Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра «Информационных систем и технологий»**

**Лабораторная работа №9**

Исследование криптографических хэш-функций

Выполнил:

Студент 3 курса, 10 группы

Баранчук Владислав

2021 г.

1. **Практическая часть**

**Цель:** изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

Для обработки MD5 получает некоторую строку. Эта строка преобразуется в последовательность из нулей и единиц. Пусть q будет длина последовательности (ровно 64 бита, возможно, с незначащими нулями). К получившейся последовательности приписывается 1.

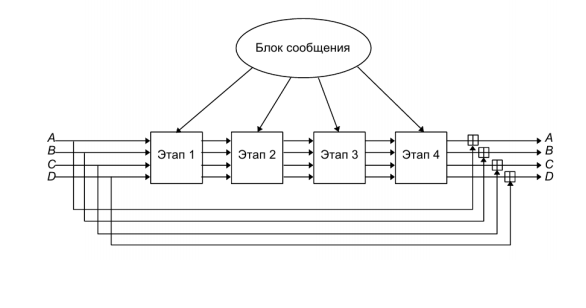


Рис. 1 – Укрупненная схема алгоритма MD-5

В результате длина последовательности увеличивается на 1. Затем к последовательности приписываются нули, пока длина не станет по модулю 512 равна 448 (length mod 512=448). Далее к последовательности дописываются младшие 32 бита числа q, а затем – старшие. Длина последовательности становится кратной 512. Полученную последовательность назовем S.

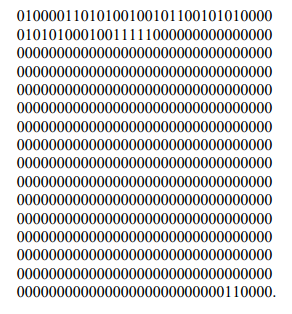


Рис. 2 – последовательность S после увеличения

Для подсчета результата используются четыре двойных слова (32 бита). Эти двойные слова инициализируются следующими шестнадцатеричными значениями, где первым следует самый младший байт:

A: 01 23 45 67  
B: 89 ab cd ef  
C: fe dc ba 98  
D: 76 54 32 10  
Также для подсчета результата используются следующие функции:  
F(X,Y,Z) = XY v not(X) Z  
G(X,Y,Z) = XZ v Y not(Z)  
H(X,Y,Z) = X xor Y xor Z  
I(X,Y,Z) = Y xor (X v not(Z))

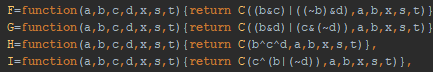


Рис. 3 – листинг кода функций F,G,H,I

X, Y, Z – это двойные слова. Результаты функций, также двойные слова. Для подсчета используется еще одна функция (назовем ее W). Она обрабатывает данные и возвращает результат. Обработка данных происходит с использованием функций F, G, H, I. Все необходимые функции и обозначения рассмотрены. Теперь рассмотрим, как происходит просчет результата:

1. Запоминаем первые 512 бит последовательности S.

2. Удаляем первые 512 бит последовательности S (можно обойтись и без удаления, но тогда на первом шаге надо брать не первые 512, а

следующие 512 бит).

3. Вызываем функцию W. Параметры A, B, C, D — это текущие значения соответствующих двойных слов. Параметр T — это запомненные 512 бит.

4. Прибавляем к A A0.

5. B=B+B0.

6. C=C+C0.

7. D=D+D0.

8. Если длина последовательности 0, выходим.

9. Переходим к шагу 1.

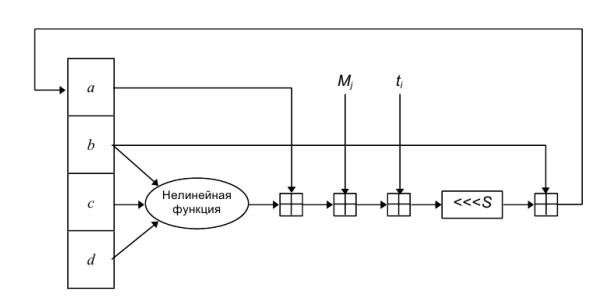


Рис. 4 – структурная схема одной операции алгоритма MD5

После выполнения этого алгоритма A, B, C, D – строка данных в шестнадцатеричном виде, имеющая длину в 128 бит.



Рис. 5 – результат выполнения алгоритма

**Вывод**

В ходе лабораторной работы были получены знания принципе работы хэш-функций. Изучен алгоритм MD5. Так же был реализован программный код, который осуществляет процесс хэширования сообщения.