Лабораторная работа №6

Реализация хеш-функции HMAC

Цель: Приобрести практические навыки в реализации криптографических хеш-функций

Введение

Одним из инструментов обеспечения контроля целостности информации от активных действий злоумышленника (имитация и подмена) являются криптографические ключевые хеш-функции (имитовставки). Рассмотрим один из подходов к построению таких функций.

Функция HMAC описана в RFC 7298.

Пусть - размер блока в битах;

- хеш-функция;

- значение 00110110, повторенное раз;

- значение 01011100, повторенное раз;

- секретный ключ с добавленными справа нулями до бит;

- сообщение.

Алгоритм HMAC можно записать в виде одной формулы:

*.*

1. Рабочее задание

1.1 Реализовать хеш-функцию HMAC на основе хеш-функций из лабораторных работ 4 и 5.

2. Требования к реализации

2.1 Должен присутствовать выбор между хеш-функциями, на основе которых должен вычисляться HMAC.

2.2 Секретный битовый ключ должен формироваться случайным образом случайной длины и записываться в файл. Должна быть предусмотрена отдельная процедура для генерации ключа.

2.3 Должна поддерживаться кодировка Unicode

2.4 Должен быть реализован выбор между вводом данных с консоли или чтения из файла.

2.5 Результат должен выводиться в шестнадцатиричном виде на экран.

2.6 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 lab6, после получения подписанного преподавателем исходного кода, прийти и защитить его.