

Національний технічний університет України
«Київський політехнічний інститут»
Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №4

Вивчення крипtosистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних крипtosистем

Виконали:

студенти групи ФБ-32

Грабовецький Микита

Драбок Алла

Київ - 2025

Мета роботи:

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної крипtosистеми 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 p_1, q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1q_1$; p і q – прості числа для побудови ключів абонента А, p_1 і q_1 – 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) , (e_1, n_1) та секретні d і d_1 .
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 M 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 $0 < k < n$.

Варіант: 13

Хід роботи:

1. Генерація простих чисел:

Для генерації простих чисел p та q використовувався імовірнісний підхід. Спочатку генерувалося випадкове непарне число заданої довжини біт. Першим етапом число проходило тест пробних ділень на малі прості числа (3, 5, 7...). Якщо число проходило цей етап, до нього застосовувався тест Міллера-Рабіна з кількістю раундів $k=40$, що забезпечує імовірність помилки не більше 4^{-40} .

2. Реалізація RSA:

- Генерація ключів: $n = p * q$, функція Ойлера $\phi(n) = (p-1)(q-1)$. Випадкове число $e=2^{16}+1$ (зазвичай обирається). Секретний ключ - для e обернений за $\text{mod}\phi(n)$ елемент d : $ed \equiv 1 \pmod{\phi(n)}$ $\Rightarrow d = e^{-1} \pmod{\phi(n)}$.
- Шифрування/Розшифрування: $C = M^e \pmod{n}$, $M = C^d \pmod{n}$.

3. Цифровий підпис:

$S = M^d \pmod{n}$, перевірка $M = S^e \pmod{n}$.

4. Протокол конфіденційного розсилання ключів:

Схема передачі секретного ключа k від користувача А до В:

- Перед початком перевіряється умова $n_B \geq n_A$. Це необхідно, щоб при операціях за модулем n_B не відбулася втрата інформації, якщо значення зашифрованого повідомлення або підпису перевищуватиме n_B .
- Крок відправлення (A):
 1. Абонент А підписує ключ k своїм секретним ключем: $S = k^d \pmod{n_A}$
 2. Абонент А шифрує ключ k відкритим ключем В: $k_1 = k^{e_B} \pmod{n_B}$.
 3. Абонент А шифрує свій підпис S відкритим ключем В: $S_1 = S^{e_B} \pmod{n_B}$ (забезпечення конфіденційності підпису).
 4. Відправляється пакет (k_1, S_1) .
- Крок отримання (B):
 1. Абонент В розшифровує k_1 своїм секретним ключем: $k = k_1^d \pmod{n_B}$.
 2. Абонент В розшифровує S_1 своїм секретним ключем: $S = S_1^d \pmod{n_B}$.
 3. Абонент В перевіряє автентичність ключа k , використовуючи відкритий ключ А: $k = S^{e_A} \pmod{n_A}$.

```
C:\Users\grabm\PycharmProjects\pythonProject\Lab4\main.py
[1] Генерація ключів для обмінів A і B...
    A Public Key (n, e): (962786647313715152652577057202648156112747154483538238349567614388958168248006215949913113985222663158252463596133288208664063156587855479643845127799, 65537)
    (Перегенерація ключів B для виконання умов n_B >= n_A)...
    (Перегенерація ключів B для виконання умов n_B >= n_A)...
    B Public Key (n1, e1): (102467811040494152348032803101567200299062810098002755301762309191740824053569526613547895179583551366310038841418481243204728313848394116261740969998249, 65537)

[2] Тест шифрування/розшифрування (Confidentiality)
Відкрите повідомлення: 123456789
Зшифроване (С): 30790238704284611876246624685322542310752967491313728291713008977688041769307610436304320123759687545463551372800207459402171330381307108868751098701131078
Розшифроване (М): 123456789
>>> Статус: Успішно

[3] Тест шифрового підпису (Integrity & Authentication)
Повідомлення для підписання: 987654321
Підпис A (S): 35760238476223018291534393846073256968263552062383539431391337715999109431711003952100612161142199107789374199393727469174533399285635581526808756571
Результат перевірки підпису: True
>>> Статус: Підпис вірний

[4] Протокол конфіденційного розслання ключів (A -> B)
Секретний ключ K, що передається: 8935017086023186420534522038864662070009962484426756245544926359113617341805513631409727756969467604877636802069111360420199923767995288679505456998
Відправлено пакет (K1, S1): (8046821161094770988952147873b9154902752822089711362257253184846958671688231110954753b88569018382489175882346259916995150899046523338874312087293478297, 56985344202044647330125339
Отримано K: 89350170860231864205345220388646042078009962484426756245544926350113617341805513631409727756949467604877636802069111360420199923767995288679505456998
Аутентифікація підтвердженна: True
>>> Висновок: Протокол виконано успішно.
```

Перевірка роботи алгоритму

Перевірка відбувається за допомогою згенерованих ключів у скрипті та за допомогою сайту asymcryptwebservice.appspot.com

```
>>> Генеруємо пару ключів...

[1] ШИФРУВАННЯ НА САЙТІ
Modulus (n): 5502d819f82b8c82721d3c25ca6a949c2f4b4697cf833de50dee688e
Public Exponent (e): 10001
```

Encryption

The form has the following fields:

- Modulus:** 5502d819f82b8c82721d3c25ca6a949c2f4b4697cf833de50dee688e
- Public exponent:** 10001
- Message:** Hello World
- Ciphertext:** 3479155A0D633E29F6B02106EF5FEE866AF8B025BD0B8F0DD4

```
Ciphertext з сайту (HEX) >>> 3479155A0D633E29F6B02106EF5FEE866AF8B025BD0B8F0DD4770D81428C94720888C168B659B7676951369F8D496D32563A212AE9BBEF5720279AF43FF027AE
Розшифровано (число): 8752161808882533792115812
Розшифровано (текст): Hello World
```

Публічний ключ «передається» сайту, де ми шифруємо повідомлення Hello World за його допомогою. Отриманий шифротекст вставляється у код й розшифровується за допомогою приватного ключа.

```
[2] ПЕРЕВІРКИ ПІДПИСУ
Message (Text): Hello World
Signature: 2ff8c1ef5dbb7cabacd63bf1e64107f4227a063bb51f279a4efe0e1a36cf24c72fb00f2e0fe110d426495b059f2b51062298d518e7e77cf0d80b8e2d5fad494d
Modulus: 5502d819f82b8c82721d3c25ca6a949c2f4b4697cf833de50dee688862af12e889f986fc5d0be3ebc40cc6611a1baff98c332f49963ba0fb8e17547d5267e823
Public Exponent: 10001
```

Verify

The screenshot shows a form for verifying a digital signature. The fields are as follows:

- Message:** Hello World (Text type)
- Signature:** 2ff8c1ef5dbb7cabacd63bf1e64107f4227a063bb51f279a4efe0e1a36cf24c72fb00f2e0fe110d426495b059f2b51062298d518e7e77cf0d80b8e2d5fad494d
- Modulus:** 5502d819f82b8c82721d3c25ca6a949c2f4b4697cf833de50dee688862af12e889f986fc5d0be3ebc40cc6611a1baff98c332f49963ba0fb8e17547d5267e823
- Public exponent:** 10001

Below the form, a status message says "Verification: true" with a green checkmark.

Для перевірки підпису, код проводить математичне перетворення повідомлення за допомогою приватного ключа й разом з публічним ключем передається на сайт.

Зі скріншоту можна зробити висновок, що підпис дійсний й код успішно пройшов тестування.

Висновки:

Було реалізовано криптосистему RSA з повним набором необхідних процедур: генерація ключових пар, шифрування та розшифрування повідомлень, створення і перевірка цифрового підпису, а також протокол конфіденційної передачі ключів між абонентами.

На тестових повідомленнях програма коректно виконала всі операції: повідомлення 123456789 після шифрування та розшифрування співпадає з оригіналом, а підпис для 987654321 успішно підтверджено відкритим ключем.

Протокол передачі секретного значення k також виконано успішно – отриманий ключ співпав із відправленим, а автентичність підтверджено.