**Математическая постановка задачи**

Для защиты при обмене данными между нашим приложением (Client) и сервером, мы использовали алгоритм шифрования RSA

**Алгоритм RSA**

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Алгоритм RSA стал первым алгоритмом, пригодным и для шифрования, и для цифровой подписи.

В данном алгоритме имеется открытый ключ и закрытый ключ. Работа алгоритма происходит следующим образом:

Осуществляется генерация ключей: выбираются два достаточно больших случайных простых числа (желательно разрядностью 100-200 единиц или больше). Для большей безопасности ключи должны иметь равную длину.

p = 3557

q = 2579

Затем вычисляется произведение N = p \* q.

N = 3557 \* 2579

N = 9173503

После рассчитывается значение функции Эйлера по формуле:

φ(n) = (p-1)\*(q-1)

φ(n) = (3557-1)\*(2579-1) = 9167365

Далее выбирается открытый ключ(открытая экспонента) e (1 < e < φ(n)), взаимно простое со значением функции Эйлера

e = 3

Следом с помощью расширенного алгоритма Евклида вычисляется закрытый ключ шифрования D(секретная экспонента), удовлетворяющий условию:

**e \*** D≡1mod **(**φ(n))

D = 6111579

Заметим, что D и N также взаимно простые числа.

Числа E и N – это открытые ключи, а число D – закрытый.

Два простых числа p и q больше не нужны. Они могут быть отброшены, но не должны быть раскрыты.

При шифровании сообщение M сначала разбивается на цифровые блоки, размерами меньше N (для двоичных данных выбирается самая большая степень числа 2, меньшая N). Зашифрованное сообщение С будет состоять из блоков Ci такой же самой длины.

Предположим текст для шифрования M = 111111

Формула шифрования выглядит так:

Ci = E(Mi) = Mie mod(N)

C = 1111113 mod(9173503) = 4051753

При расшифровке сообщения для каждого зашифрованного блока Сi вычисляется по следующей формуле:

Mi = D(Ci) = Cid mod(N)

M = 40517536111579 mod (9173503) = 111111