МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТИХНІЧНИЙ ІНСТИТУТ ІМ.ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Комп’ютерний практикум №4

Виконали:

Студенти 3 курсу

ФБ-01 Літвінчук Софія
та
ФБ-02 Косарик Дарія

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

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 pq p1q1 ; 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:

1. Згенеруємо числа p і q для абонента А:
   p -
   6380537861674221456376428616314594362813577299179518510811523627247224836621 9
   q -
   8067481122499439842494274540729045221178232833398759694578505032331726465795 1

   Згенеруємо числа p1 і q1:
   p1 -
   9142678007996601162989392096337198564494253173379234764071451153993593706826 9
   q1 -
   9424134280511798177822084255256711737840308690597187636950099497899129304703 9

   Кандидати, що не пройшли тест перевірки простоти, містяться у файлі 1.txt

2. Отримані ключі абонента А:
   Секретний -
   [3009538783446129186307216064893140715286249416150144324802951558430214611978057995103879426684453669185869384878133296056036905615221362412478818893083319,
   5147486875044972373802751282872753471255155417180910322272375381992148091004779077669943841504115792086008006540961403356386689579668904353785389618157269]
   Відкритий -
   [3931848308325093231185758246076013907086920801832150477975517941414799448904441978026747469265327590679972330003605850283449507874842632403175146256951579,

5147486875044972373802751282872753471255155417180910322272375381992148091004779077669943841504115792086008006540961403356386689579668904353785389618157269]

Отримані ключі абонента B:
Секретний -
[7708665136750411559593022994358048157092578225976102747700446906122574668950471346260118756288766372850876381347307574835315452782565893322900797455043555,
8616182523084208908852290087012230884561611593135601427238477931040839279962205125086232340776442534430103068016112948436862782707715435344344125571305491]
Відкритий -
[8196157996450647620076320382292440246204322841442415571747372949543059194543074593745092318207982269032998720056369323320863022038510849026106867822755715,
8616182523084208908852290087012230884561611593135601427238477931040839279962205125086232340776442534430103068016112948436862782707715435344344125571305491]

3. BT:
47198388636372236774343648978842520873153039551582180391073775101367928145193

ШТ абонентом A:
84356253438324893800662132920127414096385211191934917807465751550071906448779383260137242495486793581672985312112446962218493021598154707408489550493910 7

Розшифрування абонентом A:
47198388636372236774343648978842520873153039551582180391073775101367928145193

ШТ абонентом B:
30135541982456428972672859235603648437441763348917089594277128081659316354975225144489183241076899423676273707530888089132580310203867206200198040029749 63

Розшифрування абонентом B:

47198388636372236774343648978842520873153039551582180391073775101367928145193

Цифровий підпис:
18567343391307511361433762895159293507063690108770950041302364826945594477114719493937208280372807061063187707318181714630083644165752436701937818244634 80

Верифікація:
--Перевірка цифрового підпису : True

4. Протокол конфіденційного розсилання ключів(між абонентами A і B):

Згенерований ключ:

33921435922622224165037734792437621104828341405377290747645695525986649496563
Повідомлення зашифроване відкритим ключем B:

50666371189756447647009917930752928863058892694276146084316218002336368638917261272217992269375851224718057930562617599953915696980102001864304894451930 62
Підпис повідомлення секретним ключем A:

15030551942398671528097764112196507161728528443292648663319875611356745665764535854868832865236437851769064233743667752403828166474135693213660964633400 36
Отриманий розшифрований ключ:

33921435922622224165037734792437621104828341405377290747645695525986649496563

5. Перевірка:

Згенеруємо ключ сервера:

Modulus	A808A1372A745403E590C5D212ABDE6F4A6C3FB512882CD02C5C1D2C514F12B3
Public exponent	10001

Згенеруємо повідомлення:

519411252740292079700654425448215883724876613152387945897898733
30165149763129

Надсилаємо зашифроване повідомлення:
414536497420572292011253863219856656319490010152879476999944451
67449878673953

Із цифровим підписом:
382073759404756841372819253130448270477259465978246948352468
99594966689281257

Отримаємо на сервері:
72D5A295668A742EE2303B52670C1F1CB507B51B45D31C0198A6544060
B68639

Переведемо в десяткову систему:
519411252740292079700654425448215883724876613152387945897898733
30165149763129

Висновок:

У результаті виконання лабораторної роботи, ми ознайомилися з тестами перевірки чисел на простоту: тестом пробних ділень та тестом Міллера-Рабіна; методами генерації ключів для асиметричної криптосистеми типу RSA; вдалося описати даний алгоритм шифрування, показати його роботу: генерацію ключів, шифрування, розшифрування, створення цифрового підпису.