Шкурский Даниил(4 курс, 12 группа)

Параметры варианта 5:



Элементы эллиптической группы:















Суть работы алгоритма:

Первым и вторым аккаунтом генерируются собственные закрытые и открытые ключи. У первого к примеру есть закрытый ключ dA и открытый HA=dAG, ключи второго соответственно dB и HB=dB. Далее эти аккаунты обмениваются открытыми ключами (HA и HB) по незащищенному каналу.

Первый аккаунт вычисляет S=dAHB с помощью собственно закрытого ключа и публичного ключа второго аккаунта, а второй аккаунта вычисляет соответственно S=dBHA с помощью своего закрытого ключа и публичного ключа первого

Алгоритм подписывания сообщения первым аккаунтом:

1. Берём случайное целое k, выбранное из {1,…,n−1} (где n — порядок группы).

2. Вычисляем точку P=kG (где G — базовая точка подгруппы).

3. Вычисляем число r=xPmodn (где xP — это координата x P).

4. Если r=0, то выбираем другое k и пробуем снова.

5. Вычисляем s=k−1(z+rdA)modn (где dA — закрытый ключ Алисы,

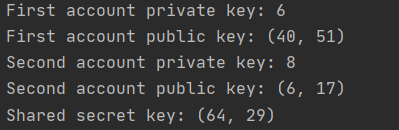
а k−1 — мультипликативная инверсия k по модулю n).

6. Если s=0, то выбираем другое k и пробуем снова.

(Пара (r,s) является подписью)

Пример работы программы:

Выданные ключи с исходными параметрами варианта 5:



Пример обмена сообщениями между аккаунтами:

