МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №12**

**″Исследование алгоритмов генерации и электронной цифровой подписи″**

Выполнила студент 3 курса 7 группы Антончиков М.В.

Проверила: Копыток Д.В.

Минск 2021

**Цель**: изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП).
* Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра, а также DSA.
* Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.
* Оценить скорость генерации и верификации ЭЦП.
* Оценить скорость зашифрования/расшифрования реализованных способов шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** Понятие «электронная цифровая подпись» было введено в 1976 году У. Диффи и М. Хеллманом. 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 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; указанная бинарная последовательность зависит от содержания подписываемого сообщения. Основным компонентом в технологии ЭЦП является ключ. Принадлежность ключа, в предположении, что он известен только законным пользователям, позволяет решать все «возложенные на ЭЦП», сформированную на основе этого ключа, задачи. 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). Первый из перечисленных методом ничем не отличается, например, от DES. Во втором случае создаются, по существу, две симметричные системы: между отправителем и посредником и между посредником и получателем. Причем посредник выдает двум сторонам различный тайный (для иных субъектов системы) ключ. Во последнем случае сообщение, отправляемое получателю, шифруется тайным ключом отправителя. Отправитель же верифицирует подпись (в данном случае – устанавливает авторство, используя для расшифрования публичный ключ отправителя, и получает гарантию в защищенности переданного сообщения от подделок, если после расшифрования формат и содержание документа имеют логическую стройность) с помощью открытого ключа отправителя. Таким образом, в этом случае, как и в первых двух случаях, ЭЦП, как отдельный, самостоятельный, присоединенный к исходному документу элемент получаемого сообщения, отсутствует. Кроме, того, в отличие от классической асимметричной криптографии, где используется ключевая информация получателя, в нашем случае используется ключевая информация отправителя: открытый ключ – для зашифрования, тайный – для расшифрования.

С учетом изложенного можем сформулировать определение ЭЦП в несколько ином виде. 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. Основу рассматриваемых протоколов составляют методы асимметричной криптографии и эллиптических кривых. Общая структура подписанного электронного документа Мо – 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. На рисунке 1 показан в общем виде порядок процесса верификации (без учета использования служебной информации).

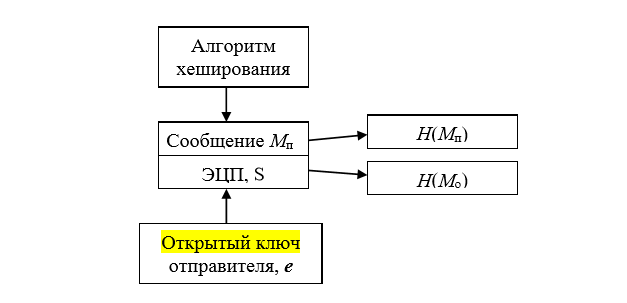


Рис. 1 – Общая схема верификации ЭЦП

Заметим, что в общем случае версии исходного документа (Мо) и полученного (Мп) могут отличаться. Если в результате устанавливается равенство хешей: Н(Мп) = Н(Мо), то принимается решение о подлинности подписи и целостности документа Мп, т. е. это также означает, что Мп = Мо. 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 = Сd(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.

**Задание.** В данной лабораторной работе необходимо было разработать авторское приложение в соответствии с целью лабораторной работы. Приложение реализует генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра и оценку времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах.

**ЭЦП на основе RSA.** Подпись S вычисляется на основе известного соотношения: S = (H(Mo)) dо mod no, где dо и no – элементы тайного ключа отправителя. Передаваемое сообщение М' = Мo||S.

Функция, реализующая генерацию ЭЦП на основе RSA, представлена на рисунке 2.

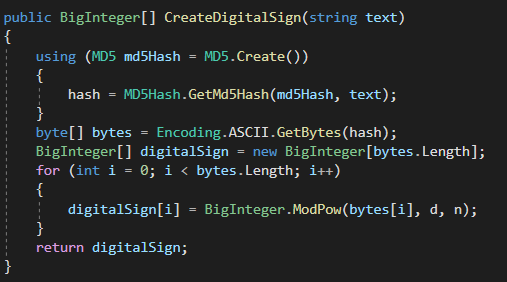


Рис. 2 – Функция генерации ЭЦП на основе RSA

Соответственно, операция расшифрования на приемной стороне (получатель анализирует Мп||S) будет производиться в соответствии с формулой с известной модификацией ключей: H(Mo) = (S)ео mod no. Далее вычисляется Н(Mп). Если H(Mo) = H(Mп), подпись верифицирована.

Функция, верифицирующая подпись, представлена на рисунке 3.

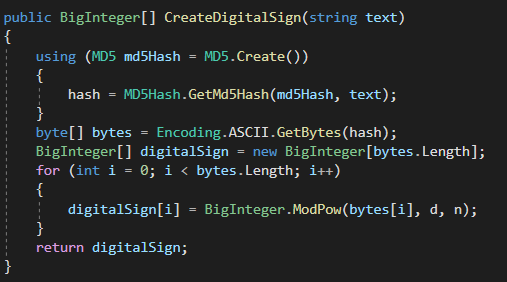


Рис. 3 – Функция верификации подписи на основе RSA

**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 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) = (xa + kb) mod (p-1). Получателю отправляется сообщение М' = Мо||S.

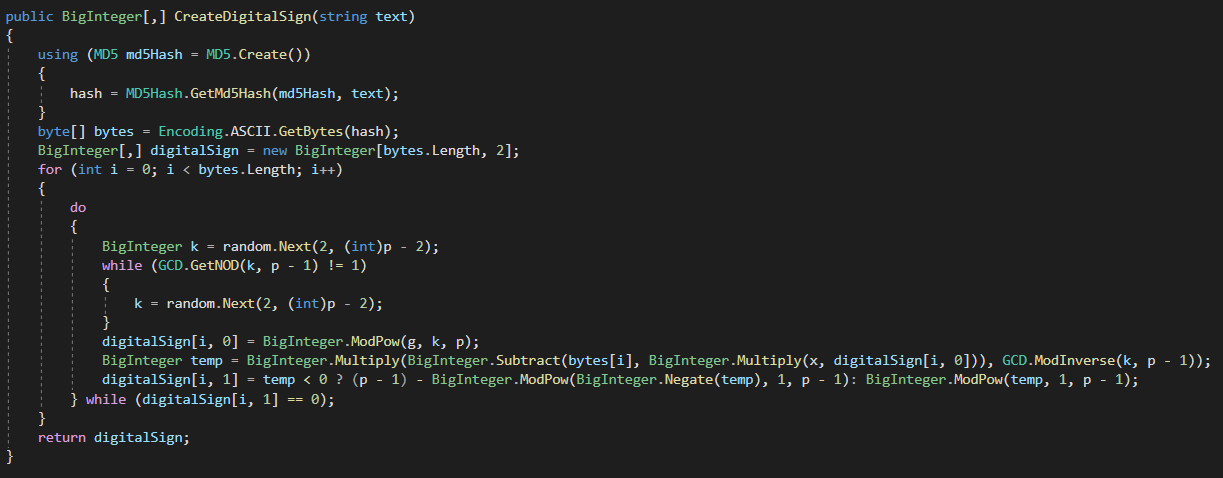


Рис. 4 – Функция генерации ЭЦП Эль-Гамаля

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

Функция, верифицирующая подпись, представлена на рисунке 5.

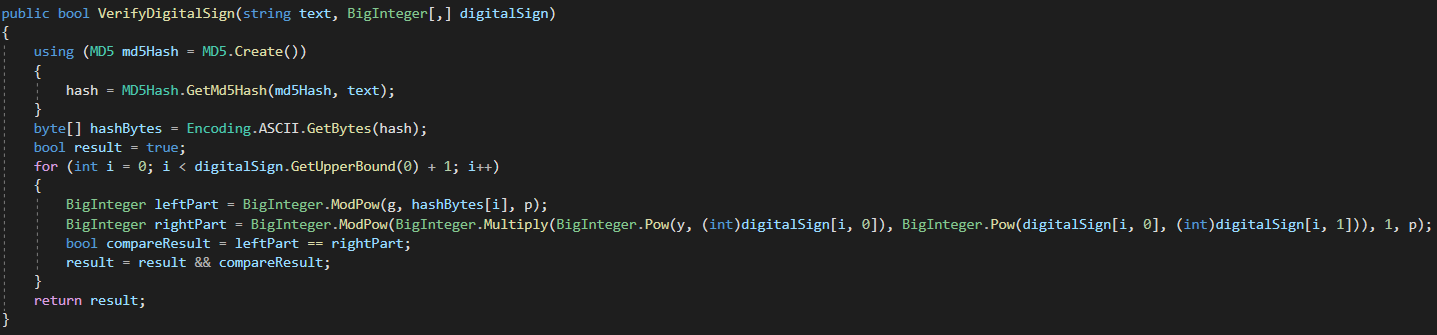


Рис. 5 – Функция верификации подписи Эль-Гамаля

**ЭЦП Шнорра.** Рассматриваемая схема является основой стандарта ЭЦП в Беларуси. Алгоритм ЭЦП К. Шнорра (К. Schnorr ) является вариантом алгоритма ЭЦП Эль-Гамаля. Одной из особенностей ЭЦП Эль-Гамаля является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуется длина p, по крайней мере, должна составлять 1024 бита. Чтобы уменьшить размер подписи, Шнорр предложил новую схему, но с уменьшенным размером подписи. Ключевая информация: p – простое число в диапазоне от 512 до 1024 бит; q –160-битное простое число, делитель p-1; любое число g (g≠1) такое, что gq=1 mod p. Числа p, g, q являются открытыми и могут применяться группой пользователей. Выбирается число х<q (х является тайным ключом) и вычисляется последний элемент открытого ключа: y = g-х mod p. (10.9) Секретный ключ имеет длину не менее 160 бит. Для подписи сообщения Мо выбирается случайное число k (1<k<q) и вычисляет параметр а: а = gk mod p. (10.10) 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 + xh) mod q. Получателю отправляются М' = Мо||S; S = {h, b}.

Функция, реализующая генерацию ЭЦП Шнорра, представлена на рисунке 6.

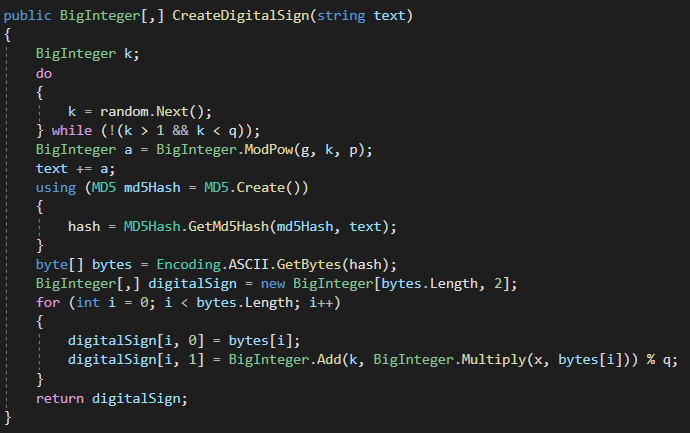


Рис. 6 – Функция генерации ЭЦП Шнорра

Для проверки подписи получатель вычисляет Х = gb yh (mod p).

Затем он проверяет выполнение равенства: h = Н(Mп||Х). Подпись достоверна, если равенство выполняется. Основные вычисления для генерации подписи могут производиться предварительно. Порядок величин х и h – около 140 двоичных разрядов, порядок числа k – около 70-72 разрядов. С учетом этого сложность операций умножения можно считать ничтожно малой по сравнению с модульным умножением в схеме RSA.

Функция, верифицирующая подпись, представлена на рисунке 7.

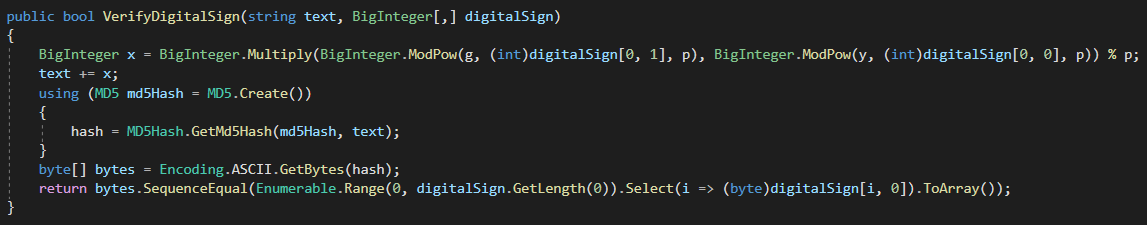


Рис. 7 – Функция верификации подписи Шнорра

Результаты работы приложения представлены на рисунке 8.

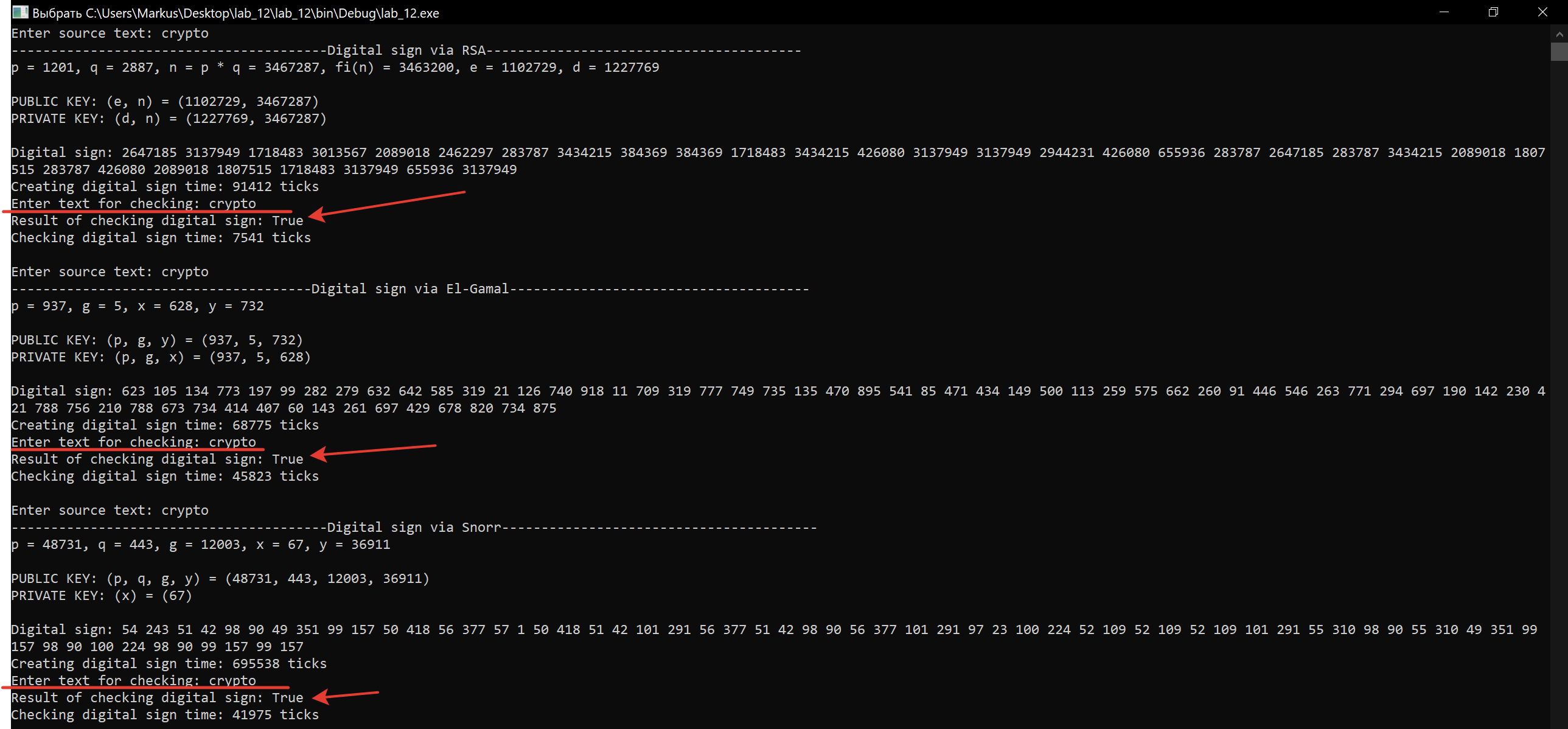


Рис. 8 – Результаты работы приложения

**Вывод:** в результате данной лабораторной работы было разработано приложение для генерации и верификации ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра. Также были проведены анализы криптостойкости и замеры времени работы алгоритмов.