Лабораторная работа №14

Одноразовые пароли

Цель: Приобрести практические навыки в реализации схемы одноразовых паролей на основе хеш-функций.

Введение

Повышению надежности идентификации служит использование одноразовых паролей, то есть паролей, которые могут быть использованы для идентификации только один раз. Такие схемы обеспечивают защиту от противника, использующего перехват паролей из незащищенного канала.

В одной из таких схем пользователи системы используют одноразовые пароли на основе хеш-функции.

При использовании данной схемы пользователь начинает с секретного пароля и с помощью хеш-функции вырабатывает n итераций .

Паролем для i-й идентификации , является значение . Для того, чтобы идентифицировать себя при i-й попытке, А передает В строку где -идентификатор пользователя . В проверяет соответствие полученного i-номеру попытки и равенство . Если оба равенства выполнены, В идентифицирует А и запоминает для следующей попытки идентификации. Для использования данной системы центру аутентификации необходимо передать вычислить значение .

1. Рабочее задание

1.1 Реализовать схему одноразовых паролей на оснве хеш-функций из лабораторных работ № 4 и 5.

2. Требования к реализации

2.1 Должен присутствовать выбор между хеш-функциями, на основе которых производится аутентификация.

2.2 Центр аутентификации должен быть реализован на отдельной виртуальной машине. Взаимодействие с данным центром осуществляется по сети.

2.3 Должна поддерживаться кодировка ASCII

2.4 Должна быть предусмотрена процедура регистрации пользователя, в результате которой производится передача пароля пользователя.

2.5 Номер попытки аутентификации должен храниться отдельно у пользователя и отдельно от центра регистрации.

2.6 Результат процедуры аутентификации должен выводиться на экран.

2.7 Нельзя пользоваться готовыми реализациями хеш-функций ГОСТ Р 34.11-2012, SHA-256 и SHA-512.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab14, после получения подписанного преподавателем исходного кода, прийти и защитить его.