Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

Лабораторна робота з Методів реалізації криптографічних механізмів

Студент групи ФІ-32мн
Карловський Володимир Олександрович

Лабораторна робота № 1. Завдання 3А

Розробка технічних вимог (із вибором або бібліотеки реалізації арифметичних операцій або бібліотеки реалізації основних криптографічних примітивів) для різних варіантів реалізації IT-систем. Вибір бібліотеки для реалізації Web-сервісу електронного цифрового підпису.

Криптографічна система має складатися з веб сторінки та cli:

Функціонал cli:

1. Отриманням ключа для підпису файлів та текстових повідомлень
2. Підпис файлу за допомогою приватного ключа і отримання сигнатури.

Функціонал веб сторінки:

1. Сторінка для перевірки підписаних файлів

Технології та бібліотеки, які будуть використовуватись для побудови системи:

1. Мова Go https://go.dev/
2. Пакети зі стандартної бібліотеки crypto, crypto/rand, crypto/rsa, crypto/sha512
3. Функції для підпису `SignPSS, VerifyPSS`

   PSS (Probabilistic Signature Scheme) - це схема підпису для цифрового підпису, яка часто використовується разом із алгоритмом RSA для забезпечення безпеки в інформаційних системах. PSS була розроблена як один із методів покращення безпеки підпису, щоб уникнути певних проблем, які можуть виникнути при використанні стандартного підпису RSA (PKCS1v15).

Лабораторна робота № 2. Завдання 3А

Розробка технічних вимог (із вибором схеми генерації ПСП та схеми управління ключами) для різних варіантів реалізацій ІТ-систем. Вибір рішень для реалізації Web-сервісу електронного цифрового підпису.

Детальний опис роботи системи:

Генерація ключа

1. Користувач, дає команду на генерацію, отримує у відповідь 2 ключі публічний і приватний
2. Генерується ключ довжини 4096 бітів, використовується джерело випадковості rand.Reader - обгортка мови над /dev/urandom - що є безпечним джерелом випадковості
3. Користувачу віддається файл публічного та приватного ключа.

Підпис

1. Користувач передає в команду на генерацію файл/текст додає приватний ключ
2. Сервер хешує контен за допомогою `sha512`
3. Підписує хеш `SignPSS`
4. Віддає файл сигнатури користувичу

Перевірка

1. Користувач завантажує файл/текст додає публічний ключ і сигнатуру
2. Сервер перевіряє підпис