Лабораторная работа №3

Карпов Алексей

12 группа кафедра ИСУ

Вариант 3

**Алгоритм ECDSA и RSA**

Алгоритм ECDSA (Elliptic Curve DSA) является аналогом алгоритма цифровой подписи DSA (Digital Signature Algorithm), реализованным с помощью эллиптических групп. Рассмотрим эллиптическую группу EM(a,b) и генерирующую точку G с порядком q, причем q простое число.  
Пользователи A генерируют свои ключи: секретный nA и открытый PA, где PA= nAG. Для постановки цифровой подписи под сообщением m пользователь A:

1. На основе хеш-функции h() находит хеш-код h(m) от m. В качестве хеш-функции должна использоваться криптографически стойкая функция, например SHA-1.
2. Генерирует случайное число k, 1 < k < q – 1.
3. Вычисляет значение kG = (x1,y1) и r = x1 mod q. Если r = 0, возвращается на шаг 2.
4. Вычисляет(mod q) . Если s = 0, то возвращается на шаг 2.
5. Подпись сообщения m – это пара целых чисел (r,s).

Для проверки цифровой подписи пользователь B использует ту же эллиптическую группу EM(a,b), генерирующую точку G, открытый ключ PA и хеш-функцию h.

На основе хеш-функции h определяем хеш-код h(m) от m.

* Проверяем, принадлежат ли числа r и s интервалу от 1 до q – 1.
* Вычисляем w = m mod q.
* Вычисляем u1 = h(m)w mod q и u2 = rw mod q.
* Вычисляем u1G + u2PA = (x1\*, y1\*) и r\*=x1\*mod q.
* Равенство r\* = r удостоверяет подпись пользователя A.

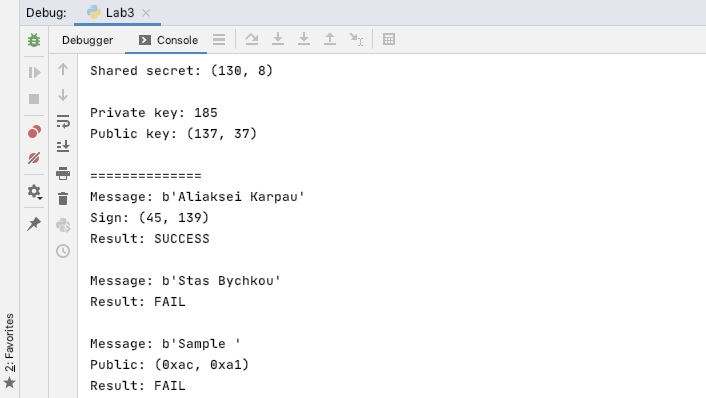
Особое достоинство криптосистем на эллиптических кривых состоит в том, что по сравнению с системами на основе алгоритма RSA они обеспечивают существенно более высокую стойкость при равной трудоемкости или, наоборот, существенно меньшую трудоемкость при равной стойкости. В результате тот уровень стойкости, который достигается в RSA при использовании 1024-битных модулей, в системах на эллиптических кривых реализуется при размере модуля 160 бит, что обеспечивает более простую как программную, так и аппаратную реализацию.

**Лабораторная работа**

Решение задачи реализовано и получены результаты по следующим пунктам:

1. Определились значения, которые позволяли построить эллептическую группу
2. Генерация всех элементов из этой группы
3. Реализован алгоритм обмен ключами
4. Разработан алгоритм цифровой подписи на основе эллиптической группы

Элементы группы получены и сгенерированы.



А также результаты верификации:

