Постановка задачи

Реализовать протокол SRP

Ход работы

Берем 2 простых числа N и q: N = 2\*q + 1. Дальше с клавиатуры вводим случайную строку s(т.н. соль). Сервер хранит пароль p , верификатор v, секретный ключ x и соль s. Дальше клиент вводит имя пользователя I. Клиент выбирает одноразовое секретное число a, вычисляет A. Тем временем сервер выбирает одноразовое секретное число b, вычисляет B. Клиент отправляет на сервер I, A, a. Сервер отправляет клиенту s, b, B. Далее и клиент, и сервер считают произвольный параметр для кодирования u = H(A, B). Дальше клиент вводит пароль, вычисляет ключ сессии S и ключ шифрования K. Сервер тоже вычисляет S и K. Дальше клиент и сервер сверяют ключи. Они это делают при помощи M = H(H(N) xor N(g), H(I), s, A, B, K) и R = H(A, M, K).

Вывод

Программа работает корректно. Параметры S, K, M, R клиента и сервера совпадут только при правильных логине и пароле.