Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

Лабораторна робота № 4

з предмету «Криптографія»

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

Виконали:
Студенти 3 курсу,
ФТІ, групи ФБ-92
Дорош Анастасія,
Шатковська Діана

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 p1, q1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб p*q<=p1*q1; p і q – прості числа для побудови ключів абонента A, p1 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), (e1,n1) 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

Для виконання даної лабораторної роботи було використано функцію знаходження НСД із ЛР №3.

Щоб зсимулювати реальні умови обміну середовища, основні функції, що були необхідні для правильної роботи алгоритму RSA, були вміщені у окремий клас користувача User. У програмі спочатку створюється користувач-отримувач і публікує свій відкритий ключ, далі створюється користувач-надсилач, що на основі отриманих відкритих ключів генерує власні ключові параметри (перегенеровує параметри p, q доки не буде виконуватись умова nB >= nA) та надсилає шифроване повідомлення.

Найскладнішим у виконанні лабораторної роботи стала реалізація тесту на простоту числа Міллера-Рабіна, адже за методичними вказівками було досить важко реалізувати алгоритм, через це тест набагато частіше, ніж очікувалось, пропускав непрості числа. Згодом це було виправлено.

Результати роботи

Параметри користувача B(отримувач):

p	18607723513730629745273163384511666114026426660516500225581291668795524972405 3
q	14965703006113008827330171803443907138324836237596513836771521138686092448990 3
n	27847766372635820486667835804671404296845884712386822186896909942676216009310657245141144273991408820721938705543946235766953296318743573260229310534736859
phi(n)	27847766372635820486667835804671404296845884712386822186896909942676216009310321510875945837605682787370059149811422723137972166178120045132154494360522904
e	77818321473466252469868902006679922745990371561327944668397710173047196464659285600763260008696278626433053520067351157400341365815324504960926582809400 53

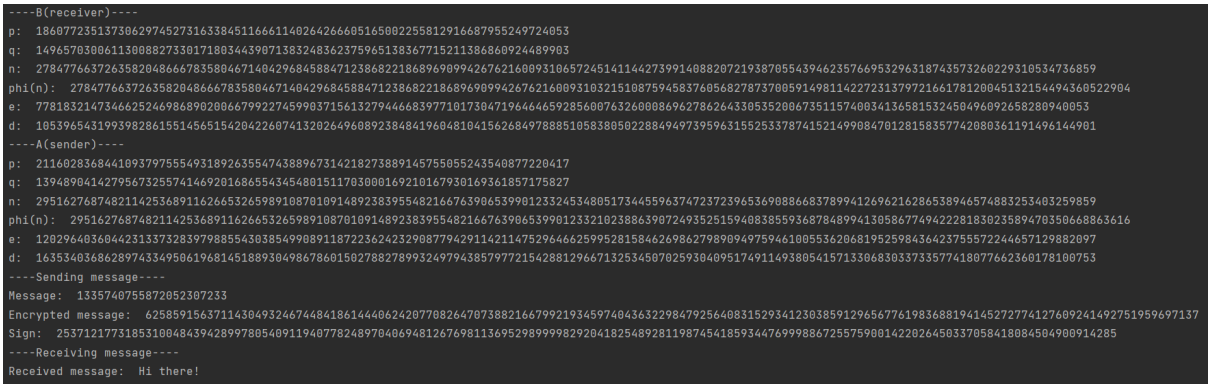
d	10539654319939828615514565154204226074132026496089238484196048104156268497888510583805022884949739596315525337874152149908470128158357742080361191496144901

Параметри користувача A:

p1	21160283684410937975554931892635547438896731421827388914575505524354087722041 7
q1	13948904142795673255741469201686554345480151170300016921016793016936185717582 7
n1	29516276874821142536891162665326598910870109148923839554821667639065399012332453480517344559637472372396536908866837899412696216286538946574883253403259859
phi(n)	29516276874821142536891162665326598910870109148923839554821667639065399012332102388639072493525159408385593687848994130586774942228183023589470350668863616
e1	12029640360442313373283979885543038549908911872236242329087794291142114752964662599528158462698627989094975946100553620681952598436423755572244657129882097
d1	16353403686289743349506196814518893049867860150278827899324979438579772154881296671325345070259304095174911493805415713306830337335774180776623601781007 53

k	Hi there! 133574075587205230723 3
k1	62585915637114304932467448418614440624207708264707388216679921934597404363229847925640831529341230385912965677619836881941452727741276092414927519596971 37
s	25371217731853100484394289978054091194077824897040694812676981136952989999829204182548928119874541859344769998867255759001422026450337058418084504900914285

Результати роботи програми:


----B(receiver)----
p: 18607723513730629745273163384511666114026426660516500225581291668795524972405 3
q: 14965703006113008827330171803443907138324836237596513836771521138686092448990 3
n: 27847766372635820486667835804671404296845884712386822186896909942676216009310657245141144273991408820721938705543946235766953296318743573260229310534736859
phi(n): 27847766372635820486667835804671404296845884712386822186896909942676216009310321510875945837605682787370059149811422723137972166178120045132154494360522904
e: 77818321473466252469868902006679922745990371561327944668397710173047196464659285600763260008696278626433053520067351157400341365815324504960926582809400 53
d: 10539654319939828615514565154204226074132026496089238484196048104156268497888510583805022884949739596315525337874152149908470128158357742080361191496144901
----A(sender)----
p: 21160283684410937975554931892635547438896731421827388914575505524354087722041 7
q: 13948904142795673255741469201686554345480151170300016921016793016936185717582 7
n: 29516276874821142536891162665326598910870109148923839554821667639065399012332453480517344559637472372396536908866837899412696216286538946574883253403259859
phi(n): 29516276874821142536891162665326598910870109148923839554821667639065399012332102388639072493525159408385593687848994130586774942228183023589470350668863616
e: 12029640360442313373283979885543038549908911872236242329087794291142114752964662599528158462698627989094975946100553620681952598436423755572244657129882097
d: 16353403686289743349506196814518893049867860150278827899324979438579772154288129667132534507025930409517491149380541571330683033733577418077662360178100753
----Sending message----
Message: 133574075587205230723 3
Encrypted message: 625859156371143049324674484186144406242077082647073882166799219345974043632298479256408315293412303859129656776198368819414527277412760924149275195969713 7
Sign: 25371217731853100484394289978054091194077824897040694812676981136952989999829204182548928119874541859344769998867255759001422026450337058418084504900914285
----Receiving message----
Received message: Hi there!

```
----B(receiver)----
p:  18607723513730629745273163384511666114026426660516500225581291668795524972405 3
q:  14965703006113008827330171803443907138324836237596513836771521138686092448990 3
n:
27847766372635820486667835804671404296845884712386822186896909942676216009310657245
14114427399140882072193870554394623576695329631874357326022931053473685 9
phi(n):
27847766372635820486667835804671404296845884712386822186896909942676216009310321510
87594583760568278737005914981142272313797216617812004513215449436052290 4
e:
77818321473466252469868902006679922745990371561327944668397710173047196464659285600
76326000869627862643305352006735115740034136581532450496092658280940053
d:
10539654319939828615514565154204226074132026496089238484196048104156268497888510583
80502288494973959631552533787415214990847012815835774208036119149614490 1
----A(sender)----
p:  21160283684410937975554931892635547438896731421827388914575505524354087722041 7
q:  13948904142795673255741469201686554345480151170300016921016793016936185717582 7
n:
29516276874821142536891162665326598910870109148923839554821667639065399012332453480
51734455963747237239653690886683789941269621628653894657488325340325985 9
phi(n):
29516276874821142536891162665326598910870109148923839554821667639065399012332102388
63907249352515940838559368784899413058677494222818302358947035066886361 6
e:
12029640360442313373283979885543038549908911872236242329087794291142114752964662599
52815846269862798909497594610055362068195259843642375557224465712988209 7
d:
16353403686289743349506196814518893049867860150278827899324979438579772154288129667
13253450702593040951749114938054157133068303373357741807766236017810075 3
----Sending message----
Message:  133574075587205230723 3
Encrypted message:
62585915637114304932467448418614440624207708264707388216679921934597404363229847925
64083152934123038591296567761983688194145272774127609241492751959697137
Sign:
25371217731853100484394289978054091194077824897040694812676981136952989999829204182
54892811987454185934476999886725575900142202645033705841808450490091428 5
----Receiving message----
Received message:  Hi there
```

Перевіримо розшифрування повідомлення Одержувачем на [сайті]():

Як бачимо, розшифроване повідомлення повністю збігається з десятковим значенням початкового повідомлення.

Висновки: При виконанні лабораторної роботи ми мали змогу ознайомитись з різними тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; також ознайомились з системою захисту інформації на основі криптосхеми RSA на практиці, організували з використанням цієї системи засекреченого зв'язку й електронного підпису та вивчили принципи протоколу розсилання ключів.