

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

Криптографія

Комп'ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису;
ознайомлення з методами генерації параметрів для асиметричних криптосистем
Варіант 4

Виконали:

Студенти 3 курсу

Загородній Я.М, Венгер П.Ю.

Перевірив:

Київ – 2024

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.

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 $1 < p, q$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1q_1$; p і q – прості числа для побудови ключів абонента А, $1 < p$ і q_1 – абонента В.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , $(,)$ і n_1 e та секретні d і d_1 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів А и В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його.
5. 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 $0 < k < n$.

Значення обраних p , q , p_1 , q_1

$p =$

87354766546536708125860530043437692278267889467788947559195344186410
445075677

$q =$

70969428545336947774909506929314876801436006294207101884960887041625
768736037

$p_1 =$

10984411098880578498951006631167091561482777068110543485602815877225
9005931803

$q_1 =$

61892729654457728640911458076385155627864595372413441094428276424293
828469689

Першій 20 кандидатів, інші наведені у файлі **numbers.csv**

1	63408891643937200933895474848358779299091836376768560987459110975124407513357
2	99708368098518120552957312017875565127702971624507297726877272202626471801341
3	101786679173078856971888809393825739493519466399384448603819202139188222273887
4	78134351701403758860725518850326760405691754749663182526388451678364317367807
5	104424133282166793104507960921383633569653011361464159284445037299253161069606
6	96641480827515436154658747328195396813802826182056305472605017017765445300885
7	93193393562996252850255937668397872191378903108415076684071263572336326749701
8	102619128418221993222405367933810212441220076640947374989165856917760780032767
9	101518029357132939272802557832958275310672745210746281498143208570109061180987
10	84295191710579959250154149624436713396964595342358976989309600997291816190988
11	81687484118635776144023626069248284841332642793046589658723205556956005731938
12	61815243586970841808536943082831040712078218717527554671002183616655186507655
13	66085279817419875732564314874132136227691924913047122330628643734159943251203
14	76504890215561541886499542329515066958425425692537696703977419437811105797034
15	64150663134968659069187938352177893798634807073217787107209273102008759872437
16	70256355202159289717774927722817147833467105227637354101518280760364386663803
17	64517220858358062802240511461461685013087844921594281487848168468912851880073
18	58643866886509744302902644935741451459545311830302077495485871579712700687113
19	66894623383651572644654227454214620128504620552732322450648447218002631285786
20	84588013367593496274327545157405189754987830629514396171296615425680934806993

Параметри криптосистеми

Відкритий ключ абонента А (e, n):

e =

20907174054622808463633333181981798910383088499948024981077088201139
92554166815991248223180605239660836595859803647886917813644932511049
381546178044082813,

n =

61995178625190273187733747302486319922085109721622080535110342850845
24491506992403880606782403101235798360836003248829638941861024033533
928858007102072049

Секретний ключ абонента А (d):

d =

48891120877716255023495235895228380920719419648949208775016071866032
44277738250851130575327851156599636655708093523640390892520709411720
88899893629721573

Відкритий ключ абонента В (e1, n1):

e1 =

53780177359862578942596973866748407386188790075515317536259997984647
39705565118294898983107754484584287912401659757811261974254651471549
589671867361653143

n1 =

67985518655644058663020311894313361979416636662388158267993563738178
31999870609882263345537738868882378356835100680207512408073103494561
490962048986619267

Секретний ключ абонента В (d1):

d1 =

67136083186453849552091519554026687965037639796845058093116319246052
48433117596407348231940792013274447013441547322663686836227226064566
10292781444058295

Результати роботи:

Випадкове повідомлення k:

42121299226924778714090655171710694660724566712666600376181423827871
02334281078445984522432429084893263603942244071447884411535319882687
025260369042191534

Зашифроване повідомлення:

85012468792994528502695227771188184501352566361029096860973368203674
12799411527585880700304670499001462379768661681087941082454253478836
72677966955802585

Зашифроване підписане повідомлення:

47282419843217438135184438250332960233453063954691505060519262133179
55263080253654757594468919308020728077233091204915339000753572108304
69730252111233477

Перевірка підпису успішна

Отриманий ключ:

42121299226924778714090655171710694660724566712666600376181423827871
02334281078445984522432429084893263603942244071447884411535319882687
025260369042191534

Кроки конфіденційного розсилання ключів з підтвердженням справжності:

1. Абонент А (відправник) шифрує відкрите повідомлення (k) відкритим ключем абонента В $\Rightarrow k1$.
2. Абонент А (відправник) підписує відкрите повідомлення (k) своїм приватним ключем $\Rightarrow s$.
3. Абонент А (відправник) шифрує підписане повідомлення (s) відкритим ключем абонента В $\Rightarrow s1$.
4. Абонент А (відправник) передає k1 та s1 абоненту В (отримувач).
5. Абонент В (отримувач) розшифровує k1 і отримує відкритий текст.
6. Абонент В (отримувач) розшифровує s1 і отримує підписаний текст.
7. Абонент В (отримувач) перевіряє підпис відкритим ключем абонента А (відправник).

Висновки

Ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практично ознайомилися з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.