Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование алгоритмов генерации и верификации**

**электронной цифровой подписи**

Студент: Решетилова Антонина

ФИТ 3 курс 4 группа

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования Python и позволяет:

* генерировать ЭЦП на основании алгоритма RSA;
* генерировать ЭЦП на основании алгоритма Эль-Гамаля;
* генерировать ЭЦП на основании алгоритма Шнорра;
* оценивать время выполнения генерации ЭЦП.

1. **Методика выполнения поставленных задач**

ЭЦП – 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.

Важнейшими отличительными особенностям ЭЦП являются:

* ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);
* указанная бинарная последовательность зависит от содержания подписываемого сообщения.

Результат работы приложения представлен на рисунке 2.1.

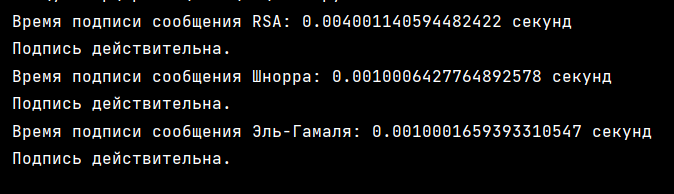


Рисунок 2.1 – Результат работы приложения

Для создания ЭЦП на основе алгоритма RSA и верификации документа, приложение высчитывает ключевую информацию, хеш текста из файла и создает подпись на основе закрытого ключа, а верификацию хеша производит на основании открытого ключа.

Если подписываемое сообщение М также должно передаваться в зашифрованном виде, то обычно М шифруется на стороне отправителя стандартным образом: с помощью открытого ключа получателя (е и n), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: d и n.

Реализация данной функции представлена на рисунке 2.2.

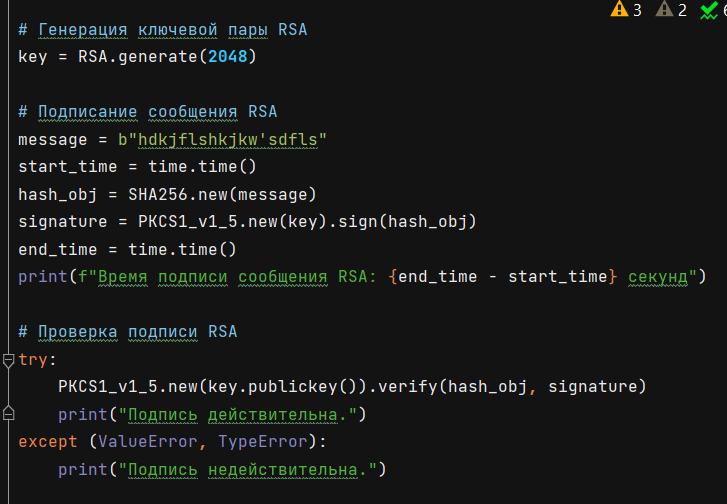


Рисунок 2.3 – Реализация функции RSA

Ключевая информация отправителя: открытый ключ: y, g и р; тайный ключ: х. Чтобы подписать сообщение М, обладатель используемых для ЭЦП ключей должен выбрать случайное число k, взаимно простое с р-1.

Затем вычисляется числа а и b, являющиеся цифровой подписью (S = {a, b}) путем возвещения числа g в степень k и деления по модулю p. Для вычисления b используется расширенный алгоритм Евклида.

Создание ЭЦП на основе Эль-Гамаля происходит в функции Crypt класса ElGamal. Реализация функции представлена на рисунке 2.4.

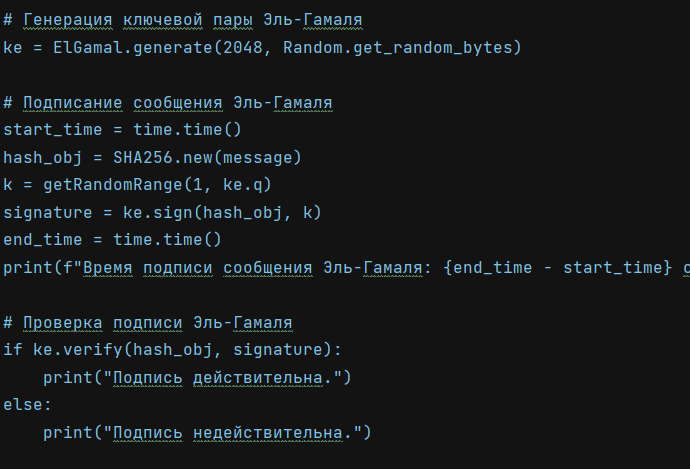


Рисунок 2.4 – Реализация функции Crypt

Создание ЭЦП на основе Шнорра происходит в функции Do класса Shnorr. Реализация функции представлена на рисуке 2.5.

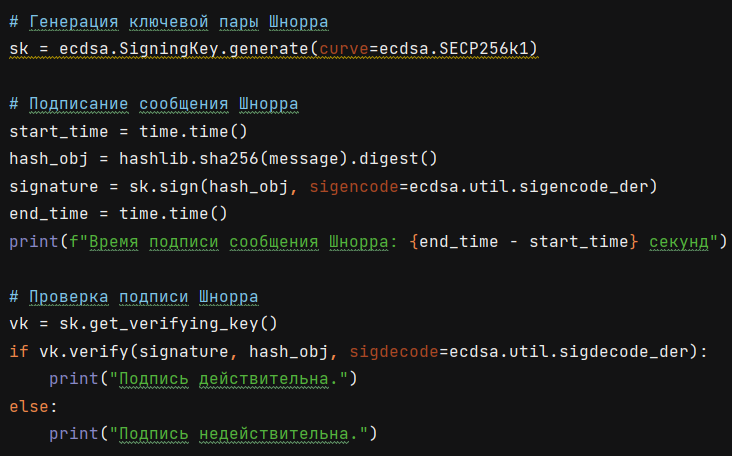


Рисунок 2.5 – Реализация функции Do

Для верификации подписи вычисляется хеш полученного сообщения, Н(М) = h. Далее нужно убедиться, что выполняется равенство ya \* ab = gh (mod p. Если равенство выполняется, подпись верифицируется.

Таким образом, были реализованы все поставленные задачи. Были исследованы асимметричные шифры.

**Вывод**

В ходе лабораторной работы были приобретены навыки подписи ЭЦП на основе алгоритмов RSA, Эль-Гамаля, Шнорра.

Также было разработано приложение, на языке программирования Python, для реализации задач, связанных подписью ЭЦП.

**Контрольные вопросы:**

**1. Дать определение ЭЦП.**

**Электронная цифровая подпись** – бинарная последовательность, прикрепляемая к отправляемому документу, которая позволяет однозначно идентифицировать отправителя.

**2. Охарактеризовать основные функции ЭЦП.**

1. Верификация автора сообщения;
2. Контроль целостности сообщения;
3. Защита сообщений от подделки;
4. Доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

**3. В чем заключаются сходства и различия между собственноручной и электронной подписью?**

Сходства заключаются в том, что ЭЦП выполняет те же функции, что и подпись от руки:

Отличия ЭЦП от ручной подписи:

• ЭЦП представляет собой бинарную последовательность.

• Бинарная последовательность зависит от содержания подписываемого сообщения.

**4.** **Охарактеризовать основные способы реализации ЭЦП.**

1. На основе симметричных систем.
2. На основе симметричных систем и посредника.
3. На основе асимметричных систем.

**5. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?**

При вычислении ЭЦП с помощью ассиметричной системы используется тайный ключ отправителя, в отличии от процесса шифрования, при котором используется публичный ключ получателя сообщения. Также стоит учесть, что подписанные сообщения можно передавать и в зашифрованном виде, так что перед отправкой сообщения могут быть одновременно использованы и публичный ключ получателя, и тайный ключ отправителя.

**6. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы Эль-Гамаля, схемы Шнорра.**

**RSA** является одним из самых широко используемых алгоритмов ЭЦП. Криптостойкость ЭЦП на основе RSA зависит от сложности факторизации больших чисел на простые множители. Для достижения достаточной криптостойкости, длина ключа RSA должна быть не менее 2048 бит. Однако, с учетом быстрого развития вычислительной техники, в будущем рекомендуется использовать более длинные ключи RSA.

**Схема Эль-Гамаля** основана на сложности дискретного логарифмирования. Криптостойкость ЭЦП на основе этой схемы также зависит от длины ключа. Рекомендуется использовать ключи длиной не менее 2048 бит.

**Схема Шнорра** также основана на сложности дискретного логарифмирования. Она обладает преимуществами перед RSA и схемой Эль-Гамаля в том, что она имеет более короткие ключи при той же криптостойкости. Однако, криптостойкость ЭЦП на основе схемы Шнорра также зависит от длины ключа. Рекомендуется использовать ключи длиной не менее 256 бит.

В целом, криптостойкость ЭЦП на основе RSA, схемы Эль-Гамаля, схемы Шнорра является достаточной для большинства практических задач.

**7. Какие элементы составляют ключевую информацию алгоритмов реализации ЭЦП, перечисленных в вопросе 6?**

Ключевая информация включает в себя параметры, используемые для генерации открытого и секретного ключей, а также сами открытый и секретный ключи. Открытый ключ является публичной информацией и может быть распространен широко. Секретный ключ, с другой стороны, должен храниться в безопасном месте и использоваться только владельцем ключа для подписи сообщений. Стоит отметить, что безопасность ЭЦП напрямую зависит от безопасности ключей. Поэтому генерация ключей должна быть проведена с учетом рекомендаций по безопасности и должна выполняться с помощью криптографически надежных методов.

**8. Дать сравнительные характеристики схемам ЭЦП, перечисленным в вопросе 6.**

**RSA:**

* Простой;
* Быстрый;
* Длина ключа может быть очень большой, что обеспечивает высокий уровень безопасности;
* Низкая производительность в режиме ЭЦП

**Схема Эль-Гамаля:**

* Производительнее RSA;
* Стойкость к атакам выше, чем у RSA;
* Длина ключа должна быть больше, чем в RSA, для обеспечения такого же уровня безопасности.

**Схема Шнорра:**

* Высокая производительность;
* Высокий уровень безопасности;
* Малая длина подписи и ключей.

**9. Охарактеризовать особенности государственного стандарта ЭЦП в Республике Беларусь.**

Согласно государственному стандарту РБ СТБ 34.101.45-2013 ЭЦП должна основывать на схеме Шнорра.