**Лабораторная работа № 13**

**Тема:** «Реализация функции вычисления ЭЦП Эль-Гамаля».

**Цель:** «изучить основные характеристики алгоритма построения электронной подписи Эль-Гамаля».

**Индивидуальное задание**

Задание:

1. Согласно своего варианта сформировать ЭЦП по алгоритму Эль-Гамаля.

2. Составить блок-схему алгоритма ЭЦП Эль-Гамаля.

Передаваемое сообщение m открытые ключи p, g, и секретный ключ представлены в таблице 1.

Таблица 1 – Задание для исследования системы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Вариант** | **Открытый ключ** | | **Закрытый ключ x** | **Сообщение m** |
| **p** | **g** |
| 4 | 31 | 10 | 10 | 14 |

**Решение:**

Открытые ключи p=31, g=10, Закрытый ключ (x)=14, Сообщение (m)=14.

y = g^x mod p = 10^10 mod 31 = 7;

Найдем взаимно простое число k (P-1 = 31 -1 = 30). Взаимно простое число k=11, так как 11 и 30 не имеют общих делителей.

a = g^k mod p = 10^11 mod 31 = 17. Далее с помощью расширенного алгоритма Евклида найдем b из уравнения m = (ax + kb) mod p – 1

(17\*10 + 11\*b) mod 30 = 14

(170 + 11\*b) mod 30 = 14

Выразим b:

11\*b = 30\*k + 14 – 170

11\*b = 30\*k – 156

b = (30\*k - 156)/11

Так как b должно быть целым числом, то подставим числа k, начиная с 1:

k = 14: b = (30\*14 - 156)/11 = 1 - подходит

Следовательно, a = 3 и b = 1. Проверим наш ответ используя формулу y^a\* a^b mod p = g^m mod p.

19^3 \* 3 ^ 1 mod 31 = 13^20 mod 31

14 = 14.

**Ответы на контрольные вопросы**

1. Охарактеризовать основные принципы построения цифровой подписи Эль-Гамаля.

Ответ: Основные принципы построения цифровой подписи Эль-Гамаля включают:

* Генерация ключей: Пользователь создает открытый и секретный ключи, используя алгоритм генерации ключей Эль-Гамаля.
* Хэширование сообщения: Сообщение, которое нужно подписать, хэшируется с использованием алгоритма хэширования.
* Создание подписи: Подпись создается путем шифрования хэш-значения сообщения с использованием частного ключа Эль-Гамаля.
* Проверка подписи: Для проверки подписи получатель должен выполнить обратный процесс: расшифровать полученную подпись с помощью открытого ключа и сравнить полученное значение с хэш-значением сообщения.

2. Изложить характеристики алгоритма Эль-Гамаля, используемого для получения цифровой подписи.

Ответ: Алгоритм Эль-Гамаля является криптографической системой, используемой для создания цифровых подписей. Он был разработан Эль-Гамалям в 1985 году и с тех пор стал одним из наиболее распространенных алгоритмов для подписания данных.

Характеристики алгоритма Эль-Гамаля:

* Использует математические операции над большими числами. Алгоритм основан на задаче Диффи-Хеллмана, которая заключается в том, что по открытому ключу и секретному числу сложно вычислить общее число.
* Алгоритм обладает свойством цифровой подписи, то есть подписывается не само сообщение, а хэш-код сообщения. Это гарантирует целостность данных, но не гарантирует их конфиденциальности.
* Алгоритм Эль-Гамаля не требует особых вычислительных мощностей. Он применяется в многочисленных приложениях, включая электронную почту, онлайн-банкинг, электронную коммерцию и другие виды электронных транзакций.
* Один из главных недостатков алгоритма Эль-Гамаля - это медленная скорость работы. Этот недостаток связан с тем, что при вычислении подписи необходимо осуществлять сложные математические преобразования.

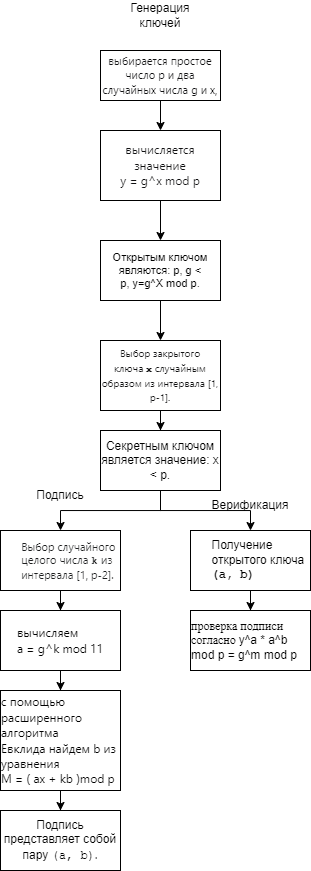
3. Изложить сравнительную характеристику алгоритмов получения цифровой подписи RSA и Эль-Гамаля.

Ответ: RSA и Эль-Гамаля являются двумя основными алгоритмами получения цифровой подписи. Оба алгоритма основаны на криптографических протоколах, которые используют математические функции для защиты информации. Однако есть несколько отличий между этими двумя алгоритмами.

* Сложность вычислений и скорость работы: RSA является более медленным, чем Эль-Гамаля, потому что он использует ряд сложных операций для шифрования и расшифровки. Эль-Гамаля использует более простой алгоритм, что обеспечивает более быструю работу.
* Надежность: оба алгоритма считаются довольно надежными, но RSA имеет некоторые уязвимости, которые могут быть использованы для взлома. Эль-Гамаля имеет меньше ошибок и уязвимостей, и считается более безопасным.
* Длина ключей: RSA обеспечивает более длинные ключи, что обеспечивает большую степень защиты. Эль-Гамаля также позволяет использовать достаточно длинные ключи, но его ключи остаются меньше, чем RSA.
* Распространенность: RSA является более распространенным алгоритмом для получения цифровой подписи, потому что он был разработан раньше Эль-Гамаля, и его быстродействие не сильно мешает ему использоваться в реальных приложениях.
* Области применения: RSA используется для шифрования симметричных ключей, сохранения цифровых сертификатов и получения цифровой подписи. Эль-Гамаля используется для шифрования, а также для аутентификации в системах, которые используют открытый ключ.

Итак, RSA и Эль-Гамаля являются двумя надежными алгоритмами, которые позволяют получать и использовать цифровую подпись. Однако, из-за некоторых различий в определенных областях, некоторые предпочитают использовать RSA, в то время как другие предпочитают Эль-Гамаля.

Схема генерации ЭЦП по алгоритму Эль-Гамаля:

Рисунок 1 – ЭЦП Эль-Гамаля