Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование алгоритмов генерации и верификации**

**электронной цифровой подписи**

Студент:Чёрная Я.Р.

ФИТ 3 курс 4 группа

Минск 2025

**1. Теоретические сведения**

Электронная цифровая подпись (ЭЦП) является важным элементом современных информационных систем, использующих методы и технологии криптографического преобразования информации. В данном разделе мы рассмотрим ключевые свойства, функции и характеристики ЭЦП. Более подробные сведения из предметной области можно найти в источниках [2, 4, 29, 50]. Понятие «электронная цифровая подпись» было введено в 1976 г. У. Диффи и М. Хеллманом. После создания алгоритма RSA были разработаны алгоритмы цифровой подписи И. Рабина и Р. Меркле. В 1984 г. Ш. Гольдвассер, С. Микали и Р. Ривест сформулировали требования безопасности к алгоритмам ЭЦП и описали атаки на ЭЦП.

**Определение ЭЦП -** Государственный стандарт Республики Беларусь [51] определяет ЭЦП следующим образом:

**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.

**Функции ЭЦП**

ЭЦП выполняет те же функции, что и собственноручная подпись:

* **Аутентификация** лица, подписавшего сообщение.
* **Контроль целостности** подписанного сообщения.
* **Защита сообщения** от подделок.
* **Доказательство авторства** лица, подписавшего сообщение, в случае отрицания им своего авторства.

**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.

**Ключевые компоненты ЭЦП**

Основным компонентом в технологии ЭЦП является **ключ**. Принадлежность ключа, в предположении, что он известен только законным пользователям, позволяет решать все задачи, возложенные на ЭЦП, сформированную на основе этого ключа. В соответствии с этим, функции ЭЦП могут быть реализованы на основе различных методов шифрования:

1. **На основе симметричных систем** (с тайным ключом).
2. **На основе симметричных систем и посредника**.
3. **На основе асимметричных систем** (с открытым ключом).

**Примеры методов шифрования**

* Первый метод не отличается, например, от DES.
* Во втором случае создаются две симметричные системы: одна между отправителем и посредником, другая — между посредником и получателем. Посредник выдает двум сторонам различный тайный ключ.
* В третьем случае сообщение, отправляемое получателю, шифруется тайным ключом отправителя. Отправитель верифицирует подпись, используя для расшифрования публичный ключ отправителя.

**Альтернативное определение ЭЦП**

С учетом изложенного, можно сформулировать определение ЭЦП следующим образом:

**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.

**2. 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.

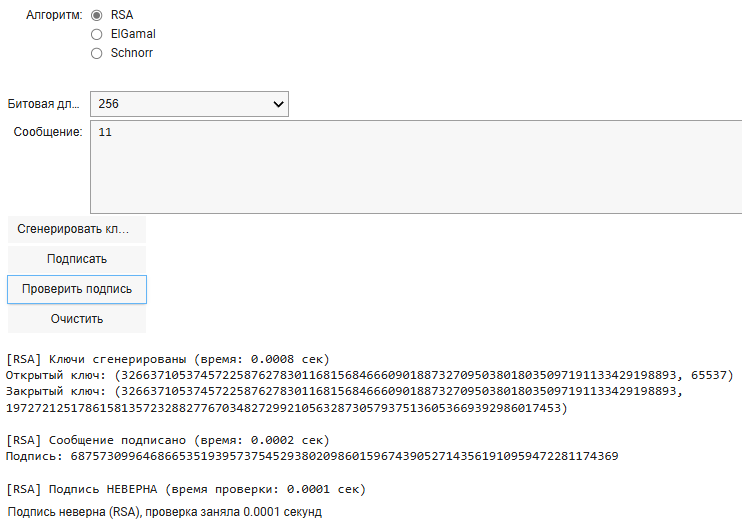


Рисунок 2.1 – Результат работы приложения для RSA

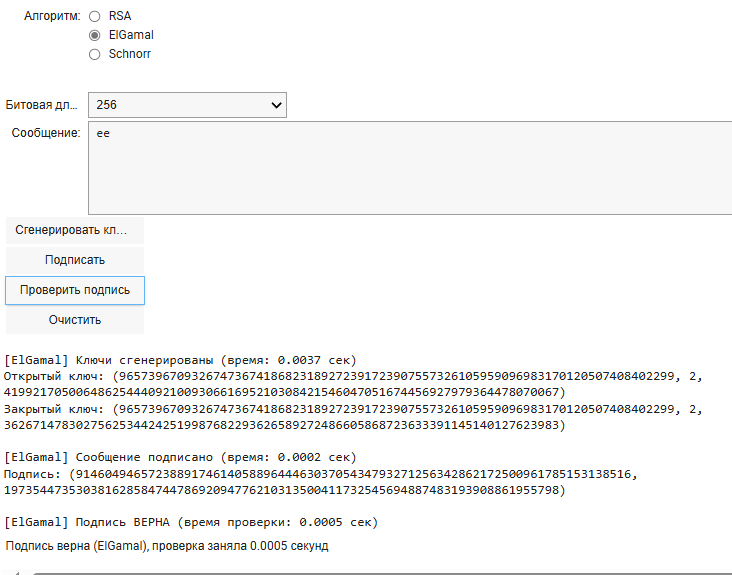


Рисунок 2.2 – Результат работы приложения для ElGamal

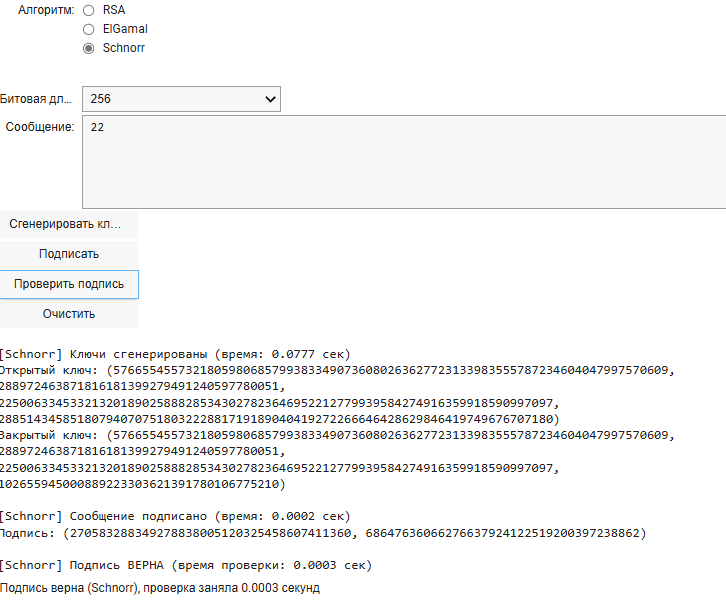


Рисунок 2.3 – Результат работы приложения для Schnorr

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 2.4.

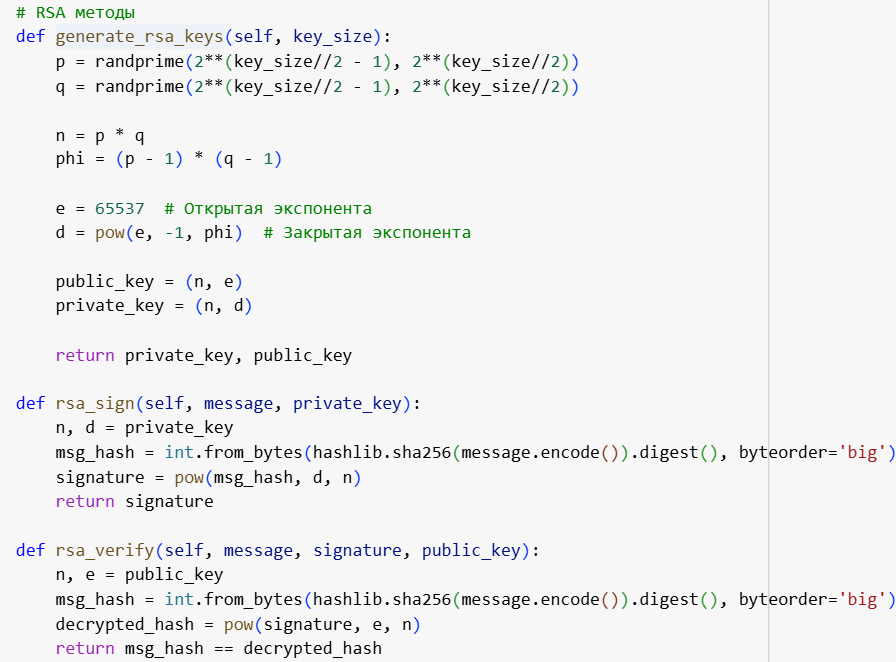


Рисунок 2.4 – Реализация функции RSA

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 2.5.

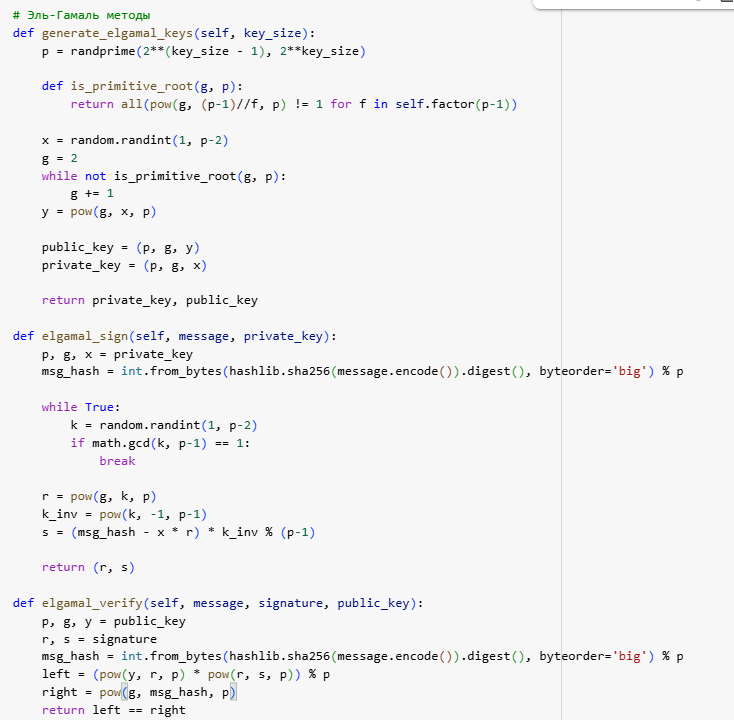


Рисунок 2.5 – Реализация функции Crypt

Создание ЭЦП на основе Шнорра происходит в функции Do класса Shnorr. Реализация функции представлена на рисуке 2.6.

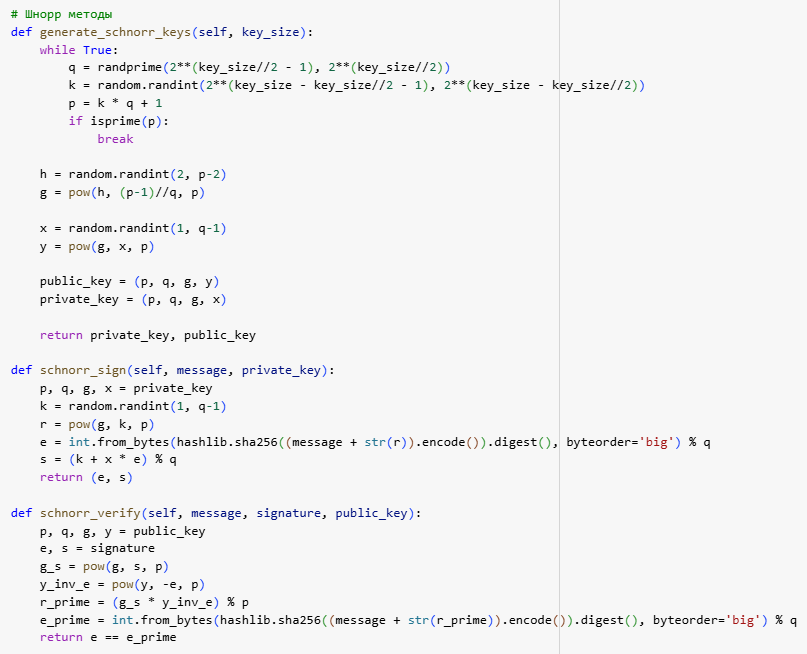


Рисунок 2.6 – Реализация функции Do

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.

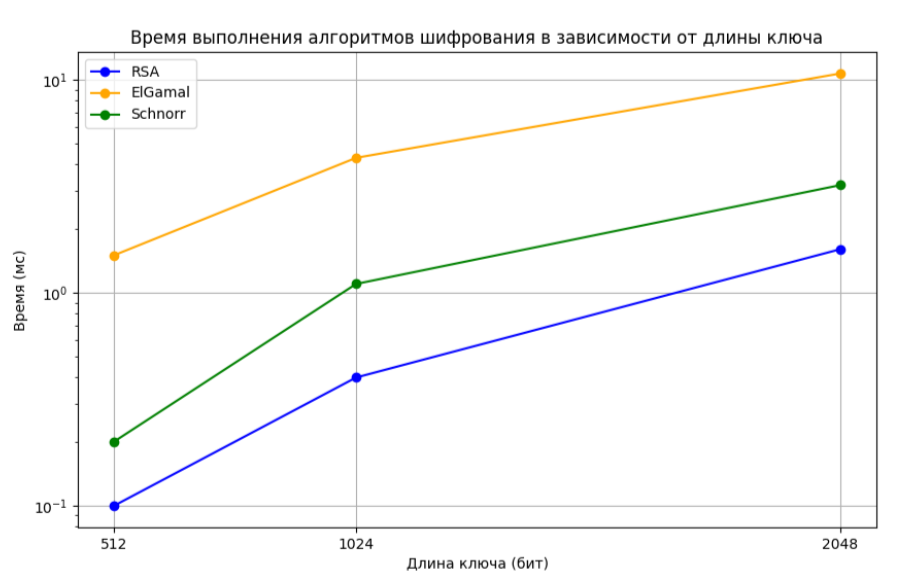


Рисунок 2.7 – зависимость времени от требований к ключу

1. **RSA**: Время растёт, но не так быстро, как у других алгоритмов.
2. **Schnorr**: Время увеличивается быстрее, чем у RSA, особенно на длинных ключах.
3. **ElGamal**: Время наибольшее среди трёх алгоритмов, заметно растёт с увеличением длины ключа.

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.