Task Breakdown:

Team Member 1: Initial Permutation (IP) and Final Permutation (FP)

- **Task**: Implement the **Initial Permutation (IP)** and **Final Permutation (FP)** steps of the DES algorithm. These steps involve rearranging the bits of the input and output blocks based on predefined tables.
- **Deliverables**:
  - Function to apply the Initial Permutation on the input data block.
  - Function to apply the Final Permutation after the 16 rounds of DES.
  - Testing these functions to ensure correct bit rearrangement based on the DES tables.

Team Member 2: Key Scheduling and Round Key Generation

- **Task**: Implement the **key scheduling** logic, including **Permuted Choice 1 (PC1)**, **Permuted Choice 2 (PC2)**, and the **Left Circular Shifts**. This will generate 16 round keys from the 64-bit key.
- **Deliverables**:
  - Function to perform **PC1** on the key.
  - Function to perform left circular shifts on the split key halves (C and D).
  - Function to generate 16 round keys by applying **PC2**.
  - Ensure the generated round keys match the expected values for testing.

Team Member 3: Feistel Function and S-Box Substitution

- **Task**: Implement the **Feistel function**, including **expansion**, **XOR with the round key**, and the **S-box substitution**. After the substitution, the result is permuted using the **P permutation**.
- **Deliverables**:
  - Expansion function to expand the 32-bit right half to 48 bits.
  - S-Box substitution function using the 8 predefined S-boxes.
  - Permutation function using the **P table** after the S-box substitution.
  - Test the Feistel function to ensure correctness of each round.

Team Member 4: DES Encryption/Decryption Logic

- **Task**: Implement the **main DES encryption/decryption logic**, which includes the **16 rounds** of the Feistel structure. This will involve alter-

nating between the left and right halves of the block and performing XOR operations between them.

- **Deliverables**:
  - Function to combine the left and right halves at each round.
  - Function to swap the left and right halves after each round.
  - Combine the outputs from the Feistel function into the final 64-bit block.
  - Ensure the encryption and decryption follow the DES standard and can process a full block correctly.

Team Member 5: File Handling, Command-line Interface, and Build System

- **Task**: Implement the **file handling** logic and the **command-line interface**. This member will also be responsible for writing the **Makefile** to automate the build process.
- **Deliverables**:
  - Functions to read input files (`plain_text.txt`, `cipher_text.dat`) and the key (`key.txt`).
  - Write the encrypted or decrypted data back to the appropriate output file.
  - Ensure the program can be run from the command line with arguments like:
    - `./des_project encrypt plain_text.txt key.txt cipher_text.dat`
    - `./des_project decrypt cipher_text.dat key.txt plain_text.txt`
  - Create the **Makefile** to automate building, cleaning, and running the project.