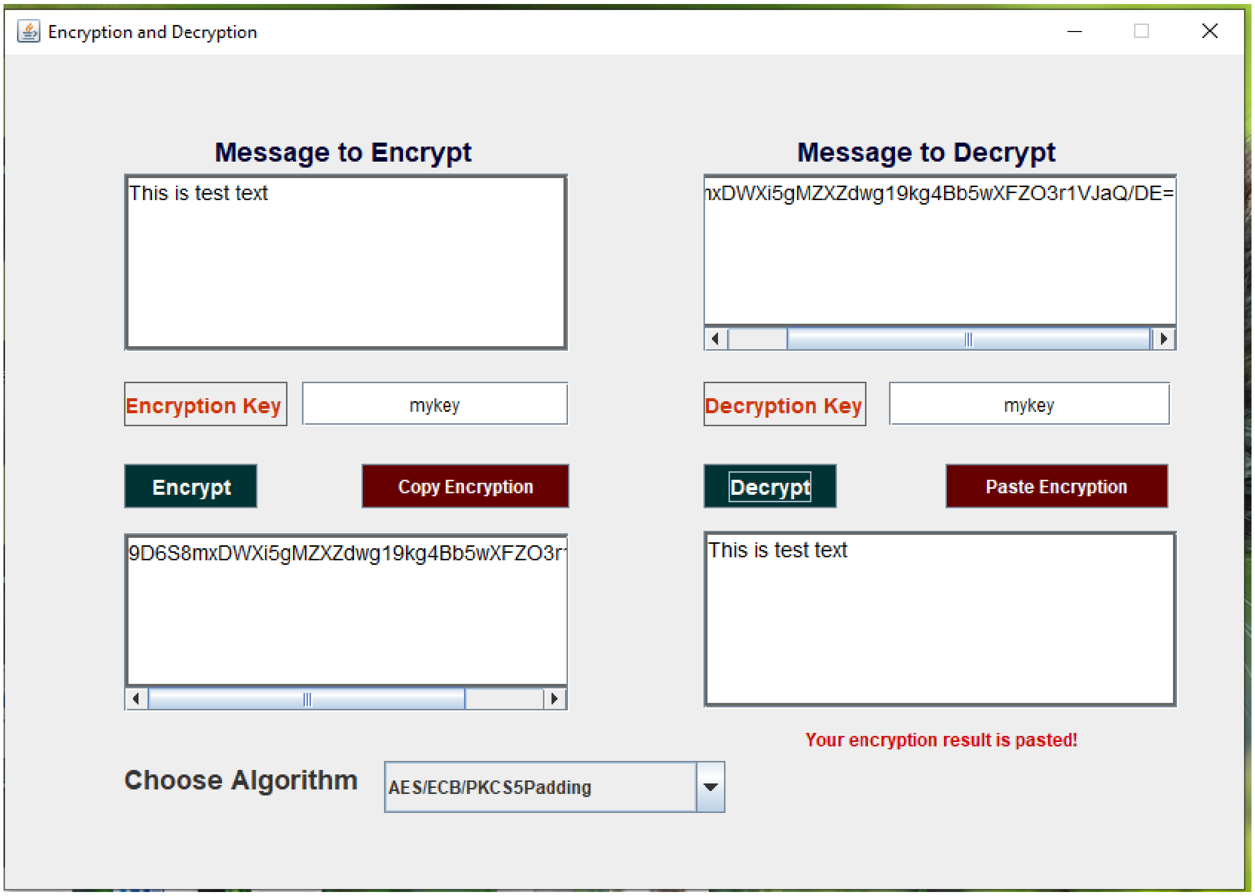
Encryption Algorithms:

1. AES (
2. Triple DES
3. One time Pad

Description of the program:

1. **AES**
   - Accept the message and the key from user
   - Change the user entered key to fixed sized 16 bytes length using sha-1 hash algorithm
   - Feed the message and the new generated key to the AES/ECB/PKCS5Padding algorithm
2. **Triple DES**
   - Accept the message and the key from user
   - Change the user entered key to fixed sized 24 bytes (8 byte for each round with the first and the last 8 bytes same) using md5 hashing algorithm.
   - Feed the message and the newly generated keys to the DESede/ECB/PKCS5Padding algorithm
3. **One time pad**
   - Accept the message and generate the key stream of 1 and 0 (8 for one character)
   - Changing the message into binary of its ascii code and also changing the key into binary
   - Xoring the message and the key and decoding the result back

Samples
1.AES message = "This is test text" key = "mykey"
2.Triple DES message = "This is test text" key = "mykey"
3. One time pad message = "This is test text" key =
1101100011001111001110101010101111000010001010100110111111101010100010001011
010000010011011001011110100001010011101011001101011010110011



Message to Encrypt: This is test text

Message to Decrypt: nxDWXi5gMZXZdwg19kg4Bb5wXFZO3r1VJaQ/DE=

Encryption Key: mykey

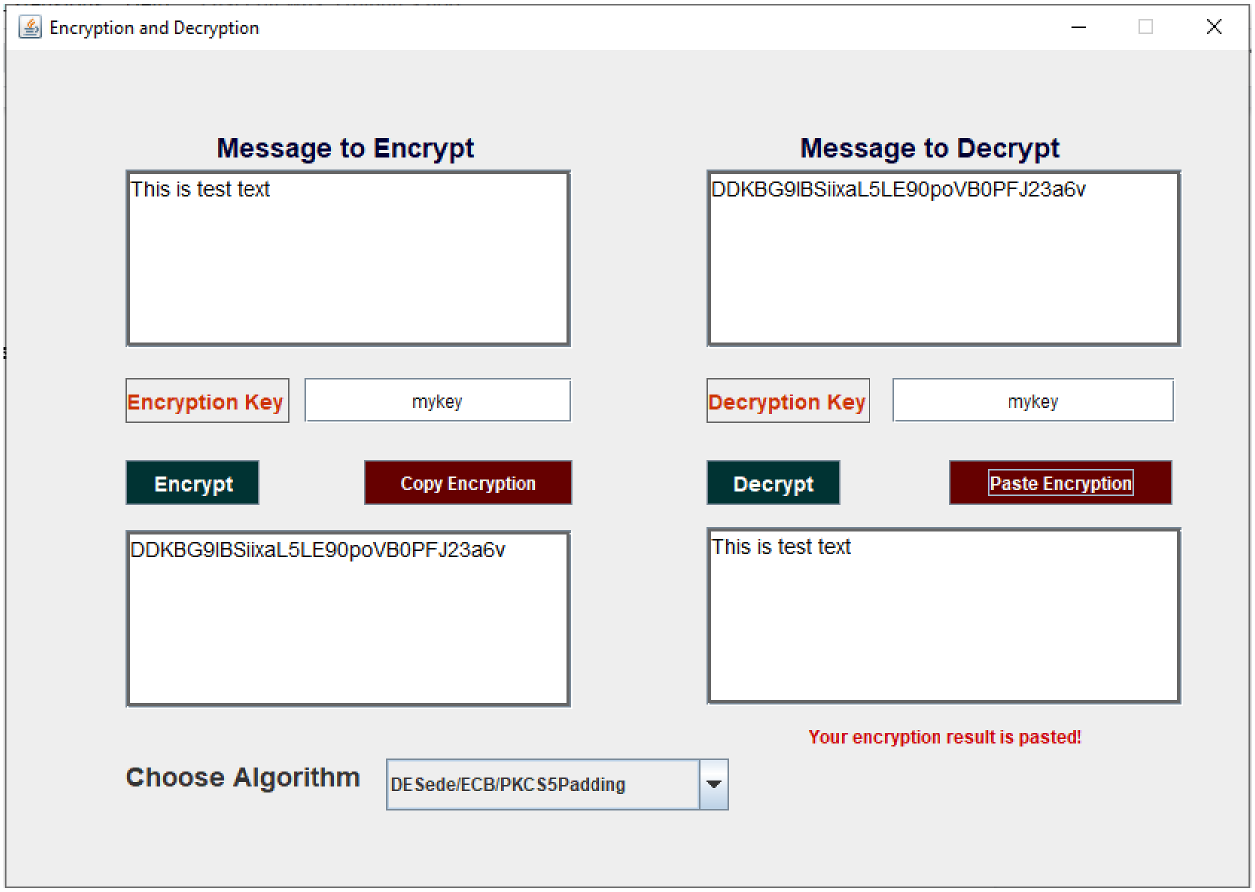
Decryption Key: mykey

9D6S8mxDWXi5gMZXZdwg19kg4Bb5wXFZO3r1

This is test text

Your encryption result is pasted!

Choose Algorithm: AES/ECB/PKCS5Padding



Message to Encrypt: This is test text

Message to Decrypt: DDKBG9IBSiixaL5LE90poVB0PFJ23a6v

Encryption Key: mykey

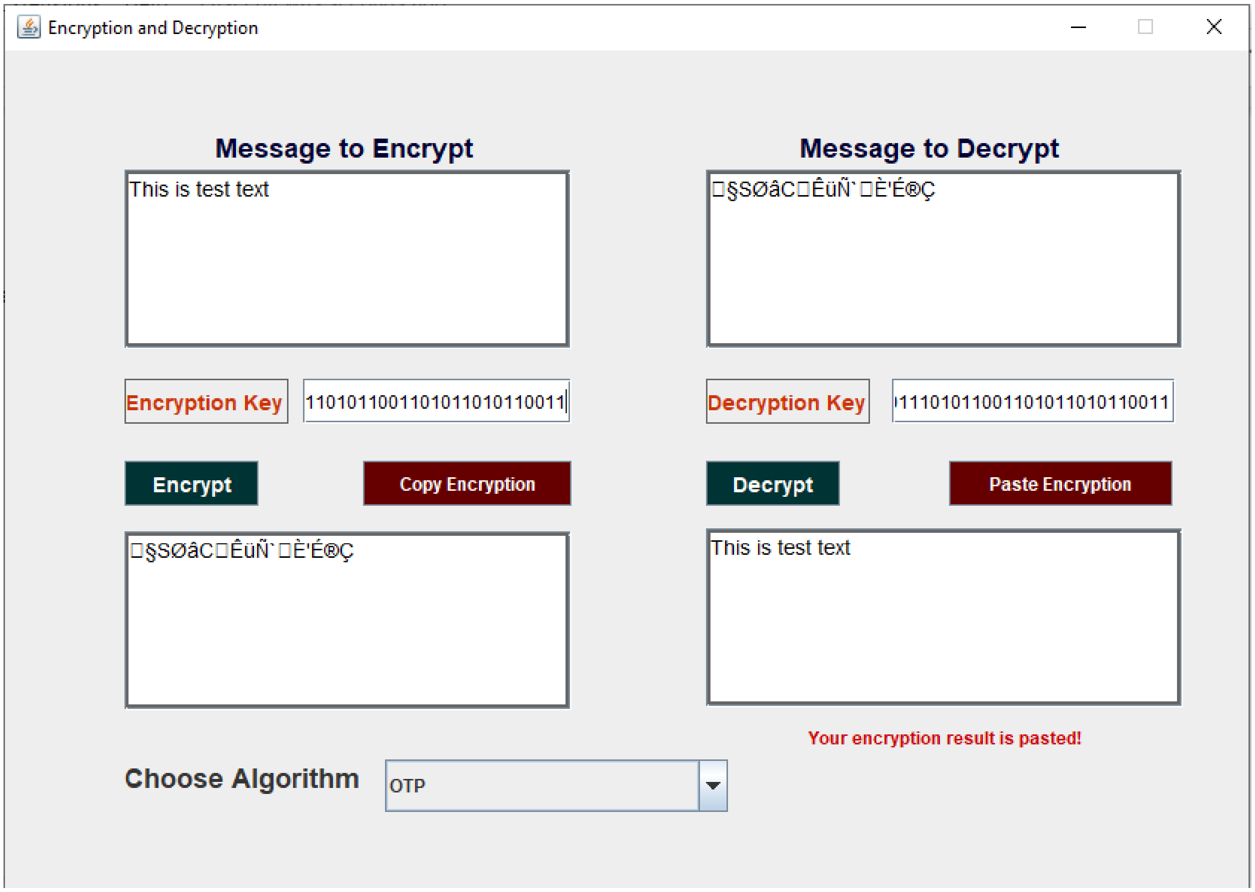
Decryption Key: mykey

DDKBG9IBSiixaL5LE90poVB0PFJ23a6v

This is test text

Your encryption result is pasted!

Choose Algorithm: DESede/ECB/PKCS5Padding



Message to Encrypt

This is test text

Encryption Key: 1101011001101011010110011

□§SØâC□ÊüÑ`□È'É®Ç

Message to Decrypt

□§SØâC□ÊüÑ`□È'É®Ç

Decryption Key: 11101011001101011010110011

This is test text

Your encryption result is pasted!

Choose Algorithm: OTP

Github link: [Tesfamariam777/CNS_EncDec_assignment (github.com)]

Windows executable is also included but it requires a java runtime environment to execute .

Name : Mekete Tafesse
ID : Atr/8212/11