Technical Report

Please read the “README.md” file for information about the application itself instead of the code

1. GUI:

The GUI was created using tkinter, and all the respective buttons and frames that appear in the applications are linked to snippets of codes in various places in the file.

root.title("Data Encryption Standard")

frame = Frame(root, *bd*=10, *width*=500, *height*=600)

In order to show an example, the above code was included. It shows setting of the name of the application (through root.title) and the creation of the application frame.

The “round” function is called in order to show the details of each round in DES by creating a new window and displaying the results from the tables created by the encrypt function.

The “enc” function is used as a driver code which calls the encrypt function and either encrypts or decrypts depending on the its input (0 for encryption and 1 for decryption)

1. Tables:

The first part of the code are the tables used in DES. This includes the initial permutation table, expansion table, permutation table, S-box table which include 8 substitution boxes, permutation choice 1 table, permutation choice 2 table, final permutation table, and the shift table which determines the number of shifts in each round.

1. Helper Functions:

The second part of the code are the helper functions used easy our work in implementing DES. This includes functions that convert between binary, hexadecimal and decimal representation of data. It also include the xor function, the permute function which permutes the bits of the data block inserted depending on a certain table specific, and the shift left function which shifts the bits to the left n times.

1. Encrypt Function:

The third part of the code is the encrypt function which implements DES encryption and is also used for decryption by reversing the keys used. It does the following steps:

1. Initial permutation
2. Splitting
3. 16 rounds each containing expansion, XOR, s-box substitution, permutation, a second XOR followed by a swap in case of the last DES round.
4. Final permutation
5. Returning the resulting text

The parameters of the encrypt function are the text, round key array in binary format, left data block array, right data block array, expansion result array, first XORing result array, S-box result array, permutation result array, and the second XORing result array. These arrays are used to show the details of each round when needed in the application. What the function needs to perform DES are the text and the round key array only.

1. Key Generation Function:

The fourth part of the code is the key generation function which generates all the round keys given a certain key from the user through the following steps:

1. Permuting the key bits through permutation choice 1 table
2. Splitting the key into a left and a right part
3. 16 rounds of shifting and permutation through permutation choice 2
4. Appends result of each round in two arrays rkb and rk which respectively contain the binary and the hex representation of each round key.
5. Testing the Application

Graphical user interface, text

Description automatically generatedFirst, we test the application using the following text “123456ABCD132536” and the following key “AABB09182736CCDD”. We can see that the cipher text and the result of each round are both correct through any online DES tool. Furthermore, we’re able to see the details of any round we want. We can also try the text and key examples given in the class PDF to check if our application is working correctly.

Next, we’re going to test the decryption. We can see that even if we put lower case characters the application still works. Putting the resulting ciphertext from before and using the same key, we see that we got the plaintext we entered initially proving that decryption is working correctly.

Graphical user interface, text, application, chat or text message

Description automatically generated