Apply DES algorithm for practical applications

Ex. No: 3

Date :

Aim:

To Apply DES algorithm for practical applications.

Algorithm:

Step 1: Obtain the text for encryption /decryption

Step 2: Get input from the user to Encrypt/Decrypt

Step 3: Get the key from the user.

Step 4: Perform an DES encryption/decryption using key.

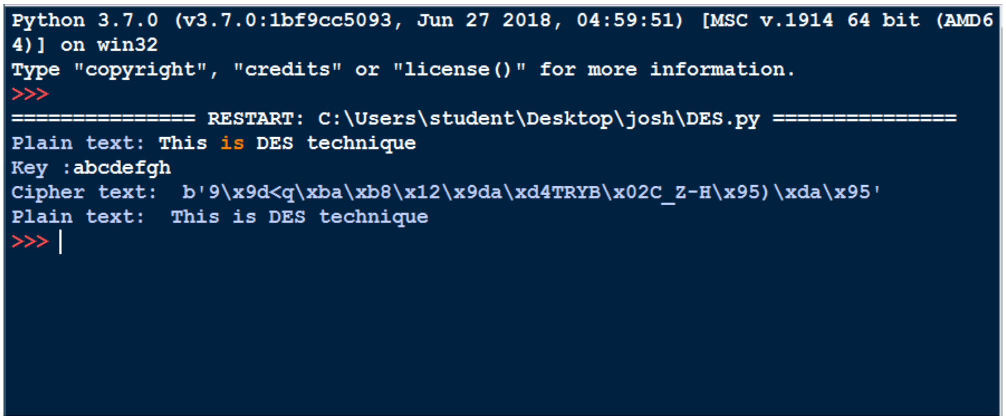
Step 5: Output the corresponding Plaintext/Cipher Text.

Source code:

```
from Crypto.Cipher import DES
from Crypto.Util.Padding import pad
from Crypto.Util.Padding import unpad

text = input("Plain text: ")
text = bytes(text,'utf-8')
key = bytes(input("Key :"),'utf-8')
cip= DES.new(key,DES.MODE_CBC)
ciptext=cip.encrypt(pad(text,DES.block_size))
print("Cipher text: ",ciptext)
```

```
cip_dec=DES.new(key,DES.MODE_CBC,iv=cip.iv)

pt=unpad(cip_dec.decrypt(ciptext),DES.block_size).decode('utf-8')

print("Plain text: ",pt)
```

Output:



```
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:59:51) [MSC v.1914 64 bit (AMD6
4)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
=============== RESTART: C:\Users\student\Desktop\josh\DES.py ===============
Plain text: This is DES technique
Key :abcdefgh
Cipher text:  b'9\x9d<q\xba\xb8\x12\x9da\xd4TRYB\x02C_Z-H\x95)\xda\x95'
Plain text:  This is DES technique
>>> |
```

Result:

The DES algorithm for practical applications was executed successfully and output was verified.