DOI: 10.58168/CISMP2024_252-256
УДК 004.051

ОЦЕНКА СТОЙКОСТИ АЛГОРИТМОВ SHA-1 И СЕМЕЙСТВА SHA-2

А.Г. Абрасимовская[1], И.С. Голубятников[1], М.А. Сиваш[2]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»
[2]Военный университет радиоэлектроники

Аннотация. В данной статье рассматривается понятие хеширования. Особое внимание уделяется алгоритмам SHA-1 и семейству SHA-2, включая детали их структуры и применения. Представлен анализ параметров стойкости этих алгоритмов, с акцентом на сравнение их устойчивости к коллизионным атакам и атакам нахождения прообраза. Обоснованный вывод о снижении надежности SHA-1 и преимуществе алгоритмов SHA-2 позволяет сформировать четкое представление о текущих угрозах и актуальных решениях в области криптографии.

Ключевые слова: хеширование, SHA-1, SHA-2, стойкость алгоритмов, коллизионные атаки, атака нахождения прообраза.

EVALUATION OF THE DURABILITY OF THE SHA-1 AND SHA-2 FAMILY ALGORITHMS

A.G. Abrasimovskaya[1], I.S. Golubyatnikov[1], M.A. Sivash[2]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov
[2] Military university of radio electronics

Abstract. This article discusses the concept of hashing. Special attention is paid to the SHA-1 algorithms and the SHA-2 family, including details of their structure and application. An analysis of the resistance parameters of these algorithms is presented, with an emphasis on comparing their resistance to collision attacks and preimage finding attacks. The reasoned conclusion about the decrease in the reliability of SHA-1 and the advantage of SHA-2 algorithms allows us to form a clear understanding of current threats and relevant solutions in the field of cryptography.

Keywords: hashing, SHA-1, SHA-2, algorithm persistence, collision attacks, preimage finding attack.

Введение

Криптографическая функция хеширования – алгоритм, преобразующий сообщение произвольного размера в массив битов фиксированного размера, именуемого хеш-значением сообщения или дайджестом. [1]

Показатели качества криптографической функции являются:

- детерминированность – результатом преобразования одинакового сообщения должен быть одинаковый дайджест;

- необратимость – высокая трудоемкость восстановления сообщения из дайджеста;

- отсутствие коллизий – каждому сообщению должен соответствовать уникальный дайджест;

- присутствие «лавинного» эффекта – любое изменение сообщения должно приводить к полному изменению дайджеста.

1 Алгоритмы криптографического шифрования SHA-1 и семейство SHA-2

Аббревиатура SHA расшифровывается как Secure Hash Algorithm. Разработан Агентством Национальной Безопасности (АНБ) США в 1990х годах. Первая спецификация SHA-1 была опубликована в 1993г, однако вскоре была отозвана в виду большого количества обнаруженных дефектов. Релиз обновленной спецификации пришелся на 1995г, а спецификации 1993г неофициально было присвоено название SHA-0 [2].

Функции семейства SHA-2 были разработаны АНБ США в 2001г и опубликованы Национальным институтом стандартов и технологий (NIST). В настоящее время популярной функцией этого семейства является SHA-256, используемая в протоколе TLS, ключах SSH, для проверки транзакций и доказательства выполнения работы в криптовалютах и пр [3].

Достаточно большое количество различных функций хеширования в семействе обусловлено различным сочетанием измененных векторов инициализации, усеченных выходов и различной длиной слов. Так, алгоритм SHA-512 похож на SHA-256, с различием в длине слова.

В рассматриваемых алгоритмах преобразования производятся со следующими элементами:

- для преобразований используются шестнадцатеричные цифры;

- слово соответствует фиксированной двоичной строке, которая преобразуется в шестнадцатеричную;

- целое между 0 и максимальной длиной слова может рассматриваться как слово;

- блок – последовательность слов.

Размеры основных элементов для рассматриваемых алгоритмов представлены в табл. 1.

Таблица 1 – Размеры основных элементов

Алгоритм	Сообщение, бит	Блок, бит	Слово, бит	Дайджест, бит
SHA-1	$<2^{64}$	512	32	160
SHA-256	$<2^{64}$	512	32	256
SHA-512	$<2^{128}$	1024	64	512

SHA-256 оперирует 32-битными словами, в то время как SHA-512 – 64-битными. Поэтому вычисление SHA-256 занимает в 2-4 раза меньше времени чем SHA-512 на 32-разрядных процессорах, а SHA-512 работает в 1,5 раза быстрее SHA-256 на 64-разрядных [4].

2 Параметры оценки стойкости алгоритмов хеширования

Самыми важными типами атак на криптографические функции считаются атаки нахождения прообраза и коллизионные атаки.

Атаки нахождения прообраза – поиск исходного сообщения по исходному дайджесту.

Коллизионная атака – поиск двух разных сообщений с одинаковыми дайджестами.

В виду неограниченности поиска одним хеш-значением, коллизионная атака является более простой, поэтому уровень стойкости криптографической функции хеширования измеряется в битах и представляет собой вычислительную сложность реализации коллизионной атаки [5].

3 Сравнительная оценка стойкости SHA-1 и SHA-2

Уровень стойкости зависит от размера вычисляемого дайджеста. Так, максимальная сложность атаки нахождения прообраза и коллизионной атаки будет вычисляться по формулам (1) и (2) соответственно [6].

$$k = 2^n \quad (1)$$

$$k = 2^{n/2} \quad (2)$$

где n – размер хеша в битах.

Уровни стойкости рассматриваемых хеш-функций представлены в табл. 2.

Таблица 2 – Уровень стойкости хеш-функции

Атака	Сложность коллизионной атаки	Сложность атаки нахождения прообраза	Уровень стойкости, бит
SHA-1	2^{80}	2^{160}	80
SHA-256	2^{128}	2^{256}	128
SHA-512	2^{256}	2^{512}	256

В виду более короткого дайджеста, SHA-1 отличается высоким быстродействием. Однако, это упрощает процесс полного перебора. В этом свете длина дайджеста следующего поколения была увеличена.

Таким образом, из-за низкой стойкости SHA-1 была признана небезопасной. Наиболее стойкой считается SHA-512, однако, она проигрывает в быстродействии. Поэтому оптимальным вариантом считается SHA-256, так как современные вычислительные мощности пока не могут осуществить достаточное количество переборов для обращения хеша такого размера [7].

Заключение

Выбор длины дайджеста сильно зависит целей использования, соответственно, от этого же зависит и стойкость самой хеш-функции. В этой связи изучение вопроса требует дальнейшей проработки с учетом конкретных исходных данных, характеризующих условия применения криптографических алгоритмов.

Разработка алгоритмов шифрования будет продолжаться, так как наука и техника стремительно развивается, предоставляя новые методы и подходы, а также наращивая вычислительные мощности.

Список литературы

1. Титов, М. Ю. Пути повышения эффективных способов защиты информации в беспилотных летательных аппаратах двойного назначения / М. Ю. Титов // Моделирование систем и процессов. – 2024. – Т. 17, № 2. – С. 82-92. – DOI 10.12737/2219-0767-2024-17-2-82-92. – EDN IQOQPI.

2. Соединенные Штаты Америки. Федеральный стандарт обработки информации (FIPS). "Стандарт безопасного хэширования": [опубликован Национальным институтом науки и технологий, апрель 1993 года].

3. Mycryptopedia. Просвещение мира о криптовалюте. – URL: https://www.mycryptopedia.com/sha-256-related-bitcoin/ (дата обращения: 07.10.2024).

4. Моисеев, В.С. Об одном подходе к обеспечению активной защиты информационных систем / В.С. Моисеев, П.И. Тутубалин // Вестник Казанского государственного технического университета им. А.Н. Туполева. - 2011. - No 2. - С. 129-135.

5. Тутубалин, П.И. Оптимизация выборочного контроля целостности информационных систем / П.И. Тутубалин // Информация и безопасность. - 2012. - Т. 15. - No 2. - С. 257-260.

6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.

7. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. — М. : Диалектика, 2004. — 432 с. — 3000 экз. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3.

References

1. Titov, M. Yu. Ways to improve effective ways of protecting information in dual-purpose unmanned aerial vehicles / M. Yu. Titov // Modeling of systems and processes. - 2024. – Vol. 17, No. 2. – pp. 82-92. – DOI 10.12737/2219-0767-2024-17-2-82-92. – EDN IQOQPI.

2. United States of American. Federal Information Processing Standard (FIPS). "Secure Hash Standard": [published by National Institute of Science и Technology, April 1993].

3. Mycryptopedia. Educating the World on Cryptocurrency. – URL: https://www.mycryptopedia.com/sha-256-related-bitcoin/ (date of access: 07.10.2024).

4. Moiseev, V.S. On one approach to ensuring active protection of information systems / V.S. Moiseev, P.I. Tutubalin // Bulletin of Kazan State Technical University named after A.N. Tupolev. - 2011. - No. 2. - pp. 129-135.

5. Tutubalin, P.I. Optimization of selective control of the integrity of information systems / P.I. Tutubalin // Information and security. - 2012. - Vol. 15. - No. 2. - pp. 257-260.

6. Schneier B. Applied cryptography. Protocols, algorithms, source texts in C. — M.: Triumph, 2002. — 816 p. — 3000 copies. — ISBN 5-89392-055-4.

7. Nils Ferguson, Bruce Schneier. Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — M. : Dialectics, 2004. — 432 p. — 3000 copies. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3.