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**

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):  
 if n <= 1:  
 return False  
 if n <= 3:  
 return True  
  
 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(2, n - 2)  
 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

def decimal\_to\_binary(decimal\_number):  
 binary\_representation = bin(decimal\_number)[2:]  
 return binary\_representation

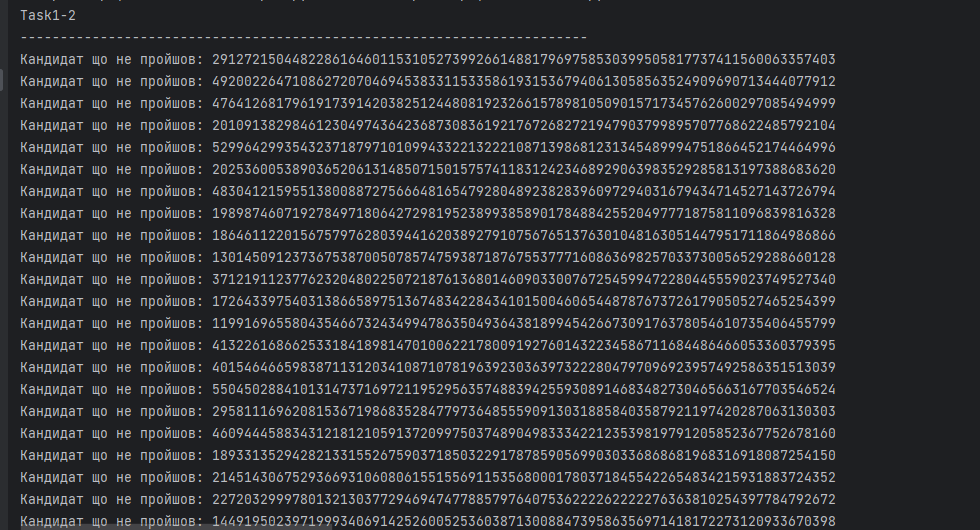
2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента А, 1 p і q1 – абонента B.

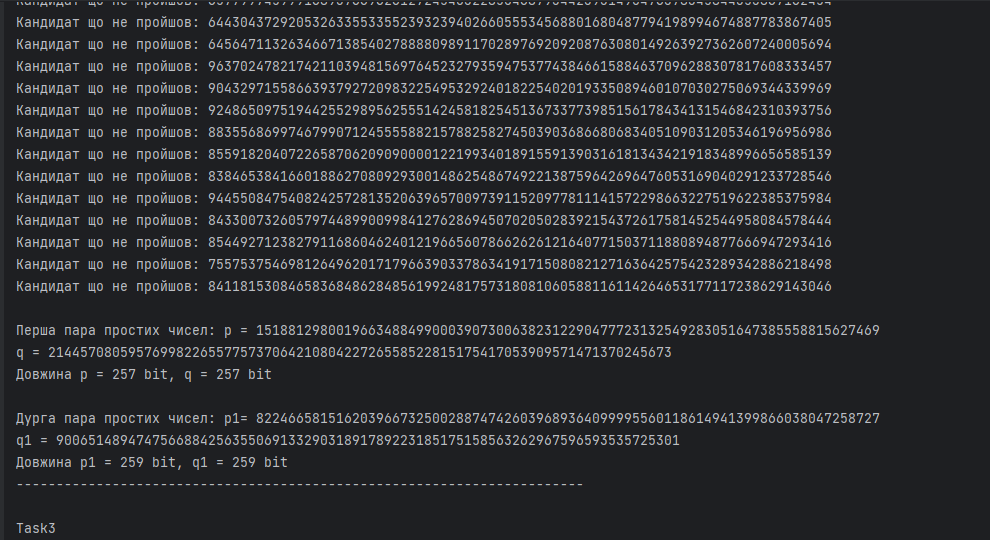
**Код**

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"Перша 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





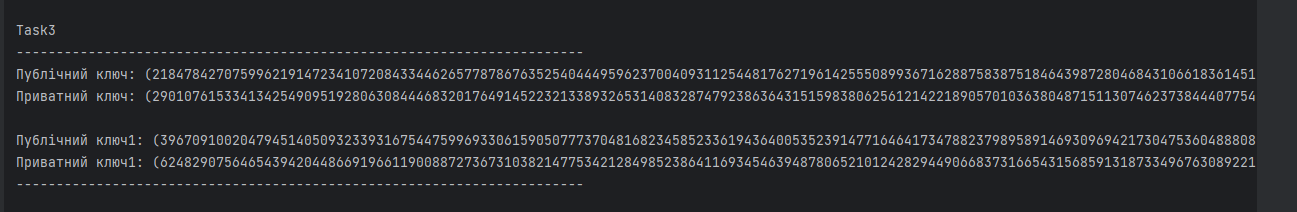
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p,q) та відкритий ключ (n,e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і B – тобто, створити та зберегти для подальшого використання відкриті ключі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

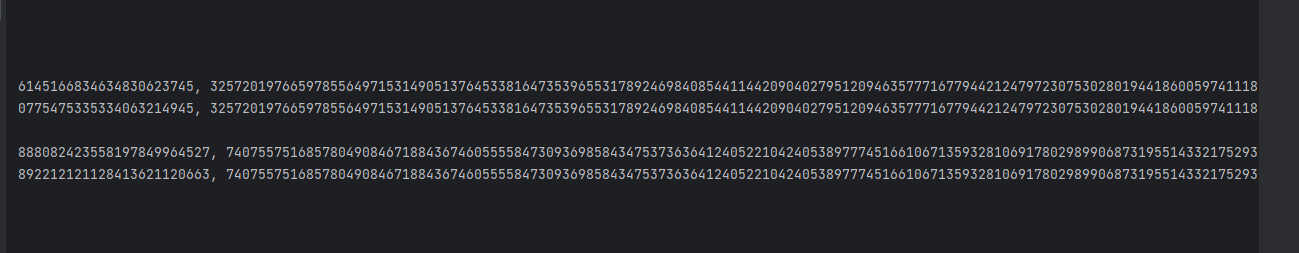
**Код**

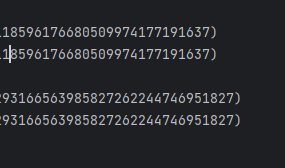
def GenerateKeyPair(p, q):  
 n = p\*q  
 totient = (p-1)\*(q-1)  
 e = random.randint(2, totient - 1)  
 (g, x, y) = ext\_gcd(e, totient)  
 while g > 1:  
 e = random.randint(2, totient-1)  
 (g, x, y) = ext\_gcd(e, totient)  
 d = mod\_inverse(e, totient)  
 public\_key = (e, n)  
 private\_key = (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\_binary(decimal\_number):  
 binary\_representation = bin(decimal\_number)[2:]  
 return binary\_representation  
  
  
def ConvertToInt\_en(text):  
 num = 0  
 for char in text:  
 num = num \* 256 + ord(char)  
 return num  
  
def ConvertToText\_en(number):  
 text = ""  
 while number > 0:  
 char\_code = number % len(alphabet)  
 text = alphabet[char\_code] + text  
 number //= len(alphabet)  
 return text  
  
def ConvertToInt\_dec(text):  
 num = 0  
 for char in text:  
 num = num \* len(alphabet) + alphabet.index(char)  
 return num  
  
  
def ConvertToText\_dec(num):  
 text = ""  
 while num > 0:  
 char\_code = num % 256  
 text = chr(char\_code) + text  
 num //= 256  
 return text  
  
  
  
  
def Encrypt(input\_text, key):  
 e, n = key  
 if len(input\_text)\*8 >= len(decimal\_to\_binary(n)):  
 blocks = []  
 for i in range(0, len(input\_text), 64):  
 block = input\_text[i:i + 64]  
 blocks.append(block)  
 enc\_text = []  
 for block in blocks:  
 text\_in\_num = ConvertToInt\_en(block)  
 number\_encrypted = pow(text\_in\_num, e, n)  
 text\_encrypted = ConvertToText\_en(number\_encrypted)  
 enc\_text.append(text\_encrypted)  
 return enc\_text  
 text\_in\_num = ConvertToInt\_en(input\_text)  
 number\_encrypted = pow(text\_in\_num, e, n)  
 text\_encrypted = ConvertToText\_en(number\_encrypted)  
 return text\_encrypted  
  
  
def Decrypt(encrypted\_text, key):  
 d, n = key  
 if isinstance(encrypted\_text, list):  
 dec\_text = ""  
 for block in encrypted\_text:  
 number\_encrypted = ConvertToInt\_dec(block)  
 number\_decrypted = pow(number\_encrypted, d, n)  
 text\_decrypted = ConvertToText\_dec(number\_decrypted)  
 dec\_text += text\_decrypted  
 return dec\_text  
 number\_encrypted = ConvertToInt\_dec(encrypted\_text)  
 number\_decrypted = pow(number\_encrypted, d, n)  
 text\_decrypted = ConvertToText\_dec(number\_decrypted)  
 return text\_decrypted  
  
  
def Sign(input\_text, my\_private\_key, public\_key):  
 sha256\_hash = hashlib.sha256()  
 sha256\_hash.update(input\_text.encode('utf-8'))  
 sha256\_hash\_value = sha256\_hash.hexdigest()  
  
 hash\_encrypted\_with\_prv = Encrypt(sha256\_hash\_value, my\_private\_key)  
 print(f"Signature: {hash\_encrypted\_with\_prv}")  
  
 hash\_encrypted\_with\_pbl = Encrypt(hash\_encrypted\_with\_prv, public\_key)  
 print(f"Signature encrypted with public key: {hash\_encrypted\_with\_pbl}")  
 return hash\_encrypted\_with\_pbl  
  
  
def Verify(input\_text, sign, public\_key, my\_private\_key):  
 hash\_decrypted\_with\_prv = Decrypt(sign, my\_private\_key)  
 print(f"Signature decrypted with private key: {hash\_decrypted\_with\_prv}")  
 hash\_decrypted\_with\_pbl = Decrypt(hash\_decrypted\_with\_prv, public\_key)  
 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.ascii\_letters + 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, public\_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, my\_private\_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")

print("Task4-5")  
print("-----------------------------------------------------------------------")  
print("From A to B")  
message\_from\_A = create\_message\_for\_abonent(e2, 200, d1)  
print(f"Encrypted message and encrypted signature from A to B: {message\_from\_A}\n")  
receive\_message\_from\_abonent(message\_from\_A, d2, e1)  
  
print("From B to A")  
message\_from\_B = create\_message\_for\_abonent(e1, 201, d2)  
print(f"Encrypted message and encrypted signature from B to A: {message\_from\_B}\n")  
receive\_message\_from\_abonent(message\_from\_B, d1, e2)  
print("-----------------------------------------------------------------------\n")

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

**Результати:**



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

Encrypted message and encrypted signature from A to B: (['1RodZKkgocChvfXK4IUH29JDPb8hcOg8b9rOx7lkRoZ7LvGKXGATd7XRGejhl5j6TacGoBMCL8Z8Z18UOJcNRb7', 'xmeUTuk0h7KZ16EigxKxaIEFRmZKGKwhly63I5rIRfNvKfSxGhK7ct7j0H7TmZXzzViNzerUVumqzkU0KowXt1v', 'my2uHIZwBiH3Al110GJEXUAv6yGuOW80tuRDNmsXG7x293XSMLoHhanrohlHjx3PuQdpPjdY7xLox5F1q7RJ8or', 'vNdM46F5czFzIH7nigX9Z8vWVtLkt9Uw74YXUSFCSolniWsOZpxIeUnuIJNKjXsO05DHGMbYRxsXswGZKZhkgIJ'], ['b0cbufWmfqljTWUmN8dFdMn197zp9Mqcvh2Hx6g9p7abJhPcaahn8f5Xey0Kl9AJ0Y4fAMsnM9lY59D3yJDj49W', 'r9IotDbocrIAH10VN3OeRd8ccRtZRofEZXYJULO9cG81ldOJhEaEH1oowVC0mKA8XExAL5NBAzni8ybD0spwmq4'])

Encrypted message and encrypted signature from B to A: (['r6Ef4JOhrAD2skvqgVtiD59ZJHqjbMNPjFEe4xey5w3d6hFoibfAuuqw2ecjCP6PoBKr7UikVpPsTPY9pK4Uvq', 'b6Yqv6DLvtskYpWlGqGtRPTpFTguV37oVabcwLNeQeN6igv5mUCUoZWWKjqj9K1z63ThGgKBYKQnaxrcAUT6sTb', 'becWciIwAvdfWZygBLFyQ3tj95DPGrpIR0lJ1OHYgjJo2kZb4vtURv9zpPgLrK071ad8sgWgfa2YhjFuI9TGX63', 'bwwd3Wfv5FtChUCRsZLwsRA0XoAjlzbEsCuZMmd9anrd2K8IOLDFVWfbQth7Fc7vZRpVeArp2tbVB6reAiCRke6'], ['bWOMZJhl2znurrYCjCehms4VEqok1c8Sy8yT5CDY8PeHhRYT1MaW52Dlvp0KeoNk5xSDPtRBdKy1xWnkwnCTBvj', '7ax2BXgaCaa4v1QqhTVrIZkvpkFYNtWYJIlWpk0vLuBH7mgReigTONr1xdp7zMpW1khAgV3Aoij6V4YdQS3JRG'])

**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.