Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ

Лабораторна робота №4

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

Виконали:
Студенти 3 курсу
Снігур А.Ю. та
Носова Є. О.

Київ – 2021

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:

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 $pq \leq p1q1$; 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 .

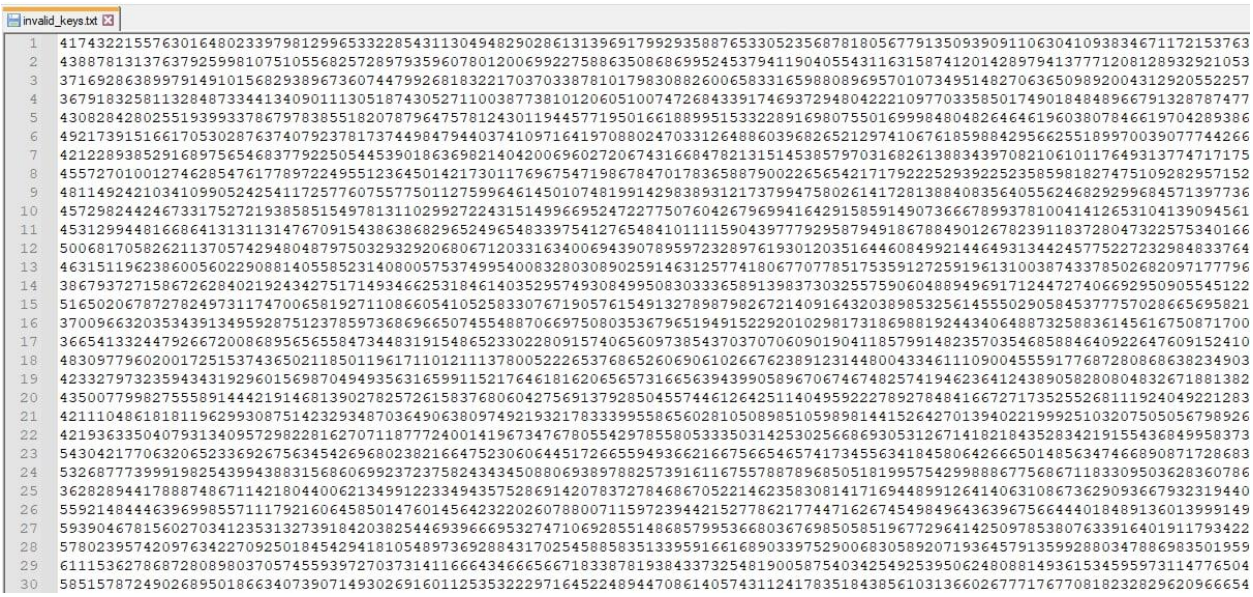
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише 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 $0 < k < n$.

Хід роботи:

Було використано функцію inverse_of_el для знаходження оберненого та нсд gcd = el * v + u * mod. Також написано Імовірнісний тест Міллера-Рабіна (miller_rabin). el_to_power - Схема Горнера швидкого піднесення до степеня. prime_check - Імовірністний тест Ферма. generate_prime - генерація простих чисел вказаної довжини в бітах. generate_keys - генерація ключів вказаної довжини в бітах. to_decrypt - Функція розшифрування. to_encrypt - Функція шифрування. to_sign - Функція цифрового підпису. to_verify - Функція перевірки цифрового підпису. to_send - Функція відправлення (формує повідомлення що буде відправлене). to_receive - Функція отримання (оброблює отримане повіжомлення, розшифровуючи його та перевіряючи його піддліність)

Кандидати, які не підійшли:



Параметри криптосистеми RSA для абонентів A і B:

pA =
252926326014400058761660302219478004948423257593202648336742890499411800858709583225662616479953167175531184956663923704986387749038125893933675616891546 37

qA =
138997786936158183855127061372131344986998381052751930522400164125774983140102013563011555672344919019835707054286233246051230688817162731860860197592989 91

pB =
137397441076542357155048864490081996869888529016023316999795080323667682792259114180059702133462558650969880623588534543968688488972116908142115050708211 43

qB =
148927662832077853518835096116026376535272006312620149035397638072925429742807249169901215522267413289037619951393286551015290560889313904313600381936784 87

A

N =
351561995738948622969312204463510471619898785571468022348677067340269328528776215975352838026906996424799617626920050163193140080405965776904363752953217348594397363550378502993385931957396665709481250731092947762958313467891579445585349533424324049254084166298341922975463019759742794260894557425474517071267

e = 65537

d =
614805687346703414537022929849748007268513966375420755319619126415128366307323223719962597712190226288146912068317239867610140601726165947342861738040621875132545330273904231152966836110936909640298543189421768443384702493085165782364559180784514729033137024879131334856172861933246950436824770669372485683 93

B

N =
20462279778637584145020386636438905713055001327286590019587232213442169672927090904
60084305290706122739043743958015333542954527770648284549650908554077214419609177624
47651294063628514864231424192520617961688071697116187667703248409554229190194705742
15363465335224472591695892907728525137365333579290082385064 1

e = 65537

d =
15570653105278793983736922372998584431848465999233749550281753368087660429816348374
39071124782146182171843561822882107569573558446713001060333716978070870940489750159
60074147493688183676652317819634916670040115019440890415772903639295594602436999347
48053306293042215919460672761921805738817202708911151692685

Чисельні значення ВТ та ШТ та цифровий підпис А та В:

open text Alice wants to send: 23238184

Encrypted text with Bob's public key:
34342800315877574336510295680424784242247219615855724896907947208648724646645382384
44333196853427531922078086276634173491651991092331423904830561988128044788099530930
84901389710915884822273964359244759947045689388059677689115396488604050107767910879
90843939099369350606875189616059791665213944966285230707211 7

The text Bob received after decryption with his private key: 23238184

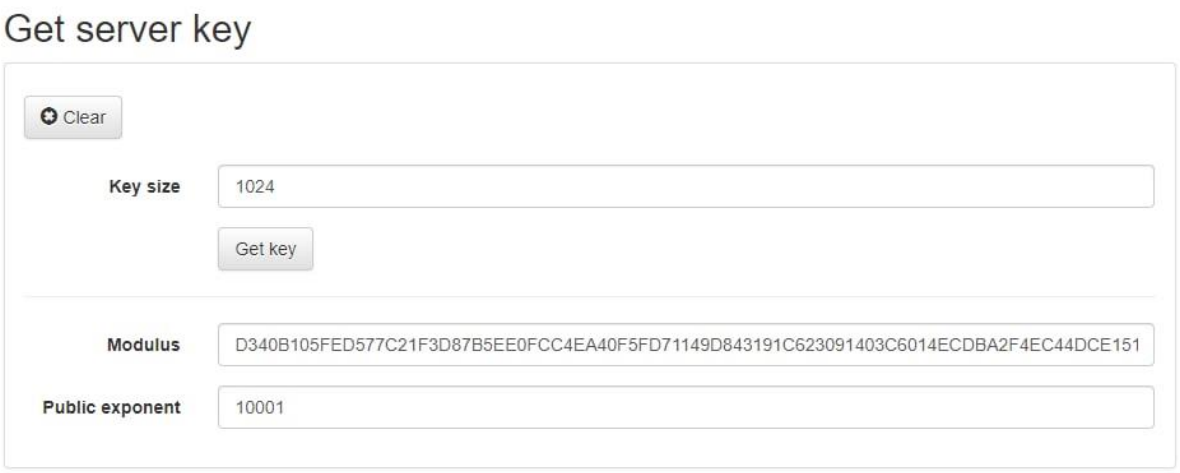
ВТ , що а надсилає б 98375224

ШТ ключем В
83577507772823599894831482758475192704524428589179374473416581757512001992613510402
73741281728237038840816420702871346213904477641711121471647050907312987074121121873
62202870037892785033420024731037941902746544609976949670111071746479061230043539052
75839885224003638357599446787363540266251021763599937705385

ВТ, що отримав В 98375224

signature is:
5fb2f7f8de8ff1095fd2c0431c86d91ba9d9009fb75279adc50dc5ca13fd49b57348e2724239e8118ef6078f
75410a13ac1cb8cc2061406cfc43c033f5d3198c9e5fdb93a54458217e8fde3b85854425463daffd324c0be
2a3490cff2e2711a71d848dbf58358a5658d9e985e939aa8c5fa7341cbd982e056f239ddbf78d295c

Signature is valid



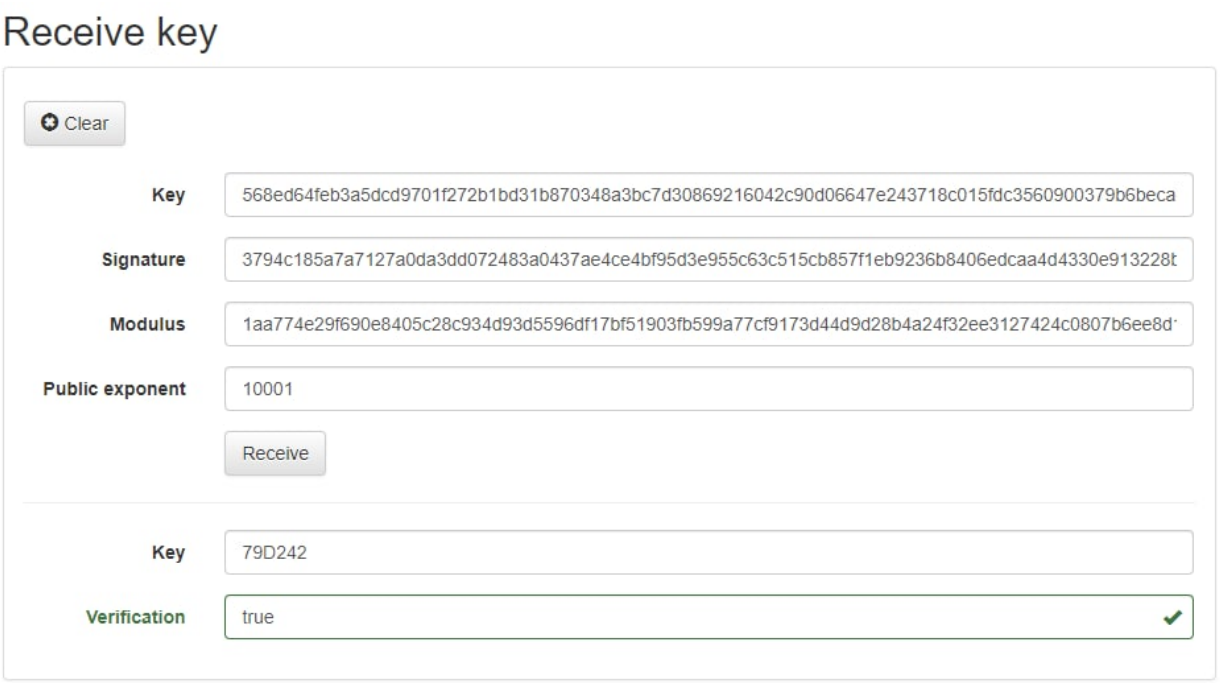
BT A 13888218

key
9fa86040d6340a944fd1afb97a22579f573dec3787c2a355ec9b5ccc354c3e583e7ac65e670bde762f40514
410b40ace981e5ba4f402d9a3737ac82523b2d0c4833bb43170322dfc3b89c2c4fe232c2764546238f4234
38b7e962dc4fd1950d238302759045c4bf79520d06d5d1d6cd2c81d0875b12815828215a92844ce994a

signature
27168dd27bcf9805abfc096442f5a50c8f57b25c6c5df644943c1abdf7c48a3208f737965cd13cb734347167
cf0b82f39fc0de511e92ef8930f4f10f4a39f7c6d7ee57c2de3364825b329ad5f1efe7d7019204d544ca46ac
2ef11c5535002cd789498699e1aabbc0f0424b09f9abbf533d6065fddacbab6c9e690feff6dbe23

modulus
1f4a41206f397eb83165a028dd3486750a029619659a0f14fd67d326347bb12f4b8ca5dcd8bc879f42ee4f3
adff5aa10d759934f346e60244a826fb490e767b443503033fdfe1f967d131999895ceeaba4e923594f8b1c
7b8e135642fd49d2aaeb0709f5ba72a29f09f817cdfd7b5cc185dccda2fbeffc85e0bc2b81c390ff5a3

publicExponent 10001



Висновок:

В ході лабораторної роботи була створена тестова модель криптосистеми RSA, тести на псевдопростість числа, алгоритм Горнера для пошуку великих степенів за модулем. Протестована робота з готовим тестовим середовищем, посилання на яке надане вище. Згенеровані тестові випадки з можливою підміною повідмолення. Покращили навички програмування на мові python, ознайомились з модулем requests та удосконалили навички роботи з сервісом контролю версій.