Лабораторная работа 5

Программная реализация ЭЦП

Цель работы – создать программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.

Задание к работе

Реализовать ЭЦП на базе алгоритма Эль-Гамаля и алгоритма *RSA*. При формировании ЭЦП на базе алгоритма *RSA* использовать результаты лабораторной работы № 2. Предусмотреть режимы формирования параметров криптосистемы Эль-Гамаля. Программу оформить, как интегрируемую среду с удобным интерфейсом формирования ЭЦП и ее проверки. Подготовить отчет, в который включить алгоритмы формирования системы Эль-Гамаля, описание функций из которых состоит программа. Подготовить для демонстрации контрольный пример. При формировании цифровой подписи предусмотреть схему ЭЦП с использованием хэш-функций (см. лабораторную работу № 3).

Теоретический материал

Алгоритм формирования схемы Эль-Гамаля

1. Выбираем простое число p.
2. Выбираем два случайных числа $g < p$ и $x < p$.
3. Вычисляем

$$y \equiv g^x \; mod \; p.$$

Открытым ключом схемы Эль-Гамаля являются числа y, g и p. Закрытым ключом – число x.

Алгоритм формирования цифровой подписи

1. Дано сообщение M, которое надо подписать.
2. Выбираем случайное число $k < p$ взаимно простое с p-1.
3. Вычисляем

$$a \equiv g^k \; mod \; p.$$

4. Из уравнения

$$M = (xa+kb) \; mod \; (p-1)$$

определяем b

$$b = (M-xa)k^{-1} \mathrm{mod} \; (p-1).$$

5. Формируем подпись. Подписью является пара чисел *(a,b)*.

Число k является секретным ключом.

Замечание. При формировании цифровой подписи на шаге 4 вместо значения M можно использовать значение $\mu = H(M)$, где H – некоторая хеш-функция.

Проверка подписи

1. Дано сообщение M и подпись (a,b).
2. Вычисляем

$$y^a a^b \ mod \ p \equiv [g^x]^a a^b \equiv g^{xa} g^{kb} \equiv$$
$$\equiv g^{xa+kb} \equiv g^M \ mod \ p.$$

3. Вычисляем

$$g^M \ mod \ p.$$

4. Если значение

$$y^a a^b \ mod \ p$$

совпало с $g^M \ mod \ p$, то подпись верна.

Цифровая подпись на базе алгоритма *RSA*

1. Есть абонент A и текст для подписи M.
2. Определяются закрытые ключи системы *RSA*, т.е. d, p, q и $\varphi(n)$.
3. Определяются открытые ключи e и n.
4. Закрытым ключом вычисляется

$$C = M^d \ mod \ n.$$

Сообщение C рассматривается как подпись абонента A, т. к. закрытый ключ d известен только ему.

5. Используя открытый ключ e, проверка подписанного документа вычисляется по формуле

$$C^e = (M^d)^e \ mod \ n \equiv M,$$

Цифровая подпись Шнорра

ЭЦП Шнорра основана на сложности задачи дискретного логарифмирования. Поэтому все параметры схемы Шнорра должны удовлетворять условиям существование дискретного логарифма.

Схема Шнорра

Параметры схемы:
p – простое число, для реальных задач $160 \leq p \leq 256$,
q – простое число, $q|p$-1, т.е. q делит p-1,
g – число g, $g \in Z_p$, где Z_p – класс вычетов по модулю p,
h – хэш-функция,
x – случайное число из интервала [1,q-1], x – секретный ключ схемы.
y – открытый ключ схемы,

$$y = g^{-x}.$$

Предположим, что существуют два участника A и B. Участник A должен подписать сообщение m для участника B.

Алгоритм схемы подписи Шнорра

1. Участник A выбирает случайное число k и вычисляется

$$r = g^k \ mod \ p.$$

2. Участник A формирует подпись, для этого вычисляются e и s по формулам

$$e = h(r, A), \ \ s = k + xe.$$

3. Подпись (e, s) и подписываемый текст m пересылается участнику B.
4. Участник B делает проверку подписи, вычисляя значения r' и e'

$$r' = g^s y^e \ mod \ p, \ \ e' = h(r', m).$$

5. Если e=e', то подпись принимается, в противном случае отвергается.

Цифровая подпись Рабина

Подпись Рабина базируется на криптографической системе с открытым ключом. Эта система основана на сложности вычисления квадратных корней по модулю n. При этом модуль n представляет собой произведение двух больших простых чисел. Параметры криптографической схемы Рабина:

p – простое число, $p \equiv 3 \ mod \ 4$, p – секретный ключ;
q – простое число, секретный ключ

$$q \equiv 3 \ mod \ 4,$$

$n = pq$ – открытый ключ криптографической системы.

Алгоритм криптографической системы Рабина

Пусть дано сообщение M, $M < n$, которое надо шифровать.

1. Участник A вычисляет значение C, которое является шифром сообщения M, по формуле

$$C = M^2 \ mod\ n.$$

2. Сообщение C отправляется адресату B, который является владельцем закрытого, секретного ключа.

3. Используя китайскую теорему об остатках и закрытый ключ, участник B вычисляет

$$m_1 \equiv C^{(p+1)/4} \ mod\ p,$$
$$m_2 \equiv (p - C^{(p+1)/4}) \ mod\ p,$$
$$m_3 \equiv C^{(q+1)/4} \ mod\ q,$$
$$m_4 \equiv (q - C^{(q+1)/4}) \ mod\ q.$$

4. Используя закрытый ключ, участник B вычисляет числа a и b по формулам

$$a = q(q^{-1} \ mod\ p), \quad b = p(p^{-1} \ mod\ q).$$

5. Возможными сообщениями, которые были отправлены, являются значения

$$M_1, M_2, M_3 \text{ и } M_4,$$

которые вычисляются по формулам

$$M_1 = (am_1 + bm_3) \ mod\ n,$$
$$M_2 = (am_1 + bm_4) \ mod\ n,$$
$$M_3 = (am_2 + bm_3) \ mod\ n,$$
$$M_4 = (am_2 + bm_4) \ mod\ n.$$

Если сообщение представляет собой осмысленный текст, то выбрать правильное M_i, $i = 1, 2, 3, 4$, легко. Если сообщение представляет собой набор битов, т.е. какое-то число, то к такому виду передаваемой информации добавляется какой-либо осмысленный текст заголовка. По заголовку и происходит выбор M_i, i=1,2,3,4. Если M число, то другого способа идентификации передаваемого сообщения M не существует.

Перейдем теперь к описанию алгоритма цифровой подписи Рабина. Предположим, что определены параметры криптографической системы

Рабина и сообщение M, которое надо подписывать. Сообщение M представляет собой некоторую последовательность

$$m_0, m_1, m_2, \ldots, m_{k-1}$$

из k бит

$$m_i \in \{0,1\}, i = 0, 1, \ldots, k-1.$$

Алгоритм схемы подписи Рабина

Формирование подписи

1. Генерируется случайная последовательность R длиной из t бит

$$R = (r_0, r_1, \ldots, r_{t-1}),$$
$$r_i \in \{0,1\}, i = 0, 1, \ldots, t-1.$$

2. Сообщение M объединяется с последовательностью R

$$M||R = (m_0, m_1, m_2, \ldots, m_{k-1}, r_0, r_1, \ldots, r_{t-1}).$$

3. Последовательности битов $M||R$ ставится в соответствии число $a < n$.
4. Проверяются условия

$$a^{(p-1)/2} \equiv 1 \; mod \; p, \;\; a^{(q-1)/2} \equiv 1 \; mod \; q.$$

5. Если условия не выполняется, то перейти на шаг 1.
6. Вычисляются значения

$$z_p \equiv a^{(p+1)/4} \; mod \; p, \;\; z_p \equiv a^{(q+1)/4} \; mod \; q.$$

7. По китайской теореме об остатках вычисляется значение

$$Z = a^{1/2} \; mod \; n.$$

8. Формируется подпись из пары чисел (R, Z) к сообщению M.

Проверка подписи

1. Вычисляется значение a'

$$a' \equiv Z^2 \; mod \; n.$$

2. Если a=a', то подпись принимается, в противном случае отвергается.

Контрольные вопросы

1. Перечислить число параметров в криптографической системе Эль-Гамаля.
2. Перечислить секретные параметры системы Эль-Гамаля.
3. Перечислить открытые параметры системы Эль-Гамаля.
4. На какой достаточно трудной задаче из теории чисел базируется криптографическая система Эль-Гамаля.
5. Описать схему формирования ЭЦП с использованием алгоритма Эль-Гамаля.
6. Описать схему проверку ЭЦП с использованием алгоритма Эль-Гамаля.
7. Описать схему формирование цифровой подписи с применение алгоритма RSA.
8. Описать схему проверки цифровой подписи с применение алгоритма RSA.
9. Что общего между обычной и цифровой подписями? Чем они различаются?
10. Какие задачи позволяет решить цифровая подпись?
11. В чем заключается принципиальная сложность в практическом применении систем цифровой подписи?
12. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать для шифрования и цифровой подписи?
13. Проверить, что указанный в тексте способ подбора подписанных сообщений для схемы Эль-Гамаля действительно дает верные цифровые подписи.