Пшенко Артем ФИТ 3-4

Отчет по лабораторной работе № 11

Исследование криптографических хеш-функций (алгоритм MD-5)

Информационная безопасность

Вариант 9

Цель данной лабораторной работы состоит в изучении алгоритма хеширования MD5.

Главный модуль состоит из четырех похожих этапов (у MD-4 было только три этапа). На каждом этапе 16 раз используются различные операции. Каждая операция представляет собой нелинейную функцию над тремя из a, b, c и d. Затем она добавляет этот результат к четвертой переменной, подблоку текста Мj и константе ti. Далее результат циклически сдвигается вправо на переменное число s битов и добавляет результат к одной из переменных a, b, c и d.

Наконец, результат заменяет одну из этих переменных. Результатом хеширования h является конкатенация последних значений указанных переменных, т. е. 32 · 4 = 128 битов.

Структурная схема одной итерации алгоритма MD-5 приведена на рисунке 1:

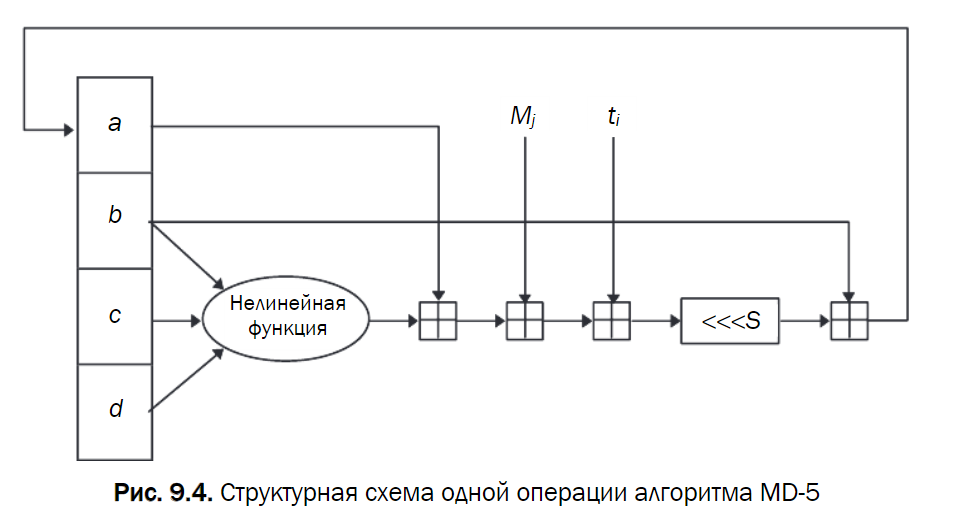


Рисунок 1. Структурная схема одной итерации алгоритма MD-5

Исходный код алгоритма MD-5 приведен в листинге 1.

Листинг 1. Исходный код алгоритма MD-5

|  |
| --- |
| import hashlib  import time  # Входные данные  data = "Pshenko Artyom Fyodorovich"  # Создаем хеш md5  start\_time = time.time()  md5\_hash = hashlib.md5()  # Обновляем хеш с помощью входных данных  md5\_hash.update(data.encode())  # Получаем конечный хеш  digest = md5\_hash.hexdigest()  end\_time = time.time()  print(f"MD5 Hash: {digest}")  print(f"Время выполнения: {end\_time - start\_time} секунд") |

Результат работы алгоритма MD-5 приведен на рисунке 2.



Рисунок 2. Результат работы программы

Таким образом, в ходе лабораторной работы была продемонстрирована работа алгоритма MD-5.