МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

Виконав:
ФБ-14 Фролов Павло

Перевірила:
Селюх П. В.

Київ 2023

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 чиселqp, i11 , qp довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб11qppq ; p і q – прості числа для побудови ключів абонента A,1p i1q – абонента B.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ),,(qpd та відкритий ключ),(en . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі
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 .

Хід роботи:

Використовував частину коду з минулих лабораторних робіт.

1. Згенерував публічний та приватний ключ для A.

```
--A--
n: 27761347864806682811465329087451049685035542831193258222849639099099082695863334721397856635309525338602094241248815086019611888856603165048462267241566 3
e: 65537
p: 36841388640373183906236061898299317173401378507317555837845981598555237521989
q: 75353695637802307732423588305155061670811923996867786289074464522156523341667
d: 11267709129253059535605501529307077248301653101450183388434020477532654225381671826090609945056188930432083430992405624156523098758759228838073154133891 3
```

2.Згенерував публічний та приватний ключ для B.

```
--B--
n: 11698778954544181451994050298239287433016064815673795396209604920478572970427443397298181854163863881985423382775654311832398786067876015485693292483583731
e: 65537
p: 10669628855000828932967971070163939069011130117268588304570512371615875894809 9
q: 10964560354937737488375174275275667886715055400375557400123695991628455314516 9
d: 67473663076249372828161665505462078776961751982491385351988473135659181791839534227580528743582752854060743660604507742510189267733452575724323365096536 1
```

3. Перевірив роботу алгоритма зашифрувавши і розшифрувавши дані за допомогою пар ключів A та B.

```
Тестування A
Дані: 97242929324436297705351337535236967238720934368713101569760050509924679381625177918923291229541446442598322978807018202199527772133333890046627843264884653
Зашифровані дані: 96777124479965147452900717962556527988163106405117936985743579943662143364828855403585436379419624636571188900161311909588334269502890473722890470146794 7
Розшифровані зашифровані дані: 97242929324436297705351337535236967238720934368713101569760050509924679381625177918923291229541446442598322978807018202199527772133333890046627843264884653
Успішна перевірка для A


Тестування B
Дані: 45255976509725265440058236150803987370566901853571075941308190441568293121792335012478179408832203473480791454778673076828795744460077086818030417854627 8
Зашифровані дані: 11581926218993964256137475970101868024113956255115878645126857568676705122707997316121630552124596395078298934221305925024638258886834738014584627710214313
Розшифровані зашифровані дані: 45255976509725265440058236150803987370566901853571075941308190441568293121792335012478179400832203473480791454778673076828795744460077086818030417854627 8
Успішна перевірка для B
```

Висновки:

Виконавши комп’ютерний практикум я отримав практичні навички роботи з RSA та розуміння роботи асиметричних криптосистем.