Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №6

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

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

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.

Алгоритм

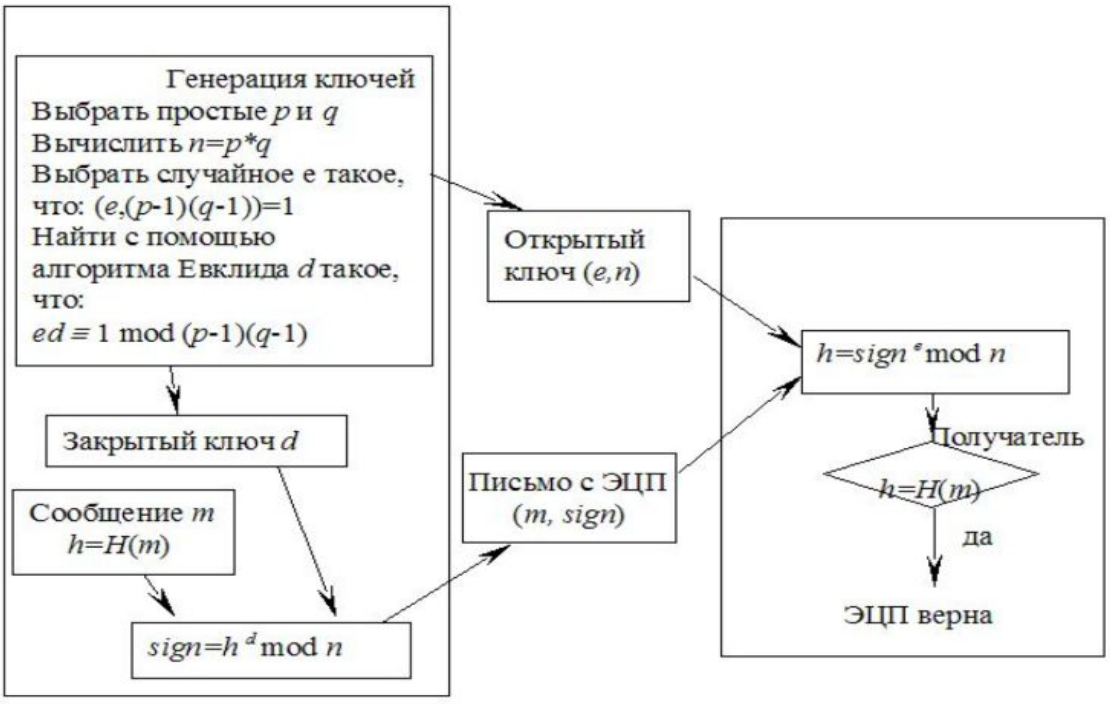

рис. 1 Схема ЭЦП на основе RSA

Результат работы программы

```
maxim@maxim-FX503VD  ~/MZI  master  /usr/bin/python3.7 /home/maxim/MZI/Lab6/digital_signature.py
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137
, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281
, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449
, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619
, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811
, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997
]
Выберите два числа из представленных выше 41, 59
Приватный ключ: (1117, 2419) Общедоступный ключ: (2293, 2419)
Введите сообщение
qwert
Полученный хэш 9e69e7e29351ad837503c44a5971edebc9b7e6d8601c89c284b1b59bf37afa80
Полученый зашифрованый хэш:  [2101, 680, 1365, 2101, 680, 1831, 680, 1649, 2101, 223, 253, 1187, 2274, 816, 306, 223, 1831, 253, 1077,
223, 486, 1161, 1161, 2274, 253, 2101, 1831, 1187, 680, 816, 680, 338, 486, 2101, 338, 1831, 680, 1365, 816, 306, 1365, 1077, 1187, 486
, 306, 2101, 486, 1649, 306, 1161, 338, 1187, 338, 253, 2101, 338, 1058, 223, 1831, 2274, 1058, 2274, 306, 1077]

Your decrypted message is:
9e69e7e29351ad837503c44a5971edebc9b7e6d8601c89c284b1b59bf37afa80
Подлино
```

Вывод

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