Лабораторная работа №4

Реализация хеш-функции ГОСТ Р 34.11-2012 "Стрибог"

Цель: Приобрести практические навыки в реализации криптографических хеш-функций

Введение

Одним из инструментов обеспечения контроля целостности информации от случайных изменений являются криптографические бесключевые хеш-функции. Рассмотрим одну из таких функций.

Алгоритм ГОСТ Р 34.11-2012

Хеш-функция ГОСТ Р 34.11-2012 позволяет получать свертку размером 512 или 256 бит.

Хешируется битовое сообщение . Также используется инициализирующий вектор , значение которого определяется в зависимости от размера получаемой свертки. Рассмотрим алгоритм вычисления свертки.

**Этап 1.**

, переход к этапу 2.

**Этап 2.**

2.1 Если , то переход к этапу 3 ( - размер сообщения ).

2.2 Вычисляется ( || - конкатенация)

2.3

2.4

2.5

2.6 , переход к шагу 2.1

**Этап 3.**

3.1

3.2

3.3

3.4

3.5

3.6 - если вычисляется 512 битовая свертка.

- если вычисляется 256 битовая свертка.

*-* 256 старших значащих бит.

Полученное значение на шаге 3.6 будет являться значением хеш-функции.

- для свертки 512 бит.

- для свертки 256 бит.

(⊕-побитовое сложение двух чисел)

;

- итерационные константы, заданные в стандарте.

*-* подстановка байт, по таблице, заданной в стандарте.

*-* перестановка байт, согласно таблице, заданной в стандарте.

- линейное преобразование множества двоичных 64-битовых векторов, которое задается перемножением данных векторов на матрицу , заданную в стандарте, справа над полем . Преобразуемое 512 битовое сообщение представляется в виде конкатенации 64 битовых векторов .

1. Рабочее задание

1.1 Реализовать хеш-функцию ГОСТ Р 34.11-2012

2. Требования к реализации

2.1 Неописанные в рамках методички переменные берутся из стандарта

2.2 Перед сдачей реализация должна быть протестирована на контрольных значениях из стандарта

2.3 Должен присутствовать выбор между вычислением 512 и 256 битовой свертки.

2.4 Должна поддерживаться кодировка Unicode

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

2.6 Результат должен выводиться в шестнадцатиричном виде на экран.

2.7 Нельзя пользоваться готовыми реализациями хеш-функции ГОСТ Р 34.11-2012

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab4, после получения подписанного преподавателем исходного кода, прийти и защитить его.