**Reflection:**

Data Encryption Standard (DES) is a symmetric block cipher published by the National Institute of Standards and Technology - NIST (Tutorialspoint, n.d.). DES is based on the Feistel Cipher which takes a block of 64-bit plaintext as input and generates a block of 64-bit ciphertext by using the 56-bit size key. In this assignment, our group has designed different Python functions to facilitate the implementation of the DES steps for 16 rounds: Initial permutation, Final permutation, Round function, Key generation and the Avalanche analysis. We started the assignment by carefully read through the lecture slides (University of Newcastle, 2025) as well as other online resources and lectures, such as Geeksgeeks’s DES article (Geeksforgeeks, 2025) and Introduction to Data Encryption Standard Youtube video from Neso Academy (Neso Academy, 2024). After that, we decided the programming language which is Python and use Github as the place where we can both collaborate and submit our works. We started by initialise the DES components such as Initial permutation, inverse initial permutation, expansion permutation, permutation function, key schedule, rotation and the 9 S-boxes tables. Additionally, we designed the bit manipulation functions and key schedule functions so that we can later design the F-function. The main part of the implementation is the decryption and encryption step where we aggregate all of the initialized functions in the past steps. Finally, an avalanche analysis file is designed to illustrates the output, input of different DES modes. The bit manipulation functions and other initialises of the tables were the most simple parts, while the inverse expansion function for the DES2 implementation is the most challenging part and we had to look for ideas and online resources online to support our works. After finishing this assignment, I have learned and gained a deeper knowledge about DES and how to implement it in Python. Moreover, by designing it from scratch, I can clearly understand the robustness of symmetric encryption and how block ciphers achieve security.

**References:**

Tutorialspoint. (n.d.). Data Encryption Standard. Tutorialspoint. <https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm>

Geeksforgeeks. (April 2025). Data Encryption Standard (DES) Set 1. Geeksforgeeks. <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>

Neso Academy. (2024). Introduction to Data Encryption Standard (DES). Youtube.