**Лабораторная работа № 12**

**Тема:** «Реализация функции вычисления ЭЦП RSA».

**Цель:** «изучить основные характеристики алгоритма построения электронной подписи на основе RSA».

**Индивидуальное задание**

Вариант 17 (4)

p = 41; q = 17; m =20.

**1 Генерация ключей**

Выберем два простых числа р = 41 и q =17;

Тогда модуль n = (pq)= 697 и функция Эйлера f(n) = (p-1) (q-1) = 640.

Закрытый ключ d выбираем из условий d<f(n) и d взаимно просто с f(n), т.е. d и f(n) не имеют общих делителей.

Пусть d = 23.

Открытый ключ: 23\*e= 1 (mod 640).

Последнее условие означает, что число 23e-1 должно делиться на 640 без остатка.

Таким образом, для определения e нужно подобрать такое число k, что 23-1 = 640 k.

При k= 6 получаем e=167.

Открытый ключ имеет значение (167, 697),

Секретный ключ имеет значение (23, 697).

**2 Шифрование**

Представим шифруемое сообщение «МВВ» как последовательность целых чисел. Пусть буква «М» соответствует числу 12, буквы «В» - числу 2.

1. Зашифруем сообщение, используя открытый ключ:

С1 = (12^167) mod 697= 432;

С2 = (2^167) mod 697= 154;

С3 = (2^167) mod 697 =31.

Таким образом, исходному сообщению соответствует криптограмма (432, 128, 128).

**3 Расшифрование**

Расшифруем сообщение, пользуясь секретным ключом:

М1 = (432^23) mod 697 = 12;

М2 = (128^23) mod 697 = 2;

М3 = (128^23) mod 697 = 2.

Ответ: в результате расшифрования было получено исходное сообщение (12, 2, 2), то есть «МВВ».

Найти хеш–образ своей Фамилии, используя хеш–функцию, где n = pq, p, q взять из предыдущего задания. Хешируемое сообщение «МИКУЦЕВИЧ». Возьмем два простых числа p=41, q=17.

Определим n = pq= 41\*17 = 697. Вектор инициализации H0 выберем равным 5. Хешируемое слово можно представить последовательностью чисел (26, 1, 17, 19, 12, 10, 11) по номерам букв в алфавите. Таким образом, n=551, H0=5, M1=8, M2=10, M3=19, M4=22, M5=5, M6=2, M7=8,

H0 = 5

H1=(H0+M1)^2 mod n = (5 + 8)^2 mod 697 = 169

H2=(H1+M2)^2 mod n = (169 + 10)^2 mod 697 = 676

H3=(H2+M3)^2 mod n = (676 + 19)^2 mod 697 = 4

H4=(H3+M4)^2 mod n = (4 + 22)^2 mod 697 = 676

H5=(H4+M5)^2 mod n = (676 + 5)^2 mod 697 = 256

H6=(H5+M6)^2 mod n = (256 + 2)^2 mod 697 = 349

H7=(H6+M7)^2 mod n = (349 + 8)^2 mod 697 = 595

H8=(H7+M8)^2 mod n = (595 + 23)^2 mod 697 = 665

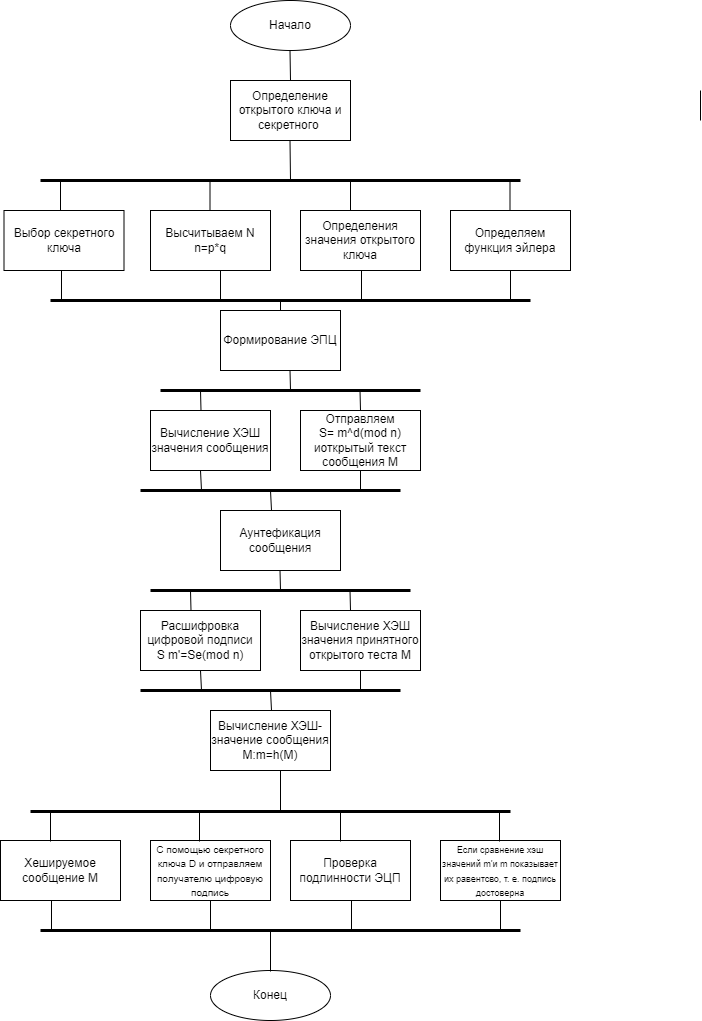
Ответ: В итоге получаем хеш-образ сообщения «МИКУЦЕВИЧ», равный H=665.

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA. Пусть хеш-образ Фамилии равен 118, а закрытый ключ алгоритма RSA равен (23, 697). Тогда электронная цифровая подпись сообщения, состоящего из Фамилии, вычисляется по правилу s = 118^23 mod 697 = 203.

Для проверки ЭЦП, используя открытый ключ (167, 697), найдем H = 203^167 mod 697 = 118.

Ответ: s = 118 Поскольку хеш-образ сообщения совпадает с найденным значением H, то подпись признается подлинной.

Блок схема:

Рисунок 1 – Блок-схема генерации и обмена ключами

**Контрольные вопросы**

1. Определение подлинности информации реализуется путем установки факта, что полученные данные была отправлена подписавшим электронно цифровой подпись, и то, что данные не были искажены. На сегодня словосочетание электронная цифровая подпись стало обыденным, а еще не давно считалось что электронный документ проще подделать чем бумажный экземпляр. Письменная подпись под документом используется в качестве доказательства, что человек согласен с содержимым документа. Основные причины доверия к подписи:

подлинность подписи можно проверить подпись, которая стоит под одним документом, не может быть использована под другим подпись нельзя подделать подписанный документ не может быть изменен подпись забрать назад нельзя, и поэтому поставив подпись вы не можете потом сказать, что не подписывали или не были уведомлены с содержимым документа.

1. Первая и самая встречаемая система ЭЦП на основе RSA. Сначала нужно вычислить пару ключей. Отправитель (автор) электронных документов вычисляет два больших простых числа P и Q, затем находит произведение и значение функции:
2. N = P \* Q; φ (N) = (Р-1) (Q-1).
3. Затем отправитель вычисляет число Е из условий:
4. Е £ φ (N), НОД (Е, φ (N)) = 1 и число D: D <N, Е\*D º 1 (mod j (N)).
5. Пара чисел (E, N) является открытым ключом. Такую пару автор передает партнерам по переписке для проверки его цифровых подписей. Число D сохраняется автором как секретный ключ для подписывания.
6. Преимущества электронно-цифровой подписи:
7. большая степень защиты от подделок
8. идентификация принадлежности подписи на основе характеристик
9. сильная связь с подписываемым документом
10. Для алгоритма цифровой подписи RSA присущи следующие недостатки:
11. при вычислении модуля N и ключей D, E для системы цифровой подписи RSA необходимо проверить большое количество дополнительных условий, что сделать достаточно трудно. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение. При подписании важных документов нельзя допустить такую возможность даже теоретически;
12. для обеспечения криптостойкости цифровой подписи RSA в соответствии со стандартом США на шифрование информации необходимо использовать для вычисления чисел N, D, E целые не менее 2512=10154, что требует больших вычислительных затрат, превышающих на 20-30% вычислительные затраты других алгоритмов электронной цифровой подписи при сохранении того же уровня криптостойкости;
13. цифровая подпись RSA уязвима к мультипликативной атаке, то есть алгоритм позволяет злоумышленнику без знания D сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов.