

Лабораторна робота №4 з предмету «Криптографія»

« Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для симетричних криптосистем»

Варіант 12

Виконав студент 3 курсу

Кравець Андрій ФБ-02

### Мета та основні завдання 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 і рекомендації щодо 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 A, 1 p 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), (a, n) 1 n1 e та секретні d i 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 М 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().

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою http://asymcryptwebservice.appspot.com/?section=rsa. Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

# Хід роботи:

```
gen_rsa_pair - генерує пару відкритий та закритий ключ
encrypt — зашифровує повідомлення
decrypt — розшифровує повідомленя
signature — обчислює сигнатуру
check — робить перевірку
send_key — шифрує ключ, сигнатуру та надсилає
receive_key — отримує ключ, сигнатуру та робить їх перевірку
```

В ході виконання лабораторної роботи, було реалізовано відповідні функції:

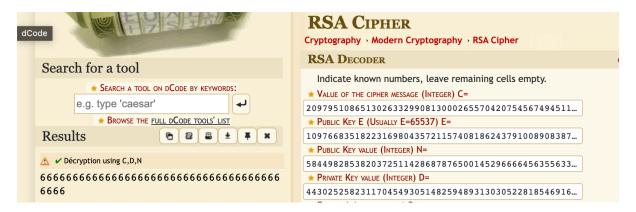
### Результат:

```
alice:
         e -> 14475164069437536031085751877395501270367192272245626706962996901584873362364864765492218945166370196783
58865470004814075554373712989116225993378778783871
- n -> 58449828538203725114286878765001452966664563556330826867356139294500137892465638711040207363999299060062
07743874523784870094980238052179034399614879052163
        - p -> 87518183459210037996308930770285421192658443873814762833818905505099695528221
          q -> 66785925196271559527580446236991049937529980299482140427354433283639996617503
-\stackrel{d}{d} \to 4430252582311704549305148259489313030522818546916860727893355285987871723283597029643443442996392318669561137247771641239018545052513032932029989037092951
bob:
    pubkey
          58852475171943547850636686787077924728420085916519

- n -> 72111336832959058311267860497161378651386398407409346648470741993207556399685411222269630176096310858761
53407804334357121956600896011321177129196889452359
        \begin{array}{lll} -p & -> 70955350604827561971051999876545147437307576838655598073659156062975857316067 \\ -q & -> 101629174147231747944660131154444579165804818853426612427404130308659674425677 \\ \end{array}
        - d -> 10561654952307710674438137385678288086494985004266426125861848856083822863811477878631049983477380987638
21585987264824513235304827555220776629485030567303
-> 5319499258076295894422844999514122494181762276475135666462788108434018230729127781677958001
545740855072746072820973851279501599476090130528087284631059601

Encrypted signature -> 3430401707297386707021410865649833485922006618052113181288778250065292851619931247758622091
316771423373635904753341583455150191519410109827195449237608256
                            2097951086513026332990813000265570420754567494511036449518976949522209507488070298738868556
4758430106945217745929521257372395870133881396272298905512020
   -> 568648587856422167305920517877704232398042067266129695385034665304358681089768946327990521546417
8708786252746565454045002288409562832538545080371305226916
```

Зробимо перевірку на online ресурсі:



Перевірка пройшла успішно.

### Висновок:

В ході виконання лабораторної роботи було здійснено ознайомлення з тестами перевірки чисел на простоту та методами генерації ключів для асиметричної криптосистеми типу RSA. Вивчено протокол розсилання ключів для асиметричної криптосистеми RSA.