УДК 519.72

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ХЭШ-ФУНКЦИЙ

Заболотникова Мария Александровна
студент
Мичуринский государственный агарный университет
г. Мичуринск, Россия,
Картечина Ольга Сергеевна,
студент
Российский университет транспорта (МИИТ),
г. Москва, Россия
Пчелинцева Наталия Викторовна
старший преподаватель
Мичуринский государственный агарный университет
г. Мичуринск, Россия,
natas79@mail.ru

Аннотация: в статье представлена сравнительная характеристика алгоритмов для вычисления хеш-функции. MD5, SHA-1, SHA-2 и другие версии SHA, а также отечественные алгоритмы, изложенные в ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 «Стрибог».

Ключевые слова: хеширование, хеш-функция, хэш, алгоритм.

В настоящее время практически ни одно приложение криптографии не обходится без использования хэширования.

Хэш-функция - это математическая или другая функция, которая для строки произвольной длины вычисляет некоторое целое значение и некую строку фиксированной длины. Криптографические хэши используют, везде начиная с хранения паролей и заканчивая системами проверки. Цель хорошей хэш-функции состоит в том, чтобы сделать чрезвычайно сложным для

злоумышленников найти способы генерации входных данных которые хэшируются с одинаковым значением [1-3].

К ключевым функциям хэширования предъявляются следующие требования: 1) невозможность фабрикации, 2) невозможность модификации.

Два разных сообщения не в коем случае не должны преобразовываться в одинаковый хэш, а два идентичных - всегда должны возвращаться в один и тот же хэш, иначе возникает явление которое называется коллизией.

Коллизия – это ситуация когда разным ключам соответствует одно значение хэш-функции. Алгоритмы хэширования должны быть устойчивыми к атакам нахождении прообраза [1, 4].

Одним из первых стандартом алгоритма был MD5 hash. Функциональность этого хэша довольно проста. Его 128 битная выходная фиксированная длина и простота операций сделали MD5 очень легким для взлома и восприимчивым к атакам.

Агентством национальной безопасности США в 1995 году был разработан и введен в качестве федерального стандарта алгоритм SHA-1. Этот алгоритм создает 160 битные выходы фиксированной длинны. SHA-1 улучшил MD5 увеличил длину вывода, количество и сложность операции и более стойким к атакам алгоритмов. Вплоть до 2017 года SHA-1был самым популярным хэшем используемым для криптографической подписи [2, 4, 5].

В хэше SHA-1 были найдены серьезные криптографические уязвимости. В феврале 2017 года была обнаружена атака на хэш с помощью коллизии, которая сделала SHA-1 бесполезной для защиты электронной подписи. SHA-2 выбран новым стандартом криптографического хэширования [9].

SHA-2 часто называют семейством хэш-функций, потому что содержит много хэшев разных размеров – 224-, 256-, 384, 512 битные последовательности. Его выходная фиксированная длина 256 битная. Некоторые его характеристики совпадают с SHA-1, но SHA-2 считается более «стойким». Индустрия инфраструктуры открытых ключей (ИОК) рекомендует для обеспечения

безопасности, чтобы любой объект инфраструктуры, использующий SHA-1 был переведен на более безопасным SHA-2 [6, 7, 9].

В России принят ГОСТ Р34.11-94, который является отечественным стандартом для хеш-функций. Его структура довольно сильно отличается от структуры алгоритмов SHA-1,2 или MD5. Длина хеш-кода, создаваемого алгоритмом ГОСТ Р 34.11-94, равна 256 битам. В качестве вспомогательной функции в ГОСТ 34.11-94 используется алгоритм по ГОСТ 28147-89 в режиме простой замены [8].

ГОСТ Р 34.11-2012 «Стрибог» - детище отечественных программистов, состоящее из пары хэш-функций, с длинами итогового значения 256 и 512 Бит. Криптографическая стойкость существенно осложняет поиск коллизий.

Таким образом, методы и сферы применения хэширования неограниченны независимо от того какие алгоритмы мы выбираем он должны обладать высокой скоростью работ и достаточной криптографической надежностью.

Список литературы:

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2020;

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019;

3. Петрушин В.Н. Нормальное и бета-распределение а оценке ограниченных случайных величин / В.Н. Петрушин, Н.В. Каречина // Вестник МГУП имени Ивана Федорова. – 2007. – № 3. – С. 63-70;

4. Пчелинцева Н.В. Методические аспекты количественной оценки риска в аграрной сфере производства / Н.В. Пчелинцева// Наука и Образование. – 2019. – № 3. – С. 37.

5. Абалуев Р.Н. Машинное обучение в среде СУБД MS SQL SERVER / Р.Н. Абалуев, А.А. Крумкаченко // Наука и Образование – 2019. – №4. – С. 52.

6. Иерархический анализ экспериментальных данных / Л.В. Бобрович, Н.В. Картечина, Н.В. Андреева, С.О Чиркин. // Наука и Образование. – 2019. – № 3. – С. 2.

7. Некоторые возможности применения Mathcad для решения инженерных задач в АПК / О.С. Дьячкова, С.В. Дьячков, О.С. Картечина, Н.В. Картечина // Наука и Образование. – 2019. – № 4. – С. 203

8. Абалуев Р.Н. Анализ и оценка материалов для 3d-печати с использованием технологии лазерной стереолитографии / С.О. Чиркин, Р.Н. Абалуев //Наука и Образование. – 2019. – № 4. – С. 131.

9. Абалуев Р.Н. Обзор современных подходов к обеспечению информационной безопасности при создании инфраструктуры интернета вещей в агропромышленном комплексе / Р.Н. Абалуев, А.А. Крумкаченко // Наука и Образование. - 2019. – № 2. – С. 289.

COMPARATIVE ANALYSIS OF HASH FUNCTION ALGORITHMS

Zabolotnikova Maria Alexandrovna,
student
Michurinsk State Agrarian University
Michurinsk, Russia
natas79@mail.ru
Kartechina Olga Sergeevna
student
Russian University of transport (MIIT),
Moscow, Russia
Pchelintseva Natalia Vladimirovna
senior lecturer
Michurinsk State Agrarian University
Michurinsk, Russia
natas79@mail.ru

Abstract: the article presents a comparative characteristic of algorithms for calculating the hash function. MD5, SHA-1, SHA-2 and other versions of SHA, as well as domestic algorithms set out in GOST R 34.11-94, GOST R 34.11-2012 "Stribog".

Keywords: hashing, hash function, hash, algorithm.