Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование алгоритмов генерации**

**и верификации электронной цифровой**

**подписи**

Студент: Гвоздовский К.В.

ФИТ 3 курс 6 группа

Преподаватель:

Нистюк Ольга Александровна

1. **Цель работы**

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

1. **Задание**
2. Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться результатами выполнения предыдущих лабораторных работ, а также доступными библиотеками либо программными кодами. Приложение должно реализовывать генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра, оценку времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах. Для вычисления хешей можно также воспользоваться доступными online-средствами, например katvin (https://katvin.com/tools/hash-generator.html).
3. Для выполнения необходимых операций передачи (по сети)/верификации информации обменяться открытой ключевой информацией с получателем подписанного сообщения для каждого исследуемого алгоритма (по согласованию с преподавателем).
4. **Ход работы**

**Теоретические сведения**

Математические основы асимметричных шифров

Электронная цифровая подпись (ЭЦП) – важный элемент 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.

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.

Основным компонентом в технологии ЭЦП является ключ.

В соответствии с этим обстоятельством перечисленные выше 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).

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.

ЭЦП на основе хешей подписываемых сообщений

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь ), а его хеша, H(), что позволяет:

– сокращает время генерации/верификации подписи;

– снизить вероятность ошибок в итоговом документе.

Общая структура подписанного документа – – представляет конкатенацию этого документа и ЭЦП *S*. И еще может конкатенироваться служебная информация (дата, время отправки, информация об отправителе).

Важное свойство цифровой подписи: её может проверить каждый, кто имеет доступ к *открытому ключу* её автора.

Если – подпись подлинная и документ целостный, что значит, что где – полученный документ, – исходный документ.

При генерации ЭЦП (по классической схеме) для сообщения *М* отправитель последовательно выполняет следующие действия:

– вычисляет хеш (хеш-образ) сообщения *М*: *Н*(*М*);

– вычисляет содержание ЭЦП (собственно ЭЦП *S*) по хешу *Н(М)* с использованием своего закрытого ключа *d*: *S* = (*Н*(*М*));

– присоединяет (конкатенирует) ЭЦП к сообщению М и некоторой служебной информации, создавая таким образом итоговое сообщение *М'*;

–  посылает сообщение *М'* получателю;

Получив сообщение *М'*, другая сторона последовательно выполняет следующие действия:

– отделяет цифровую подпись *S* от сообщения *М* (для общего случая применим одинаковые символьные обозначения);

– применяет к сообщению М операцию хеширования, используя ту же функцию, что и отправитель, и получает хеш-образ полученного сообщения;

– используя открытый ключ отправителя, расшифровывает S, т. е. извлекает из ЭЦП хеш-образ отправленного сообщения;

– проверяет соответствие (равенство) обоих хеш-образов, и если они совпадают, то отправитель действительно является тем, за кого себя выдает, а сообщение при передаче не подверглось искажению.

Необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

**Практическая часть**

* 1. **ЭЦП на основе RSA**

Цифровая подпись S вычисляется на основе известного соотношения:

, *dо* и *no* – элементы тайного ключа отправителя. Передаваемое сообщение *М' = Мo || S*.

Соответственно, операция расшифрования на приемной стороне (получатель анализирует *Мп* || *S*) будет производиться в соответствии с формулой с известной модификацией ключей: . Далее вычисляется *Н*(*Mп*). Если *H(Mo)* = *H(Mп)*, подпись верифицирована.

Код для создания и верификации ЭЦП на основе RSA представлен в классе RSA в методах CreateDigitalSignature и VerifyDigitalSignature, которые представлены на рисунках 3.1.1 и 3.1.2.

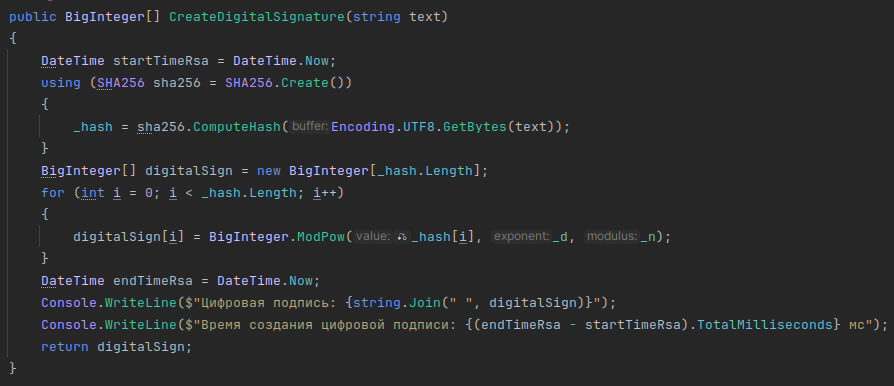


Рисунок 3.1.1 – Метод CreateDigitalSignature для создания ЭЦП на основе RSA



Рисунок 3.1.2 – Метод VerifyDigitalSignature для верификации ЭЦП на основе RSA

Результат работы этих функций представлен на рисунке 3.1.3.

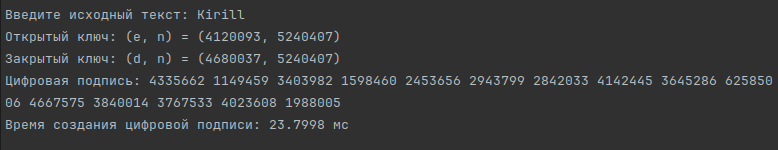


Рисунок 3.1.3 – Результат работы класса RSA

* 1. **ЭЦП Эль-Гамаля**

Ключевая информация отправителя: открытый ключ: *y*, *g* и *р*; тайный ключ: *х*. Чтобы подписать сообщение *Мо*, обладатель используемых для ЭЦП ключей должен выбрать, как и в предыдущей схеме, случайное число *k*, взаимно простое с (*р* – 1). Затем вычисляется числа *а* и *b*, являющиеся цифровой подписью (*S* = {*a*, *b*}):

*a ≡ gk*mod *p*.

Для вычисления *b* с помощью расширенного алгоритма Евклида решается уравнение:

*Н*(*Mо*) ≡ (*x  a* + *k  b*) mod (*p* – 1).

Получателю отправляется сообщение *М*' = *Мо* || *S*. Для верификации подписи вычисляется хеш полученного сообщения *Н*(*Мп*) = *h*. Далее нужно убедиться, что выполняется равенство:

*yaab* ≡ *gh* mod *p*.

Если равенство выполняется, подпись верифицируется.

Код для создания и верификации ЭЦП Эль-Гамаля представлен в классе ElGamal в методах CreateDigitalSignature и VerifyDigitalSignature, которые представлены на рисунках 3.1.1 и 3.1.2.

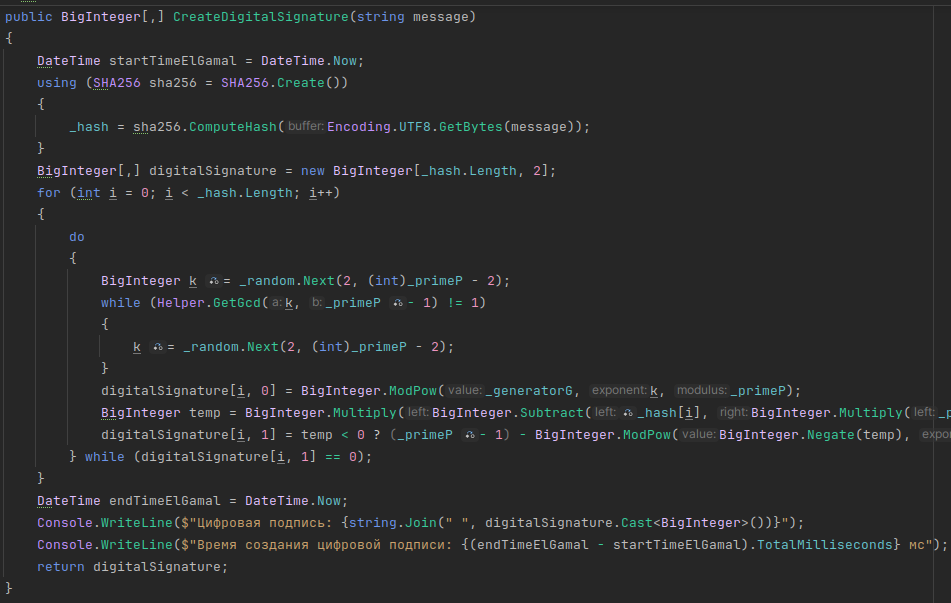


Рисунок 3.2.1 – Метод CreateDigitalSignature для создания ЭЦП Эль-Гамаля

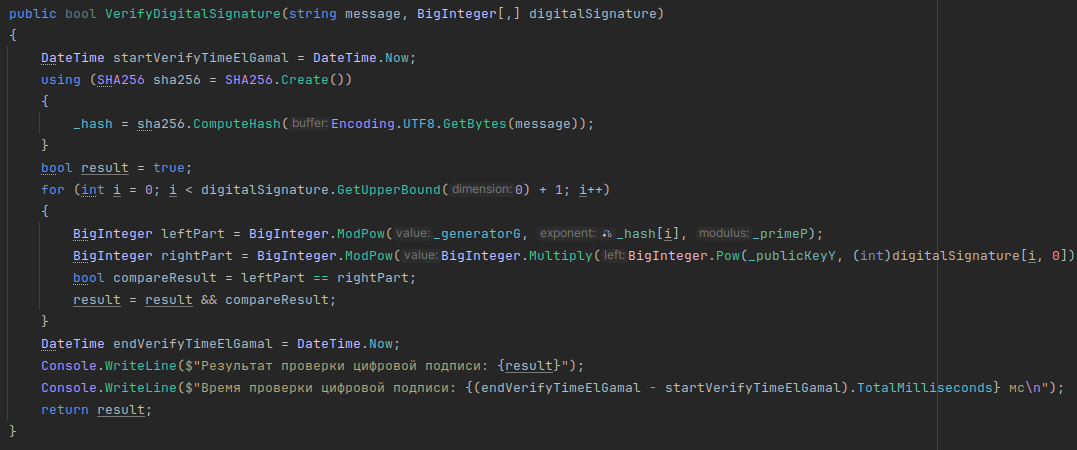


Рисунок 3.2.2 – Метод VerifyDigitalSignature для верификации ЭЦП Эль-Гамаля

Результат работы этих функций представлен на рисунке 3.2.3.

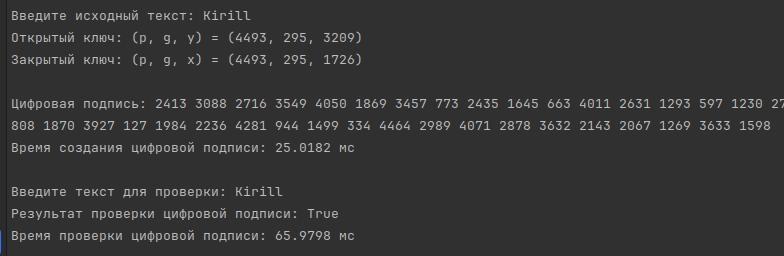


Рисунок 3.2.3 – Результат работы класса ElGamal

* 1. **ЭЦП Шнорра**

Ключевая информация: *p* – простое число в диапазоне от 512 до 1024 битов; *q* –160-битное простое число, делитель (p – 1); любое число g (g ≠ 1) такое, что *gq* ≡ 1 mod *p*.

Выбирается число *х* < *q* (*х* является тайным ключом) и вычисляется последний элемент открытого ключа: *y* ≡ *g–х* mod *p*.

Для подписи сообщения *Мо*выбирается случайное число *k* (1 < k < q) и вычисляет параметр а: *а* ≡ *gk* mod *p*.

Далее вычисляется хеш от конкатенации сообщения *Мо* и числа *а*: *h* = *H*(*Mo*||*a*). Создается хеш-образ подписываемого сообщения, спереди присоединенного к числу *а*. Далее вычисляется значение *b*: *b* ≡ (*k* + *x  h*) mod *q*.

Получателю отправляются *М'* = *Мо || S*; *S* = {*h*, *b*}.

Для проверки подписи получатель вычисляет *Х* ≡ *gbyh*(mod *p*).

Затем он проверяет выполнение равенства: *h* = *Н*(*Mп*||*Х*). Подпись достоверна, если равенство выполняется.

Код для создания и верификации ЭЦП Шнорра представлен в классе Schnorr в методах GenerateDigitalSignature и VerifyDigitalSignature, которые представлены на рисунках 3.1.1 и 3.1.2.



Рисунок 3.3.1 – Метод GenerateDigitalSignature для создания ЭЦП Шнорра

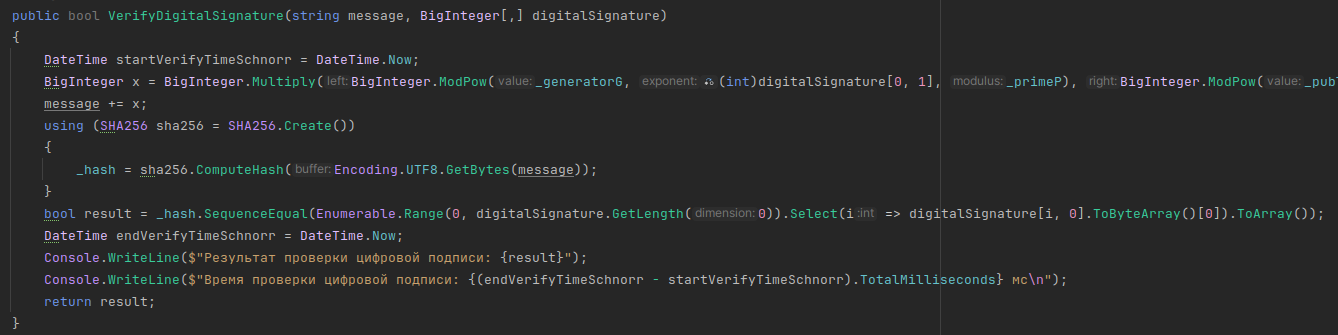


Рисунок 3.3.2 – Метод VerifyDigitalSignature для верификации ЭЦП Шнорра

Результат работы этих функций представлен на рисунке 3.3.3.

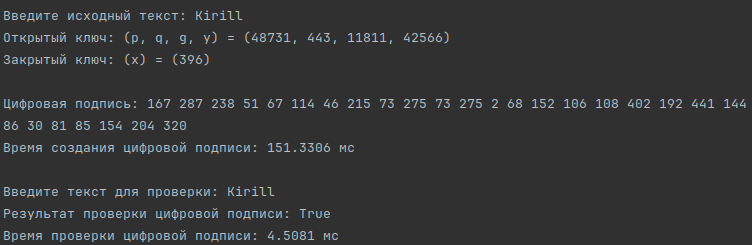


Рисунок 3.3.3 – Результат работы класса Schnorr

* 1. **Оценка времени**

Так же нужно было оценить скорость генерации и верификации ЭЦП на основе этих алгоритмов. Результаты представлены на рисунках 3.4.1 и 3.4.2.

Рисунок 3.4.1 – Скорость генерации ЭЦП

Рисунок 3.4.2 – Скорость верификации ЭЦП

Из графиков видно, что RSA имеет более быструю скорость создания и верификации ЭЦП по сравнению с ElGamal и Schnorr. ElGamal и Schnorr обладают более высокой вычислительной сложностью и требуют больше времени для создания и верификации ЭЦП. Время создания и верификации ЭЦП во всех трех алгоритмах увеличивается с увеличением количества символов.

Такие результаты обусловлены тем, что в RSA процесс создания ЭЦП включает операцию возведения в степень с большими числами и вычисление модуля. Однако, RSA позволяет выбрать маленькую экспоненту для ускорения операций и получения более быстрой скорости создания ЭЦП, в то время как в ElGamal используется операция возведения в степень с большими числами, а также вычисление модуля и умножение, а Schnorr имеет более сложный процесс создания ЭЦП, включающий операции с большими числами, такие как умножение, сложение и вычисление хеш-функций. Эти операции требуют значительно больше вычислительных ресурсов и занимают больше времени, особенно при увеличении количества символов.

**Вывод**

В ходе лабораторной работы были изучены алгоритмы генерации и верификации электронной цифровой подписи и приобретены практические навыки их реализации. Кроме того, был сделан вывод о скорости генерации и верификации ЭЦП с помощью различных алгоритмов.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.