Математические основы защиты информации и информационной безопасности

Семейство хэш-функций SHA. SHA-512.

Е. А. Баулин[1]

[1]Российский Университет Дружбы Народов
НФИмд-02-22

Содержание

Цель и задачи

Цель доклада:

Рассмотреть семейство хэш-функций SHA, а в частности алгоритм SHA-512.

Задачи:

- Ознакомиться с общим предназначением хэш-функций.
- Рассмотреть семейство хэш-функций SHA различных поколений.
- Рассмотреть алгоритм хэширования SHA-512.

Хэш-функции

Хэш-фукнция

Функция хэширования — это функция, которая принимает на вход строку битов (или байтов) произвольной длины и выдает результат фиксированной длины.

Требования:

- Односторонность (one-way property)
- Сопротивляемость коллизиям (collision resistance)

Семейство хэш-фукнций SHA

Разработка

Защищенный алгоритм хэширования (Secure Hash Algorithm — SHA) разработан Управлением национальной безопасности США (National Security Agency — NSA) и стандартизирован институтом NIST.

Версии:

- SHA (SHA-0)
- SHA 1
- SHA 2
- SHA 3 (Keccak)

Характеристики SHA-512

- Максимальная длина сообщения: $2^{128} - 1$
- Длина блока: 1024
- Длина хеш-образа: 512
- Количество итераций: 80
- Длина слова: 64

Начальные значения переменных h0—h7 в SHA-512:

h0 := 0x6a09e667f3bcc908,
h1 := 0xbb67ae8584caa73b,
h2 := 0x3c6ef372fe94f82b,
h3 := 0xa54ff53a5f1d36f1,
h4 := 0x510e527fade682d1,
h5 := 0x9b05688c2b3e6c1f,
h6 := 0x1f83d9abfb41bd6b,
h7 := 0x5be0cd19137e2179

Применения

- SSL — дайджесты сообщений.
- IPSec — для алгоритма проверки целостности в соединении «точка-точка».
- PGP — для создания электронной цифровой подписи.
- SSH — для проверки целостности переданных данных.

Заключение

- Ознакомились с общим предназначением хэш-функций.
- Рассмотрели семейство хэш-функций SHA различных поколений.
- Рассмотрели алгоритм хэширования SHA-512.

Основные источники

- Niels Ferguson Bruce Schneier. Practical cryptography. — 2003.
- SHA-2. — 2022. — online; URL: https://ru.wikipedia.org/wiki/SHA-2 SHA-256.
- Niels Ferguson Bruce Schneier. Applied Cryptography. — 1996.
- Descriptions of SHA-256, SHA-384, and SHA-512. — 2022. — online; URL: https://eips.ethereum.org/assets/eip-2680/sha256-384-512.pdf.