POIS ASSIGNMENT 1

TASK 5

USE THE CPA SECURITY AND SECURE MAC TO DESIGN A PROVABLY CCA-SECURE ENCRYPTION SCHEME

CODE EXPLANATION

ENCRYPTION :

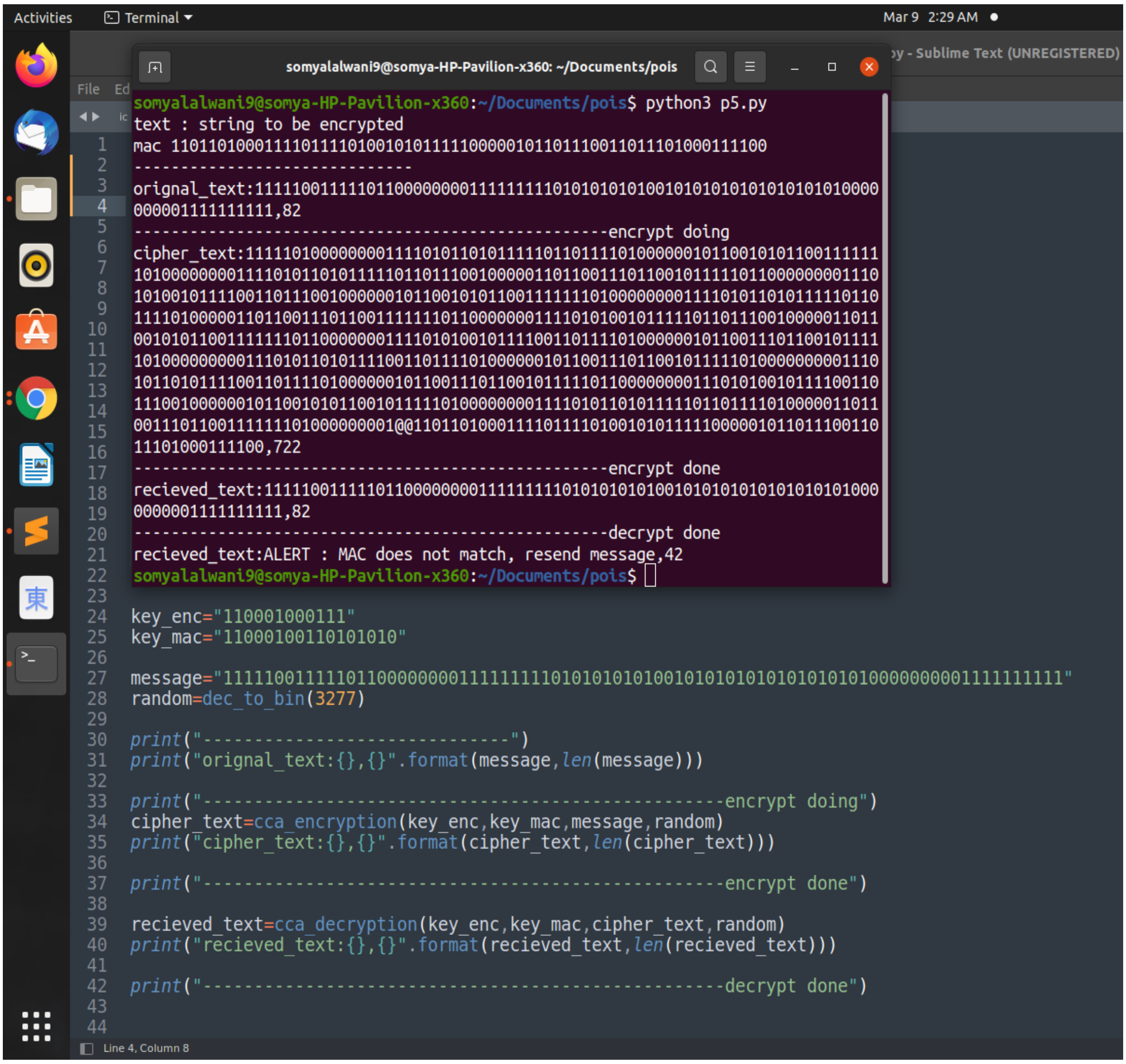
```
def cca_encryption(key_enc,key_mac,message,random):
    encrypted_message = cpa_encrypt(message,key_enc,random)
    mac = cbc_mac(encrypted_message,key_mac)
    FINAL_TEXT = encrypted_message + "@@" + mac
    return FINAL_TEXT
```

While encrypting the message, the message is first encrypted using CPA-secure encryption scheme and then further using secure mac. Both of these are combined using a symbol in between and the final encrypted mgs is sent.

AUTHENTICATION & THEN DECRYPTION :
The encrypted message is recvd and divided back in 2 parts.
The MAC is calculated again, and if found the same, means source is authenticated; and message will be further decrypted; else error shown not mac not matching.

```
def cca_decryption(key_enc,key_mac,cipher_text,random):
    rcvd_message ,rcvd_mac = cipher_text.split("@@")
    calc_mac = cbc_mac(rcvd_message , key_mac)
    if(rcvd_mac == calc_mac):
        decrypted_message = cpa_decrypt(rcvd_message, key_enc,random)
        return decrypted_message
    else:
        return "ALERT : MAC does not match, resend message"
```

OUTPUT :


Activities
Terminal
Mar 9 2:29 AM
somyalalwani9@somya-HP-Pavilion-x360: ~/Documents/pois
py - Sublime Text (UNREGISTERED)
File Ed
somyalalwani9@somya-HP-Pavilion-x360:~/Documents/pois$ python3 p5.py
text : string to be encrypted
mac 1101101000111101111010010101111100000101101110011011101000111100
----
orignal_text:1111100111110110000000011111111101010101010010101010101010101010000
000001111111111,82
--encrypt doing
cipher_text:1111101000000001111010110101111101101111010000001011001010110011111
1010000000011110101101011111011011100100000110110011101100101111101100000001110
1010010111100110111001000000101100101011001111111010000000011110101101011110110
1111010000011011001110110011111110110000000111101010010111110110111001000001101
1001010110011111110110000000111101010010111100110111101000000101100111011001011
1110100000000011101011010111100110111101000000101100111011001011111010000000001
1101011010111100110111101000000101100111011001011111011000000001110101001011110
0110111001000000101100101011001011111010000000011110101101011111011011110100000
11011001110110011111110100000000001@@11011010001111011110100101011111000001011011
10011011101000111100,722
--encrypt done
recieved_text:111110011111011000000001111111110101010101001010101010101010101000
0000001111111111,82
--decrypt done
recieved_text:ALERT : MAC does not match, resend message,42
somyalalwani9@somya-HP-Pavilion-x360:~/Documents/pois$
key_enc="110001000111"
key_mac="1100010011010101010"
message="111110011111011000000001111111110101010101001010101010101010101000000000011111111"
random=dec_to_bin(3277)
print("------------------------------")
print("orignal_text:{},{}".format(message,len(message)))
print("--encrypt doing")
cipher_text=cca_encryption(key_enc,key_mac,message,random)
print("cipher_text:{},{}".format(cipher_text,len(cipher_text)))
print("--encrypt done")
recieved_text=cca_decryption(key_enc,key_mac,cipher_text,random)
print("recieved_text:{},{}".format(recieved_text,len(recieved_text)))
print("--decrypt done")
Line 4, Column 8