Хэш-фунции

Калитеевский В.
271 группа
2012 г.

MD5

MD5 (англ. Message Digest 5) — 128-битный алгоритм хеширования.

Сообщение делится на блоки по 512 бит, затем от каждого блока вычисляется функция и все результаты функций собираются вместе в 128-битный хеш. Рассмотрим по очереди эти три этапа:

1. Разбиение на блоки.

- Записываем размер сообщения в виде 64-битного целого числа N.
- Добавляем к сообщению один бит равный 1.
- Добавляем к сообщению некоторое число нулевых битов и затем дописываем 64-битный N. Число нулевых битов выбираем так, чтобы длина сообщения была кратна 512 битам.

512б	512б		1	0000000	…..0.....	N(64б)

512 б

сообщение

MD5

2. Обработка 512-битного блока.

MD5 функция аналогична процессору, у которого 4 регистра по 32 бита (W_1,W_2,W_3,W_4). В начале эти регистры инициализируются константами:

W_1 = 01 23 45 67; W_2 = 89 ab cd ef; W_3 = fe dc ba 98; W_4 = 76 54 32 10.

После инициализации процессору подают по очереди 512-битные блоки из дополненного сообщения, чтобы тот изменил свои регистры в зависимости от содержимого блока. Для обработки блока возьмем следующую функцию:

```
md5.T = function(i)
{
    return Math.floor(0x100000000 * Math.abs(Math.sin(i)))
}
```

MD5

Назовём обрабатываемый 512-битный блок массивом X[0..15] из 16-ти 32-битных целых чисел. Процессор умеет выполнять команду [abcd k s i] которая меняет один регистр:

Wa = Wb + ((Wa + X[k] + T(i + 1) + Fi(Wb, Wc, Wd)) <<< s)

Где n <<< s означает циклический сдвиг влево на s бит . MD5 получает 512-битный блок, сохраняет регистры (Qi = Wi) и выполняет 64 команды:

[0123 00 07 00]	[1230 07 22 07]	[2301 14 17 14]
[3012 01 12 01]	[0123 08 07 08]	[1230 15 22 15]
[2301 02 17 02]	[3012 09 12 09]	[0123 01 05 16]
[1230 03 22 03]	[2301 10 17 10]	[3012 06 09 17]
[0123 04 07 04]	[1230 11 22 11]	[2301 11 14 18]
[3012 05 12 05]	[0123 12 07 12]	[1230 00 20 19]
[2301 06 17 06]	[3012 13 12 13]	. . . . .

MD5

Назовём обрабатываемый 512-битный блок массивом X[0..15] из 16-ти 32-битных целых чисел. Процессор умеет выполнять команду [abcd k s i] которая меняет один регистр:

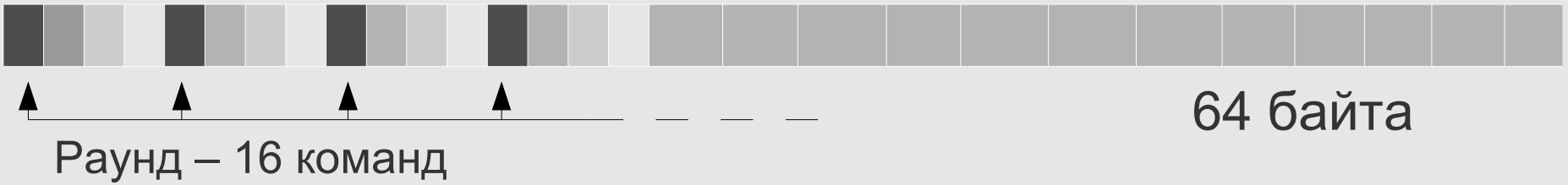
Wa = Wb + ((Wa + X[k] + T(i + 1) + Fi(Wb, Wc, Wd)) <<< s)

Где n <<< s означает циклический сдвиг влево на s бит . MD5 получает 512-битный блок, сохраняет регистры (Qi = Wi) и выполняет 64 команды:

[0123 00 07 00]	[1230 07 22 07]	[2301 14 17 14]
[3012 01 12 01]	[0123 08 07 08]	[1230 15 22 15]
[2301 02 17 02]	[3012 09 12 09]	[0123 01 05 16]
[1230 03 22 03]	[2301 10 17 10]	[3012 06 09 17]
[0123 04 07 04]	[1230 11 22 11]	[2301 11 14 18]
[3012 05 12 05]	[0123 12 07 12]	[1230 00 20 19]
[2301 06 17 06]	[3012 13 12 13]	. . . . .

MD5

Группа из 16-ти команд называется раундом. Параметры команды a, b, c, d, i можно вычислить по её номеру. Параметры k, s стандартны и беруться из таблицы. После выполнения всех 64 команд MD5 добавляет к регистрам их сохранённые значения: Wi = Wi + Qi.



MD5

3. Получение хеша.

После того как MD5 обработал последний 512-битный блок, он соединяет свои регистры в 16-байтное число: [W0, W1, W2, W3]. Это число и есть MD5 хеш.

SHA1

1. Разбиение на блоки.

- Записываем размер сообщения в виде 64-битного целого числа N.
- Добавляем к сообщению один бит равный 1.
- Добавляем к сообщению некоторое число нулевых битов и затем дописываем 64-битный N. Число нулевых битов выбираем так, чтобы длина сообщения была кратна 512 битам.

2. Обработка 512-битного блока.

Как и у MD5 у SHA1 есть 5 регистров по 32 бита.

H_0 = 01 23 45 67

H_1 = 89 ab cd ef

H_2 = fe dc ba 98

H_3 = 76 54 32 10

H_4 = f0 e1 d2 c3

SHA1

Блок сообщения преобразуется из 16 32-битовых слов в 80 32-битовых слов. Получив очередной блок, SHA1 заполняет массив W[0..79] из 32-битных чисел: первые 16 элементов копируются из блока, а остальные элементы вычисляются по очереди по формуле:

$$W_i = (W_{i-3} \text{ xor } W_{i-8} \text{ xor } W_{i-14} \text{ xor } W_{i-16}) <<< 1$$

После этого SHA1 запоминает значения своих регистров (Qi = Hi) и делает 80 одинаковых шагов: он заменяет свои пять регистров [H0, H1, H2, H3, H4] на [T, H0, H1 <<< 30, H2, H3], где T вычисляется на основе номера шага i и значений пяти регистров до замены:

$$T = (H_0 <<< 5) + F_i(H_1, H_2, H_3) + H_4 + W_i + K_i$$

SHA1

$F_i(H1, H2, H3)$	K_i	t
H1 & H2 | ~H1 & H3	**0x5a827999**	**0 ≤ t ≤ 19**
H1^H2^H3	**0x6ed9eba1**	**20 ≤ t ≤ 39**
H1 & H2 | H1 & H3 | H2 & H3	**0x8f1bbcdc**	**40 ≤ t ≤ 59**
H1^H2^H3	**0xca62c1d6**	**60 ≤ t ≤ 79**

После 80-ти шагов SHA1 добавляет к своим регистрам их сохранённые копии: Hi = Hi + Qi.

SHA1

3. Получение хеша.

Обработав все блоки, SHA1 как и MD5 соединяет свои регистры и получает 160-битный хеш (5 регистров по 32 бита). Одно из отличий в том, что SHA1 нумерует байты регистров наоборот.