Министерство образования Республики Беларусь
Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина «Методы защиты информации»

Отчет
к лабораторной работе №6

Выполнил:
студент гр.653501
Тимофеев К. А.

Проверил:
Артемьев В.С.

Минск, 2019

Введение

В лабораторной работе необходимо было реализовать программное формирования и проверки ЭЦП на основе алгоритма ГОСТ 3410.

Электро́нная по́дпись (ЭП), **Электро́нная цифровая по́дпись** (ЭЦП), **Цифровая подпись** (ЦП) позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в криптовалютной системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования.

ЭЦП — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Широко применяемая в настоящее время технология электронной подписи основана на асимметричном шифровании с открытым ключом и опирается на следующие принципы:

- Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. Механизм генерации ключей строго определён и является общеизвестным. При этом каждому открытому ключу соответствует определённый закрытый ключ. Если, например, Иван Иванов публикует свой открытый ключ, то можно быть уверенным, что соответствующий закрытый ключ есть только у него.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.
- Если электронный документ поддается расшифровке с помощью открытого ключа, то можно быть уверенным, что он был зашифрован с помощью уникального закрытого ключа. Если документ расшифрован с помощью открытого ключа Ивана Иванова, то это подтверждает его авторство: зашифровать данный документ мог только Иванов, т.к. он является единственным обладателем закрытого ключа.

Однако шифровать весь документ было бы неудобно, поэтому шифруется только его хеш - небольшой объём данных, жёстко привязанный к документу

с помощью математических преобразований и идентифицирующий его. Шифрованный хеш и является электронной подписью.

Описание алгоритма

Для реализации формирования и проверки цифровой подписи под сообщением необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи. Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи Q(xq, yq).

Формирование цифровой подписи: Для получения цифровой подписи под сообщением MϵV* необходимо выполнить следующие действия (шаги) по алгоритму:

- Шаг 1 – вычислить хэш–код сообщения M:$\bar{h}$=h(M)
- Шаг 2 – вычислить целое число a, двоичным представлением которого является вектор $\bar{h}$, и определить: e≡a(mod q) Если e=0, то определить e=1.
- Шаг 3 – сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству: 0<k<q
- Шаг 4 – вычислить точку эллиптической кривой C=kP и определить r≡x_c (mod q)
  где x_c – x-координата точки C.
  Если r=0, то вернуться к шагу 3.
- Шаг 5 – вычислить значение: s≡(rd+ke)(mod q)
  Если s=0, то вернуться к шагу 3.
- Шаг 6 – вычислить двоичные векторы $\bar{r}$ и $\bar{s}$, соответствующие r и s, и определить цифровую подпись $\zeta = (\bar{r}||\bar{s})$ как конкатенацию двух двоичных векторов. Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом – цифровая подпись ζ.

Проверка цифровой подписи: Для проверки цифровой подписи ζ под полученным сообщением M необходимо выполнить следующие действия (шаги) по алгоритму:

- Шаг 1 – по полученной подписи ζ вычислить целые числа r и s. Если выполнены неравенства 0 < r < q, 0 < s < q, то перейти к следующему шагу. В противном случае подпись неверна.
- Шаг 2 – вычислить хэш–код полученного сообщения M: $\bar{h}$=h(M)
- Шаг 3 – вычислить целое число a, двоичным представлением которого является вектор $\bar{h}$ и определить e≡a(mod q) Если e=0, то определить e=1.
- Шаг 4 – вычислить значение v≡e^(-1) (mod q)

- Шаг 5 – вычислить значения $z_1 \equiv sv \pmod q, z_2 \equiv -rv \pmod q$
- Шаг 6 – вычислить точку эллиптической кривой $C=z_1 P+z_2 Q$ и определить $R \equiv x_c \pmod q$
  где x_c – x–координата точки C.
- Шаг 7 – если выполнено равенство R=r, то подпись принимается, в противном случае - подпись неверна.
  Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись ζ и ключ проверки подписи Q, а выходным результатом – свидетельство о достоверности или ошибочности данной подписи.

Эллиптическая кривая Для описания кривой в стандарте NIST используется набор из 6 параметров D=(p,a,b,G,n,h), где:

- p — простое число, модуль эллиптической кривой;
- a, b — задают уравнение эллиптической кривой $y^2=x^3+ax+b$;
- G — точка эллиптической кривой большого порядка (это означает что, если умножать точку на числа меньшие, чем порядок точки, каждый раз будут получаться совершенно различные точки);
- n — порядок точки G;
- h — параметр, называемый кофактор. Определяется отношением общего числа точек на эллиптической кривой к порядку точки G. Данное число должно быть как можно меньше.

Хэш-функция В данном алгоритме цифровой подписи используется хэш-функция «Стрибог» обладающая следующими качествами:

- Не имеет свойств, которые позволяли бы применить известные атаки;
- Вычисление хэш-функции занимает мало времени;
- Каждое используемое в хэш-функции преобразование отвечает за определенные криптографические свойства;
- Требования, касающиеся трудоемкости атак на хэш-функцию.

Параметры: В работе использована следующая эллиптическая кривая, рекомендованная NIST, в которой значения параметров соответственно равны:

- p=6277101735386680763835789423207666416083908700390324961279;
- a=-3;
- b=245515554600894381774029391519745178476910805816119123806 5;
- xG=602046282375688656758213480587526111916698976636884684818 (x-координата точки G);

- yG=174050332293622031404857552280219410364023488927386650641 (y-координата точки G);
- n=6277101735386680763835789423176059013767194773182842284081;
- h=1.

Блок-схема алгоритма

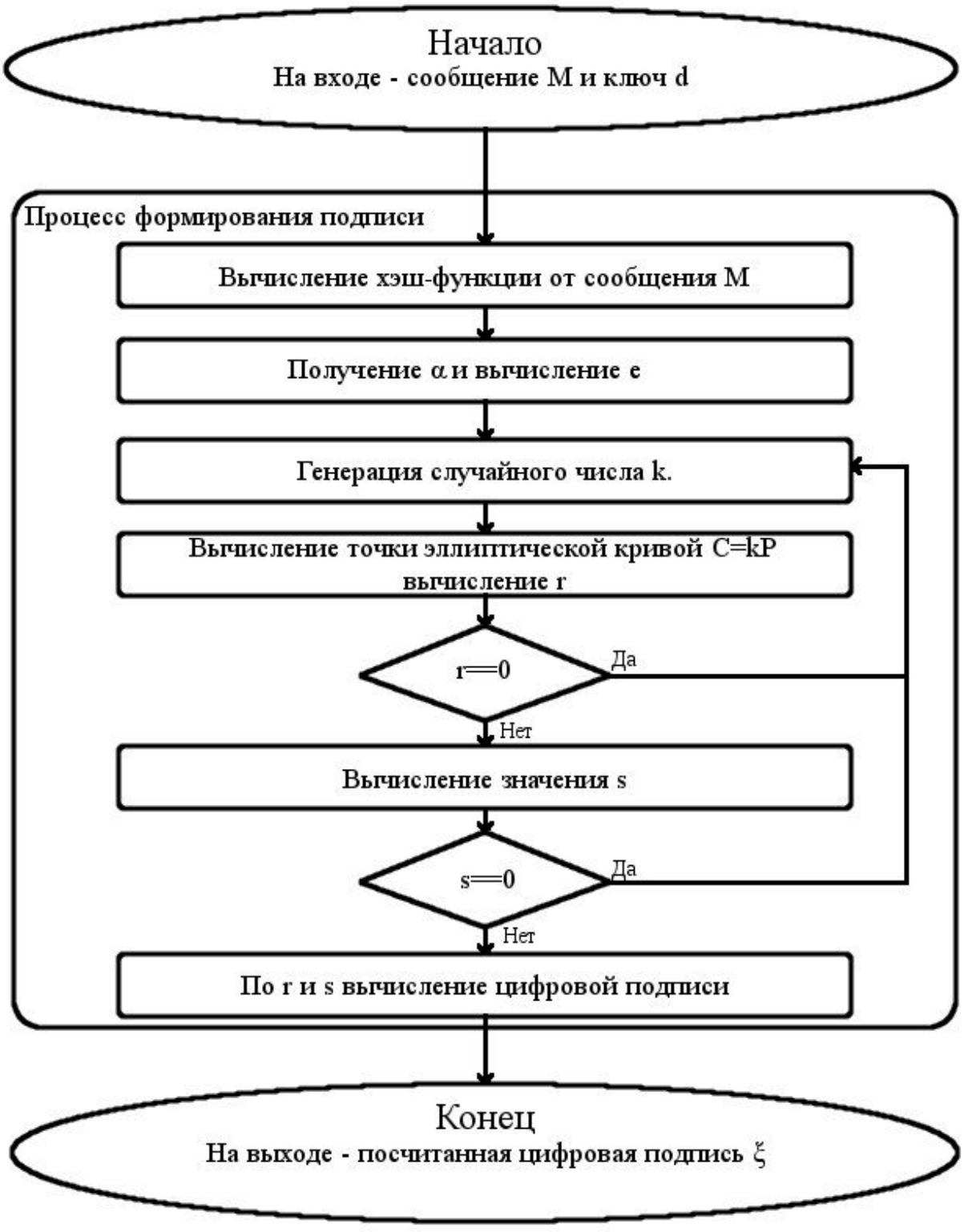

Рис.1 Блок-схема алгоритма формирования ЭЦП

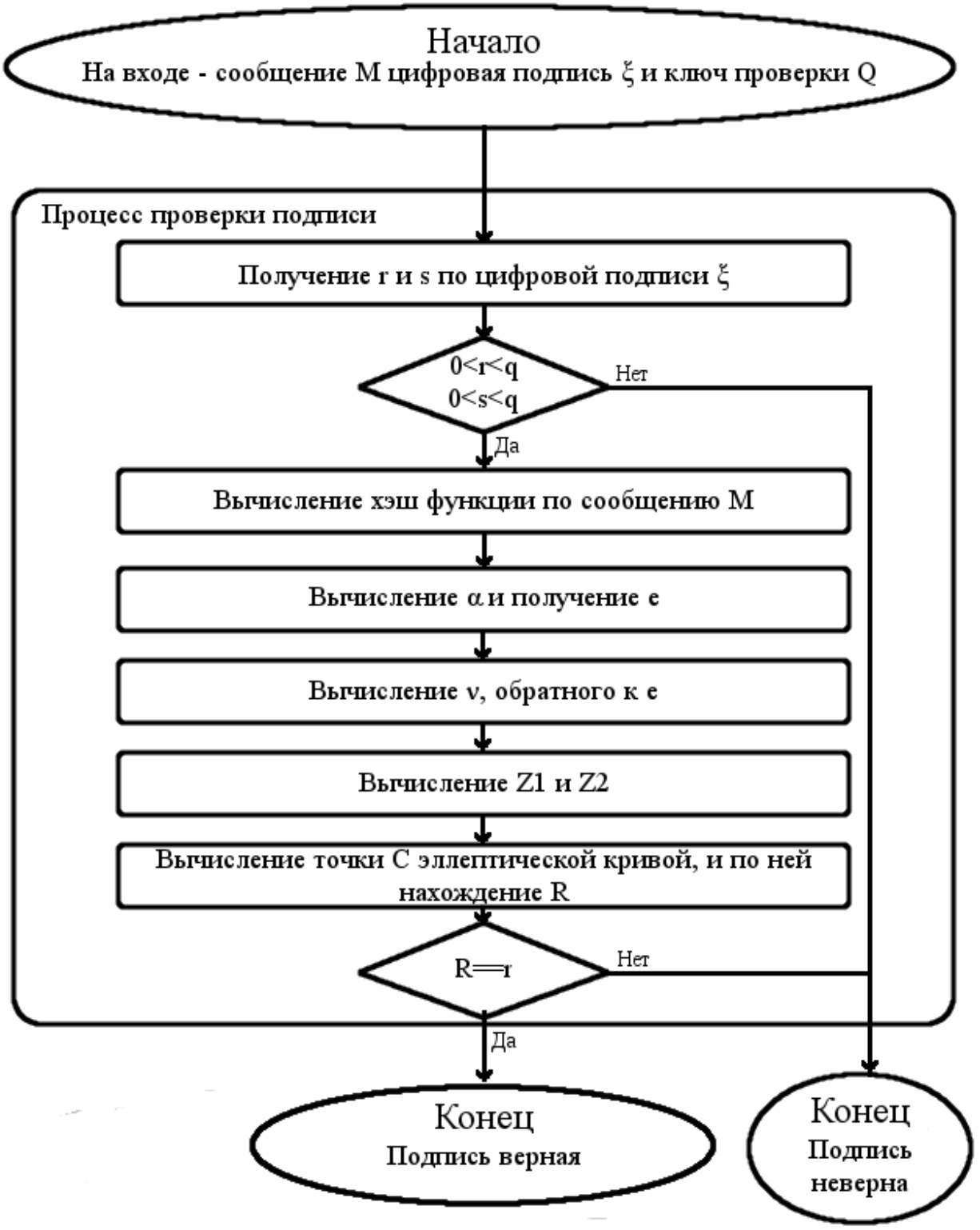

Рис.2 Блок-схема алгоритма проверки ЭЦП

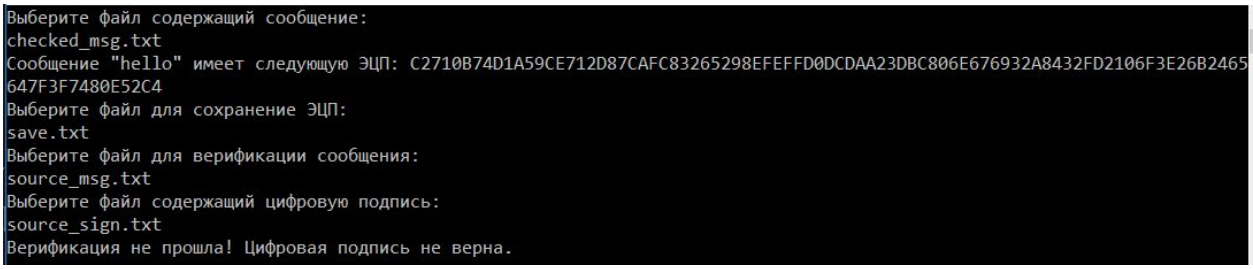

Рис.2 Результат ввода данных и исполнения программы

Вывод

Свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

- Использование в банковских платежных системах.
- Электронная коммерция (торговля).
- Электронная регистрация сделок по объектам недвижимости.
- Таможенное декларирование товаров и услуг (таможенные декларации). Контролирующие функции исполнения государственного бюджета (если речь идет о стране) и исполнения сметных назначений и лимитов бюджетных обязательств (в данном случае если разговор идет об отрасли или о конкретном бюджетном учреждении). Управление государственными заказами.
- В электронных системах обращения граждан к органам власти, в том числе и по экономическим вопросам (в рамках таких проектов как «электронное правительство» и «электронный гражданин»).
- Формирование обязательной налоговой (фискальной), бюджетной, статистической и прочей отчетности перед государственными учреждениями и внебюджетными фондами.
- Организация юридически легитимного внутрикорпоративного, внутриотраслевого или национального электронного документооборота.
- Применение ЭЦП в различных расчетных и трейдинговых системах, а также Forex.
- Управление акционерным капиталом и долевым участием.
- ЭП является одним из ключевых компонентов сделок в криптовалютах.