ИССЛЕДОВАНИЕ АЛГОРИТМА ХЭШ ФУНКЦИИ SHA-1

Полякова Н.С , Чан Тхюи Зунг
Томский политехнический университет, г. Томск
634050, Россия, г. Томск, пр-т Ленина, 30
Email: bluesky25792@gmail.com

Введение

Информация является одним из ценнейших предметов современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. В то же время, легкость и скорость такого доступа значительно повысили и угрозу нарушения безопасности данных при отсутствии мер относительно их защиты, а именно – угрозу несанкционированного доступа к информации. Поэтому проблема разработки, совершенствования и применения методов защиты информации в процессе её хранения и передачи на сегодняшний день является одной из наиболее актуальных. В современных системах защиты информации огромную роль играют не только методы стеганографии, но и методы криптографии.

Криптография – это наука об обеспечении безопасности данных, использующая математику для преобразования информации в другие форматы с целью сокрытия. На сегодняшний день, она является важной отраслью и имеет множество применений. С помощью криптографии ведется поиск решений четырех важных проблем безопасности – конфиденциальности, аутентификации, целостности и контроля участников взаймодействия.

Шифрование – это способ повышения безопасности сообщения или файла, при котором их содержимое преобразуется. После преобразования это содержимое может быть прочитано только пользователем, обладающим соответствующим ключом шифрования для его расшифровки. Например, при совершении покупки в Интернете данные сделки (такие как адрес, телефон, номер кредитной карты) обычно зашифровываются в целях безопасности. Шифрование использует ключи шифрования – расшифровки и алгоритм шифрования - расшифровки. Процесс шифрования показан на рисунке 1.

Рис.1. Процесс шифрования

Алгоритм SHA-1

Безопасный хэш-алгоритм (Secure Hash Algorithm) был разработан национальным институтом стандартов и технологии (NIST) и опубликован в качестве федерального информационного стандарта (FIPS PUB 180) в 1993 году. SHA-1, как и MD5, основан на алгоритме MD4. SHA-1 - алгоритм вычисления сжатого представления цифровых данных, которое называют дайджестом сообщения. При этом вырабатывается 160 битный хэш-код входных данных, который широко распространен в мире, используется во многих сетевых протоколах защиты информации (TLS, SSL, PGP, SSH, S/MIME, IPSec. Алгоритм состоит из следующих шагов:

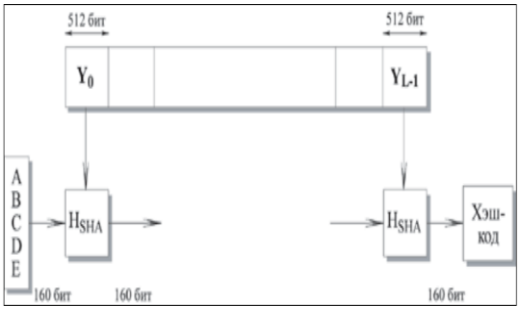

Рис.2. Алгоритм SHA-1

Шаг 1: Добавление недостающих битов. Сообщение добавляется таким образом, чтобы его длина была кратна 448 по модулю 512 (длина 448 mod 512). 1 ≡ 448 mod 512 или 1 = n* 512 +448(n,1). Таким образом, число добавляемых битов находится в диапазоне от 1 до 512.

Шаг 2 : Добавление длины. К сообщению добавляется блок из 64 битов. Этот блок трактуется как беззнаковое 64-битное целое и содержит длину исходного сообщения до добавления. Результатом первых двух шагов является сообщение, длина которого кратна 512 битам. Расширенное сообщение может быть представлено как последовательность L 512-битных блоков Y0, Y1, . . . , YL-1, так что общая длина расширенного сообщения есть N= L * 16 * (32*16) = L * 512 бит. Таким образом, результат кратен шестнадцати 32-битным словам.

Шаг 3: Инициализация SHA-1 буфера (SHA-1 buffer). Используется 160-битный буфер для хранения промежуточных и окончательных результатов хэш-функции. Буфер может быть представлен как пять 32-битных регистров A, B, C, D и E. Эти регистры инициализируются следующими шестнадцатеричными числами: A= 01 23 45 67, B= 89 AB CD EF, C= FE DC BA 89, D= 76 54 32 10, E= C3 D2 E1 F0.

Шаг 4: Обработка сообщения в 512-битных (16-словных) блоках.
Основой алгоритма является 4 циклических обработки, состоящие из 80 шагов. Все 80 циклических шагов имеют одинаковую структуру, но отдельную логическую функцию f1, f2, f3, f4.

$(0 \le t \le 19)$	$f_1 = f(t,B,C,D)$	$(B \wedge C) \vee (\neg B \wedge D)$
$(20 \le t \le 39)$	$f_2 = f(t,B,C,D)$	B xor C xor D
$(40 \le t \le 59)$	$f_3 = f(t,B,C,D)$	$(B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
$(60 \le t \le 79)$	$f_4 = f(t,B,C,D)$	B xor C xor D

Рис.3. Функции f1, f2, f3, f4

Один циклический шаг состоит из текущего 512-битного обрабатываемого блока, одного буфера ABCDE в 160 бит, и изменяет содержимое этого буфера. В каждом цикле используется дополнительная константа Kt, которая принимает только четыре различных значения. Kt= 5A827999, Kt= 8F1BBCDC (0≤t≤19), Kt= 6ED9EBA1 (20≤t≤39), Kt= 8F1BBCDC (40≤t≤59), Kt= CA62C1DC (60≤t≤79).

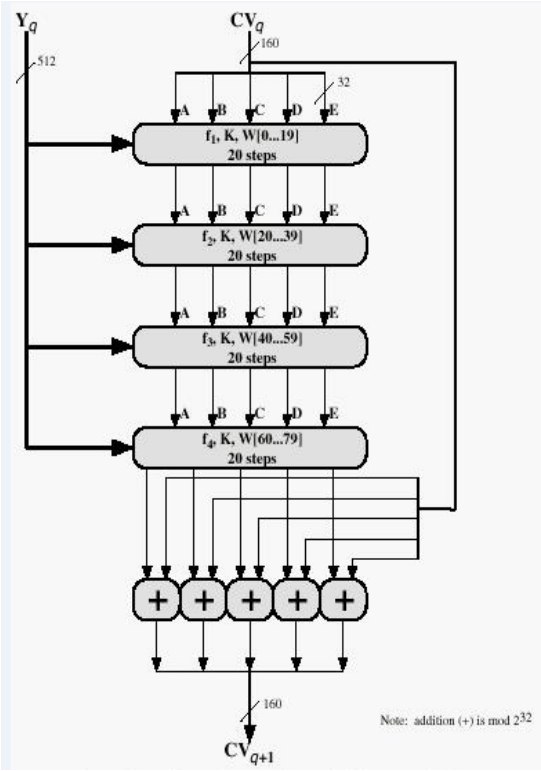

Рис.4. SHA-1 processing of a single 512 bit Block

Шаг 5: выход. После обработки всех 512-битных блоков выходом L-ой стадии является 160-битный дайджест сообщения.

Сравнение алгоритмов SHA-1 и MD5

MD5 — один из серии алгоритмов по построению дайджеста сообщения, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института.

Сравним оба алгоритма в соответствии с теми целями:

Безопасность: наиболее очевидное и наиболее важное различие состоит в том, что дайджест SHA-1 на 32 бита длиннее, чем дайджест MD5. Если предположить, что оба алгоритма не содержат каких-либо структурированных данных, которые уязвимы для криптоаналитических атак, то SHA-1 является более стойким алгоритмом. Используя лобовую атаку, труднее создать произвольное сообщение, имеющее данный дайджест, если требуется порядка 2160 операций, как в случае алгоритма SHA-1, чем порядка 2128 операций, как в случае алгоритма MD5. Используя лобовую атаку, труднее создать два сообщения, имеющие одинаковый дайджест, если требуется порядка 280 как в случае алгоритма SHA-1, чем порядка 264 операций как в случае алгоритма MD5.

Скорость: так как оба алгоритма выполняют сложение по модулю 232, они рассчитаны на 32-битную архитектуру. SHA-1 содержит больше шагов (80 вместо 64) и выполняется на 160-битном буфере по сравнению со 128-битным буфером MD5. Таким образом, SHA-1 должен выполняться приблизительно на 25% медленнее, чем MD5 на той же аппаратуре.

Простота и компактность: оба алгоритма просты и в описании, и в реализации, не требуют больших программ или подстановочных таблиц. Тем не менее, SHA-1 применяет одношаговую структуру по сравнению с четырьмя структурами, используемыми в MD5. Более того, обработка слов в буфере одинаковая для всех шагов SHA-1, в то время как в MD5 структура слов специфична для каждого шага.

Архитектуры little-endian и big-endian: MD5 использует little-endian схему для интерпретации сообщения как последовательности 32-битных слов, в то время как SHA-1 задействует схему big-endian. Каких-либо преимуществ в этих подходах не существует.

Исследование алгоритма SHA-1 проведено с целью дальнейшей реализации в приложение и тестирования его работы.

Список литературы:

1. https://ru.wikipedia.org/wiki/MD5.
2. http://doc.edu.vn/tai-lieu/de-tai-ung-dung-he-mat-ma-rsa-va-chu-ki-dien-tu-vao-viec-ma-hoa-thong-tin-trong-the-atm-7244/.
3. Баричев С.Г, Серов Р.Е, «Основы современной криптографии».
4. www.innov.ru/.../Сравнение%20SHA%20и%20MD5.doc