Сервер сайта

Клиент для шифрования

Другой клиент

зашифрованный текст

Пользователь

Сервер PH

текст

Пользователь

Клиент

расшифрованный текст

1. Пользователь пишет сообщение
2. Браузер шифрует это сообщение с использованием пользовательской соли (необходимо периодически менять)
3. Зашифрованный текст уходит на сервер, специализированному скрипту
   1. Скрипт шифрует сообщение с помощью пользовательской соли
   2. берет выданный пользователю ключ и добавляет его в случайное место сообщения
   3. Добавляет заголовок с длинной (в байтах) позиции ключа
   4. Добавляет заголовок в виде n байт с позицией ключа
   5. Шифрует всё по какому-то алгоритму с солью PH
4. Сообщение возвращается клиенту
5. Клиент шлёт его серверу PH
   1. Сообщение расшифровывается
   2. По заголовкам в сообщении находится ключ
   3. Проверяется его соответствие выданному
   4. Ключ удаляется из сообщения
   5. Из фрейма выделяются данные
   6. Сообщение шифруется
   7. Отправляется клиенту
6. Клиент, получив сообщение, отсылает его на сервер
7. На сервере
   1. Сообщение расшифровывается по алгоритму PH
   2. Расшифровывается серверной солью
   3. Отсылается клиенту
8. Клиент расшифровывает сообщение пользовательской солью
9. Показывает его конечному адресату