RSA (Rivest–Shamir–Adleman)

Submitted to: **Eng. Khaled Moataz**

Submitted by: **Zeinab Moawad Fayez Hassan**

Sec: **1**

B.N: **29**

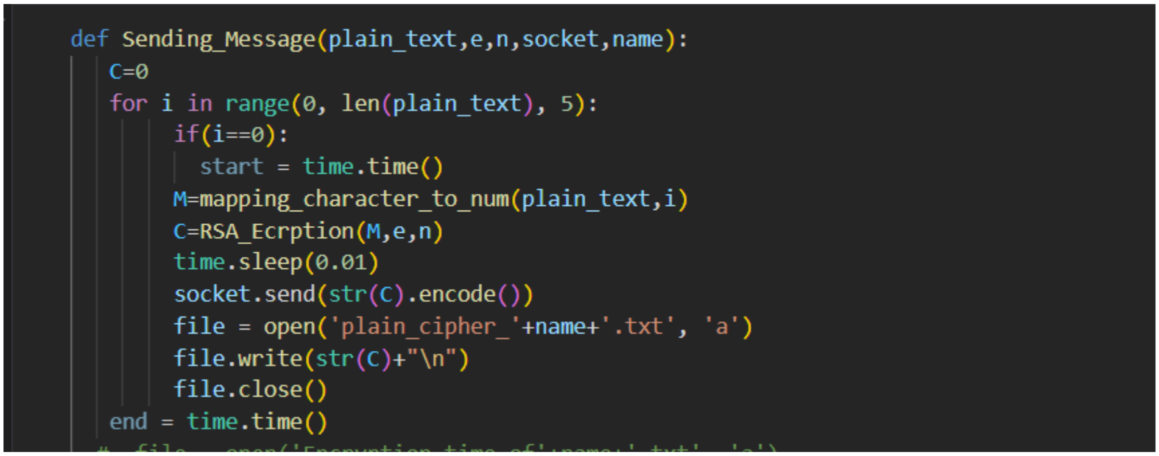
St.Code:9202611

Analysis: Time in milli seconds

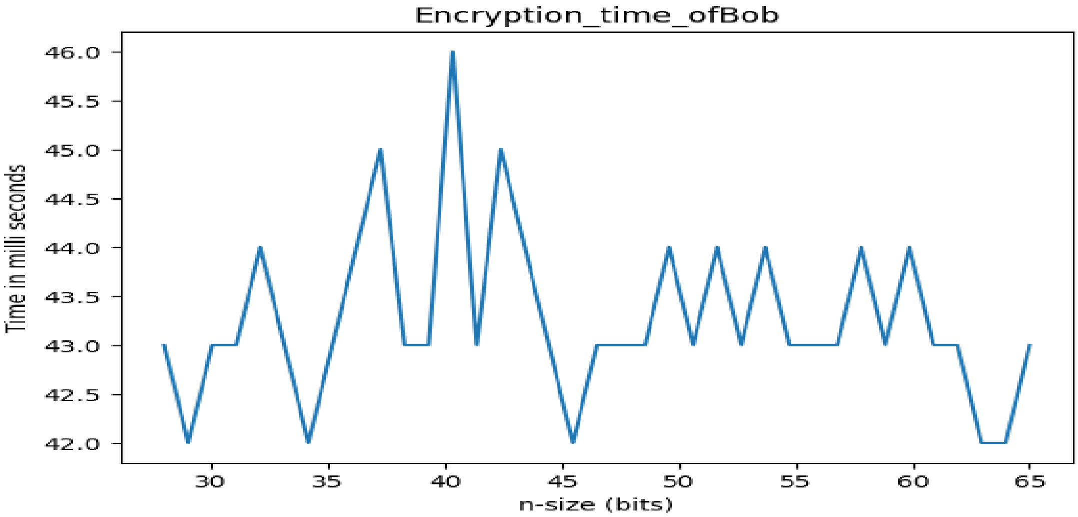
Bob (Receiver):

Encryption analysis:

I calculate time from start mapping character to send each 5 characterin plain text some extra time can excluded in result which is sleep (0.01) in socket and time open file which used to save each 5 character cipher text all of these should be in consideration will effect whole time to (map , encrypt,send)

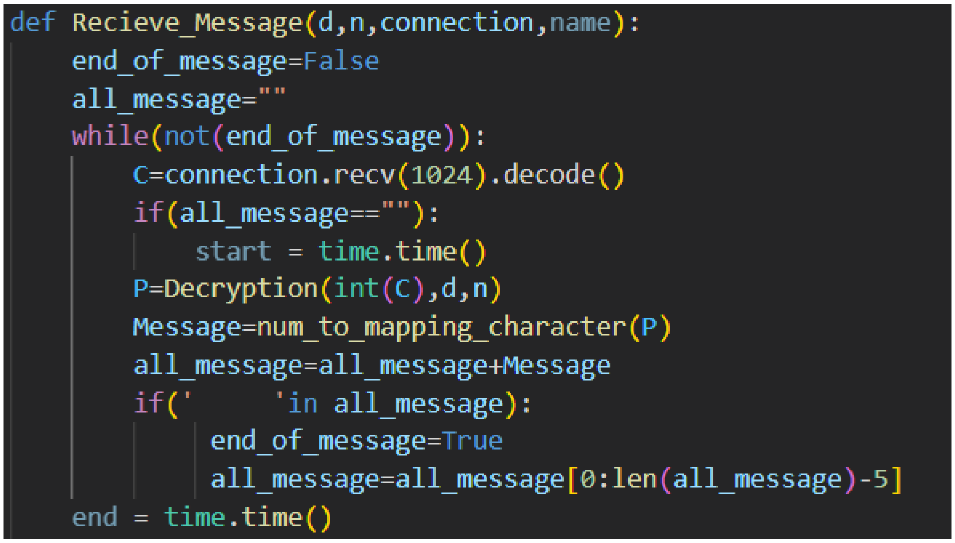


```
def Sending_Message(plain_text,e,n,socket,name):
    C=0
    for i in range(0, len(plain_text), 5):
        if(i==0):
            start = time.time()
        M=mapping_character_to_num(plain_text,i)
        C=RSA_Ecrption(M,e,n)
        time.sleep(0.01)
        socket.send(str(C).encode())
        file = open('plain_cipher_'+name+'.txt', 'a')
        file.write(str(C)+"\n")
        file.close()
    end = time.time()
   #  file = open('Encryption_time_of'+name+'.txt', 'a')
```

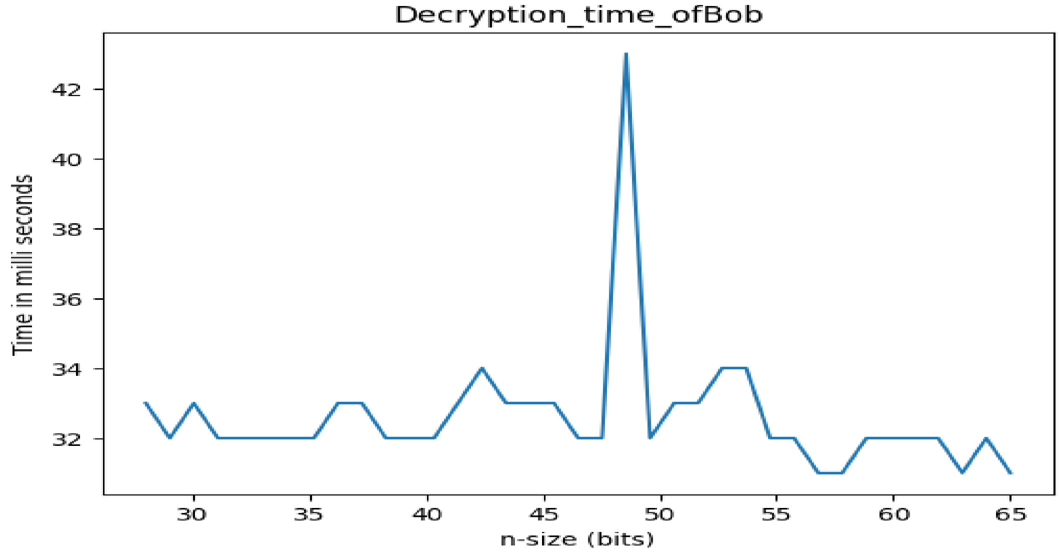


Decryption analysis:

I calculate time from start receive each 5 character to have plain an extra time as when send plain text it ends with 5 spaces extra (to know end of message) so in reciveing 5 extra spaces and decrypt them



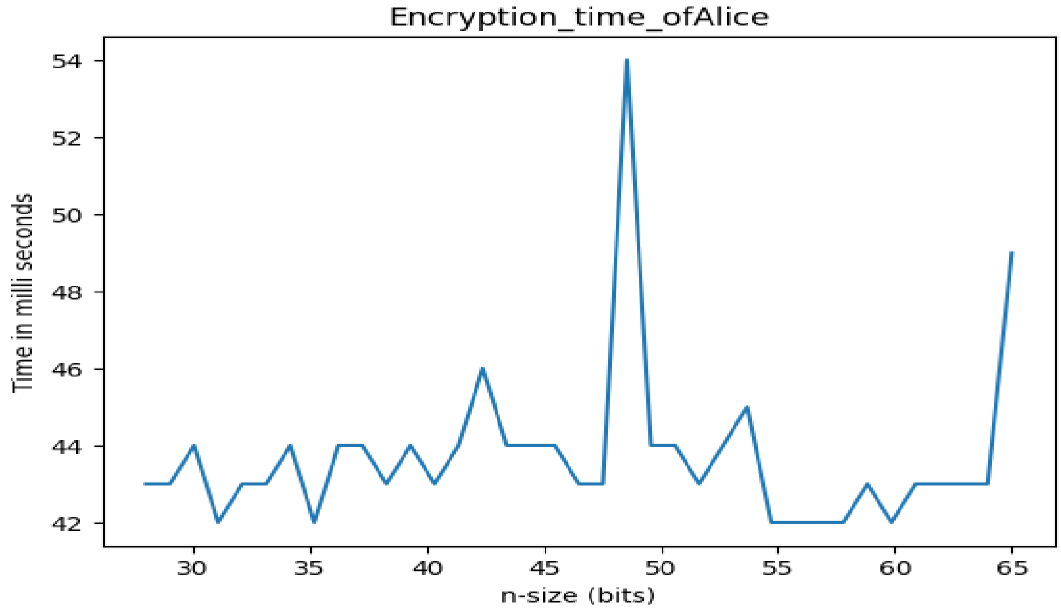
```python
def Recieve_Message(d,n,connection,name):
    end_of_message=False
    all_message=""
    while(not(end_of_message)):
        C=connection.recv(1024).decode()
        if(all_message==""):
            start = time.time()
        P=Decryption(int(C),d,n)
        Message=num_to_mapping_character(P)
        all_message=all_message+Message
        if('     'in all_message):
            end_of_message=True
            all_message=all_message[0:len(all_message)-5]
    end = time.time()
```



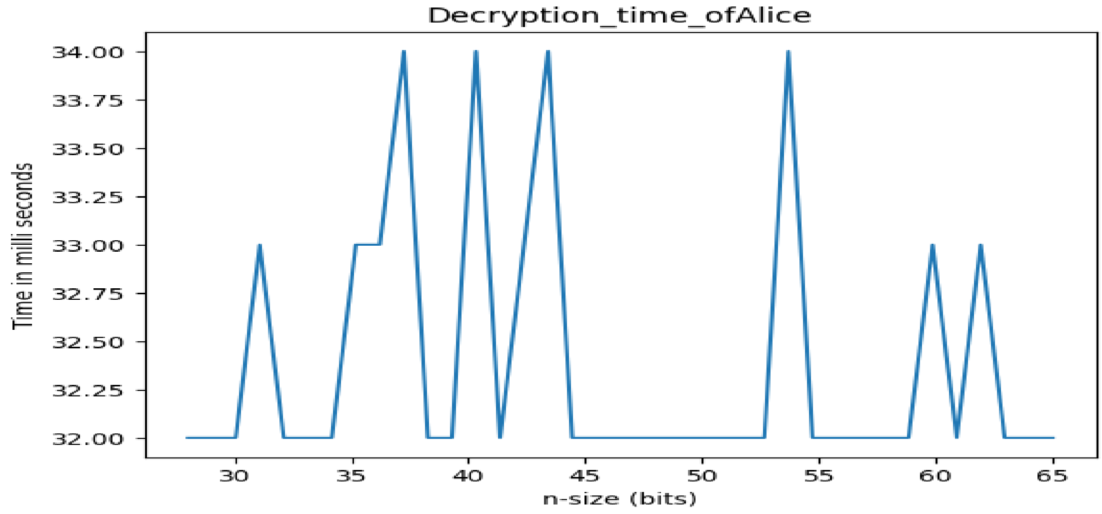
Note : time of Decryption larger than encryption as there are “ `time.sleep(0.01)`” in code due to socket only if we subtract this time from graph of encryption we will get same time graph of decryption.

Alice (Sender):

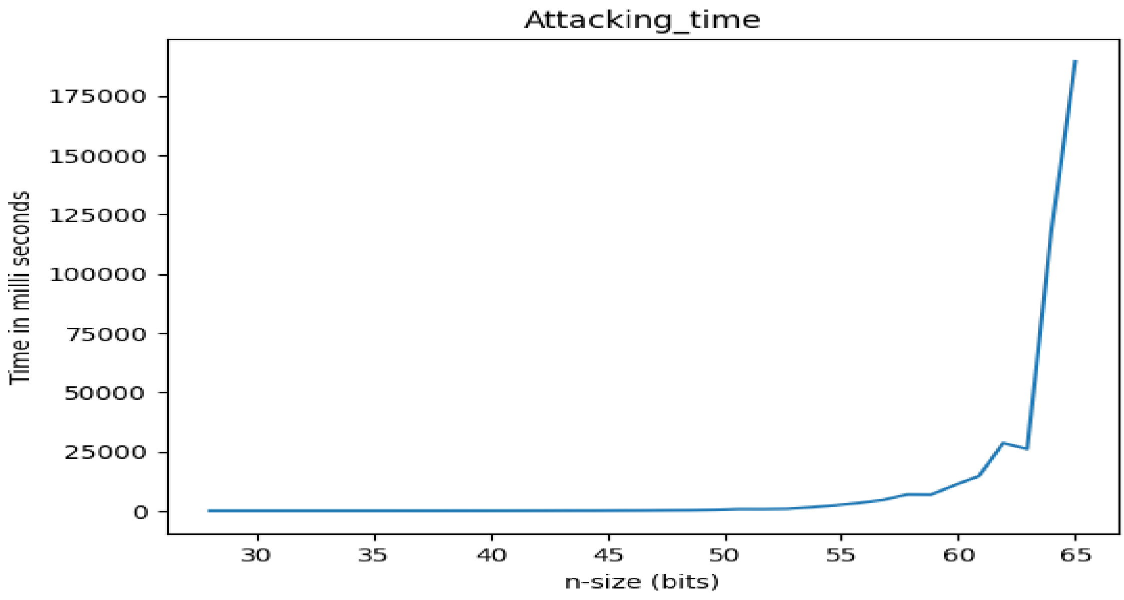
Encryption analysis:



Decryption analysis:



Attacking analysis: from 28 to 64 bits



Conclusion:

1-Number of bits effect mainly in attacking so increasing number of bits of n increasing difficulty of attacking as time increase exponentially.
2-Time of Encryption and Decryption depend on number of bits of n as time increase and decreasing with increasing n as each time e and d change and effect on calculations .

-After writing all your message to send you should end with five spaces if you don't do that code will stuck and this will not effect on result of decryption as I ignore these spaces in receiving and logic will be same.