Лабораторная работа №4

«Электронная цифровая подпись»

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1. Функция хеширования

Функцией хеширования h называется преобразование данных, переводящее строку M произвольной длины в значение $m=h(M)$ (хеш-образ) некоторой фиксированной длины.

Хорошая хеш-функция должна удовлетворять следующим условиям:

1. Хеш-функция $h(M)$ должна быть чувствительна к любым изменениям входной последовательности M.
2. Для данного значения $h(M)$ должно быть невозможным нахожение значения M.
3. Для данного значения $h(M)$ должно быть невозможным нахождение $M' \neq M$ такого, что $h(M') = h(M)$.
4. Вероятность возникновения ситуации, называемой коллизией, когда для различных входных последовательностей M и M' совпадают значения их хеш-образов: $h(M) = h(M')$, должна быть чрезвычайно мала.

При построении хеш-образа входная последовательность M разбивается на блоки M_i фиксированной длины и обрабатывается поблочно по формуле:

$$H_i = f(H_{i-1}, M_i).$$

Хеш-значение, вычисленное в результате обработки последнего блока сообщения, становится хеш-значением (хеш-образом) всего сообщения.

В качестве примера рассмотрим упрощенный вариант хеш-функции следующего вида:

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

где $n = p \cdot q$, p и q – большие простые числа, H_0 – произвольное начальное значение, M_i – i-й блок сообщения $M = \{M_1, M_2, \ldots, M_k\}$.

Пример. Вычислим хеш-образ для строки “БГУИР”.

Для перехода от символов к числовым значениям будем использовать следующее соответствие:

‘А’ – 1

‘Б’ – 2

‘В’ – 3

…

‘Ё’ – 7

…

‘Я’ – 33

Тогда сообщение M примет вид M ={2, 4, 21, 10, 18}.

Выберем 2 простых числа p=17, q=19. Тогда модуль n=323.

Положим H_0=100.

$H_1=(H_0+M_1)^2 \bmod n=(100+2)^2 \bmod 323=10404 \bmod 323=68$.

$H_2=(H_1+M_2)^2 \bmod n=(68+4)^2 \bmod 323=16.$
$H_3=(16+21)^2 \bmod 323=77.$
$H_4=(77+10)^2 \bmod 323=140.$
$H_5=(140+18)^2 \bmod 323=\mathbf{93}.$

Таким образом, $h(M)=H_5=93$.

1.2. Электронная цифровая подпись

Цифровая подпись для электронных документов играет ту же роль, что и подпись, поставленная от руки в документах на бумаге: это данные, присоединяемые к передаваемому сообщению, подтверждающие, что владелец подписи составил или заверил это сообщение. Получатель сообщения с помощью цифровой подписи может проверить, что автором сообщения является именно владелец подписи и что в процессе передачи не была нарушена целостность полученных данных.

При разработке механизма цифровой подписи возникают следующие задачи:

- формирование подписи таким образом, чтобы её невозможно было подделать;
- обеспечение возможности проверки того, что подпись действительно принадлежит указанному субъекту;
- предотвращение отказа субъекта от своей подписи.

1.2.1. Классическая схема создания цифровой подписи

При создании цифровой подписи по классической схеме отправитель должен выполнить следующие действия.

1. Вычислить хеш-образ m исходного сообщения M при помощи хеш-функции h.
2. Вычислить цифровую подпись S по хеш-образу сообщения с использованием секретного ключа K_c создания подписи.
3. Сформировать новое сообщение (M, S), состоящее из исходного сообщения и добавленной к нему цифровой подписи.

Получив подписанное сообщение (M', S), получатель должен выполнить следующие действия (принятое сообщение обозначено как M' по причине того, что оно могло быть преднамеренно либо случайно искажено в процессе передачи по каналу связи и может не совпадать с отправленным).

1. Вычислить хеш-образ m' сообщения M' при помощи хеш-функции h.
2. С использованием открытого ключа проверки подписи (K_o) извлечь хеш-образ m сообщения из цифровой подписи S.
3. Сравнить вычисленное значение m' с извлеченным из цифровой подписи значением хеш-образа m. Если хеш-образы совпадают, то подпись признается подлинной.

1.2.2. Алгоритм цифровой подписи RSA

Первой и наиболее известной во всем мире конкретной системой электронной цифровой подписи стала система RSA, математическая схема которой была разработана в 1977 г. в Массачусетском технологическом институте США.

Сначала необходимо вычислить пару ключей (секретный ключ и открытый ключ). Для этого отправитель сообщения (документа) выбирает два больших простых числа p и q, а затем находит их произведение

$$r = p \cdot q$$

и значение функции Эйлера от данного произведения

$$\varphi(r) = (p-1)\cdot(q-1).$$

Далее отправитель вычисляет значение K_o из условий:

$$K_o < \varphi(r),\ \text{НОД}(K_o, \varphi(r)) = 1$$

и значение K_c из условий:

$$K_c < \varphi(r),\ K_o \cdot K_c = 1 \bmod \varphi(r).$$

Пара значений (K_o, r) является открытым ключом. Эту пару чисел автор передает партнерам по переписке для проверки его цифровых подписей. Значение K_c сохраняется автором как секретный ключ подписи.

Обобщенная схема формирования и проверки цифровой подписи RSA показана на рис. 1.

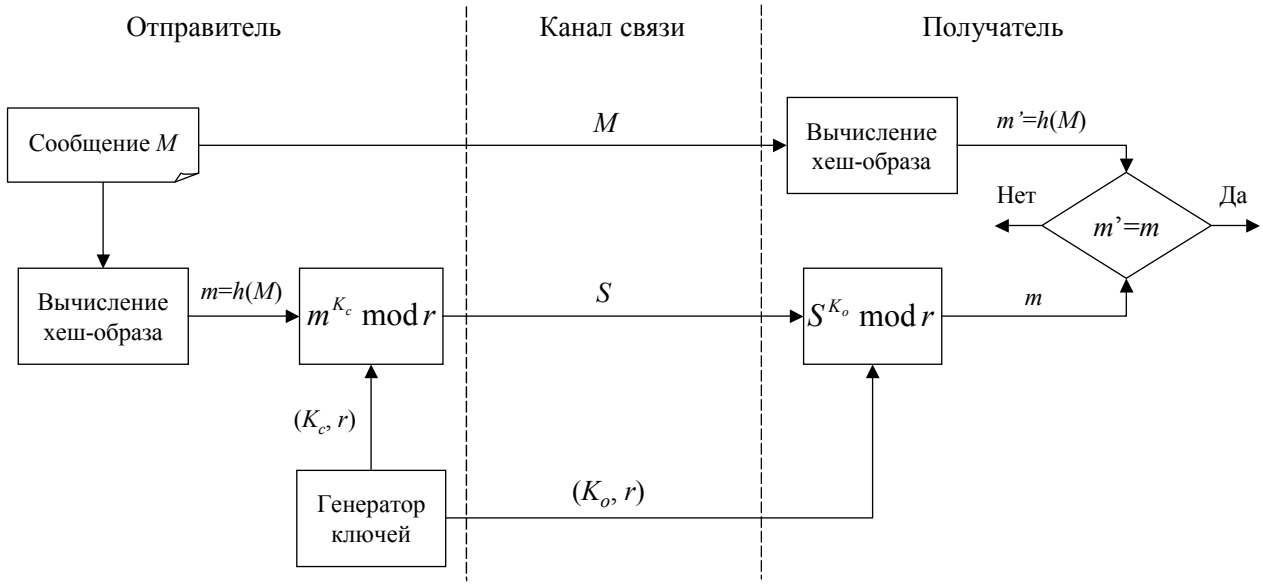

Рис. 1. Обобщенная схема цифровой подписи RSA

Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M сжимают с помощью хеш-функции h в целое число m:

$$m = h(M).$$

Затем вычисляют цифровую подпись S под электронным документом M, на основе хеш-образа m и секретного значения K_c:

$$S = m^{K_c} \bmod r\ .$$

Для возведения в степень можно воспользоваться алгоритмом быстрого возведения в степень по модулю, позволяющим вычислить $x=a^z \bmod n$.

```
FASTEXP(a; z; n)
    a1:=a; z1:=z; x:=1;
    while z1≠0 do
    begin
        while (z1 mod 2)=0 do
        begin
            z1:=z1/2;
            a1:=(a1·a1) mod n;
        end
        z1:=z1–1;
        x:=(x·a1) mod n;
    end
    return (x).
```

Пример. Возведём 45 в степень 13 по модулю 67.
$z_1:=13$; $a_1:=45$; $x:=1$

$13\neq 0$
    13 mod 2 ≠ 0
    $z_1:=13-1=12$
    $x:=1\cdot 45 \bmod 67=45$
$12\neq 0$
    12 mod 2 = 0
        $z_1:=12/2=6$
        $a_1:=45\cdot 45 \bmod 67=15$
    6 mod 2 = 0
        $z_1:=6/2=3$
        $a_1:=15\cdot 15 \bmod 67=24$
    3 mod 2 ≠ 0
    $z_1:=3-1=12$
    $x:=45\cdot 24 \bmod 67=8$
$2\neq 0$
    2 mod 2 = 0
        $z_1:=2/2=1$
        $a_1:=24\cdot 24 \bmod 67=40$
    1 mod 2 ≠ 0
    $z_1:=1-1=0$
    $x:=8\cdot 40 \bmod 67=\mathbf{52}$
$x=45^{13} \bmod 67=52$.

Пара (M, S) передается получателю как электронный документ M, подписанный цифровой подписью S, причем подпись S сформирована обладателем секретного ключа K_c.

После приема пары (M', S) получатель вычисляет хеш-образ сообщения M' двумя различными способами. Прежде всего, он восстанавливает хеш-образ m, применяя криптографическое преобразование подписи S с использованием открытого ключа K_o:

$$m = S^{K_o} \bmod r .$$

Кроме того, он находит результат хеширования *m'* принятого сообщения *M'* с помощью такой же хеш-функции *h*:

$$m' = h(M).$$

Если вычисленные значения совпадают, то есть:

$$S^{K_o} \bmod r = h(M'),$$

то получатель признает пару (*M'*, *S*) подлинной. Фальсификация сообщения при его передаче по каналу связи возможна только при получении злоумышленником секретного ключа K_c либо за счет проведения успешной атаки против хеш-функции. При использовании достаточно больших значений *p* и *q* определение секретного значения K_c по открытому ключу (K_o,*r*) является чрезвычайно трудной задачей, соответствующей по сложности разложению модуля *r* на множители. Используемые в реальных приложениях хеш-функции обладают характеристиками, делающими атаку против цифровой подписи практически не осуществимой. Пример – хеш-функция SHA-1, принятая в США в качестве стандарта в 1995 году, формирующая 160-битовый хеш-образ при обработке сообщения блоками по 512 бит. Вероятность коллизии при использовании данной хеш-функции составляет 2^{-160} или приблизительно $6.84 \cdot 10^{-49}$.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Найти хеш-образ своей фамилии, используя хеш-функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где $n = p \cdot q$.
2. Показать (вычислить $h(M')$) как меняется хеш-образ при изменении одной из букв в фамилии.
3. Показать (вычислить $h(M'')$) как меняется хеш-образ при перестановке любых двух букв в фамилии.
4. Используя полученный ранее хеш-образ вычислить электронную цифровую подпись для своей фамилии по схеме RSA. При вычислении подписи использовать алгоритм быстрого возведения в степень по модулю.

Варианты заданий.

1. p=13, q=17	11. p=17, q=19	21. p=23, q=19
2. p=23, q=13	12. p=7, q=23	22. p=17, q=13
3. p=19, q=11	13. p=7, q=29	23. p=19, q=17
4. p=17, q=23	14. p=7, q=19	24. p=13, q=23
5. p=19, q=13	15. p=7, q=31	25. p=23, q=11
6. p=11, q=29	16. p=7, q=37	26. p=29, q=13
7. p=19, q=23	17. p=5, q=31	27. p=23, q=7
8. p=11, q=23	18. p=5, q=37	28. p=31, q=7
9. p=11, q=17	19. p=5, q=29	29. p=29, q=17
10. p=13, q=29	20. p=29, q=11	30. p=23, q=29