МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №12:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

**Исследование алгоритмов генерации и верификации электронной цифровой подписи**

**Теоретические сведения**

Электронная цифровая подпись (ЭЦП) является важным элементом современных информационных систем, использующих методы и технологии криптографического преобразования информации.

Определение 1. Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

Таким образом, ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

• аутентифицировать лицо, подписавшее сообщение;

• контролировать целостность подписанного сообщения;

• защищать сообщение от подделок;

• доказать авторство лица, подписавшего сообщение, если это лицо отрицает свое авторство

Определение 2. Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь Мо), а его хеша, H(Mо). Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе.

**Практическая часть**

В данной лабораторной работе необходимо разработать приложение для генерации и верификации ЭЦП на основе алгоритмов RSA, ЭльГамаля и Шнорра.

В связи с поставленными требованиями было разработано приложение на основе встроенного пакета crypto в Node.js.

Пример реализации сервера и клиента для создание ЭЦП на основе RSA представлены на рисунке 1 и 2 соответственно.



Рисунок 1 – Сервер



Рисунок 2 – Клиент

Вызов функций сервера для генерации ЭЦП на основе RSA представлен на рисунке 3.



Рисунок 3 – Вызов функций сервера

Вызов функций клиента для генерации ЭЦП на основе RSA представлен на рисунке 4.

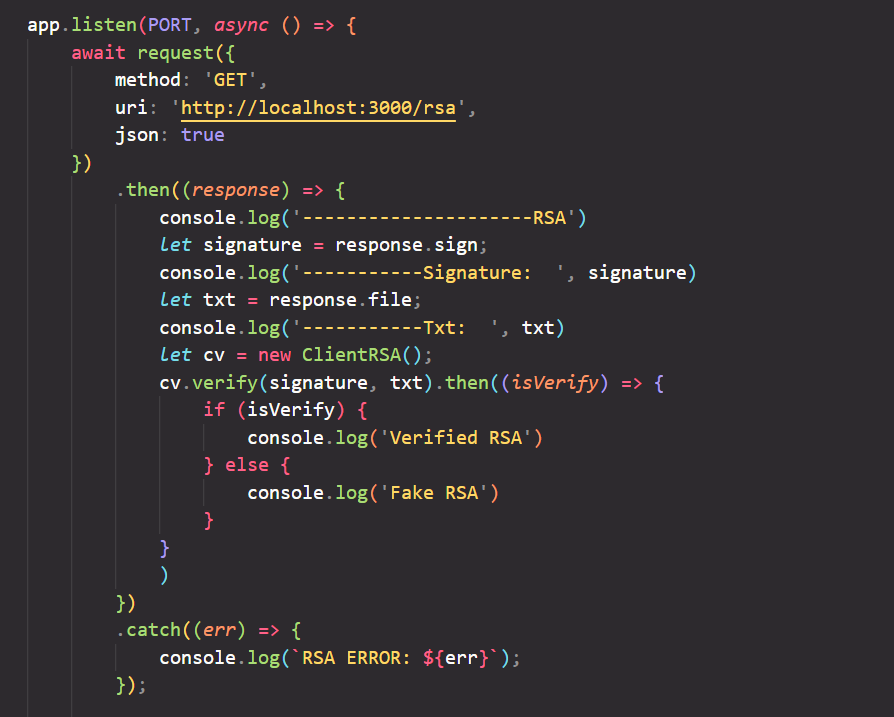


Рисунок 4 – Вызов функций клиента

Пример реализации сервера и клиента для создания ЭЦП на основе Эль-Гамаля представлены на рисунке 5 и 6 соответственно.



Рисунок 5 – Сервер

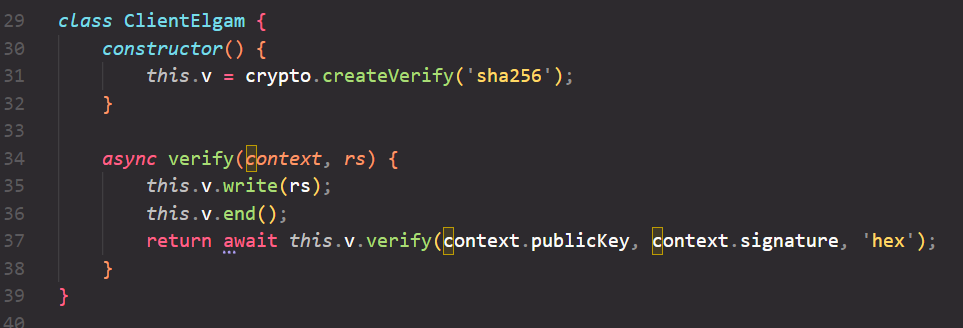


Рисунок 6 – Клиент

Вызов функций сервера для генерации ЭЦП на основе Эль-Гамаля представлен на рисунке 7.



Рисунок 7 – Вызов функций сервера

Вызов функций клиента для генерации ЭЦП на основе Эль-Гамаля представлен на рисунке 8.



Рисунок 8 – Вызов функций клиента

Пример реализации сервера и клиента для создания ЭЦП на основе Шнорра представлены на рисунке 9.

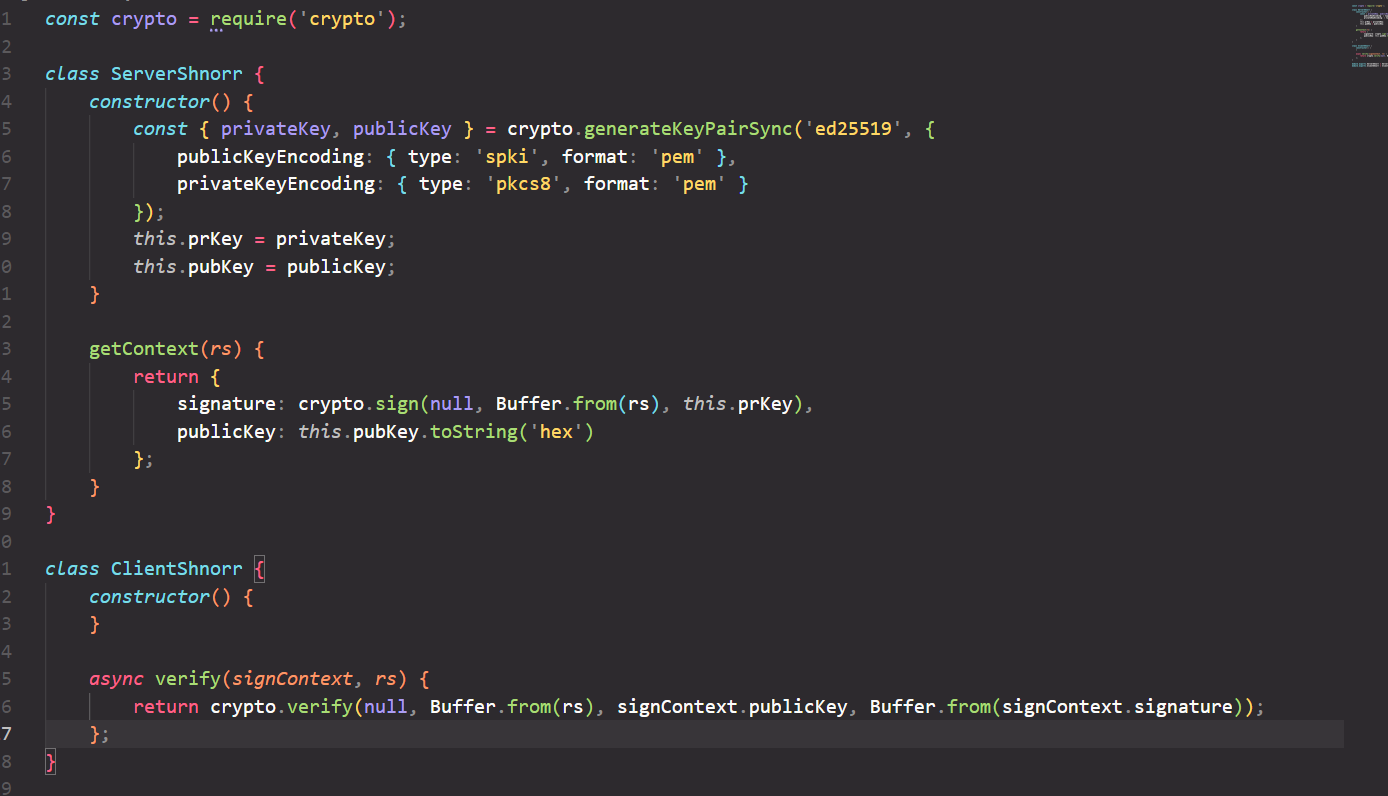


Рисунок 9 – Сервер

Вызов функций сервера для генерации ЭЦП на основе Шнорра представлен на рисунке 10.



Рисунок 10 – Вызов функций сервера

Вызов функций клиента для генерации ЭЦП на основе Шнорра представлен на рисунке 11.



Рисунок 11 – Вызов функций клиента

Рисунок 12 – Зависимости времени от кол-ва символов

**Вывод**

В данной лабораторной работе я закрепила теоретические знания по ЭЦП. А также, разработала приложение для генерации и верификации по 3 алгоритмам.