Assignment No 5

Cryptography and Network Security Lab (5CS453)

Name: Mrunal Khade PRN: 2020BTECS00057 Class: Final Year - CSE

Problem Statement:

Data Encryption Standard (DES)

→

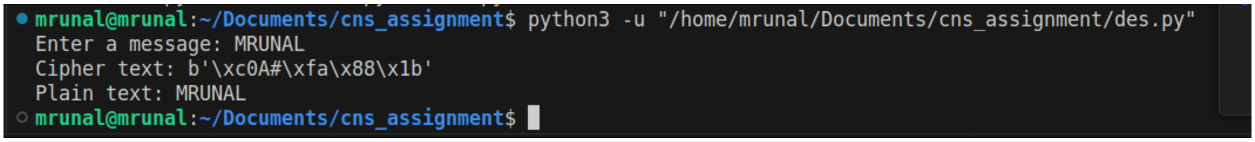
- **Data Encryption Standard (DES)** is one of the earliest and most widely used encryption standards for securing digital data.
- Developed in the early 1970s by IBM, it was adopted as a federal standard in the United States for the protection of sensitive data.
- It's a symmetric-key block cipher, meaning the same key is used for both encryption and decryption, and it operates on fixed-size data blocks.
- DES uses a 56-bit encryption key (originally 64 bits with 8 bits used for parity). The key length is relatively short by modern standards.
- DES uses a Feistel network structure, dividing data into halves and applying multiple rounds of operations with the encryption key.
- However, due to its vulnerability to brute-force attacks and advances in computing power, DES is now considered obsolete and has been largely replaced by more secure encryption algorithms like AES (Advanced Encryption Standard).

Code:

```python
from Crypto.Cipher import DES
from secrets import token_bytes

key = token_bytes(8)

def encrypt(msg):
    cipher = DES.new(key,DES.MODE_EAX)
    nonce = cipher.nonce
    ciphertext,tag = cipher.encrypt_and_digest(msg.encode('ascii'))
    return nonce, ciphertext,tag

def decrypt(nonce, ciphertext, tag):
    cipher = DES.new(key, DES.MODE_EAX, nonce=nonce)
    plaintext = cipher.decrypt(ciphertext)

    try:
        cipher.verify(tag)
        return plaintext.decode('ascii')
    except:
        return False
```

```python
print('\n*** Data Encryption Standard Algorithm ***')
nonce, ciphertext, tag = encrypt(input('Enter Plain Text:'))
plaintext = decrypt(nonce,ciphertext,tag)

print(f'Cipher Text is: {ciphertext}')

if not plaintext:
    print('Message is Corrupted!')
else:
    print(f'Plain Text is: {plaintext}')
```

Output:



```
● mrunal@mrunal:~/Documents/cns_assignment$ python3 -u "/home/mrunal/Documents/cns_assignment/des.py"
  Enter a message: MRUNAL
  Cipher text: b'\xc0A#\xfa\x88\x1b'
  Plain text: MRUNAL
○ mrunal@mrunal:~/Documents/cns_assignment$ 
```