МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
Фізико-технічний інститут

Криптографія
Комп’ютерний практикум №4

Виконали:

студенти групи ФБ-01

Чуйко О. М.

Ченський К. Ю.

Київ - 2022

ФБ-01 Чуйко Олександр, ФБ-01 Ченський Костянтин

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 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.

Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().

ФБ-01 Чуйко Олександр, ФБ-01 Ченський Костянтин

Хід роботи:

```
[***]Alice keys:

p:
623396481689780937172562405879601076883452651651541474163577614830
66701266157

q:
996240596897195690068531227810714538383894956315976829073032355592
61848518431

n:
621052883022239084534189626259151769756742026634198549213590438821
718296218648397836949969846639403760167634920298535652373894300971
681869765668225103966 7

e:
118242171991308038205373897340460337251599729191657201542528658923
188887720667824733993166363127962956434321515768373633216649542139
638776065960465978681 3

d:
501621311374069604030629410171795540482377503692853088339299575855
003772545306888430667559855881661486500900489495495266706013532153
025586848756164886363 7

========================================

[***]Bob keys:

p:
814577363083407604022785567183615057664123167776331999431573765732
62353868911

q:
115390996413526494717291259841442380330858169411793881818895367016
326231991221

n:
939948935820973561340986323606425457519159270430957370932605755592
269876815217557860932710249411021824399838984218234673563587250221
081253026836873683033 1
```

ФБ-01 Чуйко Олександр, ФБ-01 Ченський Костянтин

e:
393962554437393424722314553067835451613847715957119532316720852552
556465193218104266628903381513548634999849369146264687628428753151
1271734380072387511009

d:
283673534312267463947715387113402545331869355743637408357266560562
807610694537157750804158667035216760916012885135741387394339816690
7752206363594041545689

==========

[***]

Message:

3178915031257831918729774999887252000191491965881258737313293444212
8869042079256256491299672515590627107232242506596148578289166042951
2572717118200088545426

Random 0<k<n:

3753807742638764320393701354935220277185065192065362357317573172283
6908396446236207583859949406667330179263718588355680574005278766470
2048471216769874631 8

==========

[***]Result:

CypherText:
2708879375305616227394880454544183683705942421705115781948722890115
4814728923264376353551434148860839961920921685660982488224267775315
2547118989470983143 88

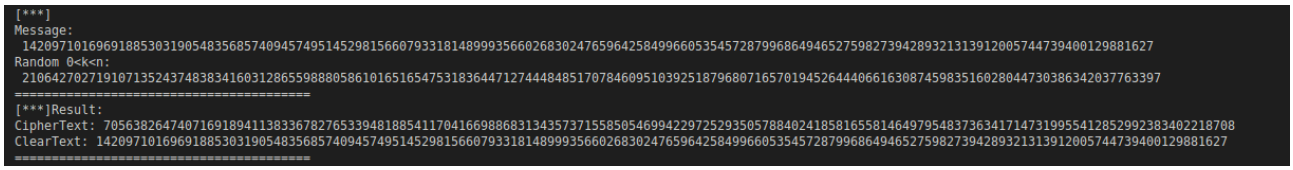
ClearText:
3178915031257831918729774999887252000191491965881258737313293444212
8869042079256256491299672515590627107232242506596148578289166042951
2572717118200088545426

==========

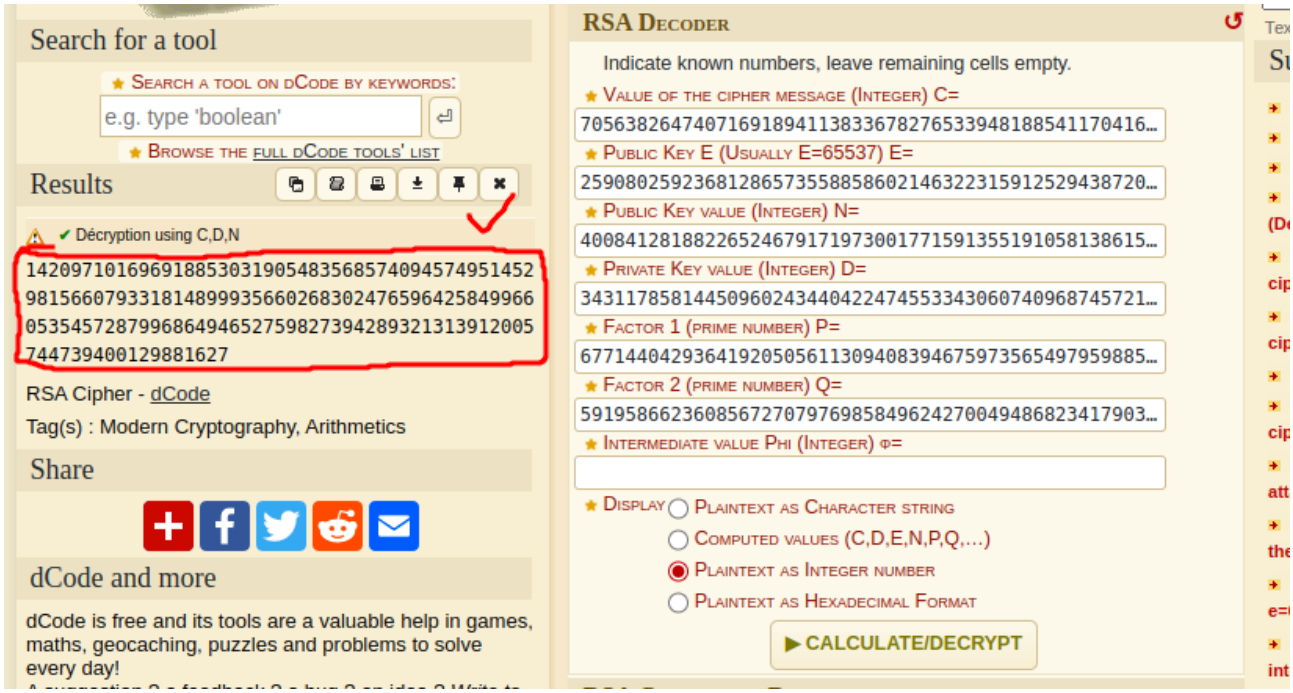
ФБ-01 Чуйко Олександр, ФБ-01 Ченський Костянтин

```
[***]Cheks:

Message: True

Key: True
```

Перевірка шляхом взаємодії із онлайн засобами RSA:



Згенеруємо повідомлення, після чого за допомогою декодеру на сайті перевіримо чи співпаде ВТ:



Як бачимо, ВТ Співпало.

ФБ-01 Чуйко Олександр, ФБ-01 Ченський Костянтин

Висновки:

Виконавши цю лабораторну роботу, ми ознайомились з тестами перевірки чисел на простосу і методами генерації ключів для асиметричної криптосистеми RSA.

Виконали практичне завдання де ознайомились з системою захисту інформації на основі RSA та організували засекречений зв’язок й електронний підпис, використавши цю систему.