КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

***ФБ-13 Владислав Садохін та Данило Розумовський***

**Мета роботи**

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

**Порядок виконання роботи**

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.

**Код**

import random  
import hashlib  
import string  
  
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"  
  
  
def ext\_gcd(a, b):  
 if a == 0:  
 return (b, 0, 1)  
 else:  
 g, x, y = ext\_gcd(b % a, a)  
 return (g, y - (b // a) \* x, x)  
  
  
def mod\_inverse(a, m):  
 g, x, y = ext\_gcd(a, m)  
 if g != 1:  
 return None # Оберненого елемента не існує  
 else:  
 return (x % m + m) % m  
  
  
def trial\_division(n):  
 if n < 2:  
 return False  
 for i in range(2, 100):  
 if n % i == 0:  
 return False  
 return True  
  
  
def is\_prime\_miller\_rabin(n, k=10):  
 def find\_s\_d(n):  
 s = 0  
 while n % 2 == 0:  
 s += 1  
 n //= 2  
 return s, n  
  
 s, d = find\_s\_d(n - 1)  
  
 for i in range(k):  
 a = random.randint(1, n - 1)  
 x = pow(a, d, n)  
 if x == 1 or x == n - 1:  
 continue  
 else:  
 for j in range(s - 1):  
 x = pow(x, 2, n)  
 if x == n - 1:  
 break  
 if x == 1:  
 return False  
 if x == n - 1:  
 continue  
 return False  
  
 return True  
  
  
def generate\_random\_prime\_number(min\_value, max\_value):  
 while True:  
 n = random.randint(min\_value, max\_value)  
 if trial\_division(n):  
 if is\_prime\_miller\_rabin(n):  
 return n  
 # else:  
 # print(f"Кандидат що не пройшов: {n}")  
  
  
def decimal\_to\_binary(decimal\_number):  
 binary\_representation = bin(decimal\_number)[2:]  
 return binary\_representation

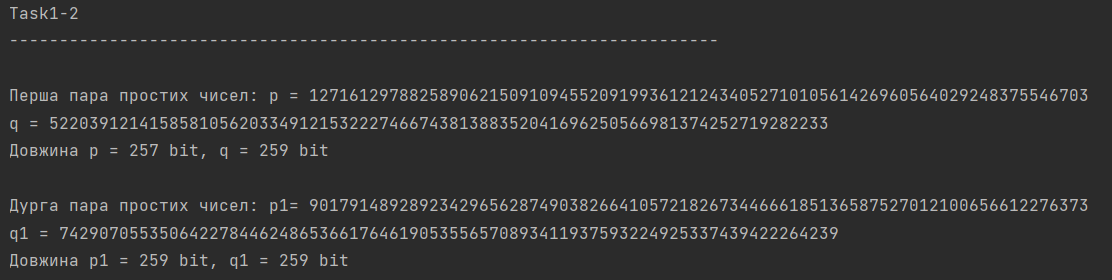
2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента А, 1 p і q1 – абонента B.

**Код**

print("Task1-2")  
print("-----------------------------------------------------------------------")  
p1 = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
q1 = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
  
p2 = generate\_random\_prime\_number(555555555555555555555555555555555555555555555555555555555555555555555555555555, 999999999999999999999999999999999999999999999999999999999999999999999999999999)  
q2 = generate\_random\_prime\_number(555555555555555555555555555555555555555555555555555555555555555555555555555555, 999999999999999999999999999999999999999999999999999999999999999999999999999999)  
  
print(f"\nПерша пара простих чисел: p = {p1}\nq = {q1}")  
print(f"Довжина p = {len(decimal\_to\_binary(p1))} bit, q = {len(decimal\_to\_binary(q1))} bit\n")  
print(f"Дурга пара простих чисел: p1= {p2}\nq1 = {q2}")  
print(f"Довжина p1 = {len(decimal\_to\_binary(p2))} bit, q1 = {len(decimal\_to\_binary(q2))} bit")  
print("-----------------------------------------------------------------------\n")

**Результати:**

Так як чисел що не пройшли перевірку дуже багато, то всі не влізли в скріншоти тому ми тільки початок та кінець цих чисел вставили в протокол, також в кінці числа які є прості та їхня довжина, яка має бути мінімум 256 біт



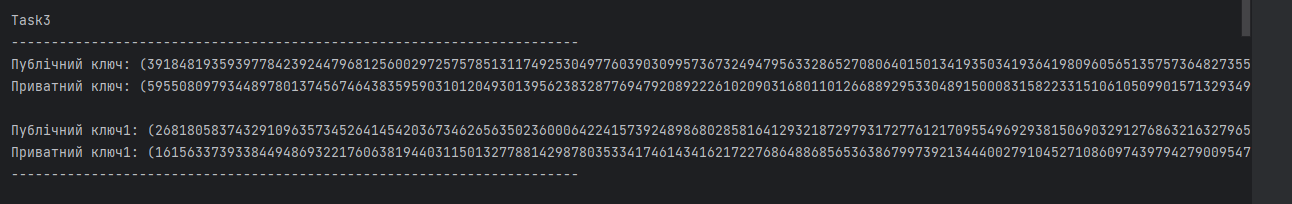
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p,q) та відкритий ключ (n,e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , ( , ) 1 n1 e та секретні d і d1 .

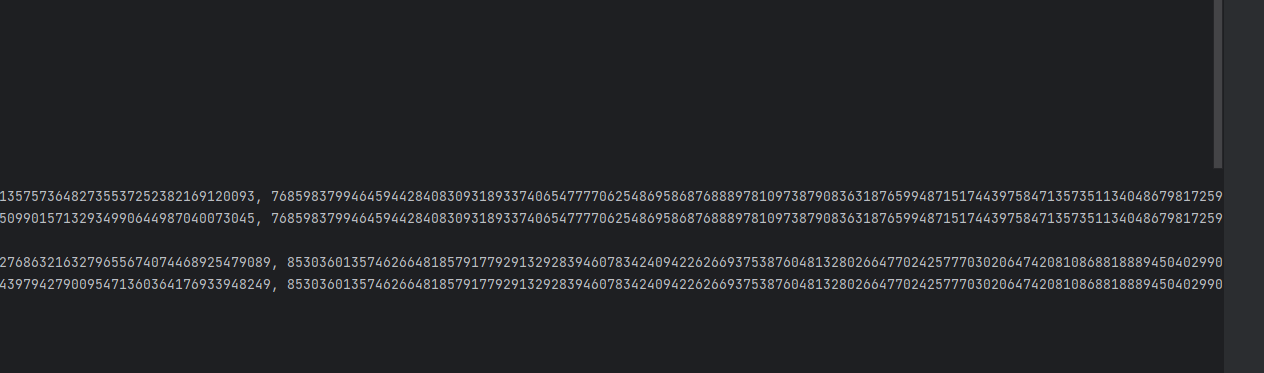
**Код**

def GenerateKeyPair(p, q):  
 n = p\*q  
 totient = (p-1)\*(q-1)  
 e = random.randint(2, totient - 1)  
 (g, x, y) = ext\_gcd(e, totient)  
 while g > 1:  
 e = random.randint(2, totient-1)  
 (g, x, y) = ext\_gcd(e, totient)  
 d = mod\_inverse(e, totient)  
 public\_key = (e, n)  
 private\_key = (d, n)  
 return public\_key, private\_key

print("Task3")  
print("-----------------------------------------------------------------------")  
key1 = GenerateKeyPair(p1, q1)  
key2 = GenerateKeyPair(p2, q2)  
  
e1, d1 = key1  
e2, d2 = key2  
  
print(f"Публічний ключ: {e1}\nПриватний ключ: {d1}\n")  
print(f"Публічний ключ1: {e2}\nПриватний ключ1: {d2}")  
print("-----------------------------------------------------------------------\n")

**Результати:**





4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів А и B, перевірити правильність розшифрування. Скласти для А і B повідомлення з цифровим підписом і перевірити його.

**Код**

def decimal\_to\_hexadecimal(decimal\_num):  
 decimal\_num = int(decimal\_num)  
 hexadecimal\_num = hex(decimal\_num)  
 return hexadecimal\_num[2:]  
  
  
def hex\_to\_decimal(hex\_string):  
 decimal\_result = int(hex\_string, 16)  
 return decimal\_result  
  
  
def GenerateKeyPair(p, q):  
 n = p\*q  
 totient = (p-1)\*(q-1)  
 e = random.randint(2, totient - 1)  
 (g, x, y) = ext\_gcd(e, totient)  
 while g > 1:  
 e = random.randint(2, totient-1)  
 (g, x, y) = ext\_gcd(e, totient)  
 d = mod\_inverse(e, totient)  
 public\_key = (e, n)  
 private\_key = (d, n)  
 return public\_key, private\_key  
  
  
def Encrypt(input\_text, key, server = False):  
 e, n = key  
 if server:  
 number\_decrypted = pow(input\_text, e, n)  
 number\_decrypted = decimal\_to\_hexadecimal(number\_decrypted)  
 return number\_decrypted  
 input\_text = int(input\_text)  
 text\_encrypted = pow(input\_text, e, n)  
 text\_encrypted = str(text\_encrypted)  
 return text\_encrypted  
  
  
def Decrypt(encrypted\_text, key, server = False):  
 d, n = key  
 if server:  
 encrypted\_text = str(encrypted\_text)  
 encrypted\_text = encrypted\_text.lower()  
 number\_encrypted = hex\_to\_decimal(encrypted\_text)  
 number\_decrypted = pow(number\_encrypted, d, n)  
 return number\_decrypted  
 encrypted\_text = int(encrypted\_text)  
 text\_decrypted = pow(encrypted\_text, d, n)  
 text\_decrypted = str(text\_decrypted)  
 return text\_decrypted  
  
  
def Sign(input\_text, my\_private\_key):  
 input\_text = str(input\_text)  
 sha256\_hash = hashlib.sha256()  
 sha256\_hash.update(input\_text.encode('utf-8'))  
 sha256\_hash\_value = sha256\_hash.hexdigest()  
 sha256\_hash\_value = hex\_to\_decimal(sha256\_hash\_value)  
 hash\_encrypted\_with\_prv = Encrypt(sha256\_hash\_value, my\_private\_key)  
 print(f"Signature: {hash\_encrypted\_with\_prv}")  
 return hash\_encrypted\_with\_prv  
  
  
def Verify(input\_text, sign, public\_key):  
 hash\_decrypted\_with\_pbl = Decrypt(sign, public\_key)  
 hash\_decrypted\_with\_pbl = decimal\_to\_hexadecimal(hash\_decrypted\_with\_pbl)  
 print(f"Hash decrypted with public key(signature is verified): {hash\_decrypted\_with\_pbl}")  
 sha256\_hash\_cal = hashlib.sha256()  
 sha256\_hash\_cal.update(input\_text.encode('utf-8'))  
 sha256\_hash\_value = sha256\_hash\_cal.hexdigest()  
 print("Hash calculated from received message: ", sha256\_hash\_value)  
  
 if hash\_decrypted\_with\_pbl == sha256\_hash\_value:  
 return True  
 else:  
 return False

5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа 0 < k < n.

**Код**

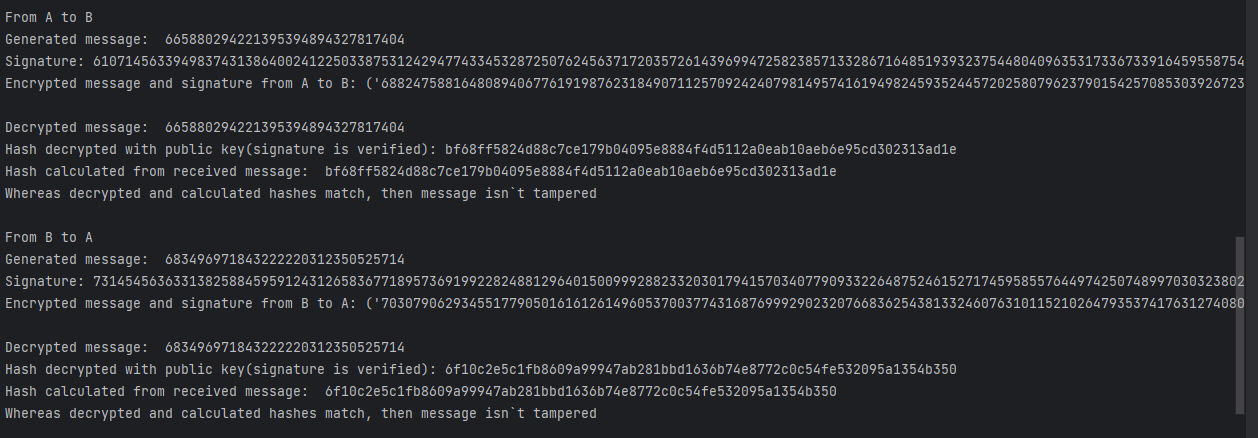
def create\_message\_for\_abonent(public\_key, length, my\_private\_key):  
 characters = string.digits  
 random\_message = ''.join(random.choice(characters) for i in range(length))  
 print("Generated message: ", random\_message)  
 encrypted\_message = Encrypt(random\_message, public\_key)  
 signed\_message = Sign(random\_message, my\_private\_key)  
 message = (encrypted\_message, signed\_message)  
 return message  
  
  
def receive\_message\_from\_abonent(message, my\_private\_key, public\_key):  
 enc\_mes, signed\_mes = message  
 decrypted\_message = Decrypt(enc\_mes, my\_private\_key)  
 print("Decrypted message: ", decrypted\_message)  
 ver\_mes = Verify(decrypted\_message, signed\_mes, public\_key)  
 if ver\_mes:  
 print("Whereas decrypted and calculated hashes match, then message isn`t tampered\n")  
 else:  
 print("Message is tampered by someone\n")

def Send\_key(public\_key, my\_private\_key):  
 d, n = my\_private\_key  
 k = random.randint(0, n)  
 print("Generated secret k: ", k)  
 encrypted\_message = Encrypt(k, public\_key)  
 signed\_message = Sign(k, my\_private\_key)  
 signed\_message\_enc = Encrypt(signed\_message, public\_key)  
 message = (encrypted\_message, signed\_message\_enc)  
 return message  
  
  
def Receive\_key(message, my\_private\_key, public\_key):  
 enc\_mes, signed\_mes\_enc = message  
 decrypted\_message = Decrypt(enc\_mes, my\_private\_key)  
 print(f"\nDecrypted secret key: {decrypted\_message}", )  
 signed\_mes\_dec = Decrypt(signed\_mes\_enc, my\_private\_key)  
 ver\_mes = Verify(decrypted\_message, signed\_mes\_dec, public\_key)  
 if ver\_mes:  
 print("Whereas decrypted and calculated hashes match, then message isn`t tampered\n")  
 return decrypted\_message  
 else:  
 print("Message is tampered by someone\n")

Опис кроків протоколу конфіденційного розсилання ключів з підтвердженням справжності:  
Спочатку генерується секретний ключ, потім він зашифровується з публічним ключем отримувача, потім вираховується хеш із секретного ключа(не зашифрований) і шифрується з моїм приватним ключем(підписується) потім зашифрований моїм приватним ключем хеш секретного ключа, шифрується публічним ключем отримувача, щоб тільки він міг подивитися цей підпис. Далі зашифроване повідомлення та зашифрований підпис повертаються функцією як кортеж (зашифроване повідомлення, зашифрований підпис).

**Результати ось цього коду:**

def create\_message\_for\_abonent(public\_key, length, my\_private\_key):  
 characters = string.digits  
 random\_message = ''.join(random.choice(characters) for i in range(length))  
 print("Generated message: ", random\_message)  
 encrypted\_message = Encrypt(random\_message, public\_key)  
 signed\_message = Sign(random\_message, my\_private\_key)  
 message = (encrypted\_message, signed\_message)  
 return message  
  
  
def receive\_message\_from\_abonent(message, my\_private\_key, public\_key):  
 enc\_mes, signed\_mes = message  
 decrypted\_message = Decrypt(enc\_mes, my\_private\_key)  
 print("Decrypted message: ", decrypted\_message)  
 ver\_mes = Verify(decrypted\_message, signed\_mes, public\_key)  
 if ver\_mes:  
 print("Whereas decrypted and calculated hashes match, then message isn`t tampered\n")  
 else:  
 print("Message is tampered by someone\n")



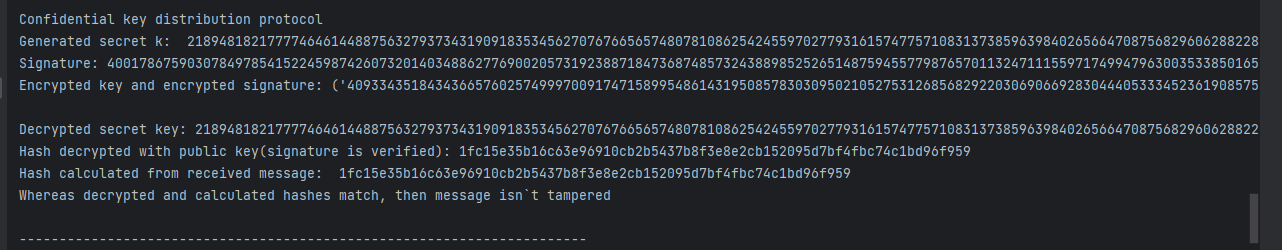
Так як зашифровані повідомлення та підпис не влізли в скріншот, то ми написали їх нижче, спочатку від A до B, потім від B до A, інші дані видно на скріншоті, тому ми їх не переписували

**Encrypted message and signature from A to B: ('68824758816480894067761919876231849071125709242407981495741619498245935244572025807962379015425708530392672300327125195082856293594354144064517715897099944', '61071456339498374313864002412250338753124294774334532872507624563717203572614396994725823857133286716485193932375448040963531733673391645955875403124468400')**

**Encrypted message and signature from B to A: ('70307906293455177905016161261496053700377431687699929023207668362543813324607631011521026479353741763127408008993033870082834832465643857807749267445036865', '731454563633138258845959124312658367718957369199228248812964015009992882332030179415703407790933226487524615271745958557644974250748997030323802278314269976')**

**Ось результати виконання коду самого протоколу конф. розсилання ключів:**

def Send\_key(public\_key, my\_private\_key):  
 d, n = my\_private\_key  
 k = random.randint(0, n)  
 print("Generated secret k: ", k)  
 encrypted\_message = Encrypt(k, public\_key)  
 signed\_message = Sign(k, my\_private\_key)  
 signed\_message\_enc = Encrypt(signed\_message, public\_key)  
 message = (encrypted\_message, signed\_message\_enc)  
 return message  
  
  
def Receive\_key(message, my\_private\_key, public\_key):  
 enc\_mes, signed\_mes\_enc = message  
 decrypted\_message = Decrypt(enc\_mes, my\_private\_key)  
 print(f"\nDecrypted secret key: {decrypted\_message}", )  
 signed\_mes\_dec = Decrypt(signed\_mes\_enc, my\_private\_key)  
 ver\_mes = Verify(decrypted\_message, signed\_mes\_dec, public\_key)  
 if ver\_mes:  
 print("Whereas decrypted and calculated hashes match, then message isn`t tampered\n")  
 return decrypted\_message  
 else:  
 print("Message is tampered by someone\n")

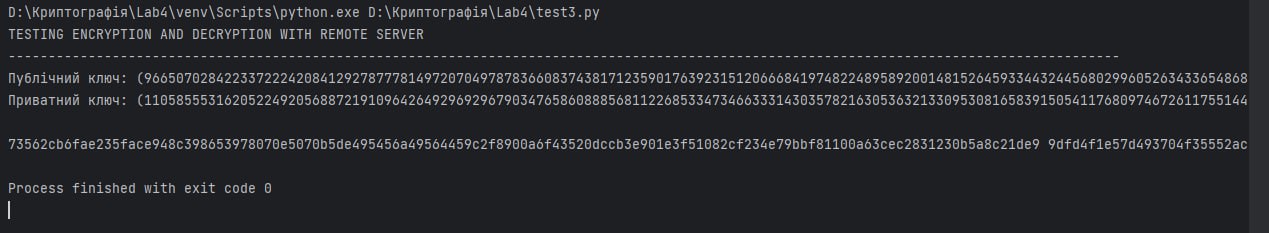
****

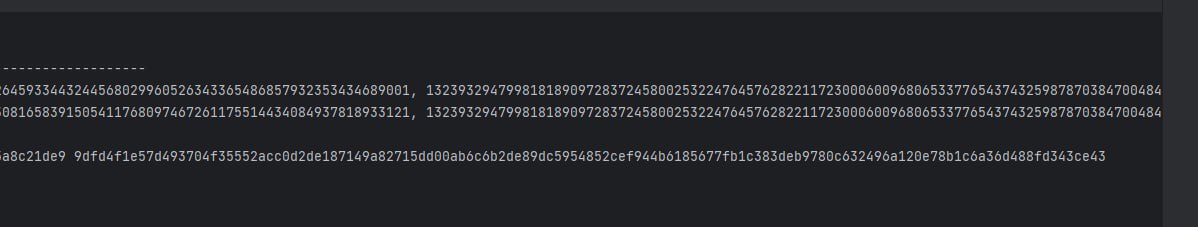
**Та перевірку на сайті:**

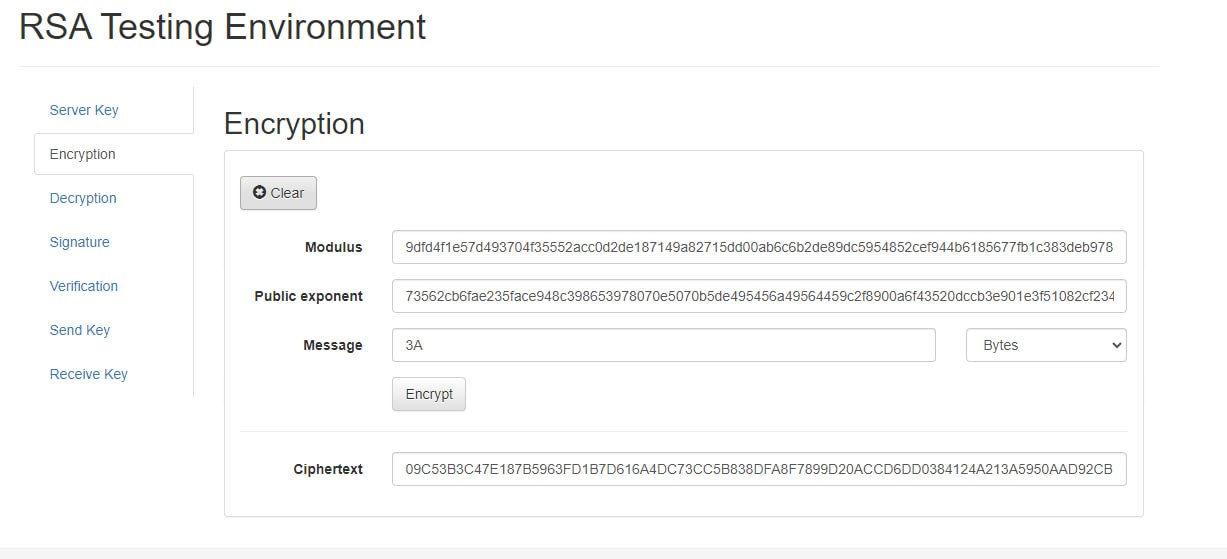
Тут ми спочатку генеруємо ключі потім перетворюємо публічний ключ у шістнадцяткове число потім на сервері вводимо шістнадцятковий ключ тобто модуль і сам ключ і шістнадцяткове число далі на сервері ми зашифровуємо його і потім у себе локально за допомогою нашого приватного ключа його розшифровуємо

Ось код що генерує ключі та виводить спочатку обидва в десяткових значеннях , а потім виводить публічний ключ в шістнадцятковому виді для сервера(деякі рядки, які не треба закоментовані):

print("TESTING ENCRYPTION AND DECRYPTION WITH REMOTE SERVER ")  
print("-------------------------------------------------------------------------------------------------------------------------------------------")  
  
p = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
q = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
  
key = GenerateKeyPair(p, q)  
  
  
e, d = key  
print(f"Публічний ключ: {e}\nПриватний ключ: {d}\n")  
# d = (11058555316205224920568872191096426492969296790347658608885681122685334734663331430357821630536321330953081658391505411768097467261175514434084937818933121, 132393294799818189097283724580025322476457628221172300060096806533776543743259878703847004843444809937171904193824003421582514129868174195636919541092830787)  
# print(d)  
e1, n1 = e  
e1 = decimal\_to\_hexadecimal(e1)  
n1 = decimal\_to\_hexadecimal(n1)  
print(e1, n1)  
  
# num\_enc\_hex = "09C53B3C47E187B5963FD1B7D616A4DC73CC5B838DFA8F7899D20ACCD6DD0384124A213A5950AAD92CBD94D018F45A6977BC124DD9DC67CEFD9B977F87FDF1D6DD"  
# print("Num encrypted in hex: ", num\_enc\_hex)  
# num\_dec\_hex = Decrypt(num\_enc\_hex, d, True)  
  
# print("Num decrypted: ", decimal\_to\_hexadecimal(num\_dec\_hex))  
print("-------------------------------------------------------------------------------------------------------------------------------------------")

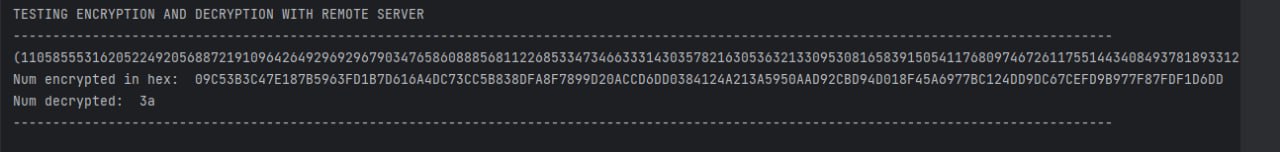
****

****

****

Ось код який розшифровує число, яке сайт зашифрував моїм публічним ключем(непотрібні рядки закоментовані)**:**

print("TESTING ENCRYPTION AND DECRYPTION WITH REMOTE SERVER ")  
print("-------------------------------------------------------------------------------------------------------------------------------------------")  
  
# p = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
# q = generate\_random\_prime\_number(100000000000000000000000000000000000000000000000000000000000000000000000000000, 555555555555555555555555555555555555555555555555555555555555555555555555555555)  
#  
# key = GenerateKeyPair(p, q)  
  
  
# e, d = key  
# print(f"Публічний ключ: {e}\nПриватний ключ: {d}\n")  
d = (11058555316205224920568872191096426492969296790347658608885681122685334734663331430357821630536321330953081658391505411768097467261175514434084937818933121, 132393294799818189097283724580025322476457628221172300060096806533776543743259878703847004843444809937171904193824003421582514129868174195636919541092830787)  
print(d)  
# e1, n1 = e  
# e1 = decimal\_to\_hexadecimal(e1)  
# n1 = decimal\_to\_hexadecimal(n1)  
# print(e1, n1)  
  
num\_enc\_hex = "09C53B3C47E187B5963FD1B7D616A4DC73CC5B838DFA8F7899D20ACCD6DD0384124A213A5950AAD92CBD94D018F45A6977BC124DD9DC67CEFD9B977F87FDF1D6DD"  
print("Num encrypted in hex: ", num\_enc\_hex)  
num\_dec\_hex = Decrypt(num\_enc\_hex, d, True)  
  
print("Num decrypted: ", decimal\_to\_hexadecimal(num\_dec\_hex))  
print("-------------------------------------------------------------------------------------------------------------------------------------------")

****

Як бачимо цифри збігаються ,що означає правильність роботи нашої реалізацій алгоритму з довільно вибраним корректним джерелом,у нашому випадку – навчальним сайтом.

**Висновки:**

У ході виконання даної роботи було досягнуто поставленої мети, яка передбачала ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. Практичне засвоєння цих тестів та методів генерації ключів дозволило глибше зрозуміти принципи роботи криптосистеми RSA, що є однією з ключових технологій у сфері інформаційної безпеки. Також, робота надає можливість вивчити систему захисту інформації на основі криптосхеми RSA. Встановлення концепції захисту інформації з використанням даної системи, організація засекреченого зв'язку та електронного підпису, є важливим етапом для забезпечення конфіденційності та цілісності обмінюваної інформації.  
  
**ПРИМІТКА ПО КОДОВІ:**  
На гітхаб ви просили також прикріпити код який шифрує і текст і також великий текст який розбиває на блоки, тому ми його також прикріпили, основний код це той який шифрує тільки числа