Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №5

По дисциплине «Методы защиты информации»
По теме «Хэш функции»

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

Минск 2019

Введение

HMAC (сокращение от англ. hash-based message authentication code, код аутентификации (проверки подлинности) сообщений, использующий хеш-функции) — в информатике (криптографии), один из механизмов проверки целостности информации, позволяющий гарантировать то, что данные, передаваемые или хранящиеся в ненадёжной среде, не были изменены посторонними лицами

Преимущества HMAC:

- возможность использования хеш-функций, уже имеющихся в программном продукте;
- отсутствие необходимости внесения изменений в реализации существующих хеш-функции (внесение изменений может привести к ухудшению производительности и криптостойкости);
- возможность замены хеш-функции в случае появления более безопасной или более быстрой хеш-функции.

В зависимости от используемой хеш-функции выделяют HMAC-MD5, HMAC-SHA1, HMAC-RIPEMD128, HMAC-RIPEMD160 и т. п.

В ходе лаб. работы была реализована хэш функция SHA-256

Хэш-функции предназначены для создания «отпечатков» или «дайджестов» для сообщений произвольной длины. Применяются в различных приложениях или компонентах, связанных с защитой информации.

Хэш-функции SHA-2 разработаны Агентством национальной безопасности США и опубликованы Национальным институтом стандартов и технологий в федеральном стандарте обработки информации FIPS PUB 180-2 в августе 2002 года

Алгоритм хэш функции SHA-256

1. Исходное сообщение после дополнения разбивается на блоки, каждый блок — на 16 слов.
2. Алгоритм пропускает каждый блок сообщения через цикл с 64 или 80 итерациями (раундами). На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова.
3. Результаты обработки каждого блока складываются, сумма является значением хеш-функции.

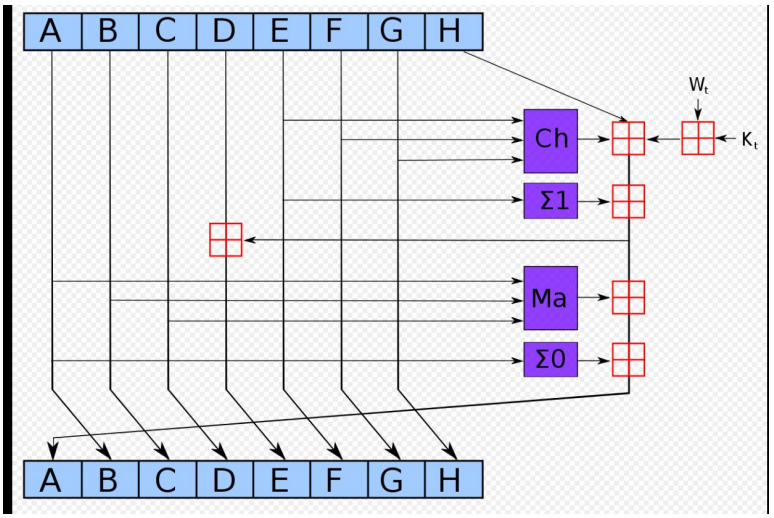


рис.1 Схема одной итерации алгоритмов SHA

Алгоритм HMAC

Алгоритм HMAC можно записать в виде одной формулы

$$\mathrm{HMAC}_K(text) = \mathrm{H}\left((K \oplus opad) \| \mathrm{H}\left((K \oplus ipad) \| text\right)\right),$$

где

- `b`, `block_size` — размер блока в байтах;
- `H`, `hash` — хеш-функция;
- `ipad` — блок вида `( 0x36 0x36 0x36 ... 0x36 )`, где байт `0x36` повторяется `b` раз; `0x36` — константа, магическое число, приведённое в RFC 2104; «i» от «inner»[1];
- `K`, `key` — секретный ключ (общий для отправителя и получателя);
- K_0 — изменённый ключ `K` (уменьшенный или увеличенный до размера блока (до `b` байт));
- `L` — размер в байтах строки, возвращаемой хеш-функцией `H`; `L` зависит от выбранной хеш-функции и обычно меньше размера блока;
- `opad` — блок вида `( 0x5c 0x5c 0x5c ... 0x5c)`, где байт `0x5c` повторяется `b` раз; `0x5c` — константа, магическое число, приведённое в RFC 2104; «o» от «outer»[1];
- `text` — сообщение (данные), которое будет передаваться отправителем и подлинность которого будет проверяться получателем;
- `n` — длина сообщения `text` в битах.

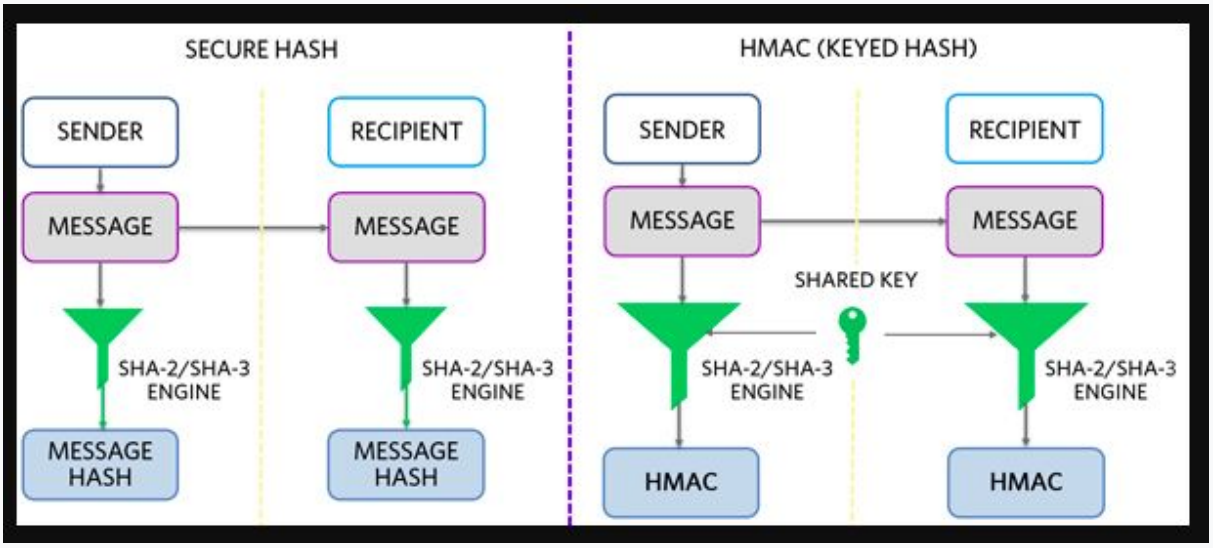
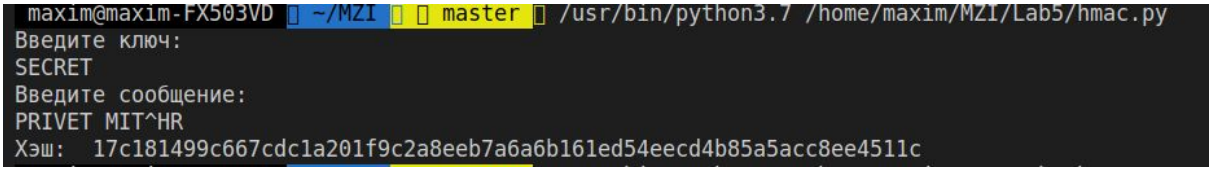


рис.2 Алгоритм HMAC

Результат работы программы

Вводимое сообщение - PRIVET MIT^HR



Выводы

HMAC позволяет быстро проверить подлинность сообщений на основе любой хэш функции.