Криптографія

Лабораторна робота 4. Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

ФБ-13 Ігнатенко Данило

Варіант 5

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

Задача

- 0. Прочитати методичку. Напевно, більше трьох разів
- 1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини. Перевірити простоту числа тестом Міллера-Рабіна
- 2. Написати функцію генерування ключових пар для RSA та згенерувати ключові пари для абонентів A та B
- 3. Написати функції шифрування, розшифрування, підпису, перевірки підпису повідомлення, надсилання та отримання секретного ключа по відкритій мережі
- 4. Перевірити роботу всього цього добра за допомогою наданого ресурсу

Хід роботи

Спершу були написані допоміжні функції – тест Міллера-Рабіна та генерація випадкового простого числа потрібної довжини

З їх використанням були написані 7 основних функцій лабораторної роботи

Останнім етапом стала перевірка коректності реалізації усіх функцій за наданим посиланням

Труднощі

Допоміжні функції зайняли трохи часу, але без бетонних стін – потихеньку все зробилося Основні функції труднощів, загалом, не викликали

Шляхи розв'язання

Вони точно існують

Результати

Далі наведені скріни використання реалізованих процедур. В якості абонента В виступає сервер

Генерація ключової пари

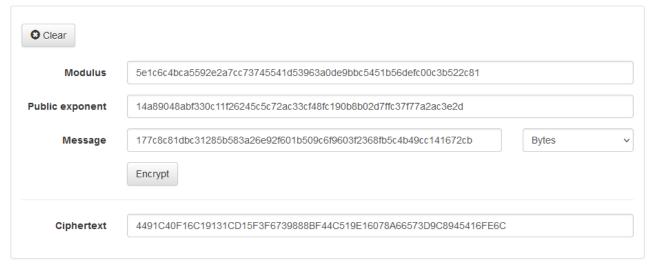
Get server key





Перевірка правильності шифрування та розшифрування

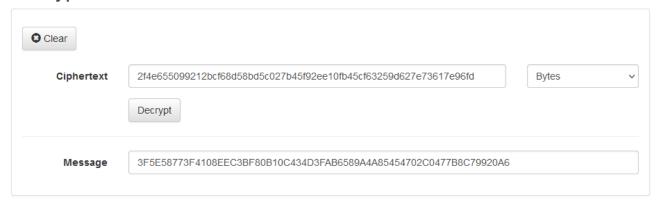
Encryption



Encryption
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d
Message: 177c8c81dbc31285b583a26e92f601b509c6f9603f2368fb5c4b49cc141672cb
B Encrypted message: 4491C40F16C19131CD15F3F6739888BF44C519E16078A66573D9C8945416FE6C
B Encrypted message and A Encrypted message match: True
Original Message and A Decrypted message match: True

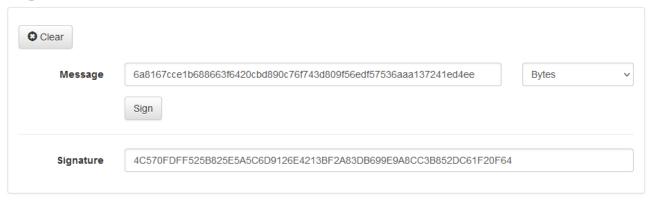
Ще одна подібна

Decryption



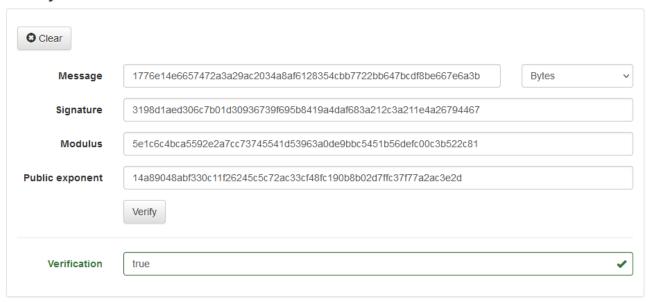
Перевірка підпису

Sign



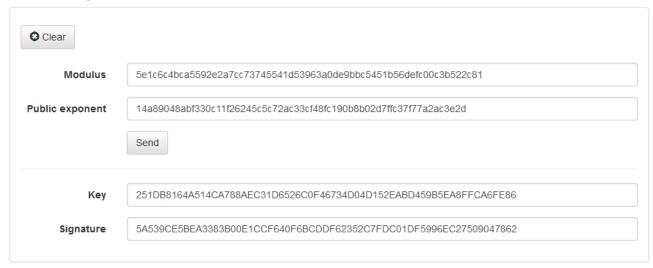
Підписування повідомлення

Verify



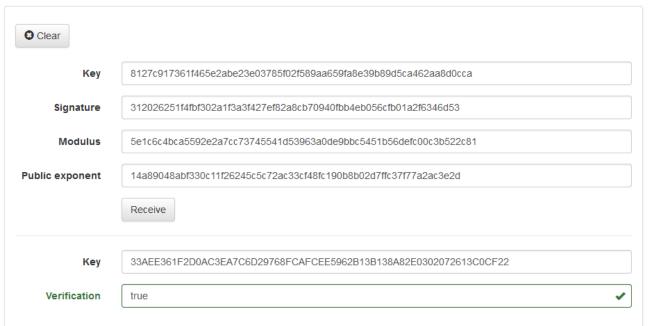
Отримання ключа

Send key



Надсилання ключа

Receive key



Висновки

Було реалізовано процедуру перевірки числа на простоту за тестом Міллера-Рабіна, процедуру генерації випадкового простого числа заданої довжини, основні процедури схеми RSA, а також процедури для розсилання ключів відкритою мережею. Усі процедури пройшли перевірку на коректність