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 отличие от традиционных симметричных систем шифрования, RSA работает с двумя различными ключами: публичным и частным. Оба они дополняют друг друга, что означает, что сообщение, зашифрованное одним из них, может быть дешифровано только его дополняющей стороной. Поскольку частный ключ не может быть вычислен из открытого ключа, последний, как правило, доступен для общественности.

Безопасность алгоритма RSA основана на трудоемкости разложения на множители (факторизации) больших чисел. Открытый и закрытый ключ являются функциями двух больших простых чисел, разрядностью 100-200 десятичных цифр или даже больше. Предполагается, что восстановление открытого текста по шифрованным данным и открытому ключу равносильно разложению числа на два больших простых множителя.

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

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

Затем вычисляется произведение N = p * q.

После случайно выбирается ключ шифрования E, такой, что

E и (p-1)*(q-1) являются взаимно простыми числами.

Следом с помощью расширенного алгоритма Евклида вычисляется закрытый ключ шифрования D, удовлетворяющий условию:

E * D ≡ 1 * mod *(p−1) * (q−1)

Где

- E – открытый ключ шифрования
- D - закрытый ключ шифрования
- p и q – случайные простые числа.

Заметим, что D и N также взаимно простые числа. Числа E и N – это открытый ключ, 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). То есть, если p и q являются 100-разрядными простыми числами, то N будет содержать около 200 разрядов, и каждый блок сообщения M_i должен быть около 200 разрядов в длину (Если нужно зашифровать фиксированное число блоков, их можно дополнить несколькими нулями слева, чтобы гарантировать, что блоки всегда будут меньше N). Зашифрованное сообщение C будет состоять из блоков C_i такой же самой длины. Формула шифрования выглядит так:

$M_i = C_i^E \ mod \ N$

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

$M_i = C_i^D \ mod \ N$

Точно также сообщение может быть зашифровано с помощью D, а расшифровано с помощью E.