Министерство образования Республики Беларусь
Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина «Методы защиты информации»

Отчет
к лабораторной работе №5
По дисциплине «Методы защиты информации»
По теме «Хэш-функции»

Выполнил:
студент гр.653501
Хамицевич Ф. С.

Проверил:
Артемьев В.С.

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

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»;
- 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»;
- text — сообщение (данные), которое будет передаваться отправителем и
- подлинность которого будет проверяться получателем;
- n — длина сообщения text в битах.

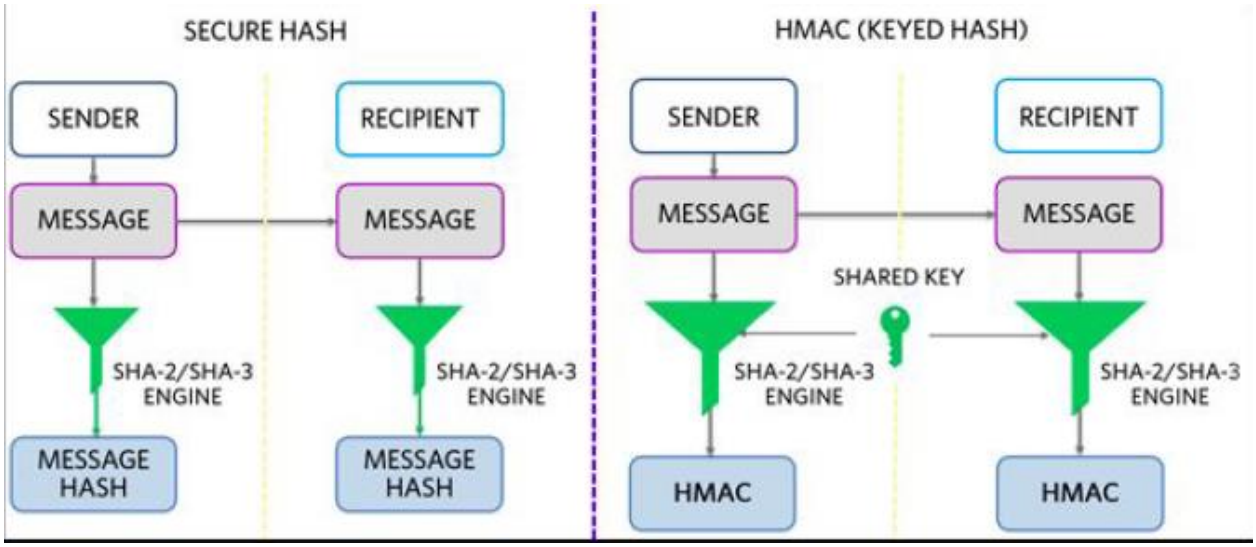

Рисунок 1. Алгоритм HMAC

Пример работы программы

Зашифруем сообщение “hello” (см. Рис. 2).

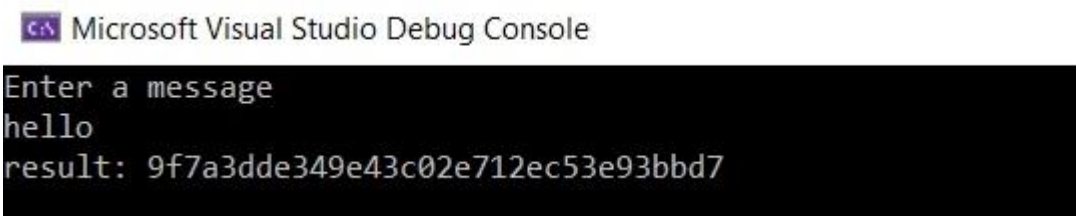

Рисунок 2. Пример работы программы.

Вывод

HMAC позволяет быстро проверить подлинность сообщений на основе любой хэш-функции. Реализация HMAC является обязательной
других протоколах интернета, например, TLS. Ожидается, что TLS вскоре
з
а
м
е
н
и
т
SSL и SET (англ.).
HYPERLINK "https://ru.wikipedia.org/wiki/Secure_Sockets_Layer" \o "Secure Sockets Layer"
SSL и SET (англ.).