**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

**Цель: изучить и закрепить умение реализации ЭЦП на примере RSA.**

Разберем наглядный «бумажный» пример и пример с кодом. Возьмем основу 6-ой лабораторной работы.

**«Бумажный» пример**

p = 89

q = 17

Сообщение: AAC

n = p \* q = 89 \* 17 = 1513

f(n) = (p - 1) \* (q - 1) = 88 \* 16 = 1408

e = 5;

Открытый ключ шифра: (5, 1513)

http://altaev-aa.narod.ru/security/images/im7.png

d вычисляется до тех пор, пока не получится первое целое число.

Причем k = 1, 2, 3 …

При k = 1, d – не целое число,

При k = 2, d – не целое число,

При k = 3, d = 845

Тогда закрытый ключ шифра: (845, 1513).

*Отправка сообщения и электронной подписи:*

Отправка сообщения и ЭЦП на базе алгоритма RSA (отправитель **A**).



Возьмем хеш-образ из примера h = 7.

Тогда цифровая подпись s = 7^845 mod 1513 = 1485

Далее получателю отправляется исходное сообщение и цифровая подпись.

*Получение сообщения и проверка электронной подписи:*

Получение сообщения и проверка ЭЦП на базе алгоритма RSA (получатель **B**).



**Программная реализация этой же задачи (на основе 6-ой лабораторной работы)**

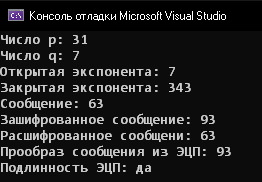


Рисунок 7.1 – Реализация ЭЦП на примере алгоритма RSA

**Контрольные вопросы:**

**1. Дайте определение понятию "электронная цифровая подпись".**

**Ответ:** реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (Федеральный закон "Об электронной цифровой подписи").

**2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.**

**Ответ:** *отправитель* применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения, вычисляет цифровую подпись **s** по хеш- образу **r** с использованием своего закрытого ключа, посылает сообщение **T** вместе с цифровой подписью **s** получателю. *Получатель* применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения, расшифровывает хеш-образ **r’** из цифровой подписи **s** с использованием открытого ключа отправителя, проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

**3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?**

**Ответ:** вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

**4. Опишите схему протокола ЭЦП на основе алгоритма RSA.**

**Ответ:** выработка ЭЦП по формуле s = h^d mod n, где (d, n) – закрытый ключ отправителя. Вычисление хеш-образа из цифровой подписи по формуле h**”**= s^e mod n, где (e, n) – открытый ключ отправителя.

**5. Перечислите специальные схемы ЭЦП.**

**Ответ:**

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен;
* и др.

**Вывод:** в ходе лабораторной работы была изучена и реализована ЭЦП на основе алгоритма RSA.