Національний технічний університет України «КПІ ім. Ігоря Сікорського»
Факультет Інформатики та Обчислювальної Техніки
Кафедра Автоматизованих Систем Обробки Інформації та Управління

Лабораторна робота №5

з дисципліни «Системи Безпеки Програм і Даних»

Виконав:
студент гр. ІС-91
Мягков Герман

Київ – 2021

Зміст

1 Постановка задачі

Лаб. Робота 5. Розробка програми керування ключами шифрування за схемою RSA або El-Gamal (за варіантами). Програма реалізує ту чи іншу схему розрахунку ключів шифрування, обов'язково використовуючи для цього розширений або класичний алгоритми Евкліда, і формуючи відкриті і закриті (секретні) ключі шифрування, які відразу ж використовуються для шифрування повідомлень. Програма реалізує два режими шифрування і дешифрування повідомлень з перевіркою достовірності результатів на основі аналізу цифрового паспорта-сертифіката відкритих ключів.

2 Розв’язок

Програма реалізована на язику Javascript за допомогою модуля Crypto.
Crypto Модуль надає криптографічні функції, які включають набір оболонок для функцій хеша OpenSSL, HMAC, шифрування, дешифрування, підписи та перевірки.

- На початку виконання програма генерує RSA ключ пару довжиною 2048 бітів

```
const generateKeyPair = (length = 2048) => {
    const {publicKey, privateKey} = crypto.generateKeyPairSync('rsa', {
        modulusLength: length,
    });
    return {
        public: publicKey,
        private: privateKey,
    };
};
```

- За допомогою модуля crypto та згенерованої пари відбувається шифрування відкритим ключем, та дешифрування закритим.

- Для приклада візьмемо фразу “supersecretpassword”, та проведемо її шифрування та дешифрування, звіряючи у кінці результат:

```
  isEqual: true,
  data: 'supersecretpassword',
  encrypted: '\x13&\x19W\x13°xS$$L~Jw#w^Aa\b+f\x04Y#Nl\x10G1Aze\x11-fw\x1D+
^"<~x(\\Jc\x13"w@cjc\b\x00H3/\x14DE \x13\x10k\x1F,\x17 o=sR`xWr\x19N+hu\x12r\x1DG@e\
x18F P\x1A \x1F=\n' +
    "Hg@Q'LF/&\x0F\x00q@^@#jr@\x14\x1A\x7FM\x18$$3k8\x0ByFLE@\x05@",
  decrypted: 'supersecretpassword'
```

Як можна бачити, при дешифруванні ми отримали первісну строку.

3 Лістинг програми

GitHub:
https://github.com/ldvy/infosec/tree/main/lab5