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:

$\varphi(n) = (p-1)*(q-1)$

$\varphi(n) = (3557-1)*(2579-1) = 9167365$

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

$e = 3$

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

$$\mathbf{e} * D \equiv 1 \bmod (\varphi(n))$$

$$D = 6111579$$

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 C будет состоять из блоков C_i такой же самой длины.

Предположим текст для шифрования M = 111111

Формула шифрования выглядит так:

$$C_i = E(M_i) = M_i^e \bmod(N)$$

$$C = 111111^3 \bmod(9173503) = 4051753$$

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

$$M_i = D(C_i) = C_i^d \bmod(N)$$

$$M = 4051753^{6111579} \bmod (9173503) = 111111$$