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

[Зміст 2](#_Toc91173305)

[1 Постановка задачі 3](#_Toc91173306)

[2 Розв’язок 4](#_Toc91173307)

[3 Лістинг програми 5](#_Toc91173308)

### 1 Постановка задачі

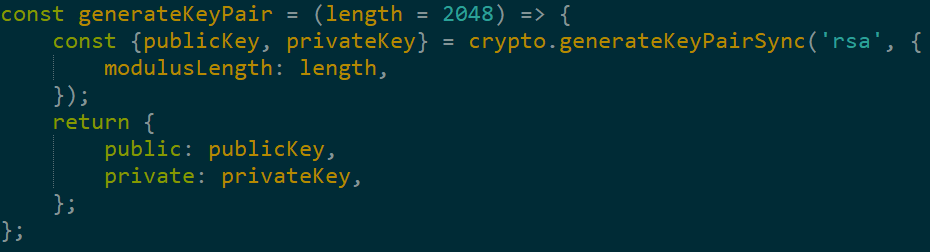
**Лаб. Робота 5.** Розробка програми керування ключами шифрування за схемою RSA або El-Gamal (за варіантами). Програма реалізує ту чи іншу схему розрахунку ключів шифрування, обов'язково використовуючи для цього розширений або класичний алгоритми Евкліда, і формуючи відкриті і закриті (секретні) ключі 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.

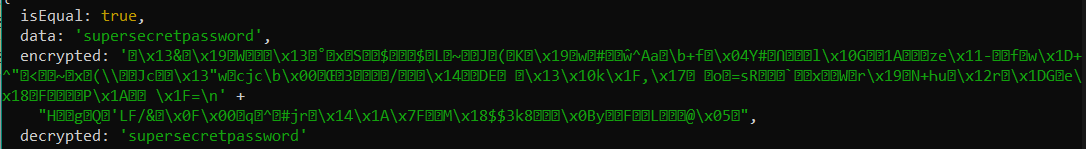
Crypto Модуль надає криптографічні функції, які включають набір оболонок для функцій хеша OpenSSL, HMAC, шифрування, дешифрування, підписи та перевірки.

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



- 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:



Як можна бачити, при дешифруванні ми отримали первісну строку.

### 3 Лістинг програми

GitHub:

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