Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

“Криптография и информационная безопасность”

Аттестационная работа 1

Проверил: Чербу Ольга

Выполнил: Чобану Артём

Кишинев 2022

**Алгоритм MD4**

Шифруемое слово: **aclanguage**

Строка в двоичном представлении:

01100001 01100011 01101100 01100001 01101110 01100111 01110101 01100001 01100111 01100101

Строка состоит из 10 символов. Следовательно, длина двоичного сообщения составляет 80 бит.

**Шаг 1. Добавление недостающих битов**

Добавим один один бит, равый 1 и 367 битов, равынх 0, для того чтобы общая длина сообщения была 448:

01100001 01100011 01101100 01100001 01101110 01100111 01110101 01100001 01100111 01100101 10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

**Шаг 2. Добавление длины сообщения**

Длина сообщения – 80 бит. Двоичное представление:

64-битное представление длины сообщения:

00000000 00000000 00000000 00000000 00000000 00000000 00000000 01010000

Добавим его к результату предыдущего шага:

01100001 01100011 01101100 01100001 01101110 01100111 01110101 01100001 01100111 01100101 10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 01010000

**Шаг 3. Инициализация MD-буфера**

Инициализируем регистры А, B, C, D, из которых состоит 32-битный буфер, следующими числами:

word A: 01 23 45 67

word B: 89 ab cd ef

word C: fe dc ba 98

word D: 76 54 32 10

**Шаг 4. Обработка сообщения блоками по 16 слов**

Принято определять следующие вспомогательные функции:

F (X, Y, Z) = XY | !XZ

G (X, Y, Z) = XY | XZ | YZ}

H (X, Y, Z) = X ^ Y ^ Z}

Происходит обработка каждого блока из 16 слов.

Для каждого блока производятся 3 раунда:

1. Пусть [abcd k s] означает следующую операцию:

a = (a + F(b,c,d) + X[k]) <<< s.

Необходимо провести 16 следующих операций:

[ABCD 0 3] [DABC 1 7] [CDAB 2 11] [BCDA 3 19]

[ABCD 4 3] [DABC 5 7] [CDAB 6 11] [BCDA 7 19]

[ABCD 8 3] [DABC 9 7] [CDAB 10 11] [BCDA 11 19]

[ABCD 12 3] [DABC 13 7] [CDAB 14 11] [BCDA 15 19]

1. Пусть [abcd k s] означает следующую операцию:

a = (a + G(b,c,d) + X[k] + 5A827999) <<< s.

Необходимо провести 16 следующих операций:

[ABCD 0 3] [DABC 4 5] [CDAB 8 9] [BCDA 12 13]

[ABCD 1 3] [DABC 5 5] [CDAB 9 9] [BCDA 13 13]

[ABCD 2 3] [DABC 6 5] [CDAB 10 9] [BCDA 14 13]

[ABCD 3 3] [DABC 7 5] [CDAB 11 9] [BCDA 15 13]

1. Пусть [abcd k s] означает следующую операцию:

a = (a + H(b,c,d) + X[k] + 6ED9EBA1) <<< s

Необходимо провести 16 следующих операций:

[ABCD 0 3] [DABC 8 9] [CDAB 4 11] [BCDA 12 15]

[ABCD 2 3] [DABC 10 9] [CDAB 6 11] [BCDA 14 15]

[ABCD 1 3] [DABC 9 9] [CDAB 5 11] [BCDA 13 15]

[ABCD 3 3] [DABC 11 9] [CDAB 7 11] [BCDA 15 15]

К каждому из регистров А, B, C и D добавляем их значения, имеющиеся в начале итерации.

**Шаг 5. Формирование хеша.**

Резутат – ABCD, то есть конкатенация значений, содержащихся в данных регистрах.

Результат: **5756edfff3c3f65ee8cf02d4f37216f0**