ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет информатики и вычислительной техники

Дисциплина:
«*Теория информационной безопасности и методология защиты информации*»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

Выполнил:
Студент гр. P3231
Кислицин Алексей Андреевич

Проверил:
Есипов Дмитрий Андреевич,
инженер ФБИТ

Санкт-Петербург
2022г.

Семейство хэш-функций SHA
SHA-2 (Secure Hash Algorithm 2)

Семейство криптографических алгоритмов: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224.
Число в названии алгоритма означает, что на выходе мы получим строку **фиксированной длины**, например, 256 бит независимо от того, какие данные поступят на вход.
Разработано Агентством национальной безопасности США и опубликованы Национальным институтом стандартов и технологий в FIPS PUB 180-2 в **августе 2002 года**. Постепенно добавлялись новые алгоритмы.

История создания SHA-3

Национальный институт стандартов и технологий (NIST) в течение 2007—2012 провёл конкурс на новую криптографическую хеш-функцию, предназначенную для замены SHA-1 и SHA-2.

Организаторами были опубликованы критерии:

• Безопасность

• Производительность и стоимость

• Гибкость и простота дизайна

В финальный тур попали всего 5 алгоритмов:

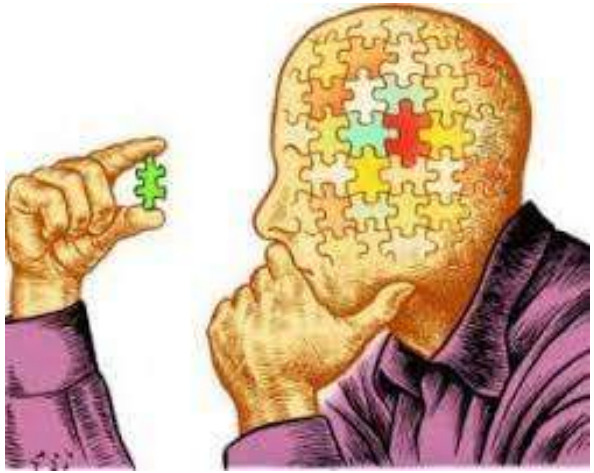
BLAKE, Grøstl, JH, Keccak, Skein

Победителем и новым SHA-3 стал алгоритм Keccak.

Область применения SHA-3

•Проверка целостности сообщений и файлов
•Верификация пароля
•Цифровая подпись

•Криптовалюты (позволяет вводить и
•выводить огромные объемы данных, лучше SHA - 2)



Алгоритм SHA-3

-Sponge-функция - многораундовая функция. На каждом этапе применяется одна и та же функция, реализующая псевдо-случайную перестановку

-Absorbing - на каждом раунде очередной кусок строки подмешивается только к части состояния, тогда как псевдо-случайная перестановка f обрабатывает всё состояние целиком, размазывая таким образом строку по состоянию и делая его зависимым от всей строки.

-Squeezing - Чтобы получить собсно хэш, мы продолжаем применять функцию перестановки f к состоянию, и на каждом этапе копируем из него лишь кусок размера r до тех пор, пока не получим хэш необходимой длины(эти куски мы конкатенируем). Это т.н. «отжатие» губки.

идеальная хеш-функция must have

-детерминирована

-быстро вычисляется для любого

-необратимая

-отсутствие коллизий

-малые отличия в сообщении = большие отличия в хэшах

УНИВЕРСИТЕТ ИТМО

Источники

https://habr.com/ru/post/168707/

https://tproger.ru/translations/sha-2-step-by-step/

https://m.habr.com/ru/company/selectel/blog/530262/

ITMO more than a UNIVERSITY

Спасибо за внимание!

ITMOre than a UNIVERSITY