МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп’ютерний практикум
№4
З дисципліни

Криптографія

Виконав студент групи ФБ-81

Середа А. С.

Перевірив

Чорний О. М.

Київ – 2020
19.11

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

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.

Завдання: Варіант (18)

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.

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 A, 1 p і q1 – абонента B.

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 A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .

4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A 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 A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.

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. Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey(). Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою

http://asymcryptwebservice.appspot.com/?section=rsa.

Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Хід роботи:

Спершу я створив функції для обробки даних, такі як find_random_bin (для створення зовсім випадкового числа), bin_to_int (для переводу бінарного масива в cpp_int), mod та перегрузив функцію pow.
Потім я створив функції для пошуку p та q та функцію перевірки простоти. Також я створив декілька допоміжних функцій.
Потім я створи функції Encrypt(), Decrypt(), Sign(), Verify(), та вирішив створити псевдосистему з двома користувачами і можливістю змінювати користувача.
Потім я створив функції SendKey() та ReceiveKey().
Я перевірив працювання функцій на малих розмірах (5, 10, 15), та почав чекати (поки виконається програма для 256 бітів).

Проблеми з якими я зіткнувся:

- Час обробки програми для 256 бітних чисел. Було вирішено за допомогою функції powm(a, b, c) (a^b mod c);
- Спочатку я не знав що можна використовувати бібліотеки для великих чисел, та почав (та майже повністю реалізував) власну бібліотеку для обробки чисел у двійковій формі.

Параметри криптосистеми:
P1 = 9774576551737791979522086164941769880099474497791353251754391422136428184664 3
Відсіяні кандидати:
9774576551737791979522086164941769880099474497791353251754391422136428184641 9
9774576551737791979522086164941769880099474497791353251754391422136428184642 1
9774576551737791979522086164941769880099474497791353251754391422136428184642 3
9774576551737791979522086164941769880099474497791353251754391422136428184642 5
9774576551737791979522086164941769880099474497791353251754391422136428184642 7
9774576551737791979522086164941769880099474497791353251754391422136428184642 9
9774576551737791979522086164941769880099474497791353251754391422136428184643 1
9774576551737791979522086164941769880099474497791353251754391422136428184643 3
9774576551737791979522086164941769880099474497791353251754391422136428184643 5
9774576551737791979522086164941769880099474497791353251754391422136428184643 7
9774576551737791979522086164941769880099474497791353251754391422136428184643 9
9774576551737791979522086164941769880099474497791353251754391422136428184644 1
9774576551737791979522086164941769880099474497791353251754391422136428184644 3
9774576551737791979522086164941769880099474497791353251754391422136428184644 5
9774576551737791979522086164941769880099474497791353251754391422136428184644 7
9774576551737791979522086164941769880099474497791353251754391422136428184644 9
9774576551737791979522086164941769880099474497791353251754391422136428184645 1
9774576551737791979522086164941769880099474497791353251754391422136428184645 3
9774576551737791979522086164941769880099474497791353251754391422136428184645 5
9774576551737791979522086164941769880099474497791353251754391422136428184645 7
9774576551737791979522086164941769880099474497791353251754391422136428184645 9
9774576551737791979522086164941769880099474497791353251754391422136428184646 1
9774576551737791979522086164941769880099474497791353251754391422136428184646 3
9774576551737791979522086164941769880099474497791353251754391422136428184646 5
9774576551737791979522086164941769880099474497791353251754391422136428184646 7
9774576551737791979522086164941769880099474497791353251754391422136428184646 9
9774576551737791979522086164941769880099474497791353251754391422136428184647 1
9774576551737791979522086164941769880099474497791353251754391422136428184647 3
9774576551737791979522086164941769880099474497791353251754391422136428184647 5
9774576551737791979522086164941769880099474497791353251754391422136428184647 7
9774576551737791979522086164941769880099474497791353251754391422136428184647 9
9774576551737791979522086164941769880099474497791353251754391422136428184648 1
9774576551737791979522086164941769880099474497791353251754391422136428184648 3
9774576551737791979522086164941769880099474497791353251754391422136428184648 5

9774576551737791979522086164941769880099474497791353251754391422136428184648 7
9774576551737791979522086164941769880099474497791353251754391422136428184648 9
9774576551737791979522086164941769880099474497791353251754391422136428184649 1
9774576551737791979522086164941769880099474497791353251754391422136428184649 3
9774576551737791979522086164941769880099474497791353251754391422136428184649 5
9774576551737791979522086164941769880099474497791353251754391422136428184649 7
9774576551737791979522086164941769880099474497791353251754391422136428184649 9
9774576551737791979522086164941769880099474497791353251754391422136428184650 1
9774576551737791979522086164941769880099474497791353251754391422136428184650 3
9774576551737791979522086164941769880099474497791353251754391422136428184650 5
9774576551737791979522086164941769880099474497791353251754391422136428184650 7
9774576551737791979522086164941769880099474497791353251754391422136428184650 9
9774576551737791979522086164941769880099474497791353251754391422136428184651 1
9774576551737791979522086164941769880099474497791353251754391422136428184651 3
9774576551737791979522086164941769880099474497791353251754391422136428184651 5
9774576551737791979522086164941769880099474497791353251754391422136428184651 7
9774576551737791979522086164941769880099474497791353251754391422136428184651 9
9774576551737791979522086164941769880099474497791353251754391422136428184652 1
9774576551737791979522086164941769880099474497791353251754391422136428184652 3
9774576551737791979522086164941769880099474497791353251754391422136428184652 5
9774576551737791979522086164941769880099474497791353251754391422136428184652 7
9774576551737791979522086164941769880099474497791353251754391422136428184652 9
9774576551737791979522086164941769880099474497791353251754391422136428184653 1
9774576551737791979522086164941769880099474497791353251754391422136428184653 3
9774576551737791979522086164941769880099474497791353251754391422136428184653 5
9774576551737791979522086164941769880099474497791353251754391422136428184653 7
9774576551737791979522086164941769880099474497791353251754391422136428184653 9
9774576551737791979522086164941769880099474497791353251754391422136428184654 1
9774576551737791979522086164941769880099474497791353251754391422136428184654 3
9774576551737791979522086164941769880099474497791353251754391422136428184654 5
9774576551737791979522086164941769880099474497791353251754391422136428184654 7
9774576551737791979522086164941769880099474497791353251754391422136428184654 9
9774576551737791979522086164941769880099474497791353251754391422136428184655 1
9774576551737791979522086164941769880099474497791353251754391422136428184655 3
9774576551737791979522086164941769880099474497791353251754391422136428184655 5
9774576551737791979522086164941769880099474497791353251754391422136428184655 7
9774576551737791979522086164941769880099474497791353251754391422136428184655 9
9774576551737791979522086164941769880099474497791353251754391422136428184656 1
9774576551737791979522086164941769880099474497791353251754391422136428184656 3
9774576551737791979522086164941769880099474497791353251754391422136428184656 5
9774576551737791979522086164941769880099474497791353251754391422136428184656 7
9774576551737791979522086164941769880099474497791353251754391422136428184656 9
9774576551737791979522086164941769880099474497791353251754391422136428184657 1
9774576551737791979522086164941769880099474497791353251754391422136428184657 3
9774576551737791979522086164941769880099474497791353251754391422136428184657 5
9774576551737791979522086164941769880099474497791353251754391422136428184657 7
9774576551737791979522086164941769880099474497791353251754391422136428184657 9
9774576551737791979522086164941769880099474497791353251754391422136428184658 1
9774576551737791979522086164941769880099474497791353251754391422136428184658 3
9774576551737791979522086164941769880099474497791353251754391422136428184658 5
9774576551737791979522086164941769880099474497791353251754391422136428184658 7
9774576551737791979522086164941769880099474497791353251754391422136428184658 9
9774576551737791979522086164941769880099474497791353251754391422136428184659 1
9774576551737791979522086164941769880099474497791353251754391422136428184659 3
9774576551737791979522086164941769880099474497791353251754391422136428184659 5
9774576551737791979522086164941769880099474497791353251754391422136428184659 7
9774576551737791979522086164941769880099474497791353251754391422136428184659 9
9774576551737791979522086164941769880099474497791353251754391422136428184660 1
9774576551737791979522086164941769880099474497791353251754391422136428184660 3
9774576551737791979522086164941769880099474497791353251754391422136428184660 5
9774576551737791979522086164941769880099474497791353251754391422136428184660 7
9774576551737791979522086164941769880099474497791353251754391422136428184660 9
9774576551737791979522086164941769880099474497791353251754391422136428184661 1

97745765517377919795220861649417698800994744977913532517543914221364281846613
97745765517377919795220861649417698800994744977913532517543914221364281846615
97745765517377919795220861649417698800994744977913532517543914221364281846617
97745765517377919795220861649417698800994744977913532517543914221364281846619
97745765517377919795220861649417698800994744977913532517543914221364281846621
97745765517377919795220861649417698800994744977913532517543914221364281846623
97745765517377919795220861649417698800994744977913532517543914221364281846625
97745765517377919795220861649417698800994744977913532517543914221364281846627
97745765517377919795220861649417698800994744977913532517543914221364281846629
97745765517377919795220861649417698800994744977913532517543914221364281846631
97745765517377919795220861649417698800994744977913532517543914221364281846633
97745765517377919795220861649417698800994744977913532517543914221364281846635
97745765517377919795220861649417698800994744977913532517543914221364281846637
97745765517377919795220861649417698800994744977913532517543914221364281846639
97745765517377919795220861649417698800994744977913532517543914221364281846641
97745765517377919795220861649417698800994744977913532517543914221364281846643

Q1 = 98219030841433552464311142587428173157294506280006971099954355202407009277971

Відсіяні кандидати:

98219030841433552464311142587428173157294506280006971099954355202407009277537
98219030841433552464311142587428173157294506280006971099954355202407009277539
98219030841433552464311142587428173157294506280006971099954355202407009277541
98219030841433552464311142587428173157294506280006971099954355202407009277543
98219030841433552464311142587428173157294506280006971099954355202407009277545
98219030841433552464311142587428173157294506280006971099954355202407009277547
98219030841433552464311142587428173157294506280006971099954355202407009277549
98219030841433552464311142587428173157294506280006971099954355202407009277551
98219030841433552464311142587428173157294506280006971099954355202407009277553
98219030841433552464311142587428173157294506280006971099954355202407009277555
98219030841433552464311142587428173157294506280006971099954355202407009277557
98219030841433552464311142587428173157294506280006971099954355202407009277559
98219030841433552464311142587428173157294506280006971099954355202407009277561
98219030841433552464311142587428173157294506280006971099954355202407009277563
98219030841433552464311142587428173157294506280006971099954355202407009277565
98219030841433552464311142587428173157294506280006971099954355202407009277567
98219030841433552464311142587428173157294506280006971099954355202407009277569
98219030841433552464311142587428173157294506280006971099954355202407009277571
98219030841433552464311142587428173157294506280006971099954355202407009277573
98219030841433552464311142587428173157294506280006971099954355202407009277575
98219030841433552464311142587428173157294506280006971099954355202407009277577
98219030841433552464311142587428173157294506280006971099954355202407009277579
98219030841433552464311142587428173157294506280006971099954355202407009277581
98219030841433552464311142587428173157294506280006971099954355202407009277583
98219030841433552464311142587428173157294506280006971099954355202407009277585
98219030841433552464311142587428173157294506280006971099954355202407009277587
98219030841433552464311142587428173157294506280006971099954355202407009277589
98219030841433552464311142587428173157294506280006971099954355202407009277591
98219030841433552464311142587428173157294506280006971099954355202407009277593
98219030841433552464311142587428173157294506280006971099954355202407009277595
98219030841433552464311142587428173157294506280006971099954355202407009277597
98219030841433552464311142587428173157294506280006971099954355202407009277599
98219030841433552464311142587428173157294506280006971099954355202407009277601
98219030841433552464311142587428173157294506280006971099954355202407009277603
98219030841433552464311142587428173157294506280006971099954355202407009277605
98219030841433552464311142587428173157294506280006971099954355202407009277607
98219030841433552464311142587428173157294506280006971099954355202407009277609
98219030841433552464311142587428173157294506280006971099954355202407009277611
98219030841433552464311142587428173157294506280006971099954355202407009277613
98219030841433552464311142587428173157294506280006971099954355202407009277615
98219030841433552464311142587428173157294506280006971099954355202407009277617
98219030841433552464311142587428173157294506280006971099954355202407009277619
98219030841433552464311142587428173157294506280006971099954355202407009277621
98219030841433552464311142587428173157294506280006971099954355202407009277623

98219030841433552464311142587428173157294506280006971099954355202407009277625
98219030841433552464311142587428173157294506280006971099954355202407009277627
98219030841433552464311142587428173157294506280006971099954355202407009277629
98219030841433552464311142587428173157294506280006971099954355202407009277631
98219030841433552464311142587428173157294506280006971099954355202407009277633
98219030841433552464311142587428173157294506280006971099954355202407009277635
98219030841433552464311142587428173157294506280006971099954355202407009277637
98219030841433552464311142587428173157294506280006971099954355202407009277639
98219030841433552464311142587428173157294506280006971099954355202407009277641
98219030841433552464311142587428173157294506280006971099954355202407009277643
98219030841433552464311142587428173157294506280006971099954355202407009277645
98219030841433552464311142587428173157294506280006971099954355202407009277647
98219030841433552464311142587428173157294506280006971099954355202407009277649
98219030841433552464311142587428173157294506280006971099954355202407009277651
98219030841433552464311142587428173157294506280006971099954355202407009277653
98219030841433552464311142587428173157294506280006971099954355202407009277655
98219030841433552464311142587428173157294506280006971099954355202407009277657
98219030841433552464311142587428173157294506280006971099954355202407009277659
98219030841433552464311142587428173157294506280006971099954355202407009277661
98219030841433552464311142587428173157294506280006971099954355202407009277663
98219030841433552464311142587428173157294506280006971099954355202407009277665
98219030841433552464311142587428173157294506280006971099954355202407009277667
98219030841433552464311142587428173157294506280006971099954355202407009277669
98219030841433552464311142587428173157294506280006971099954355202407009277671
98219030841433552464311142587428173157294506280006971099954355202407009277673
98219030841433552464311142587428173157294506280006971099954355202407009277675
98219030841433552464311142587428173157294506280006971099954355202407009277677
98219030841433552464311142587428173157294506280006971099954355202407009277679
98219030841433552464311142587428173157294506280006971099954355202407009277681
98219030841433552464311142587428173157294506280006971099954355202407009277683
98219030841433552464311142587428173157294506280006971099954355202407009277685
98219030841433552464311142587428173157294506280006971099954355202407009277687
98219030841433552464311142587428173157294506280006971099954355202407009277689
98219030841433552464311142587428173157294506280006971099954355202407009277691
98219030841433552464311142587428173157294506280006971099954355202407009277693
98219030841433552464311142587428173157294506280006971099954355202407009277695
98219030841433552464311142587428173157294506280006971099954355202407009277697
98219030841433552464311142587428173157294506280006971099954355202407009277699
98219030841433552464311142587428173157294506280006971099954355202407009277701
98219030841433552464311142587428173157294506280006971099954355202407009277703
98219030841433552464311142587428173157294506280006971099954355202407009277705
98219030841433552464311142587428173157294506280006971099954355202407009277707
98219030841433552464311142587428173157294506280006971099954355202407009277709
98219030841433552464311142587428173157294506280006971099954355202407009277711
98219030841433552464311142587428173157294506280006971099954355202407009277713
98219030841433552464311142587428173157294506280006971099954355202407009277715
98219030841433552464311142587428173157294506280006971099954355202407009277717
98219030841433552464311142587428173157294506280006971099954355202407009277719
98219030841433552464311142587428173157294506280006971099954355202407009277721
98219030841433552464311142587428173157294506280006971099954355202407009277723
98219030841433552464311142587428173157294506280006971099954355202407009277725
98219030841433552464311142587428173157294506280006971099954355202407009277727
98219030841433552464311142587428173157294506280006971099954355202407009277729
98219030841433552464311142587428173157294506280006971099954355202407009277731
98219030841433552464311142587428173157294506280006971099954355202407009277733
98219030841433552464311142587428173157294506280006971099954355202407009277735
98219030841433552464311142587428173157294506280006971099954355202407009277737
98219030841433552464311142587428173157294506280006971099954355202407009277739
98219030841433552464311142587428173157294506280006971099954355202407009277741
98219030841433552464311142587428173157294506280006971099954355202407009277743
98219030841433552464311142587428173157294506280006971099954355202407009277745
98219030841433552464311142587428173157294506280006971099954355202407009277747
98219030841433552464311142587428173157294506280006971099954355202407009277749

98219030841433552464311142587428173157294506280006971099954355202407009277751
98219030841433552464311142587428173157294506280006971099954355202407009277753
98219030841433552464311142587428173157294506280006971099954355202407009277755
98219030841433552464311142587428173157294506280006971099954355202407009277757
98219030841433552464311142587428173157294506280006971099954355202407009277759
98219030841433552464311142587428173157294506280006971099954355202407009277761
98219030841433552464311142587428173157294506280006971099954355202407009277763
98219030841433552464311142587428173157294506280006971099954355202407009277765
98219030841433552464311142587428173157294506280006971099954355202407009277767
98219030841433552464311142587428173157294506280006971099954355202407009277769
98219030841433552464311142587428173157294506280006971099954355202407009277771
98219030841433552464311142587428173157294506280006971099954355202407009277773
98219030841433552464311142587428173157294506280006971099954355202407009277775
98219030841433552464311142587428173157294506280006971099954355202407009277777
98219030841433552464311142587428173157294506280006971099954355202407009277779
98219030841433552464311142587428173157294506280006971099954355202407009277781
98219030841433552464311142587428173157294506280006971099954355202407009277783
98219030841433552464311142587428173157294506280006971099954355202407009277785
98219030841433552464311142587428173157294506280006971099954355202407009277787
98219030841433552464311142587428173157294506280006971099954355202407009277789
98219030841433552464311142587428173157294506280006971099954355202407009277791
98219030841433552464311142587428173157294506280006971099954355202407009277793
98219030841433552464311142587428173157294506280006971099954355202407009277795
98219030841433552464311142587428173157294506280006971099954355202407009277797
98219030841433552464311142587428173157294506280006971099954355202407009277799
98219030841433552464311142587428173157294506280006971099954355202407009277801
98219030841433552464311142587428173157294506280006971099954355202407009277803
98219030841433552464311142587428173157294506280006971099954355202407009277805
98219030841433552464311142587428173157294506280006971099954355202407009277807
98219030841433552464311142587428173157294506280006971099954355202407009277809
98219030841433552464311142587428173157294506280006971099954355202407009277811
98219030841433552464311142587428173157294506280006971099954355202407009277813
98219030841433552464311142587428173157294506280006971099954355202407009277815
98219030841433552464311142587428173157294506280006971099954355202407009277817
98219030841433552464311142587428173157294506280006971099954355202407009277819
98219030841433552464311142587428173157294506280006971099954355202407009277821
98219030841433552464311142587428173157294506280006971099954355202407009277823
98219030841433552464311142587428173157294506280006971099954355202407009277825
98219030841433552464311142587428173157294506280006971099954355202407009277827
98219030841433552464311142587428173157294506280006971099954355202407009277829
98219030841433552464311142587428173157294506280006971099954355202407009277831
98219030841433552464311142587428173157294506280006971099954355202407009277833
98219030841433552464311142587428173157294506280006971099954355202407009277835
98219030841433552464311142587428173157294506280006971099954355202407009277837
98219030841433552464311142587428173157294506280006971099954355202407009277839
98219030841433552464311142587428173157294506280006971099954355202407009277841
98219030841433552464311142587428173157294506280006971099954355202407009277843
98219030841433552464311142587428173157294506280006971099954355202407009277845
98219030841433552464311142587428173157294506280006971099954355202407009277847
98219030841433552464311142587428173157294506280006971099954355202407009277849
98219030841433552464311142587428173157294506280006971099954355202407009277851
98219030841433552464311142587428173157294506280006971099954355202407009277853
98219030841433552464311142587428173157294506280006971099954355202407009277855
98219030841433552464311142587428173157294506280006971099954355202407009277857
98219030841433552464311142587428173157294506280006971099954355202407009277859
98219030841433552464311142587428173157294506280006971099954355202407009277861
98219030841433552464311142587428173157294506280006971099954355202407009277863
98219030841433552464311142587428173157294506280006971099954355202407009277865
98219030841433552464311142587428173157294506280006971099954355202407009277867
98219030841433552464311142587428173157294506280006971099954355202407009277869
98219030841433552464311142587428173157294506280006971099954355202407009277871
98219030841433552464311142587428173157294506280006971099954355202407009277873
98219030841433552464311142587428173157294506280006971099954355202407009277875

98219030841433552464311142587428173157294506280006971099954355202407009277877
98219030841433552464311142587428173157294506280006971099954355202407009277879
98219030841433552464311142587428173157294506280006971099954355202407009277881
98219030841433552464311142587428173157294506280006971099954355202407009277883
98219030841433552464311142587428173157294506280006971099954355202407009277885
98219030841433552464311142587428173157294506280006971099954355202407009277887
98219030841433552464311142587428173157294506280006971099954355202407009277889
98219030841433552464311142587428173157294506280006971099954355202407009277891
98219030841433552464311142587428173157294506280006971099954355202407009277893
98219030841433552464311142587428173157294506280006971099954355202407009277895
98219030841433552464311142587428173157294506280006971099954355202407009277897
98219030841433552464311142587428173157294506280006971099954355202407009277899
98219030841433552464311142587428173157294506280006971099954355202407009277901
98219030841433552464311142587428173157294506280006971099954355202407009277903
98219030841433552464311142587428173157294506280006971099954355202407009277905
98219030841433552464311142587428173157294506280006971099954355202407009277907
98219030841433552464311142587428173157294506280006971099954355202407009277909
98219030841433552464311142587428173157294506280006971099954355202407009277911
98219030841433552464311142587428173157294506280006971099954355202407009277913
98219030841433552464311142587428173157294506280006971099954355202407009277915
98219030841433552464311142587428173157294506280006971099954355202407009277917
98219030841433552464311142587428173157294506280006971099954355202407009277919
98219030841433552464311142587428173157294506280006971099954355202407009277921
98219030841433552464311142587428173157294506280006971099954355202407009277923
98219030841433552464311142587428173157294506280006971099954355202407009277925
98219030841433552464311142587428173157294506280006971099954355202407009277927
98219030841433552464311142587428173157294506280006971099954355202407009277929
98219030841433552464311142587428173157294506280006971099954355202407009277931
98219030841433552464311142587428173157294506280006971099954355202407009277933
98219030841433552464311142587428173157294506280006971099954355202407009277935
98219030841433552464311142587428173157294506280006971099954355202407009277937
98219030841433552464311142587428173157294506280006971099954355202407009277939
98219030841433552464311142587428173157294506280006971099954355202407009277941
98219030841433552464311142587428173157294506280006971099954355202407009277943
98219030841433552464311142587428173157294506280006971099954355202407009277945
98219030841433552464311142587428173157294506280006971099954355202407009277947
98219030841433552464311142587428173157294506280006971099954355202407009277949
98219030841433552464311142587428173157294506280006971099954355202407009277951
98219030841433552464311142587428173157294506280006971099954355202407009277953
98219030841433552464311142587428173157294506280006971099954355202407009277955
98219030841433552464311142587428173157294506280006971099954355202407009277957
98219030841433552464311142587428173157294506280006971099954355202407009277959
98219030841433552464311142587428173157294506280006971099954355202407009277961
98219030841433552464311142587428173157294506280006971099954355202407009277963
98219030841433552464311142587428173157294506280006971099954355202407009277965
98219030841433552464311142587428173157294506280006971099954355202407009277967
98219030841433552464311142587428173157294506280006971099954355202407009277969
98219030841433552464311142587428173157294506280006971099954355202407009277971

P2 = 10509148907451447570427553195667095500613830295992339222674800703638145844726 9

Відсіяні кандидати:

10509148907451447570427553195667095500613830295992339222674800703638145844668 1
10509148907451447570427553195667095500613830295992339222674800703638145844668 3
10509148907451447570427553195667095500613830295992339222674800703638145844668 5
10509148907451447570427553195667095500613830295992339222674800703638145844668 7
10509148907451447570427553195667095500613830295992339222674800703638145844668 9
10509148907451447570427553195667095500613830295992339222674800703638145844669 1
10509148907451447570427553195667095500613830295992339222674800703638145844669 3
10509148907451447570427553195667095500613830295992339222674800703638145844669 5
10509148907451447570427553195667095500613830295992339222674800703638145844669 7
10509148907451447570427553195667095500613830295992339222674800703638145844669 9
10509148907451447570427553195667095500613830295992339222674800703638145844670 1
10509148907451447570427553195667095500613830295992339222674800703638145844670 3

105091489074514475704275531956670955006138302959233922267480070363814584467 05
105091489074514475704275531956670955006138302959233922267480070363814584467 07
105091489074514475704275531956670955006138302959233922267480070363814584467 09
105091489074514475704275531956670955006138302959233922267480070363814584467 11
105091489074514475704275531956670955006138302959233922267480070363814584467 13
105091489074514475704275531956670955006138302959233922267480070363814584467 15
105091489074514475704275531956670955006138302959233922267480070363814584467 17
105091489074514475704275531956670955006138302959233922267480070363814584467 19
105091489074514475704275531956670955006138302959233922267480070363814584467 21
105091489074514475704275531956670955006138302959233922267480070363814584467 23
105091489074514475704275531956670955006138302959233922267480070363814584467 25
105091489074514475704275531956670955006138302959233922267480070363814584467 27
105091489074514475704275531956670955006138302959233922267480070363814584467 29
105091489074514475704275531956670955006138302959233922267480070363814584467 31
105091489074514475704275531956670955006138302959233922267480070363814584467 33
105091489074514475704275531956670955006138302959233922267480070363814584467 35
105091489074514475704275531956670955006138302959233922267480070363814584467 37
105091489074514475704275531956670955006138302959233922267480070363814584467 39
105091489074514475704275531956670955006138302959233922267480070363814584467 41
105091489074514475704275531956670955006138302959233922267480070363814584467 43
105091489074514475704275531956670955006138302959233922267480070363814584467 45
105091489074514475704275531956670955006138302959233922267480070363814584467 47
105091489074514475704275531956670955006138302959233922267480070363814584467 49
105091489074514475704275531956670955006138302959233922267480070363814584467 51
105091489074514475704275531956670955006138302959233922267480070363814584467 53
105091489074514475704275531956670955006138302959233922267480070363814584467 55
105091489074514475704275531956670955006138302959233922267480070363814584467 57
105091489074514475704275531956670955006138302959233922267480070363814584467 59
105091489074514475704275531956670955006138302959233922267480070363814584467 61
105091489074514475704275531956670955006138302959233922267480070363814584467 63
105091489074514475704275531956670955006138302959233922267480070363814584467 65
105091489074514475704275531956670955006138302959233922267480070363814584467 67
105091489074514475704275531956670955006138302959233922267480070363814584467 69
105091489074514475704275531956670955006138302959233922267480070363814584467 71
105091489074514475704275531956670955006138302959233922267480070363814584467 73
105091489074514475704275531956670955006138302959233922267480070363814584467 75
105091489074514475704275531956670955006138302959233922267480070363814584467 77
105091489074514475704275531956670955006138302959233922267480070363814584467 79
105091489074514475704275531956670955006138302959233922267480070363814584467 81
105091489074514475704275531956670955006138302959233922267480070363814584467 83
105091489074514475704275531956670955006138302959233922267480070363814584467 85
105091489074514475704275531956670955006138302959233922267480070363814584467 87
105091489074514475704275531956670955006138302959233922267480070363814584467 89
105091489074514475704275531956670955006138302959233922267480070363814584467 91
105091489074514475704275531956670955006138302959233922267480070363814584467 93
105091489074514475704275531956670955006138302959233922267480070363814584467 95
105091489074514475704275531956670955006138302959233922267480070363814584467 97
105091489074514475704275531956670955006138302959233922267480070363814584467 99
105091489074514475704275531956670955006138302959233922267480070363814584468 01
105091489074514475704275531956670955006138302959233922267480070363814584468 03
105091489074514475704275531956670955006138302959233922267480070363814584468 05
105091489074514475704275531956670955006138302959233922267480070363814584468 07
105091489074514475704275531956670955006138302959233922267480070363814584468 09
105091489074514475704275531956670955006138302959233922267480070363814584468 11
105091489074514475704275531956670955006138302959233922267480070363814584468 13
105091489074514475704275531956670955006138302959233922267480070363814584468 15
105091489074514475704275531956670955006138302959233922267480070363814584468 17
105091489074514475704275531956670955006138302959233922267480070363814584468 19
105091489074514475704275531956670955006138302959233922267480070363814584468 21
105091489074514475704275531956670955006138302959233922267480070363814584468 23
105091489074514475704275531956670955006138302959233922267480070363814584468 25
105091489074514475704275531956670955006138302959233922267480070363814584468 27
105091489074514475704275531956670955006138302959233922267480070363814584468 29

105091489074514475704275531956670955006138302959233922267480070363814584468 31
105091489074514475704275531956670955006138302959233922267480070363814584468 33
105091489074514475704275531956670955006138302959233922267480070363814584468 35
105091489074514475704275531956670955006138302959233922267480070363814584468 37
105091489074514475704275531956670955006138302959233922267480070363814584468 39
105091489074514475704275531956670955006138302959233922267480070363814584468 41
105091489074514475704275531956670955006138302959233922267480070363814584468 43
105091489074514475704275531956670955006138302959233922267480070363814584468 45
105091489074514475704275531956670955006138302959233922267480070363814584468 47
105091489074514475704275531956670955006138302959233922267480070363814584468 49
105091489074514475704275531956670955006138302959233922267480070363814584468 51
105091489074514475704275531956670955006138302959233922267480070363814584468 53
105091489074514475704275531956670955006138302959233922267480070363814584468 55
105091489074514475704275531956670955006138302959233922267480070363814584468 57
105091489074514475704275531956670955006138302959233922267480070363814584468 59
105091489074514475704275531956670955006138302959233922267480070363814584468 61
105091489074514475704275531956670955006138302959233922267480070363814584468 63
105091489074514475704275531956670955006138302959233922267480070363814584468 65
105091489074514475704275531956670955006138302959233922267480070363814584468 67
105091489074514475704275531956670955006138302959233922267480070363814584468 69
105091489074514475704275531956670955006138302959233922267480070363814584468 71
105091489074514475704275531956670955006138302959233922267480070363814584468 73
105091489074514475704275531956670955006138302959233922267480070363814584468 75
105091489074514475704275531956670955006138302959233922267480070363814584468 77
105091489074514475704275531956670955006138302959233922267480070363814584468 79
105091489074514475704275531956670955006138302959233922267480070363814584468 81
105091489074514475704275531956670955006138302959233922267480070363814584468 83
105091489074514475704275531956670955006138302959233922267480070363814584468 85
105091489074514475704275531956670955006138302959233922267480070363814584468 87
105091489074514475704275531956670955006138302959233922267480070363814584468 89
105091489074514475704275531956670955006138302959233922267480070363814584468 91
105091489074514475704275531956670955006138302959233922267480070363814584468 93
105091489074514475704275531956670955006138302959233922267480070363814584468 95
105091489074514475704275531956670955006138302959233922267480070363814584468 97
105091489074514475704275531956670955006138302959233922267480070363814584468 99
105091489074514475704275531956670955006138302959233922267480070363814584469 01
105091489074514475704275531956670955006138302959233922267480070363814584469 03
105091489074514475704275531956670955006138302959233922267480070363814584469 05
105091489074514475704275531956670955006138302959233922267480070363814584469 07
105091489074514475704275531956670955006138302959233922267480070363814584469 09
105091489074514475704275531956670955006138302959233922267480070363814584469 11
105091489074514475704275531956670955006138302959233922267480070363814584469 13
105091489074514475704275531956670955006138302959233922267480070363814584469 15
105091489074514475704275531956670955006138302959233922267480070363814584469 17
105091489074514475704275531956670955006138302959233922267480070363814584469 19
105091489074514475704275531956670955006138302959233922267480070363814584469 21
105091489074514475704275531956670955006138302959233922267480070363814584469 23
105091489074514475704275531956670955006138302959233922267480070363814584469 25
105091489074514475704275531956670955006138302959233922267480070363814584469 27
105091489074514475704275531956670955006138302959233922267480070363814584469 29
105091489074514475704275531956670955006138302959233922267480070363814584469 31
105091489074514475704275531956670955006138302959233922267480070363814584469 33
105091489074514475704275531956670955006138302959233922267480070363814584469 35
105091489074514475704275531956670955006138302959233922267480070363814584469 37
105091489074514475704275531956670955006138302959233922267480070363814584469 39
105091489074514475704275531956670955006138302959233922267480070363814584469 41
105091489074514475704275531956670955006138302959233922267480070363814584469 43
105091489074514475704275531956670955006138302959233922267480070363814584469 45
105091489074514475704275531956670955006138302959233922267480070363814584469 47
105091489074514475704275531956670955006138302959233922267480070363814584469 49
105091489074514475704275531956670955006138302959233922267480070363814584469 51
105091489074514475704275531956670955006138302959233922267480070363814584469 53
105091489074514475704275531956670955006138302959233922267480070363814584469 55

105091489074514475704275531956670955006138302959923392226748007036381458446957
105091489074514475704275531956670955006138302959923392226748007036381458446959
105091489074514475704275531956670955006138302959923392226748007036381458446961
105091489074514475704275531956670955006138302959923392226748007036381458446963
105091489074514475704275531956670955006138302959923392226748007036381458446965
105091489074514475704275531956670955006138302959923392226748007036381458446967
105091489074514475704275531956670955006138302959923392226748007036381458446969
105091489074514475704275531956670955006138302959923392226748007036381458446971
105091489074514475704275531956670955006138302959923392226748007036381458446973
105091489074514475704275531956670955006138302959923392226748007036381458446975
105091489074514475704275531956670955006138302959923392226748007036381458446977
105091489074514475704275531956670955006138302959923392226748007036381458446979
105091489074514475704275531956670955006138302959923392226748007036381458446981
105091489074514475704275531956670955006138302959923392226748007036381458446983
105091489074514475704275531956670955006138302959923392226748007036381458446985
105091489074514475704275531956670955006138302959923392226748007036381458446987
105091489074514475704275531956670955006138302959923392226748007036381458446989
105091489074514475704275531956670955006138302959923392226748007036381458446991
105091489074514475704275531956670955006138302959923392226748007036381458446993
105091489074514475704275531956670955006138302959923392226748007036381458446995
105091489074514475704275531956670955006138302959923392226748007036381458446997
105091489074514475704275531956670955006138302959923392226748007036381458446999
105091489074514475704275531956670955006138302959923392226748007036381458447001
105091489074514475704275531956670955006138302959923392226748007036381458447003
105091489074514475704275531956670955006138302959923392226748007036381458447005
105091489074514475704275531956670955006138302959923392226748007036381458447007
105091489074514475704275531956670955006138302959923392226748007036381458447009
105091489074514475704275531956670955006138302959923392226748007036381458447011
105091489074514475704275531956670955006138302959923392226748007036381458447013
105091489074514475704275531956670955006138302959923392226748007036381458447015
105091489074514475704275531956670955006138302959923392226748007036381458447017
105091489074514475704275531956670955006138302959923392226748007036381458447019
105091489074514475704275531956670955006138302959923392226748007036381458447021
105091489074514475704275531956670955006138302959923392226748007036381458447023
105091489074514475704275531956670955006138302959923392226748007036381458447025
105091489074514475704275531956670955006138302959923392226748007036381458447027
105091489074514475704275531956670955006138302959923392226748007036381458447029
105091489074514475704275531956670955006138302959923392226748007036381458447031
105091489074514475704275531956670955006138302959923392226748007036381458447033
105091489074514475704275531956670955006138302959923392226748007036381458447035
105091489074514475704275531956670955006138302959923392226748007036381458447037
105091489074514475704275531956670955006138302959923392226748007036381458447039
105091489074514475704275531956670955006138302959923392226748007036381458447041
105091489074514475704275531956670955006138302959923392226748007036381458447043
105091489074514475704275531956670955006138302959923392226748007036381458447045
105091489074514475704275531956670955006138302959923392226748007036381458447047
105091489074514475704275531956670955006138302959923392226748007036381458447049
105091489074514475704275531956670955006138302959923392226748007036381458447051
105091489074514475704275531956670955006138302959923392226748007036381458447053
105091489074514475704275531956670955006138302959923392226748007036381458447055
105091489074514475704275531956670955006138302959923392226748007036381458447057
105091489074514475704275531956670955006138302959923392226748007036381458447059
105091489074514475704275531956670955006138302959923392226748007036381458447061
105091489074514475704275531956670955006138302959923392226748007036381458447063
105091489074514475704275531956670955006138302959923392226748007036381458447065
105091489074514475704275531956670955006138302959923392226748007036381458447067
105091489074514475704275531956670955006138302959923392226748007036381458447069
105091489074514475704275531956670955006138302959923392226748007036381458447071
105091489074514475704275531956670955006138302959923392226748007036381458447073
105091489074514475704275531956670955006138302959923392226748007036381458447075
105091489074514475704275531956670955006138302959923392226748007036381458447077
105091489074514475704275531956670955006138302959923392226748007036381458447079
105091489074514475704275531956670955006138302959923392226748007036381458447081

105091489074514475704275531956670955006138302959233922267480070363814584470 83
105091489074514475704275531956670955006138302959233922267480070363814584470 85
105091489074514475704275531956670955006138302959233922267480070363814584470 87
105091489074514475704275531956670955006138302959233922267480070363814584470 89
105091489074514475704275531956670955006138302959233922267480070363814584470 91
105091489074514475704275531956670955006138302959233922267480070363814584470 93
105091489074514475704275531956670955006138302959233922267480070363814584470 95
105091489074514475704275531956670955006138302959233922267480070363814584470 97
105091489074514475704275531956670955006138302959233922267480070363814584470 99
105091489074514475704275531956670955006138302959233922267480070363814584471 01
105091489074514475704275531956670955006138302959233922267480070363814584471 03
105091489074514475704275531956670955006138302959233922267480070363814584471 05
105091489074514475704275531956670955006138302959233922267480070363814584471 07
105091489074514475704275531956670955006138302959233922267480070363814584471 09
105091489074514475704275531956670955006138302959233922267480070363814584471 11
105091489074514475704275531956670955006138302959233922267480070363814584471 13
105091489074514475704275531956670955006138302959233922267480070363814584471 15
105091489074514475704275531956670955006138302959233922267480070363814584471 17
105091489074514475704275531956670955006138302959233922267480070363814584471 19
105091489074514475704275531956670955006138302959233922267480070363814584471 21
105091489074514475704275531956670955006138302959233922267480070363814584471 23
105091489074514475704275531956670955006138302959233922267480070363814584471 25
105091489074514475704275531956670955006138302959233922267480070363814584471 27
105091489074514475704275531956670955006138302959233922267480070363814584471 29
105091489074514475704275531956670955006138302959233922267480070363814584471 31
105091489074514475704275531956670955006138302959233922267480070363814584471 33
105091489074514475704275531956670955006138302959233922267480070363814584471 35
105091489074514475704275531956670955006138302959233922267480070363814584471 37
105091489074514475704275531956670955006138302959233922267480070363814584471 39
105091489074514475704275531956670955006138302959233922267480070363814584471 41
105091489074514475704275531956670955006138302959233922267480070363814584471 43
105091489074514475704275531956670955006138302959233922267480070363814584471 45
105091489074514475704275531956670955006138302959233922267480070363814584471 47
105091489074514475704275531956670955006138302959233922267480070363814584471 49
105091489074514475704275531956670955006138302959233922267480070363814584471 51
105091489074514475704275531956670955006138302959233922267480070363814584471 53
105091489074514475704275531956670955006138302959233922267480070363814584471 55
105091489074514475704275531956670955006138302959233922267480070363814584471 57
105091489074514475704275531956670955006138302959233922267480070363814584471 59
105091489074514475704275531956670955006138302959233922267480070363814584471 61
105091489074514475704275531956670955006138302959233922267480070363814584471 63
105091489074514475704275531956670955006138302959233922267480070363814584471 65
105091489074514475704275531956670955006138302959233922267480070363814584471 67
105091489074514475704275531956670955006138302959233922267480070363814584471 69
105091489074514475704275531956670955006138302959233922267480070363814584471 71
105091489074514475704275531956670955006138302959233922267480070363814584471 73
105091489074514475704275531956670955006138302959233922267480070363814584471 75
105091489074514475704275531956670955006138302959233922267480070363814584471 77
105091489074514475704275531956670955006138302959233922267480070363814584471 79
105091489074514475704275531956670955006138302959233922267480070363814584471 81
105091489074514475704275531956670955006138302959233922267480070363814584471 83
105091489074514475704275531956670955006138302959233922267480070363814584471 85
105091489074514475704275531956670955006138302959233922267480070363814584471 87
105091489074514475704275531956670955006138302959233922267480070363814584471 89
105091489074514475704275531956670955006138302959233922267480070363814584471 91
105091489074514475704275531956670955006138302959233922267480070363814584471 93
105091489074514475704275531956670955006138302959233922267480070363814584471 95
105091489074514475704275531956670955006138302959233922267480070363814584471 97
105091489074514475704275531956670955006138302959233922267480070363814584471 99
105091489074514475704275531956670955006138302959233922267480070363814584472 01
105091489074514475704275531956670955006138302959233922267480070363814584472 03
105091489074514475704275531956670955006138302959233922267480070363814584472 05
105091489074514475704275531956670955006138302959233922267480070363814584472 07

105091489074514475704275531956670955006138302959233922267480070363814584472 09
105091489074514475704275531956670955006138302959233922267480070363814584472 11
105091489074514475704275531956670955006138302959233922267480070363814584472 13
105091489074514475704275531956670955006138302959233922267480070363814584472 15
105091489074514475704275531956670955006138302959233922267480070363814584472 17
105091489074514475704275531956670955006138302959233922267480070363814584472 19
105091489074514475704275531956670955006138302959233922267480070363814584472 21
105091489074514475704275531956670955006138302959233922267480070363814584472 23
105091489074514475704275531956670955006138302959233922267480070363814584472 25
105091489074514475704275531956670955006138302959233922267480070363814584472 27
105091489074514475704275531956670955006138302959233922267480070363814584472 29
105091489074514475704275531956670955006138302959233922267480070363814584472 31
105091489074514475704275531956670955006138302959233922267480070363814584472 33
105091489074514475704275531956670955006138302959233922267480070363814584472 35
105091489074514475704275531956670955006138302959233922267480070363814584472 37
105091489074514475704275531956670955006138302959233922267480070363814584472 39
105091489074514475704275531956670955006138302959233922267480070363814584472 41
105091489074514475704275531956670955006138302959233922267480070363814584472 43
105091489074514475704275531956670955006138302959233922267480070363814584472 45
105091489074514475704275531956670955006138302959233922267480070363814584472 47
105091489074514475704275531956670955006138302959233922267480070363814584472 49
105091489074514475704275531956670955006138302959233922267480070363814584472 51
105091489074514475704275531956670955006138302959233922267480070363814584472 53
105091489074514475704275531956670955006138302959233922267480070363814584472 55
105091489074514475704275531956670955006138302959233922267480070363814584472 57
105091489074514475704275531956670955006138302959233922267480070363814584472 59
105091489074514475704275531956670955006138302959233922267480070363814584472 61
105091489074514475704275531956670955006138302959233922267480070363814584472 63
105091489074514475704275531956670955006138302959233922267480070363814584472 65
105091489074514475704275531956670955006138302959233922267480070363814584472 67
105091489074514475704275531956670955006138302959233922267480070363814584472 69

Q2 = 10780765823273250028076422171436891821357907315476627707752435243209145425 5523

Відсіяні кандидати:

107807658232732500280764221714368918213579073154766277077524352432091454255433
107807658232732500280764221714368918213579073154766277077524352432091454255435
107807658232732500280764221714368918213579073154766277077524352432091454255437
107807658232732500280764221714368918213579073154766277077524352432091454255439
107807658232732500280764221714368918213579073154766277077524352432091454255441
107807658232732500280764221714368918213579073154766277077524352432091454255443
107807658232732500280764221714368918213579073154766277077524352432091454255445
107807658232732500280764221714368918213579073154766277077524352432091454255447
107807658232732500280764221714368918213579073154766277077524352432091454255449
107807658232732500280764221714368918213579073154766277077524352432091454255451
107807658232732500280764221714368918213579073154766277077524352432091454255453
107807658232732500280764221714368918213579073154766277077524352432091454255455
107807658232732500280764221714368918213579073154766277077524352432091454255457
107807658232732500280764221714368918213579073154766277077524352432091454255459
107807658232732500280764221714368918213579073154766277077524352432091454255461
107807658232732500280764221714368918213579073154766277077524352432091454255463
107807658232732500280764221714368918213579073154766277077524352432091454255465
107807658232732500280764221714368918213579073154766277077524352432091454255467
107807658232732500280764221714368918213579073154766277077524352432091454255469
107807658232732500280764221714368918213579073154766277077524352432091454255471
107807658232732500280764221714368918213579073154766277077524352432091454255473
107807658232732500280764221714368918213579073154766277077524352432091454255475
107807658232732500280764221714368918213579073154766277077524352432091454255477
107807658232732500280764221714368918213579073154766277077524352432091454255479
107807658232732500280764221714368918213579073154766277077524352432091454255481
107807658232732500280764221714368918213579073154766277077524352432091454255483
107807658232732500280764221714368918213579073154766277077524352432091454255485
107807658232732500280764221714368918213579073154766277077524352432091454255487
107807658232732500280764221714368918213579073154766277077524352432091454255489

1078076582327325002807642217143689182135790731547662770775243524320914542555491
1078076582327325002807642217143689182135790731547662770775243524320914542555493
1078076582327325002807642217143689182135790731547662770775243524320914542555495
1078076582327325002807642217143689182135790731547662770775243524320914542555497
1078076582327325002807642217143689182135790731547662770775243524320914542555499
1078076582327325002807642217143689182135790731547662770775243524320914542555501
1078076582327325002807642217143689182135790731547662770775243524320914542555503
1078076582327325002807642217143689182135790731547662770775243524320914542555505
1078076582327325002807642217143689182135790731547662770775243524320914542555507
1078076582327325002807642217143689182135790731547662770775243524320914542555509
1078076582327325002807642217143689182135790731547662770775243524320914542555511
1078076582327325002807642217143689182135790731547662770775243524320914542555513
1078076582327325002807642217143689182135790731547662770775243524320914542555515
1078076582327325002807642217143689182135790731547662770775243524320914542555517
1078076582327325002807642217143689182135790731547662770775243524320914542555519
1078076582327325002807642217143689182135790731547662770775243524320914542555521
1078076582327325002807642217143689182135790731547662770775243524320914542555523

Alice Open keys:

e = 4097;
n =
96004943579708741433352605170903879406739674391447382932159132937919289836954660211576886362269385420192649106307020547544932115055175483038571099802013533;

Alice Close keys:

d =
16426523175341915485667604643593756276330122467269859759688443297408206535441504294628489644015206214353269888688990431090475809109914413166067294169008533;
p = 97745765517377919795220861649417698800994744977913532517543914221364281846643;
q = 98219030841433552464311142587428173157294506280006971099954355202407009277971;

Bob Open keys:

e = 4097;
n =
11329667337314198123316216042608319464890485418534865704983523210609309246519353825464366245774270895941927259788050453234285942360081675766343945947516687;

Bob Close keys:

d =
32133447512714420842795809229950859697834376510465008418820732171657352561521214928924634016606317219650363015721340773900890885102961539562580667967912249;
p = 105091489074514475704275531956670955006138302959923392226748007036381458447269;
q = 1078076582327325002807642217143689182135790731547662770775243524320914542555523;

Процедура пересилання ключів:

Key sending has begun ...
Encryption has begun ...
Message k = 230015237079771095267514696669563837602249922658699942850800281185034878522208;
e = 4097;
n =
960049435797087414333526051709038794067396743914473829321591329379192898369546602115768863622
69385420192649106307020547544932115055175483038571099802013533
236357737817339757917944686997110516638624047852305142013788344740258292488841660938290045213
4337244285275309879276846086329673508279253761396882030470036
Encypted message k1 =
236357737817339757917944686997110516638624047852305142013788344740258292488841660938290045213
4337244285275309879276846086329673508279253761396882030470036
Encryption end.
Signing ...
Encryption has begun ...
Message k = 230015237079771095267514696669563837602249922658699942850800281185034878522208;
d =
321334475127144208427958092299508596978343765104650084188207321716573525615212149289246340166
06317219650363015721340773900890885102961539562580667967912249;

n =
113296673373141981233162160426083194648904854185348657049835232106093092465193538254643662457
742708959419272597880504532342859423600816757663439459475166875926388083579354335725749212569106154549000053539922453236753118916641029491968143677402459055738136623571952722301187722295491710075691363266345049631427
Encypted message S =
592638808357935433572574921256910615454900005353992245323675311891664102949196814367740245905
5738136623571952722301187722295491710075691363266345049631427
Encryption end.
Encryption has begun ...
Message S =
592638808357935433572574921256910615454900005353992245323675311891664102949196814367740245905
5738136623571952722301187722295491710075691363266345049631427;
d = 4097;
n =
960049435797087414333526051709038794067396743914473829321591329379192898369546602115768863622
693854201926491063070205475449321150551754830385710998020135325425655477213534578261706255583266891457650110357782215281860100561805550490070940783218352674625411203464731746775865927103110816280453761748365175660315425655477213534578261706255583266891457650110357782215281860100561805550490070940783218352674625411203464731746775865927103110816280453761748365175660315k1 =
236357737817339757917944686997110516638624047852305142013788344740258292488841660938290045213433724428527530987927684608632967350827925376139688203047003650
S =
592638808357935433572574921256910615454900005353992245323675311891664102949196814367740245905
5738136623571952722301187722295491710075691363266345049631427
S1 =
254256554772135345782617062555832668914576501103577822152818601005618055504900709407832183526
746254112034647317467758659271031108162804537617483651756603150
Key sended.
User switched to Alice ...
Key receiving has begun ...
Decryption has begun ...
Encrypted message k1 =
236357737817339757917944686997110516638624047852305142013788344740258292488841660938290045213433724428527530987927684608632967350827925376139688203047003650;
d =
164265231753419154856676046435937562763301224672698597596884432974082065354415042946284896440152062143532698886889904310904758091099144131660672941690085;
n =
960049435797087414333526051709038794067396743914473829321591329379192898369546602115768863622693854201926491063070205475449321150551754830385710998020135;
Decrypted message k =
230015237079771095267514696669563837602249922658699942850800281185034878522 08
Dencryption end.
Dencryption has begun ...
Encrypted message S1 =
254256554772135345782617062555832668914576501103577822152818601005618055504900709407832183526746254112034647317467758659271031108162804537617483651756603150315;
d =
164265231753419154856676046435937562763301224672698597596884432974082065354415042946284896440152062143532698886889904310904758091099144131660672941690085;
n =
960049435797087414333526051709038794067396743914473829321591329379192898369546602115768863622693854201926491063070205475449321150551754830385710998020135325425655477213534578261706255583266891457650110357782215281860100561805550490070940783218352674625411203464731746775865927103110816280453761748365175660315k = 230015237079771095267514696669563837602249922658699942850800281185034878522 08 ~ 15

S1 =
592638808357935433572574921256910615454900005353992245323675311891664102949196814367740245905
573813662357195272230118772229549171007569136326634504963142 7
Verifying ...
Dencryption has begun ...
Encrypted message S1 =
592638808357935433572574921256910615454900005353992245323675311891664102949196814367740245905
573813662357195272230118772229549171007569136326634504963142 7;
e = 4097;
n =
113296673373141981233162160426083194648904854185348657049835232106093092465193538254643662457
742708959419272597880504532342859423600816757663439459475166 87
Decrypted message k =
230015237079771095267514696669563837602249922658699942850800281185034878522 08
Dencryption end.
Message verified!
Key receiving end.

Висновок

Під час цієї лабораторної я розібрався та реалізував власноруч алгоритм шифрування та електронного підпису RSA.