Петров Д.М. КІТ-М120Б

Лабораторна робота №6

RSA Algorithm

Мета: Дослідити і реалізувати механізм ассиметричного алгоритму шифрування RSA на основі згеренованих ключів.

Розробити додаток обміну таємними посиланнями між двома клієнтами за допомогою алгоритму шифрування RSA

Алгоритм дій

- творити ключову пару: приватний та публічний ключ. Ключ(і) повинні бути розташовані поряд з виконуючим файлом
- текст повідомлення розташованно в файлі message.txt
- клієнт1 зчитує повідомлення, кодує його за допомогою свого приватного ключа та "відправляє" до його клієнту2 (у найпростішому випадку - розташовує кодований файл поряд з виконуючим файлом клієнта2). Для підтвердження у подальшому коректності дешифрування, клієнт1 повідомляє також геш суму орігінального повідомлення.
- клієнт2 зчитує кодоване повідомлення, дешифрує його за допомогою публічного ключа, знаходить геш суму дешифрованого повідомлення, порівнює її з вказаною. Та, нарешні виводить результат о коректності дешифрування.

1. **RSA**

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних застосунків.

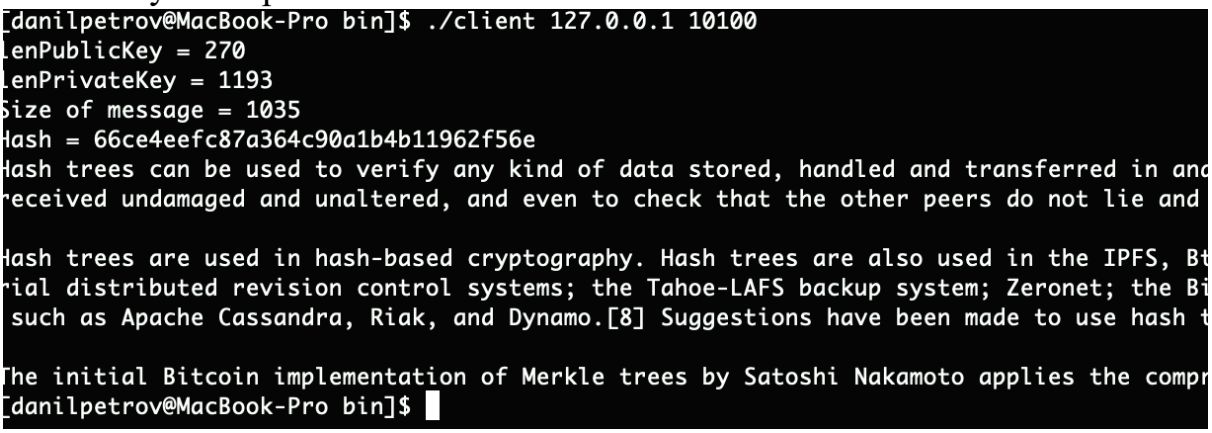
Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

В ході лабораторної роботи була розроблена програма в форматі клієнт-сервер. Клієнт генерує публічний та приватний ключі за допомогою алгоритму RSA, підключається до сервера та відправляє публічний ключ серверу. Сервер зберігає публічний ключ клієнта та відкриває message.txt з текстом, отримує з нього розмір та весь текст. Геширує його та відправляє

розмір та геш до клієнта. Після цього починає відправляти весь файл у закодованому форматі. Клієнт тим часом отримує тест з файлу розшифровує його та отримує геш. Після отримання всього файлу перевіряє геш файлу та порахований геш. Якщо співпадають, виводить на екран текст.

Результат роботи клієнта:



Висновок

Дослідив і реалізував механізм ассиметричного алгоритму шифрування RSA на основі згеренованих ключів.