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

Лабораторна робота №6

з дисципліни «Системи Безпеки Програм і Даних»

Виконав:
студент гр. ІС-91
Мягков Герман

Київ – 2021

Зміст

1 Постановка задачі

Лаб. Робота 6. Розробка програми формування сигнатури повідомлення (цифровий підпис) на основі симетричного алгоритму шифрування. Програма реалізує два режими роботи: просте поблокове шифрування і дешифрування повідомлень (режим електронної кодової книги), а також зчеплення блоків шифру при формуванні цифрового підпису. Схема управління ключами шифрування генерує ключі як випадкові двійкові числа довжиною декількох десятків біт (за варіантами), які зберігаються і можуть бути повторно використані.

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, згенероване повідомлення підписується закритим ключем.
Перевірка підпису проводиться за допомогою відкритого ключа.

- Для перевірки програми створимо два об’єкти – signature та invalidSignature.
В першому зберігається справжній підпис повідомлення, інший заповнюється випадковими символами.

При запуску програма перевіряє підписи и виводить на екран що invalidSignature некоректна:

```
{
  case: 'validSig',
  message: 'supersecretpassword',
  signature: 'm□u_□□1□□□□AK\\□V□□□\x1E□\x04.□f□□\x13□R□\x00D□□□<□□□5\x16□□Z\b□□,□L□□□□;X~3□□1□□u□9□□<T*□\x07c>□\x05R□\x0
BNn/.□=qbI\x10}□□\t□Z`□h3W□S□□□9t□Vey\\\x04k□|b□X□□v□c□}□□1-\b□]□xE6H□□he□s□5A□m\b□u□□□□ d\x15□vƥ□□\n' +
    `\x18□_~\x0E□cC"□!□□G□t'R\x03□□S}K□nF□r□\x1Ci□□□TBA<□□□\x15□#\x0F□□□□k□\x10□□Ce□Z□|□□□];$□□□\x14]□□f\x1B□6\x13□n`,
  isCorrect: true
}
{
  case: 'invalidSig',
  message: 'supersecretpassword',
  signature: '\x01\x01\x01\x01\x01\x01\x01\x01\x01\x01\x01\x01',
  isCorrect: false
}
```

3 Лістинг програми

GitHub:
https://github.com/ldvy/infosec/tree/main/lab6