Apply AES algorithm for practical applications

Ex. No: 4

Date :

Aim:

To Apply AES 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 AES encryption/decryption using key.

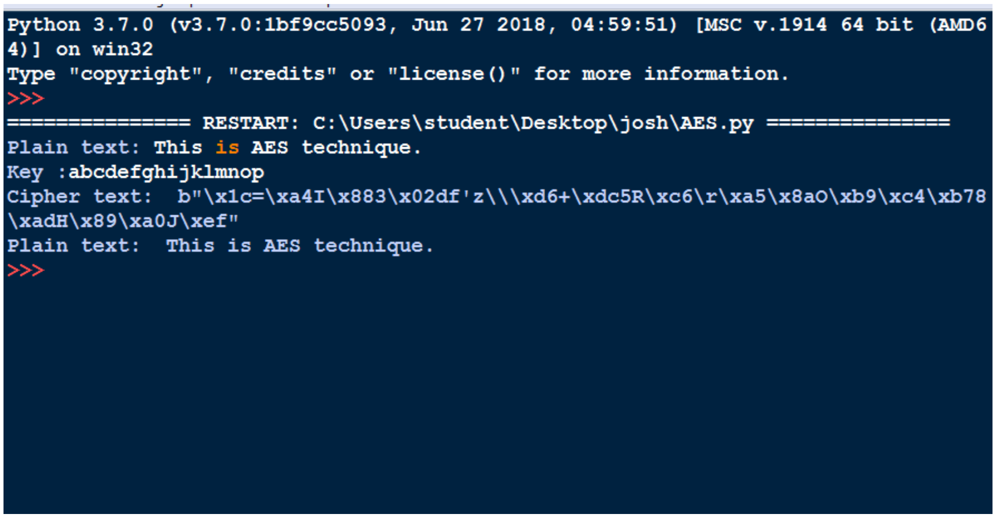
Step 5: Output the corresponding Plaintext/Cipher Text.

Source code:

```
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
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= AES.new(key,AES.MODE_CBC)
ciptext=cip.encrypt(pad(text,AES.block_size))
```

```
print("Cipher text: ",ciptext)



cip_dec=AES.new(key,AES.MODE_CBC,iv=cip.iv)

pt=unpad(cip_dec.decrypt(ciptext),AES.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\AES.py ===============
Plain text: This is AES technique.
Key :abcdefghijklmnop
Cipher text:  b"\x1c=\xa4I\x883\x02df'z\\\xd6+\xdc5R\xc6\r\xa5\x8aO\xb9\xc4\xb78
\xadH\x89\xa0J\xef"
Plain text:  This is AES technique.
>>>
```

Result:

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