Алтухова Валентина Александровна
студентка
Анфилова Екатерина Борисовна
студентка
Тезик Константин Анатольевич
канд. техн. наук, доцент
ФГБОУ ВО «Юго-Западный государственный университет»
г. Курск, Курская область

АЛГОРИТМЫ ХЭШИРОВАНИЯ ГОСТ Р 34.11-2012 И SHA-3

Аннотация*: в данной статье освещается понятие «хэш-функции». В работе рассмотрены криптографические стандарты РФ (ГОСТ Р 34.11-2012) и США (SHA-3).*

Ключевые слова*: хэш-функция, электронная цифровая подпись, ЭЦП, SHA-3, ГОСТ Р 34, 11-2012, криптографическая губка.*

Проблема защиты информации в настоящее время является актуальной. Существует большое число способов и методов повышения уровня безопасности, в том числе и применение алгоритмов шифрования. На сегодняшний день хэш-функции часто используются в информационной сфере. С помощью хэш-функций реализуют:

1. Проверку целостности данных.

Идея заключается в сохранении хэш-кода и последующем сравнении с эталоном повторно вычисленного для тех же данных хэш-значения. Неравенство сравниваемых величин означает нарушение целостности;

2. Системы аутентификации (используют хэш-функций для паролей).

3. Создание и проверку электронно-цифровой подписи (ЭЦП) [2].

Рассмотрим алгоритмы хеширования, такие как SHA-3 – действующий с 5 августа 2015 года криптографический стандарт США и ГОСТ Р 34.11–2012, действующий российский криптографический стандарт с 1 января 2013 года.

Keccak (SHA-3) реализуется с помощью принципа «sponge function», то есть криптографической конструкции губки, в основе которой лежит многораундовая блочная бесключевая перестановка, которая выполняется по тому же принципу, как блочные шифры. Функция губки используется для создания алгоритмов шифрования с переменной длиной на входе и переменной длиной на выходе.

Конструкцию губки можно отобразить через две стадии:

1) absorbing (абсорбция, впитывания) – сначала задаётся исходное состояние из нулевого вектора размером до 1600 бит. Далее выполняется операция *xor* очередного блока исходного сообщения с первой частью состояния S_1 размера *r* (бит), оставшаяся часть S_2 состояния ёмкостью *c* остается незатронутой. Результат помещается в S_1, а затем состояние *S* обрабатывается функцией *f* – многораундовой бесключевой псевдослучайной перестановкой, и так повторяется до исчерпания блоков исходного сообщения;

2) squeezing (фаза сжатия, отжатия) – состояние *S* подаётся на функцию *f*, после чего часть S_1 подаётся на выход. Эти действия повторяются, пока не будет получена последовательность нужной длины (например, длины хэша).

Необходимо отметить то, что мельчайшее изменение исходного текста приводит к существенным переменам хеш-значения, вследствие такого свойства криптографии как лавинный эффект [3]. Рассмотрим пример: «A little body often harbours a great soul» содержит значение хеш-функции размером 224 бита: Z=2730e312ble5459a3cc23100a838a02c683a4ba926d03257e27a5a84.

При добавлении точки в конец строки хеш-значение станет отличным от Z: Z_1=e109fd01088302f20159ee5ec87239bd3bb01bf9e600f8cc81858c56.

Особенность алгоритма шифрования Keccak происходит из запутанной, мультикруглой перестановки *f*.

ГОСТ Р 34.11–2012 (Стрибог) является новым криптографическим стандартом, действующим в Российской Федерации. ГОСТ Р 34.11–2012 – это совокупность хеш-функций, содержащее в себя 2 функции. Функцию с длиной выходного значения в 256 или 512 бит и размер блока входных данных в 512 бит. Обе эти функции обладают одинаковой структурой и различаются лишь начальным

внутренним состоянием. Входными данными для этих функций является 512 битовый блок данных. При условии, что исходные данные больше 512 бит происходит разделение сообщения на блоки. Но если длина меньше 512 бит, то в таком случае выполняется дополнение сообщения [1].

Основной особенностью современной хеш-функции Стрибог является функция сжатия. Главным в функции сжатия, основанной на конструкции Миагучи-Пренели, стали три преобразования: нелинейное биективное преобразование, перестановка байт, линейное преобразование. После выполнения функции сжатия, в результате действия которой обновляется внутреннее состояние хеш-алгоритма, вычисляется контрольная сумма блоков и число обработанных бит. Когда все блоки исходных данных обработаны, производятся вычисления: обработка функцией сжатия блока с общей длиной сообщения и обработка функцией сжатия блока с контрольной суммой. Что и является завершением вычисления хеш-функции Стрибог.

В заключении стоит отметить, что с хешированием мы сталкиваемся практически на каждом шагу: при работе с браузером (список Web-ссылок), текстовым редактором и переводчиком, языками скриптов (Perl, PHP), компилятором (таблица символов).

Список литературы

1. Бородин М.А. Эффективная реализация базовых криптографических конструкций: перспективного алгоритма блочного шифрования с длиной блока 128 бит, функции хеширования ГОСТ Р 34.11-2012 и ЭЦП ГОСТ Р 34.10-2012 / М.А. Бородин, А.С. Рыбкин. – М.: ИнфоТеКС, 2014. – 33 с.

2. Спеваков А.Г. Основы правового обеспечения информационной безопасности [Текст]: Учебное пособие / А.Г. Спеваков, А.П. Фисун. – Курск: Юго-Зап. гос. ун-т, 2013. Ч. 1. – 150 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М.: Триумф, 2002. – 816 с.