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

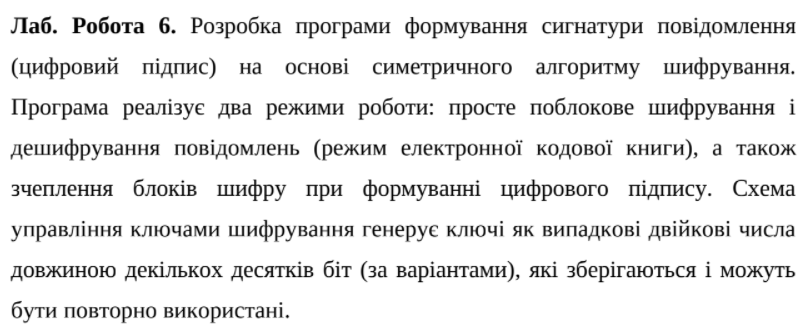
[Зміст 2](#_Toc91173305)

[1 Постановка задачі 3](#_Toc91173306)

[2 Розв’язок 4](#_Toc91173307)

[3 Лістинг програми 5](#_Toc91173308)

### 1 Постановка задачі

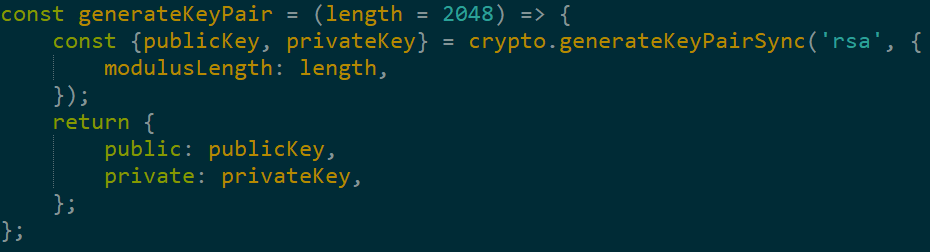


### 2 Розв’язок

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.

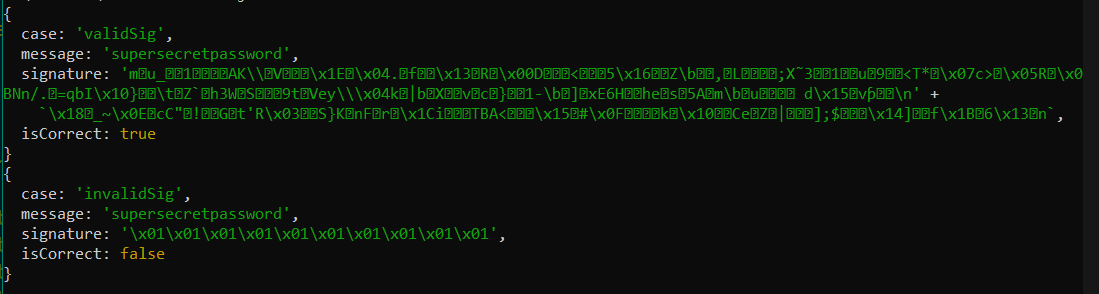
- На початку виконання програма генерує RSA ключ пару довжиною 2048 бітів



- 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:



### 3 Лістинг програми

GitHub:

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