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 5

Виконали:

Студенти груп ФБ-01 та ФБ-03

Маковська М. В.

Ващенок Д. О.

Перевірив:

Чорний О. М.

Київ – 2022

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 роботи

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 А, 1 p і q1 – 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) , (,) 1 n1 e та секретні d і d1

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 М і знайти криптограму для абонентів А и В, перевірити правильність розшифрування. Скласти для А і В 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

Обрані числа:

p	204901066145616790514004106998368362225858044793392992932266945703983824399231
q	475082654572977601398337425500715893335301346496660089680978710628964109092793
p1	950075130747087145724280024757783903589003705789106214814659724171947301949323
q1	961041902946252604261396586347033381793219428283214806965755047060359634028493

Кандидати, які не пройшли перевірку простоти (в таблиці наведено лише 20 кандидатів, всі інші знаходяться в файлику new.txt):

№	Число
1	73453770711712884183237724545411805131917937767496824672627089687785193367189 3
2	66794316436966271507167435255717180218934903884454291015368097395972476607563 9
3	32324240190500017661935672228969531592830615713121271240720320599889562225378 3
4	51076880528539517933441105223424851064403143907234248321973272659485272239316 9
5	96064148219948906383255850327812504331795196515724595630516619877293676632144 5
6	21465162582910055625372521063775576272422013555342075569438057232367975349671 3
7	47979745091091300155088499876237606248973928966086652514318244013063484873064 5
8	16753344103375306903784064914112732681694629710755475391406945491041074013125 3
9	81538006879085687960755113182000119872318184306375236696074626661418135333072 7
10	34575007140206692592801755438891960002036956762193612024791961048097228956070 9
11	46916776271206244037830587601045154938411529751541890294918785841837150653266 9
12	29953378984974979203630346311446932111692966515210568342666977744365512161834 5
13	58459099170000233826573635642122889755863875850985293441684883100783831475336 9
14	55368575208266915487162096719430268010592241793223303067037579566104194369797 5
15	83491340900017870807179859697857064173997630264959947625236607854850250505936 3
16	74142786527615166195393647565985895674801254572424504457590915417147104355680 3
17	76807162189439486015593134507363800844239840145413440331199015657675204924307 1
18	10462329562006808938358846266749103557162549040804918997778080491478956511626 1
19	25599528808343677084629168363142732611325956028518598279830707365505794175375 1
20	69561278839933155251075447116546258310277192508905114286443266088162975480237 7

Маємо наступні параметри криптосистеми RSA:
-Перший набір:

n	97344942429292896708432683784515333078537407546561739218560401448468381982691693718926286211948711507764538976708390043747279439835261928394557217656842183
e	69542412498258837415532782246404634337180862035691600727250919886554844328753341335710209992668871537977445869246893042971437261499307546354073953345459277

d	69435979944044534922039975851219677728897078242276375359869841861230808170850162182662661902135081426869688481440134205761163931599958927103442072505571013

ВТ:
55853877372247607935678112557338729809978440155745030452287075773330625369217768964517701384207319774256827184089528075173602320573668678454296501100602432

ШТ:
42583673414514619088305703782047023663816806166239778243132719954868467461701354544604280496834185322730576339706414855704608732187406532295596946184060153

Розшифрований текст:
55853877372247607935678112557338729809978440155745030452287075773330625369217768964517701384207319774256827184089528075173602320573668678454296501100602432

Цифровий підпис:
84036223822904153795257918739008260426128319190150052078288066185025838264813799198130190591554508904309121717991302488978201659385641021572504932429233282

- Другий набір:

n1	913062011595090378200031315580855166380006291636312553195535779963570904443672392672470746224801209109696975034179253920118180116203417216960917302224060239
e1	737265546911271285660113872947002231710956724204656284344452187907178373633215344387855152927909486454292739989373846833575011539855441169668841259402080 43
d1	702420454858164938280499556266615520021866555544465145974540653840375767348815401494282536752317306991622796770669000618767972084025231445229585788720908059

ВТ:
86952378368108420624758415100048835919256315456688789313295449733923695113305183018951184676925662524975080387028377477779929819139317969370158430611991859 6

ШТ:
17091586924277614222935652187738543695276412079654090622838583817921094097788321856917392768057624811181924149600254960635444019326272656832953496700439101 5

Розшифрований текст:
86952378368108420624758415100048835919256315456688789313295449733923695113305183018951184676925662524975080387028377477779929819139317969370158430611991859 6

Цифровий підпис:
27523902420765100982048052595711949148006302530780494062566485772384456 9

40491712357923982629728366782059419654564117442939322725536072968117727824997153508 7

Абонент А формує повідомлення:
Число k зашифровується за допомогою відкритого ключа отримувача та зберігається в змінній k1. Змінна k підписується за допомогою секретного ключа та модуля відправника й потім підписується s за допомогою відкритого ключа отримувача та зберігається в змінній s1

k1	52001063392354104799845159449700231053684355333886180899555776532698743515135780449799401040672535698625221397772149501796574922507973635009605581628628402 31
s1	54920977363069764979591671856862622544405855718403171231890943797580165973223279823618694601662112969125877823673233648463390505287390159413061028512177352 8

Абонент В за допомогою свого секретного ключа d1 знаходить наступні значення:

k	20769882764365311766744216593186697187478312716927826972055835337021144706132374377066973255507864346755834221515754582114952671772503843953842368995618021
s	31045917921584200782726491709202573249811765349824397351071545408869043805720986334606096660883141170634550159676977186662795140179896411701255081652463 70

Абонент В за допомогою відкритого ключа (e, n) абонента А перевіряє підпис А.

Висновки:
У ході виконання даної лабораторної роботи, ми зрозуміли, як працює криптосистема типу RSA, навчились організовувати засекречений зв’язок і генерувати цифровий підпис з використанням цієї системи. Ми також ознайомились з рядом сучасних методів, що використовуються для тестування великих чисел на простоту і навчились використовувати її на практиці