Chapter Two

Lab #2

1. Write a program to implement the DES key generation process to generate subkeys. Also, show the subkeys generated at each round.
2. Implement the initial permutation of the DES algorithm by applying the initial permutation to a given plaintext block and observe the result.
3. Write a program to apply the round function to a given 32-bit data and subkey, and display the intermediate results.
4. Implement the IDEA key scheduling algorithm to generate subkeys from the main encryption key
5. Write a program to implement the AES SubBytes and ShiftRows operations for encryption. Apply these operations to a given state matrix and show the results.
6. Write a program to implement the AES MixColumns operation for encryption. Apply the operation to a given state matrix and round key, and show the results.