Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №12**

Исследование алгоритмов генерации и верификации

электронной цифровой подписи

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

В данной лабораторной работе было разработано приложение используя язык программирования Python.

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

**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**:

• аутентифицирование лица, подписавшего сообщение;

• контроль целостности подписанного сообщения;

• защита сообщения от подделок;

• доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

**Важнейшие отличительные особенности ЭЦП:**

• ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);

• указанная бинарная последовательность зависит от содержания подписываемого сообщения.

**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 *М0*), а его хеша, *H(M0).* Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе.

Основу рассматриваемых протоколов составляют методы асимметричной криптографии и эллиптических кривых. Общая структура подписанного электронного документа – *М0* – *М'* – представляет собой, как правило, конкатенацию этого документа и ЭЦП *S*. Кроме этих двух элементов, интегральный документ может содержать некоторую служебную информацию (дата, время отправки или различные данные об отправителе).

Важное свойство цифровой подписи заключается в том, что ее может проверить (верифицировать) каждый, кто имеет доступ к открытому ключу ее автора. Заметим, что в общем случае версии исходного документа (*М0*) и полученного (*Мп*) могут отличаться.

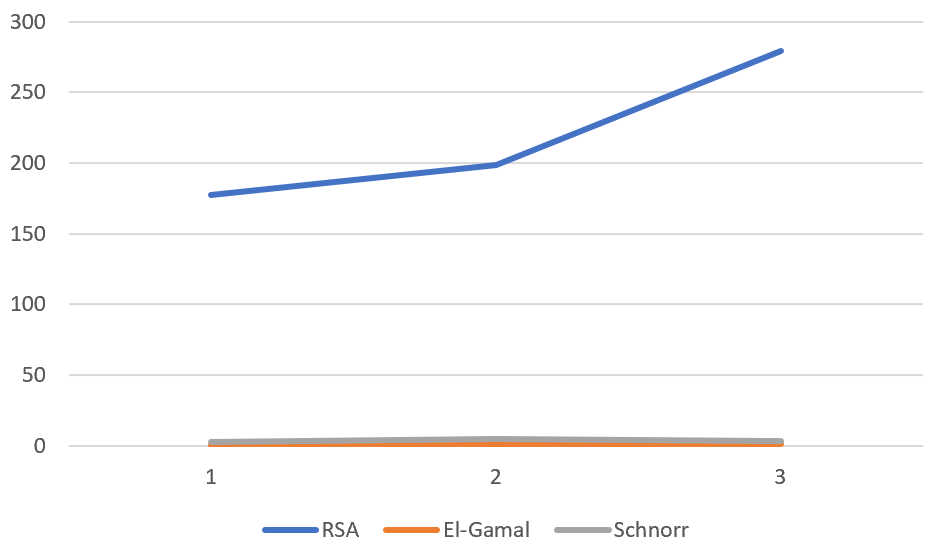


Рисунок – Время верификации и генерации ЭЦП

Как видно из графика, вне зависимости от длины входного сообщения время генерации и верификации почти не меняется.

**Вывод.** В данной лабораторной работе были исследованы алгоритмы генерации и верификации ЭЦП. Как видно из графика время генерации и верификации при использовании алгоритмов Эль-Гамаля и Шнорра существенно отличается.