РЕАЛИЗАЦИЯ ХЭШ ФУНКЦИЙ И СПОСОБЫ ИХ ВЫЧИСЛЕНИЯ

Гридюшко А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Качиснкий М.В. – к.т.н.,доцент

Функцией хэширования называется отображение H:V*→Vn,где n ∈ N — натуральное число, V* — множество всех двоичных векторов(строк) конечной размерности (включая пустую строку), Vn—множество всех n-мерных двоичных векторов. Аргумент M ∈ V* функции хэширования называется сообщением. Частью сообщения называется любой подвектор сообщения M. Хэш-кодом(хэш-значением) сообщения M ∈ V* называется значение H(M) ∈ Vn.

На сегодняшний день наиболее распространены функции хэширования, построенные по итеративному принципу (итеративные функции хэширования). Он восходит к работам [6, 7] Р. Меркля (Ralph C. Merkle) и И. Дамгорда(Ivan Damgard) 1989 года, в связи с чем итеративная конструкция получила название конструкции Меркля–Дамгорда. Конструкция Меркля – Дамгорда позволяет свести задачу построения хэш-функции H:V*→Vn к задаче построения отображения g:Vq×V_l→Vq с определенными свойствами. По итеративному принципу построены такие хэш-функции, как MD5 [8], SHA-1 [3, 4], семейство хэш-функций SHA-2 [4], хэш-функции ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012. Опишем итеративные хэш-функции в общем виде и введем обозначения, которые будут использоваться в дальнейшем. Перед вычислением значения итеративной функции хэширования исходное сообщение M∈V* преобразуется в сообщение M∈V*, длина которого кратна l. Данное преобразование называется процедурой дополнения сообщения(message padding), а сообщение M— расширенным сообщением(padded message). Дополнение сообщения может осуществляться различными способами, но, как правило, включает два этапа: конкатенация сообщения со значением его длины, записанным в двоичном виде, и с некоторой последовательностью до длины, кратной l, так, чтобы каждому исходному сообщению соответствовало единственное расширенное сообщение. Пусть теперь M — сообщение, полученное с помощью процедуры дополнения сообщения M, и M=m1‖m2‖⋯‖m_t, m_i ∈ V_l, i=1,...,t. Векторы m_i ∈ V_l, i= 1,...,t, называются блоками сообщения M. Алгоритм вычисления хэш-кода h=H(M) итеративной функции хэширования состоит из последовательного вычисления значений так называемой функции сжатия(compression function) g:Vq×V_l→Vq от результата предыдущей итерации и очередного блока сообщения:

$$h_i = g(h_i{-}1,\ m_i),\ i=1,...,t, \qquad (1),$$

где h_0 равно заданному фиксированному значению из множества Vq. Значение h_0 принято называть инициализационным вектором (initialization vector, initial value, IV). Значение хэш-кода h полагается равным f (h_t, M), где f:Vq×V*→Vn— некоторое заключительное преобразование. Завершающее преобразование f часто не зависит от M и является тождественным преобразованием первого аргумента (в этом случае q=n) или операцией редуцирования первого аргумента (в этом случае q>n). Для хэш-функции ГОСТ Р 34.11-94 завершающее преобразование заключается в применении функции сжатия к блоку, являющемуся суммой по модулю 2^{256} всех блоков сообщения : f(h_t, M)=g(h_t, Σ), Σ=m1⊞...⊞m_t. Данный подход эквивалентен дополнению исходного сообщения помимо двоичной записи длины значением Σ, которое принято называть контрольной суммой блоков сообщения.

Список использованных источников:

1.Колчин В.Ф., Севастьянов Б.А., Чистяков В.П.Случайные размеще-ния. — М.: Наука, 1976.

2.Матюхин Д.В., Шишкин В.А.О криптографической стойкости хэш-функции ГОСТ Р 24.11-94 // Обозр. прикл. и промыш. матем. — 2010. —Т. 17. — С. 750–751.

3. FIPS PUB 180-1. Secure hash standard. — April, 1995. —http://www.itl.nist.gov/fipspubs/fip180-1.htm.

4. FIPS PUB 180-2. Secure hash standard. — August, 2002. —http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

5.Aumasson J.-P.Faster multicollisions //INDOCRYPT'08. Lect. NotesComput. Sci. — 2008. — V. 5365. — P. 67–77.

6.Damgaard I.A design principle for hash functions // CRYPTO'89. Lect. NotesComput. Sci. — 1990. — V. 435. — P. 416–427.

7.Merkle R.C.One way hash functions and DES // CRYPTO'89. Lect. NotesComput. Sci. — 1990. — V. 435. — P. 428–446.

8.Rivest R.The MD5 message-digest algorithm. Request for comments (RFC)1321, Internet Activities Board, Internet Privacy Task Force, April 1992.