. If an adversary obtains the public key PU = {e, n}, demonstrate how the adversary uses the exhaustive search to get the private key d and show the time cost of the search.

1.1 Overview

1. **Prime number Check** The primality check function works by first checking the edge cases of divisibility by 2 and 3, then iterates through potential factors of the form $6k \pm 1$ up to $\sqrt{n}$.

```python
def is_prime(n: int) -> bool:
    if n <= 1:
        return False
    if n <= 3:
        return True
    if n % 2 == 0 or n % 3 == 0:
        return False
    i = 5
    while i * i <= n:
        if n % i == 0 or n % (i + 2) == 0:
            return False
        i += 6
    return True
```

2. **Key Generation** The following logic finds the 10th and 19th prime numbers p and q between 1000 and 10000, the public key PU = {e, n}, and private key PR = {d, p, q}. The inclusive range was iterated over with the is_prime function to yield the 10th and 19th prime numbers. The modulus was then computed using $n = p \times q$ and Euler's totient function using $\phi(n) = (p - 1)(q - 1)$. The common public exponent e = 65,537 was used after confirming $\gcd(e, \phi(n)) = 1$. The private exponent d was determined using the extended euclidean algorithm to satisfy the congruence $e \cdot d \equiv 1 \pmod{\phi(n)}$.

```python
def find_primes_in_range(start: int, end: int) -> List[int]:
    logger.debug(f"Finding primes between {start} and {end}")
    primes = [n for n in range(start, end + 1) if is_prime(n)]
    logger.debug(f"Found {len(primes)} primes in range")
    return primes

def ext_euclidean(a: int, b: int) -> Tuple[int, int, int]:
if a == 0:
    return (b, 0, 1)
g, y, x = ext_euclidean(b % a, a)
return (g, x - (b // a) * y, y)

def mod_inv(a: int, m: int) -> int:
    logger.debug(f"Computing modular inverse of {a} mod {m}")
    g, x, _ = ext_euclidean(a, m)
    if g != 1:
        logger.error(f"Modular inverse does not exist for {a} mod {m}")
        raise ValueError(f"Modular inverse does not exist for {a} mod {m}")
    inverse = x % m
```

```
    logger.debug(f"Modular inverse is {inverse}")
    return inverse

def generate_rsa_keys() -> Tuple[int, int, int, int, int]:
    primes = find_primes_in_range(1000, 10000)
    p = primes[9]   # 10th prime
    q = primes[18]  # 19th prime
    logger.debug(f"Selected primes p={p}, q={q}")
    n = p * q
    phi = (p - 1) * (q - 1)
    logger.debug(f"Calculated n={n} and phi={phi}")

    e = 65537
    if math.gcd(e, phi) != 1:
        logger.warning("65537 not coprime to phi; finding alternative e")
        e = 3
        while math.gcd(e, phi) != 1:
            e += 2
    logger.debug(f"Using public exponent e={e}")

    d = mod_inv(e, phi)
    logger.debug(f"Computed private exponent d={d}")
    return p, q, e, n, d
```

3. **Encryption and Decryption** The encipher and decipher of the plaintext `rsa` was implemented by mapping the lowercase letters a-z to integers 0-25, performing a modular exponention $c \equiv m^e \mod n$ for each integer m. The decypher process computed $m \equiv c^d \mod n$ to recover the integer representation of the plaintext.

```
def str_to_nums(s: str) -> list:
    return [string.ascii_lowercase.index(ch) for ch in s]

def nums_to_str(nums: list) -> str:
    return ''.join(string.ascii_lowercase[n] for n in nums)

def encrypt(m: int, e: int, n: int) -> int:
    logger.debug(f"Encrypting message m={m} with e={e}, n={n}")
    c = pow(m, e, n)
    logger.debug(f"Encrypted ciphertext c={c}")
    return c


def decrypt(c: int, d: int, n: int) -> int:
    logger.debug(f"Decrypting ciphertext c={c} with d={d}, n={n}")
    m = pow(c, d, n)
    logger.debug(f"Decrypted message m={m}")
    return m
```

4. **Cryptanalysis by Brute-Force** A brute-force key recovery attack was used to recover the prime numbers (feasible only when small primes are used). Initial factorization of n was performed by trial

division up to $\sqrt{n}$ to recoer p and q. Euler's totient function was computed using $\phi(n) = (p - 1)(q - 1)$, and the private exponent d was recovered by brute force searching for an integer that satisifed the moduluar inverse condition $e \cdot d \equiv 1 \pmod{\phi(n)}$.

```
def brute_force_private_key(e: int, n: int) -> Tuple[int, int, int, float]:
    start = time.perf_counter()
    p = None
    for candidate in range(2, int(math.isqrt(n)) + 1):
        if n % candidate == 0 and is_prime(candidate):
            q = n // candidate
            if is_prime(q):
                p = candidate
                break
    if p is None:
        logger.error("Failed to factor n")
        return None, None, None, 0.0
    phi = (p - 1) * (q - 1)
    d = None
    for i in range(2, phi):
        if (e * i) % phi == 1:
            d = i
            break
    elapsed = time.perf_counter() - start
    logger.debug(f"Brute-forced p={p}, q={q}, d={d} in {elapsed:.4f}
seconds")
    return p, q, d, elapsed
```

1.3 Code Example

The following entry point script computes the RSA keys from a pre-defined integer, encrypts the message, decrypts the message, and then brute-forces the private key. The log output details the internal logic being performed by the script.

```
if __name__ == '__main__':
    setup_logging()

    # 1) Primality test on a pre-defined integer
    num = 7919
    result = is_prime(num)
    logger.info(f"{num} is {'a prime' if result else 'not a prime'}.\n")

    # 2) Generate RSA keys
    p, q, e, n, d = generate_rsa_keys()
    logger.info("Generated RSA key pair:")
    logger.info(f"PU = {{e: {e}, n: {n}}}")
    logger.info(f"PR = {{d: {d}, p: {p}, q: {q}}}\n")

    # 3) Encrypt/decrypt a fixed message "rsa"
    message = "rsa"
    logger.info(f"Original message: \"{message}\"")
```

```
    message_int = str_to_nums(message)
    logger.info(f"Mapped to integers: {message_int}")

    ciphertexts = [encrypt(m_i, e, n) for m_i in message_int]
    logger.info(f"Encrypted ciphertexts: {ciphertexts}")

    decrypted_ints = [decrypt(c_i, d, n) for c_i in ciphertexts]
    logger.info(f"Decrypted integers: {decrypted_ints}")

    decrypted_msg = nums_to_str(decrypted_ints)
    logger.info(f"Recovered message: \"{decrypted_msg}\"\n")

    # 4) Brute-force the private key and measure time
    p_b, q_b, d_b, elapsed = brute_force_private_key(e, n)
    if p_b is None:
        logger.info("4) Brute-force failed to factor n.\n")
    else:
        logger.info("4) Adversary brute-forces the private key:")
        logger.info(f"Found p = {p_b}, q = {q_b}, d = {d_b}")
        logger.info(f"Time taken: {elapsed:.4f} seconds\n")
```

Log Output

```
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:120 INFO: 7919 is a
prime.

2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:31 DEBUG: Finding
primes between 1000 and 10000
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:33 DEBUG: Found 1061
primes in range
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:59 DEBUG: Selected
primes p=1061, q=1117
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:62 DEBUG: Calculated
n=1185137 and phi=1182960
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:70 DEBUG: Using
public exponent e=65537
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:45 DEBUG: Computing
modular inverse of 65537 mod 1182960
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:51 DEBUG: Modular
inverse is 200033
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:73 DEBUG: Computed
private exponent d=200033
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:124 INFO: Generated
RSA key pair:
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:125 INFO: PU = {e:
65537, n: 1185137}
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:126 INFO: PR = {d:
200033, p: 1061, q: 1117}

2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:130 INFO: Original
message: "rsa"
```

```
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:132 INFO: Mapped to
integers: [17, 18, 0]
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:101 DEBUG:
Encrypting message m=17 with e=65537, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:103 DEBUG: Encrypted
ciphertext c=665120
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:101 DEBUG:
Encrypting message m=18 with e=65537, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:103 DEBUG: Encrypted
ciphertext c=1081927
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:101 DEBUG:
Encrypting message m=0 with e=65537, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:103 DEBUG: Encrypted
ciphertext c=0
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:135 INFO: Encrypted
ciphertexts: [665120, 1081927, 0]
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:108 DEBUG:
Decrypting ciphertext c=665120 with d=200033, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:110 DEBUG: Decrypted
message m=17
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:108 DEBUG:
Decrypting ciphertext c=1081927 with d=200033, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:110 DEBUG: Decrypted
message m=18
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:108 DEBUG:
Decrypting ciphertext c=0 with d=200033, n=1185137
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:110 DEBUG: Decrypted
message m=0
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:138 INFO: Decrypted
integers: [17, 18, 0]
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:141 INFO: Recovered
message: "rsa"

2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:96 DEBUG: Brute-
forced p=1061, q=1117, d=200033 in 0.0187 seconds
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:148 INFO: 4)
Adversary brute-forces the private key:
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:149 INFO: Found p =
1061, q = 1117, d = 200033
2025-04-27 21:14:44 cs7349_001c_1252_final.scripts.rsa_cipher:150 INFO: Time
taken: 0.0187 seconds
```