Практическое занятие №13

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ

ДЛЯ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО

И АССИМЕТРИЧНОГО ШИФРОВАНИЯ

С ИСПОЛЬЗОВАНИЕМ SUBTLECRYPTO В JS

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель:** изучить интерфейс SubtleCrypto, основные классы и

структуры данных: разработать приложение для шифрования фай-

лов, использующих симметричные и ассиметричные алгоритмы

шифрования.

**Краткие теоретические сведения:**

* **Web Crypto API** — это API, предоставляющее доступ к криптографическим функциям браузера. Оно предоставляет низкоуровневые функции для работы с криптографией, включая создание ключей, шифрование, хеширование и многое другое.
* **AES-GCM** — это алгоритм симметричного шифрования с аутентификацией, который используется для защиты данных. Он использует ключ для шифрования и может быть использован для шифрования данных в сочетании с механизмом аутентификации для предотвращения атак.
* **SHA-512** — это алгоритм хеширования, который генерирует 512-битный хеш. Он используется для защиты данных от модификации и для создания уникальных представлений данных.
* **AES-KW** — алгоритм для упаковки и распаковки симметричных ключей, используемый для безопасного обмена криптографическими ключами.
* **RSA-PSS** — алгоритм подписи, использующий алгоритм RSA и схему подписания с подтверждением (PSS). Он предоставляет высокую степень безопасности для подписанных данных.

**Условие задания**

Выполнить криптографические операции с использованием Web Crypto API в Node.js:

1. Генерация случайных чисел и вывод их в консоль.
2. Шифрование и дешифрование строки (фамилии "Васильев") с использованием алгоритма шифрования **AES-GCM**.
3. Хеширование строки "Васильев" с использованием алгоритма **SHA-512**.
4. Упаковка и распаковка ключа с использованием алгоритма **AES-KW**.
5. Подпись и проверка подлинности сообщения с использованием алгоритма **RSA-PSS**.

**Исполнительная часть**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

Использованные источники

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.