Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №12**

**Тема «****исследование алгоритмов генерации и верификации электронной цифровой подписи»**

Цель изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП).
2. . Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра
3. Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.
4. Оценить скорость генерации и верификации ЭЦП.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**ЭЦП**

**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.

Общая схема ЭЦП на основе хешей предоставлена на рисунке 1.1.

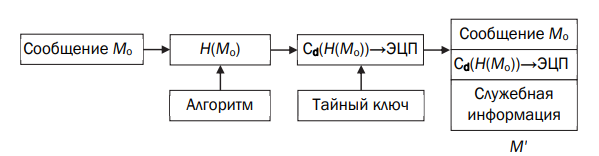


Рисунок 1.1 – общая схема ЭЦП на основе хэшей

**ЭЦП на основе RSA**

Для создания ЭЦП на основе RSA, отправитель выполняет следующие действия:

1. Хэширует сообщение, которое необходимо подписать, с помощью криптографической хэш-функции, такой как SHA-256. Это позволяет получить фиксированный размер хэша, который является уникальным для каждого сообщения.
2. Затем отправитель использует свой закрытый ключ RSA для создания цифровой подписи хэша. Для этого он вычисляет значение, которое является результатом возведения хэша в степень, равную закрытому ключу по модулю открытого ключа.
3. Полученное значение является ЭЦП, которую отправитель может прикрепить к исходному сообщению.
4. Получатель, имеющий доступ к открытому ключу отправителя, может проверить подлинность и целостность сообщения, используя следующие шаги.

Пример кода для создания ЭЦП на основе RSA и её верификации предоставлен на рисунке 1.2, а результат работы на рисунке 1.3.

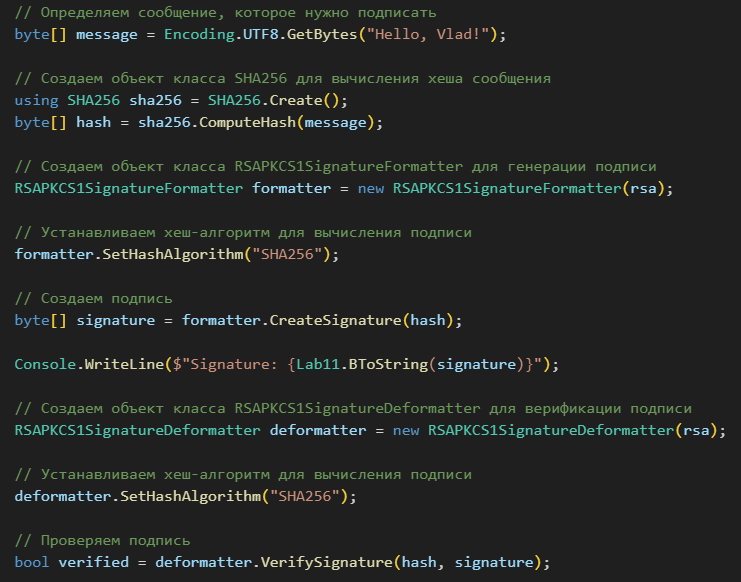


Рисунок 1.2 – Код ЭЦП на основе RSA

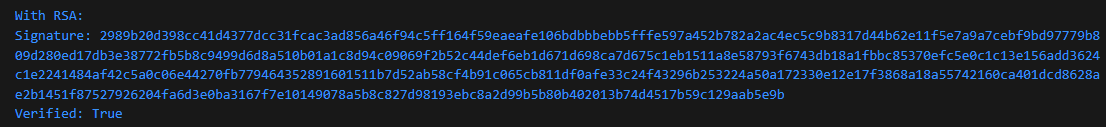


Рисунок 1.3 – Результат работы кода

Скорость выполнения алгоритма предоставления на рисунке 1.4

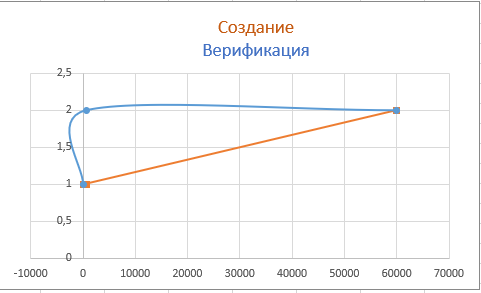


Рисунок 1.4 – Скорость ЭЦП на основе RSA

**ЭЦП Эль-Гамаля**

Алгоритм Эль-Гамаля используется для создания пары ключей: публичного и приватного, которые используются для шифрования и расшифрования сообщений и создания электронной цифровой подписи.

Для создания ЭЦП на основе Эль-Гамаля, сначала генерируется пара ключей: публичный и приватный. Затем, чтобы создать ЭЦП для сообщения, отправитель вычисляет хеш-функцию сообщения и шифрует ее своим приватным ключом. Полученный результат называется цифровой подписью и прикрепляется к сообщению.

Получатель сообщения, чтобы проверить ЭЦП, расшифровывает цифровую подпись с помощью публичного ключа отправителя и вычисляет хеш-функцию самого сообщения.Если полученный результат совпадает с расшифрованной цифровой подписью, то ЭЦП считается действительной и сообщение не подделано.

Подпись в ЭЦП Эль-Гамаля состоит из двух чисел – r и s.

Число r вычисляется на основе случайного числа k и публичного ключа получателя y по формуле *r* = *gk* mod *p*, где *g* - генератор циклической группы , *p* - большое простое число.

Число *s* вычисляется на основе хэш-значения сообщения, подписываемого отправителем, с использованием секретного ключа отправителя x и числа r по формуле s = k-1 (*H*(*m*) - *x*×*r*) mod (*p*-1), где *H*(*m*) - хэш-значение сообщения, k-1 - обратное к случайному числу *k* по модулю *p*-1.

Итоговая подпись (*r*, *s*) передается вместе с сообщением получателю, который может проверить ее на подлинность, сравнивая ее с помощью открытого ключа отправителя и хэш-значения сообщения.

Пример кода предоставлен на рисунке 1.5, а результат работы на рисунке 1.6

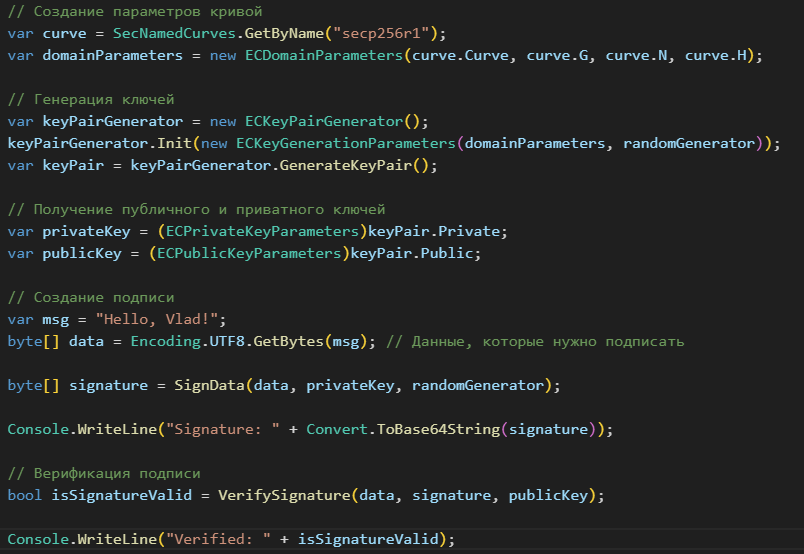


Рисунок 1.5 – Код ЭЦП Эль-Гамаля

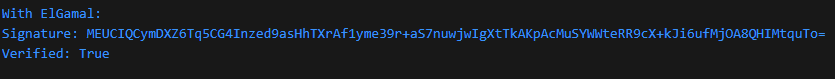


Рисунок 1.6 – Результат работы кода

Скорость выполнения алгоритма предоставления на рисунке 1.7



Рисунок 1.7 – Скорость ЭЦП Эль-Гамаля

**ЭЦП Шнорра**

Основная идея метода заключается в использовании криптографических хеш-функций и математических операций для создания цифровой подписи, которая может быть проверена для подлинности и целостности данных.

Создание цифровой подписи на основе Шнорра происходит в несколько этапов:

1. Генерация ключей. Пользователь генерирует пару ключей - открытый и закрытый. Открытый ключ может быть распространен и использован для проверки цифровой подписи, а закрытый ключ должен быть известен только владельцу.
2. Создание хеш-значения. Данные, которые нужно подписать, подвергаются хешированию с помощью криптографической хеш-функции, например, SHA-256. Хеш-значение представляет собой фиксированную последовательность байтов, которая является уникальным представлением данных.
3. Создание подписи. Для создания подписи пользователь использует закрытый ключ и хеш-значение данных. На основе этих данных вычисляется подпись, которая также представляет собой фиксированную последовательность байтов.
4. Проверка подписи. Другой пользователь, имеющий открытый ключ, может проверить подлинность и целостность данных, используя полученную подпись и хеш-значение данных. Для этого он вычисляет определенное математическое выражение, которое должно быть равно открытому ключу пользователя, создавшего подпись. Если значения совпадают, то подпись считается действительной.

Пример кода предоставлен на рисунке 1.7, а результат работы на рисунке 1.8.



Рисунок 1.7 – Код ЭЦП Эль-Гамаля

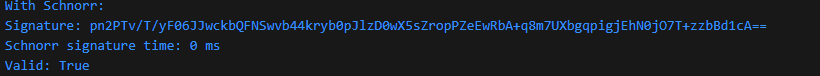


Рисунок 1.8 – Результат работы кода

Скорость выполнения алгоритма предоставления на рисунке 1.9



Рисунок 1.9 – Скорость ЭЦП Эль-Гамаля

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации алгоритмов генерации и верификации электронной цифровой подписи.