5.9. Хэш-функция ГОСТ 3411

Алгоритм *ГОСТ 3411* является отечественным стандартом для хэш-функций. Длина хэш-кода, создаваемого алгоритмом *ГОСТ 3411*, равна 256 битам. Алгоритм разбивает сообщение на блоки, длина которых также равна 256 битам. Кроме того, параметром алгоритма является стартовый вектор хэширования *H* - произвольное фиксированное значение длиной также 256 бит.

Алгоритм обработки одного блока сообщения

Сообщение обрабатывается блоками по 256 бит справа налево.

Каждый блок сообщения обрабатывается по следующему алгоритму.

1. Генерация четырех ключей длиной 256 бит каждый.
2. Шифрование 64-битных значений промежуточного хэш-кода H на ключах K_i(i = 1, 2, 3, 4) с использованием алгоритма ГОСТ 28147 в режиме простой замены.
3. Перемешивание результата шифрования.

Для генерации ключей используются следующие данные:

- промежуточное значение хэш-кода H длиной 256 бит;
- текущий обрабатываемый блок сообщения M длиной 256 бит;
- параметры - три значения C_2, C_3 и C_4 длиной 256 бит следующего вида: C_2 и C_4 состоят из одних нулей, а C_3 равно

$1^8\ 0^8\ 1^{16}\ 0^{24}\ 1^{16}\ 0^8\ (0^8\ 1^8)^2\ 1^8\ 0^8\ (0^8\ 1^8)^4\ (1^8\ 0^8)^4$

где степень обозначает количество повторений 0 или 1.

Используются две формулы, определяющие перестановку и сдвиг.

Перестановка P битов определяется следующим образом: каждое 256-битное значение рассматривается как последовательность тридцати двух 8-битных значений.

Перестановка P элементов 256-битной последовательности выполняется по формуле y = φ(x), где x - порядковый номер 8-битного значения в исходной последовательности; y - порядковый номер 8-битного значения в результирующей последовательности.

$\varphi(i + 1 + 4(k - 1)) = 8i + k\ ;\ i = 0 \div 3,\ k = 1 \div 8$

Сдвиг A определяется по формуле

$A(x) = (x_1 \oplus x_2) \,||\, x_4 \,||\, x_3 \,||\, x_2$

Где

x_i - соответствующие 64 бита 256-битного значения x,

|| обозначает конкатенацию.

Присваиваются следующие начальные значения:

i = 1, U = H, V = M.

$W = U \oplus V$, $K_1 = P(W)$

Ключи K_2, K_3, K_4 вычисляются последовательно по следующему алгоритму:

$U = A(U) \oplus C_i$, $V = A(A(V))$, $W = U \oplus V$, $K_i = P(W)$

Далее выполняется шифрование 64-битных элементов текущего значения хэш-кода H с ключами K_1, K_2, K_3 и K_4. При этом хэш-код H рассматривается как последовательность 64-битных значений:

$H = h_4 \| h_3 \| h_2 \| h_1$

Выполняется шифрование алгоритмом ГОСТ 28147:

$s_i = E_{Ki} [h_i] \quad i = 1, 2, 3, 4$

$S = s_1 \| s_2 \| s_3 \| s_4$

Наконец на заключительном этапе обработки очередного блока выполняется перемешивание полученной последовательности. 256-битное значение рассматривается как последовательность шестнадцати 16-битных значений. Сдвиг обозначается Ψ и определяется следующим образом:

$\eta_{16} \| \eta_{15} \| ... \| \eta_1$ - исходное значение

$\eta_1 \oplus \eta_2 \oplus \eta_3 \oplus \eta_4 \oplus \eta_{13} \oplus \eta_{16} \| \eta_{16} \| ... \| \eta_2$ - результирующее значение

Результирующее значение хэш-кода определяется следующим образом:

$X(M, H) = \psi^{61} (H \oplus \psi (M \oplus \psi^{12}(S)))$

где

H - предыдущее значение хэш-кода,

M - текущий обрабатываемый блок,

Ψ^i - i-ая степень преобразования Ψ.

Входными параметрами алгоритма являются:

- исходное сообщение M произвольной длины;
- стартовый вектор хэширования H, длина которого равна 256 битам;
- контрольная сумма Σ, начальное значение которой равно нулю и длина равна 256 битам;
- переменная L, начальное значение которой равно длине сообщения.

Сообщение M делится на блоки длиной 256 бит и обрабатывается справа налево. Очередной блок i обрабатывается следующим образом:

1. $H = X(M_i, H)$
2. $\Sigma = \Sigma \oplus' M_i$
3. L рассматривается как неотрицательное целое число, к этому числу прибавляется 256 и вычисляется остаток от деления получившегося числа на 2^{256}. Результат присваивается L.

Где $\oplus'$ обозначает следующую операцию: Σ и M_i рассматриваются как неотрицательные целые числа длиной 256 бит. Выполняется обычное сложение этих чисел и находится остаток от деления результата сложения на 2^{256}. Этот остаток и является результатом операции.

Самый левый, т.е. самый последний блок M' обрабатывается так:

1. Блок добавляется слева нулями так, чтобы его длина стала равна 256 битам.
2. Вычисляется $\Sigma = \Sigma \oplus' M_i$.
3. L рассматривается как неотрицательное целое число, к этому числу прибавляется длина исходного сообщения M и находится остаток от деления результата сложения на 2^{256}.
4. Вычисляется H = X(M', H).
5. Вычисляется H = X(L, H).
6. Вычисляется H = X(Σ, H).

Значением функции хэширования является H.