Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование алгоритмов генерации и верификации эцп

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Дубалеко В.В.

Минск 2020

1. **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

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.

Функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования

• на основе симметричных систем (с тайным ключом),

• на основе симметричных систем и посредника,

• на основе асимметричных систем (с открытым ключом).

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.

1. **Практическая часть**

В данной лабораторной работе нужно было Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра;

• оценку времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах;

В связи с поставленными требованиями в данной лабораторной работе были разработано приложение которые позволяли создавать цифровую подпись и проводить ее верификацию на основе встроенного пакета security в Java.

Пример ЭЦП RSA:

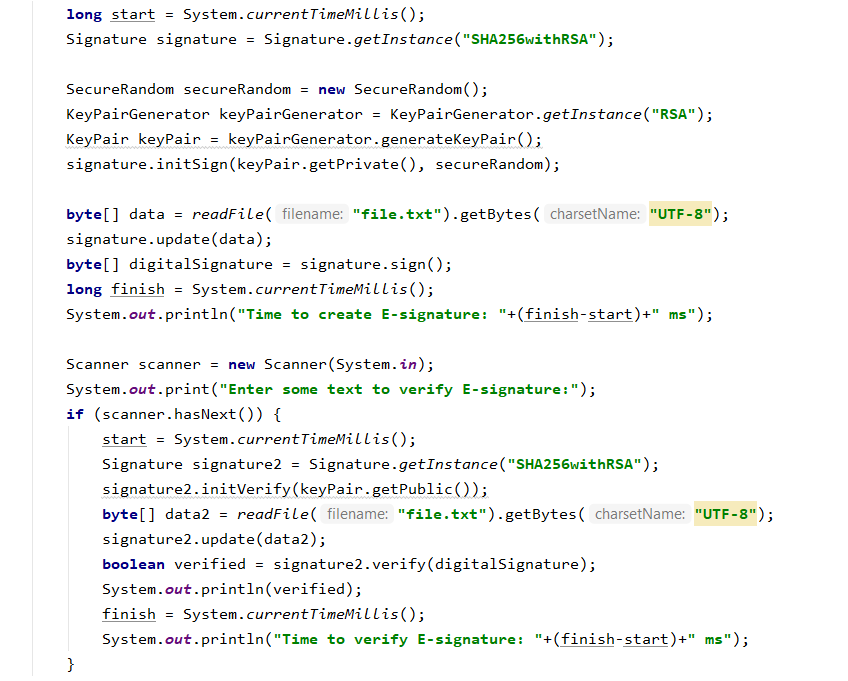


Рисунок 2.1 – Листинг кода для RSA

Похожие по структуре на метод на рисунке 2.1 были воссозданы методы так же для создания и верификации цифровой для других алгоритмов, указанных в задании.

Принцип работы приложения состоит в том, чтобы создать цифровую подпись для файла.



Рисунок 2.2 – Содержимое файла

После того как будет создана цифровая подпись в консоль будет выдан текст который будет просить что, бы мы ввели текст для верификации нашей цифровой подписи, а так же время которое было затрачено на создание цифровой подписи.



Рисунок 2.3 – Просьба о вводе текста для проверки эцп

После того как текст будет нами введен есть два варианта развития событий. В первом случае, если с эцп все хорошо там будет выдано true и время которое понадобилось для проверки эцп.

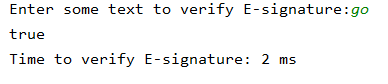


Рисунок 2.4 - Успешная проверка эцп

Но не всегда эта проверка будет проходить успешно в случае если проверка не пройдет успешно будет выдано false и время которое было затрачено на проверку.

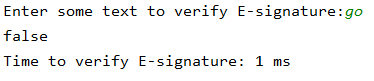


Рисунок 2.5 – Провал при проверке эцп

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по эцп. А также, разработал приложение для генерации и верификации по 3 алгоритмам.