Ex.No:12

TRIPLE DES

Date:

AIM:

To use the Triple DES algorithm for encryption and decryption.

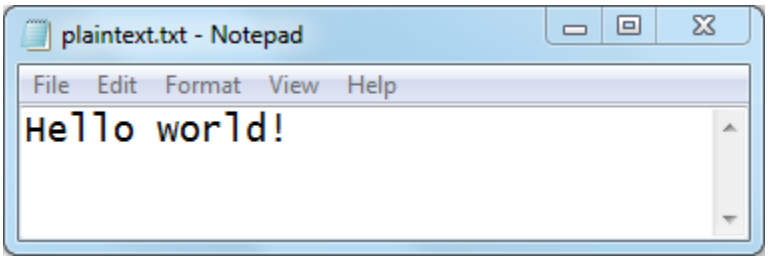
PROCEDURE:

1. Start the program.
2. Import required modules.
3. Generate Keys and get the plaintext.
4. Use DES3.encrypt() to encrypt the plaintext.
5. To decrypt the ciphertext, use DES3.decrypt().

PROGRAM:

```
from Crypto.Cipher import DES3
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad
from Crypto.Util.Padding import unpad

key = get_random_bytes(16)

cipher = DES3.new(key, DES3.MODE_CBC)
plaintext = None

with open('plaintext.txt', 'rb') as file:
   plaintext = file.read()

ciphertext = cipher.encrypt(pad(plaintext, DES3.block_size))

with open('ciphertext.txt', 'wb') as file:
   file.write(ciphertext)
   print(f'Encrypted contents: {ciphertext}')

cipher_decrypt = DES3.new(key, DES3.MODE_CBC, iv=cipher.iv)
to_be_decrypted = None

with open('ciphertext.txt', 'rb') as file:
   to_be_decrypted = file.read()
print(f'Decrypted contents: {unpad(cipher_decrypt.decrypt(to_be_decrypted),
DES3.block_size).decode("utf-8")}')
```

OUTPUT:




```
PS C:\Users\student\Desktop\cns> & "D:/Program Files/Python37/python.exe" c:/Users/student/Desktop/cns/des3.py
Encrypted contents: b'\xb4/\xa6\x88b6\x8e\xa9\x9b0\x8b6rb\x19\xd2'
Decrypted contents: Hello world!
PS C:\Users\student\Desktop\cns>
```

RESULT:

Thus encryption and decryption using 3DES is demonstrated successfully and the output is verified