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
По дисциплине «Методы защиты информации»
По теме «Цифровая подпись»

Выполнил:
студент гр.653501
Хамицевич Ф. С.

Проверил:
Артемьев В.С.

Минск, 2019

Введение

Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Электронно-цифровая подпись - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Использование электронно-цифровой подписи позволяет:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

построить корпоративную систему обмена документами.

Блок-схема алгоритма

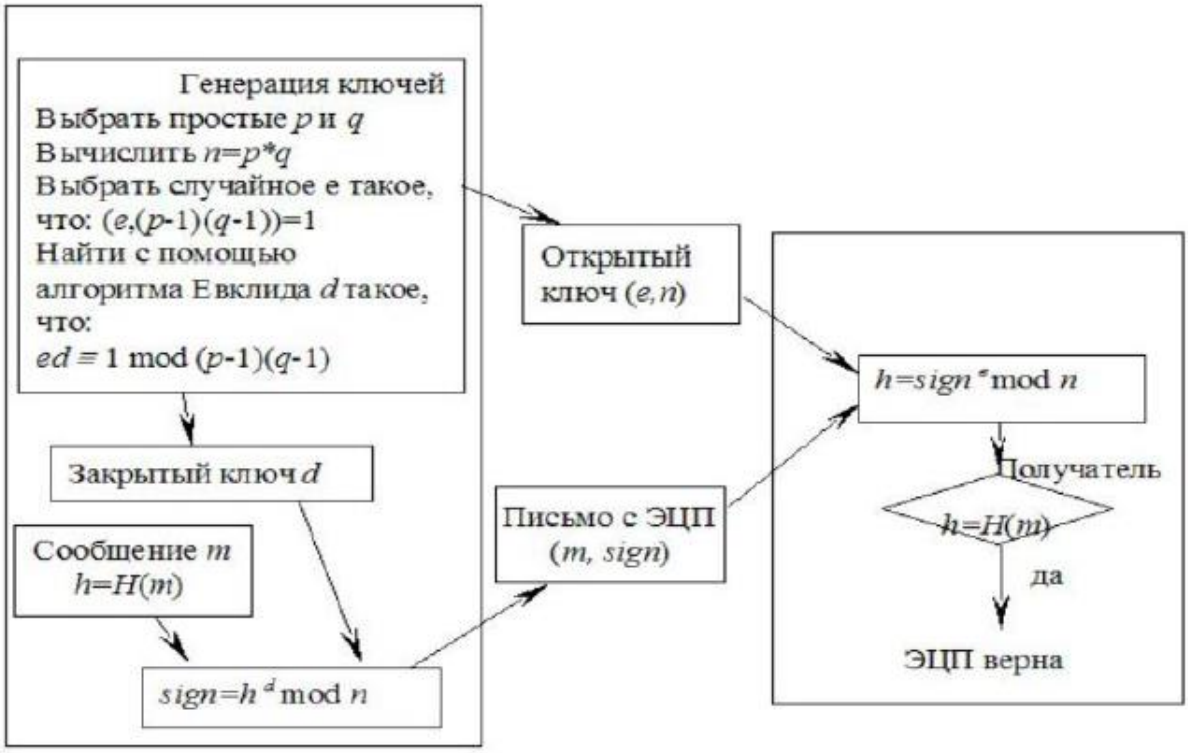

Рисунок 1. Блок-схема ЭЦП на основа RSA.

Пример работы программы

Зашифруем сообщение «Source msg to encrypt» (см. Рис. 2), сгенерированный приватный ключ – это (35, 391), а публичный – это (171,

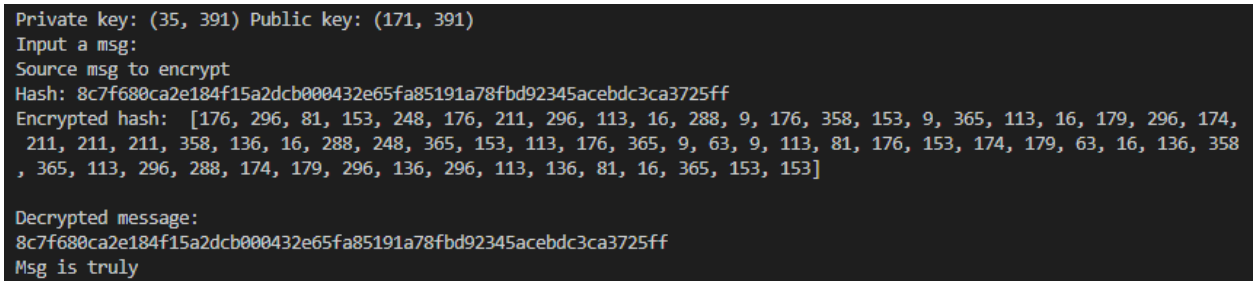

Рисунок 2. Пример работы программы.

Далее было выведено зашифрованное сообщение и информация о том, что оно достоверно.

Вывод

Электронная цифровая подпись позволяет удостовериться что документ во время пересылки не был изменен намеренно либо случайно, что позволяет доверять тому что написано в документе подтвержденной Электронная цифровая подпись.