Міністерство освіти і науки України

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота №4

Виконав студент групи ФБ-13

Нійозов Рустам

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

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 i 1 1 p, q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq p1q1; p i q прості числа для побудови ключів абонента A, 1 p i 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), (,) 1 n1 е 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 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 п. 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 Епстурт(), 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:

- 1. Із тестом Міллера-Рабіна проблем багато не виникло. Для перевірки чи правильно зробилено тест, було використано сайт: https://planetcalc.ru/8995/
- 2. Згенерував числа, так, щоб pq <= p1q1:
- $\begin{array}{l} p = & 114893576615012767532631617462266153531956267357783648861491082899568397195091 \\ q = & 58900183899818136254803171219179457679020479081697934423863264607746985268011 \\ p1 = & 112988788668750763609699926596140978736789755768783595000344553991545243073851 \\ q1 = & 113329302157219497734891659533221069041902924052190802623646108652814389334531. \end{array}$



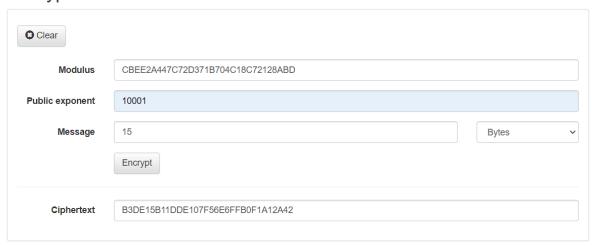
перевірка на сайті:

Get server key

| • Clear | |
|-----------------|-----------------------------------|
| Key size | 128 |
| | Get key |
| Modulus | ODEFOA 447070D074D704040070400ADD |
| Modulus | CBEE2A447C72D371B704C18C72128ABD |
| Public exponent | 10001 |
| | |

Створено ключі для Абонента

Encryption



Зашифровано повідомлення 21, що у 16-ковому представленні буде 15 За допомогою коду отримано наступне:

```
n = 271069907083902572793476553998716799677

# CBEE2A447C72D371B704C18C72128ABD (у 16-ковій)

e = int('10001', 16)

some_message = 21 #(15 у 16-ковій)

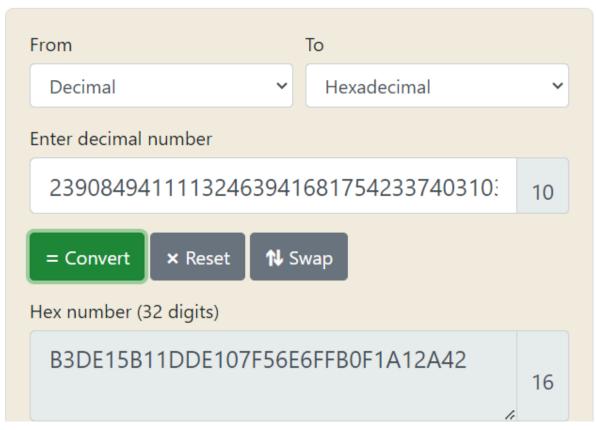
A = SubscriberKey('A', e, n, d=None)

print(A.encrypt(21))

# 239084941111324639416817542337403103810
```

239084941111324639416817542337403103810

Decimal to Hexadecimal converter

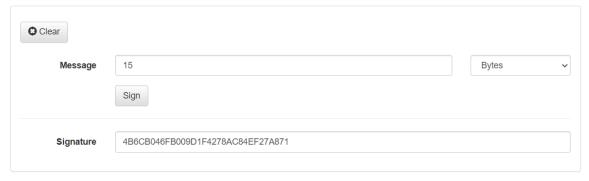


Як видно, це те саме число, що й на сайті

Decryption



Sign



Verify



signed_message = int('4B6CB046FB009D1F4278AC84EF27A871', 16)
print(A.verify(some_message, signed_message))

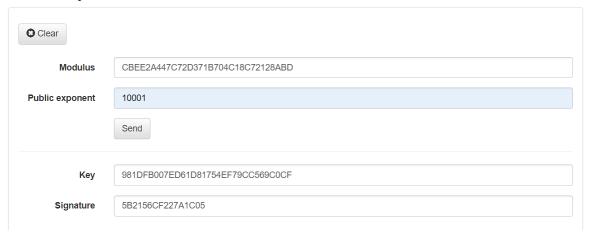
Вивід:

259064941111524059410617542557405105610

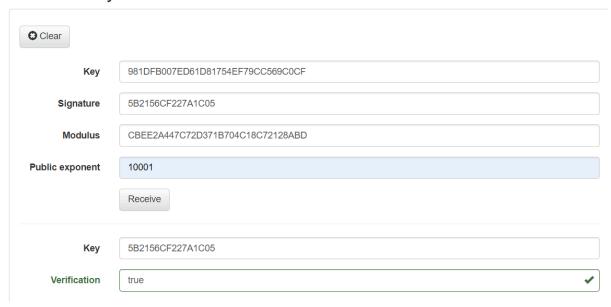
1

DS C+\3 xvnc\xnuntornahig\lah\lllah4\ \[\]

Send key



Receive key



Висновок:

По ходу роботи я ознайомився та використав на практиці тест Міллера-Рабіна для перевірки текстів на простоту. Також дізнався про методи генерації ключів для криптосистеми RSA. Практично по-працював з системою RSA організував секретний зв'язок та обмін даними за електронним підписом. Перевірив правильність нашої системи завдяки онлайн ресурсу.