МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Виконав:

студенти 3 курсу ФТІ

групи ФБ-93

Денисюк Артем

Товстоноженко Михайло

КИЇВ 2021

Мета: 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.

Постановка задачі

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

Кандидати, що не пройшли перевірку частоти

DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043946 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043947 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043947 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043947 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043947 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043947 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043948 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043948 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043948 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043948 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043948 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043949 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043949 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043949 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043949 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043949 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043950 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043950 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043950 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043950 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043950 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043951 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043951 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043951 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043951 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043951 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043952 1 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043952 3 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043952 5 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043952 7 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043952 9 is not suitable
DEBUG:from rsa_tools:Candidate 18753643386680983322328524564620960150898025761732232957245488881791161043953 1 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843093 9 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843094 1 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843094 3 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843094 5 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843094 7 is not suitable
DEBUG:from rsa_tools:Candidate 45160268789871430237151801756555910438578031403489063192016073968781539843094 9 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540151 5 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540151 7 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540151 9 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540152 1 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540152 3 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540152 5 is not suitable
DEBUG:from rsa_tools:Candidate 83490765286333438719280218749653729013331755213885854288889048451782043540152 7 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 83 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 85 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 87 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 89 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 91 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 93 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 95 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 97 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267201 99 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 01 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 03 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 05 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 07 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 09 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 11 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 13 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 15 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 17 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 19 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 21 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 23 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 25 is not suitable
DEBUG:from rsa_tools:Candidate 15456105854443588250960788408891603810240513068780344730662246241237222267202 27 is not suitable

DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672022 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672023 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672023 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672023 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672023 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672023 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672024 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672024 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672024 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672024 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672024 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672025 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672025 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672025 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672025 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672025 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672026 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672026 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672026 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672026 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672026 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672027 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672027 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672027 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672027 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672027 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672028 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672028 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672028 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672028 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672028 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672029 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672029 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672029 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672029 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672029 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672030 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672030 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672030 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672030 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672030 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672031 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672031 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672031 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672031 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672031 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672032 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672032 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672032 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672032 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672032 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672033 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672033 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672033 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672033 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672033 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672034 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672034 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672034 5 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672034 7 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672034 9 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672035 1 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672035 3 is not suitable
DEBUG:from rsa_tools:Candidate 154561058544435882509607884088916038102405130687803447306622462412372222672035 5 is not suitable

Відкритий текст:

13068639714549859410063711922612088288555797766615155063128434112799337018825

Для абонента А:

p=187536433866809833223285245646209601508980257617322329572454888817911610439533

q=45160268789871430237151801756555910438578031403489063192016073968781539843095 1

n=84691957613190796133509812264796286027118281589886027244252008655356419802948216746862360401981786620988295275621784292283782054960430749143171759661185883

oyler_f=84691957613190796133509812264796286027118281589886027244252008655356419802947577607740594877846191817725083506915889531712129841998938133514666032652315400

e=65537

d=60355797188215452849773040905554275278034687911494680904569785987280796907039788396928826216790612766023010287173758648986298186834313525577955613699534473

Для абонента Б:

p=83490765286333438719280218749653729013331755213885854288889048451782043540152 9
q=15456105854443588250960788408891603810240513068780344730662246241237222267203 57
n=12904421061340737709297596102174899681641167269091530874393649211520826780119698281017439285367104037169319293118250499990782633377753107420659470680932258 53
oyler_f=12904421061340737709297596102174899681641167269091530874393649211520826780119674475835056208434981148359035436141538926302192464447593556269573055254311039 68
e=65537
d=12430279035985465170060392516199997589183594740840735043862195112289214852711825838610117389906341836134665121201446677121795445139572052638080434031911769 29

Результат роботи програми:

```
INFO:from rsa_tools:Key data for subscriber A:
    p=191220004509714803408013426273250542454442890569311789721031209183837672238843
    q=341621555280322762999598016677104674754456944424485346727122282509803001173 99
    n=653248753413190967340187079458668727142582442828310267608290485164160136513740925283387290703342248951632741337231463433520492800694997289838466760679293 57
    oyler_f=65324875341319096734018707945866872714258244282831026760829048516416013651374355968677893903280451692193533317271321645476703751974510598554641185809557311 6
    e=65537
    d=463793956029659210985228265059612980056218030498821684724869253622966738666465009418469571874878949658612852667401004263287952728037563743759180883651527 7
INFO:from rsa_tools:Key data for subscriber B:
    p=72344999016180077414369444083330618163558365411930365714588023552943997062799 9
    q=10084297261734902018957322080100287120344788153234144389426950158711953396908049
    n=72954847547907893519094996549786267214615071585682966100133333416288768678471467218595972750905067401598808739354412260154255049157519084481416623387863951
    oyler_f=72954847547907893519094996549786267214615071585682966100133333416288768678469735338879637459929027974949965404460742197684812331061430509230015230020327904
    e=65537
    d=48137486801565238559076932660976357678282489900051703664617936946946877678201728436240859610112930034516015920754834482589200512126111112059803696525274332 9
INFO:root:Chosen value for k:272709009934895552566487229445197588850689449213457412677760489375903595407538
INFO:from rsa_tools:Subscriber A has encrypted k:
    S=60053521961005986961579449692489128247079942857277273781152896083578891061604401885979210404476045858712286875056264213251855942943563708987591562072167150
    k1=36827241611646375525634796268664709479188660727259949977246032778168846492582126551628345766725302767186746556133090485378340809181201850593000220540530571 0
    S1=35988453786738270643723836357196593948068334767776983012815003231779624395305514100988443478481566610911011810789184981939400691692734841134644663319052464 8
INFO:from rsa_tools:Subscriber B has decrypted k1 and S1:
    k=272709009934895552566487229445197588850689449213457412677760489375903595407538
    S=60053521961005986961579449692489128247079942857277273781152896083578891061604401885979210404476045858712286875056264213251855942943563708987591562072167150
    S1=35988453786738270643723836357196593948068334767776983012815003231779624395305514100988443478481566610911011810789184981939400691692734841134644663319052464 8
Successfully sent a key
```

Перевірка на сайті: