Лабораторная работа №5

Реализация хеш-функций SHA-256, SHA-512

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.

SHA-256

Хеш-функция SHA-256 (описана в стандарте FIPS 180-4) позволяет получать свертку размером 256 бит из сообщений менее бит. Данная хеш-функция обрабатывает блоки размером 512 бит. Опишем процедуру дополнения блоков до размера 512 бит.

Предположим, что длина сообщения , . Тогда к сообщению добавляется 1 бит «1» и бит «0», где . Затем добавляется 64-битный блок, который равен числу , выраженному в двоичном виде.

Опишем функции, используемые в рамках преобразований. Все функции работают с 32-битовыми словами.

, где (∧- побитовое И; - побитовое НЕ).

.

, где ( - циклический сдвиг вправо).

.

, где ( - сдвиг вправо).

.

В алгоритме используется 64 32-битных константы (указаны в тексте стандарта).

Пусть после дополнения сообщение состоит из 512-битовых блоков: . Каждый из блоков делится на 16 32-битовых слова: .

В алгоритме используются 8 инициализирующих значений хеш-функций .

Опишем алгоритм преобразования:

Для

1. Рассчитать элементы :

2.

3. Для

4.

После обработки блока итоговое значение хеш-функции определяется как .

SHA-512

Хеш-функция SHA-512 (описана в стандарте FIPS 180-4) позволяет получать свертку размером 512 бит из сообщений менее бит. Данная хеш-функция обрабатывает блоки размером 1024 бит. Опишем процедуру дополнения блоков до размера 1024 бит.

Предположим, что длина сообщения , . Тогда к сообщению добавляется 1 бит «1» и бит «0», где . Затем добавляется 128-битный блок, который равен числу , выраженному в двоичном виде.

Опишем функции, используемые в рамках преобразований. Все функции работают с 64-битовыми словами.

.

.

.

.

.

.

В алгоритме используется 80 64-битных константы (указаны в тексте стандарта).

Пусть после дополнения сообщение состоит из 1024-битовых блоков: . Каждый из блоков делится на 16 64-битовых слова: .

В алгоритме используются 8 инициализирующих значений хеш-функций .

Опишем алгоритм преобразования:

Для

1. Рассчитать элементы :

2.

3. Для

4.

После обработки блока итоговое значение хеш-функции определяется как .

1. Рабочее задание

1.1 Реализовать хеш-функции SHA-256 и SHA-512

2. Требования к реализации

2.1 Неописанные в рамках методички переменные берутся из стандарта

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

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 SHA-256 и SHA-512.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab5, после получения подписанного преподавателем исходного кода, прийти и защитить его.