Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических хеш-функций

Студент: Точило О. В.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

# **Алгоритм хеширования**

Базовые алгоритмы обоих рассматриваемых семейств (MD и SHA) условно можно разделить на 5 стадий:

* расширение входного сообщения;
* разбивка расширенного сообщения на блоки;
* инициализация начальных констант;
* обработка сообщения поблочно;
* вывод результата.

Входное сообщение «дополняется» (расширяется) так, чтобы его длина (в битах) была конгруэнтной к 448 по модулю 512. Это значит, что сообщение начальной длиной *L* битов расширяется так, что остаются незаполненными всего лишь 64 бита, чтобы итоговая длина *L*' была кратной 512. В указанные 64 бита записывается двоичная длина. Расширение происходит всегда, даже если длина сообщения уже соответствует 448, по модулю 512.

Эта операция выполняется следующим образом: один бит «1» добавляется к сообщению, а затем добавляются биты «0», так что длина в битах дополненного сообщения стала конгруэнтной 448 по модулю 512. Добавляется не менее одного бита, но не более 448 битов.

Основой рассматриваемых базовых алгоритмов является модуль, состоящий из циклических преобразований каждого 512-битного блока, который делится на подблоки длиной 32 либо 64 бита. При длине подблока в 16 битов каждый 512-битный блок должен состоять из 32 подблоков.

Код функции для вычисления хеша на основе алгоритма MD5 представлен на рисунке 1.1.

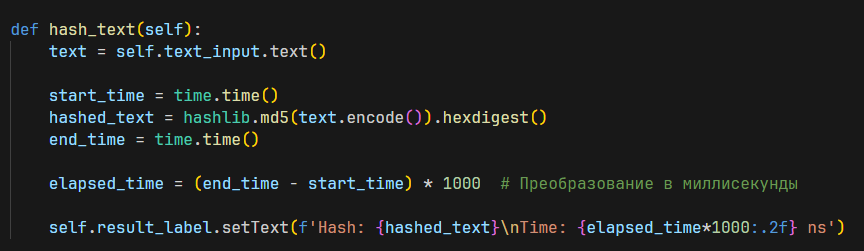


Рисунок 1.1 – Код функции вычисления хеша на основе алгоритма MD5

# **Вывод**

В данный лабораторной работе были изучены и приобретены практические навыки реализации и использования в криптографии алгоритмов хеширования SHA-1 и MD5.