

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

Выполнил:
студент гр.653501
Тимофеев К. А.

Проверил:
Артемьев В.С.

Минск, 2019

Введение

В лабораторной работе необходимо было реализовать программное средство контроля целостности сообщений с помощью алгоритма HMAC.

Алгоритм HMAC (Hash-based Message Authentication Code – код аутентификации сообщения на основе хэширования). Данный вид аутентификации подразумевает наличие у клиента и сервера некоего секретного ключа, который известен только им двоим. То есть это механизм, который использует криптографические хеш-функции в сочетании с секретным ключом. HMAC является одним из вариантов MAC и, следовательно, используется для контроля целостности сообщений. В данном случае в основе алгоритма лежит функция хэширования, которая позволяет вычислить код аутентификации сообщения.

Преимущества HMAC:

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

Механизм HMAC был описан в стандартах организаций ANSI, IETF, ISO и NIST.

В ходе настоящей лабораторной работы был использован алгоритм MD5 в качестве хеш-функции.

- 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.

Алгоритм HMAC можно записать в виде одной формулы^[1]: $\text{HMAC}(k, m) = \text{hash}((k \oplus C2) \parallel \text{hash}((k \oplus C1) \parallel m))$. где:

- « \oplus » — операция «побитовое исключающее ИЛИ» или «xor»;
- « \parallel » — операция «склейка строк» (последовательностей байт).

Блок-схема алгоритма

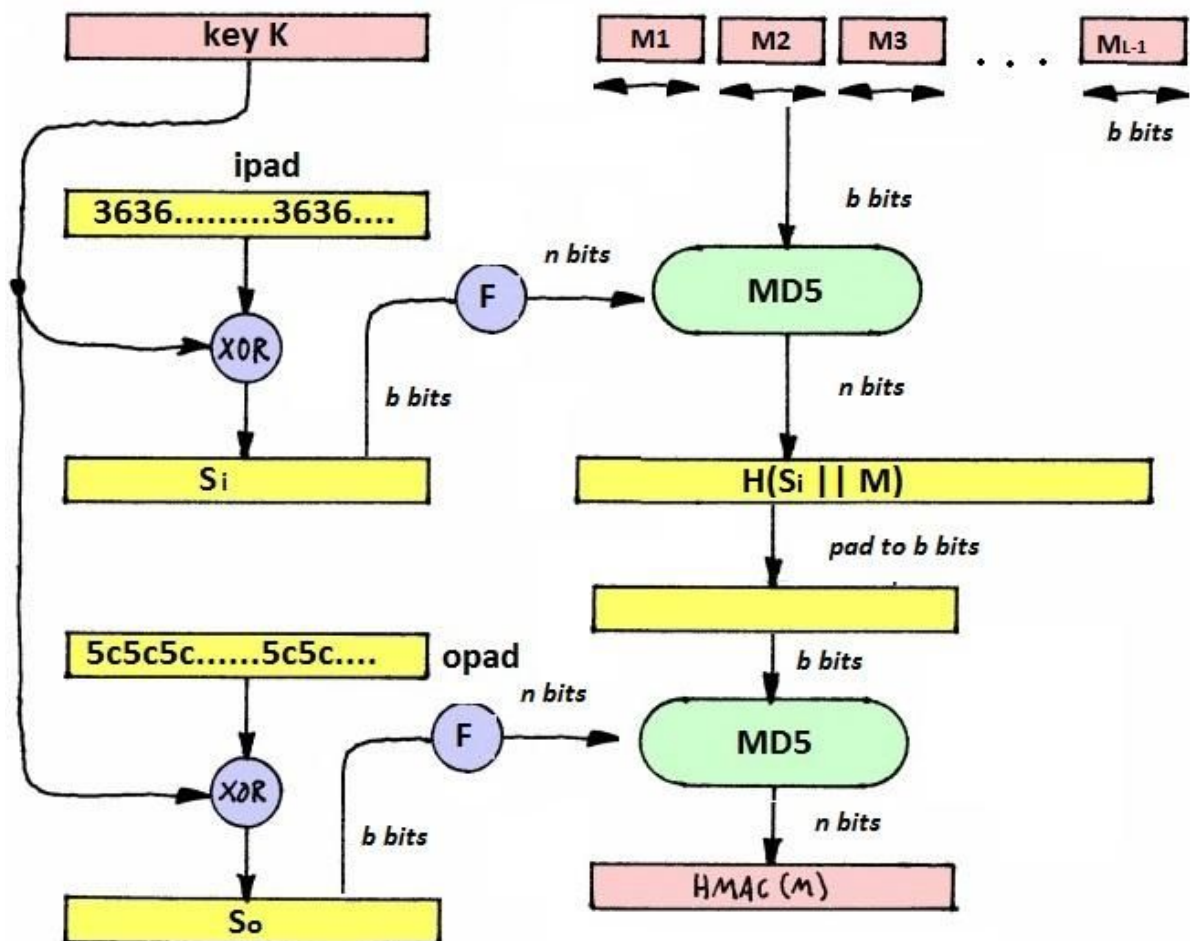
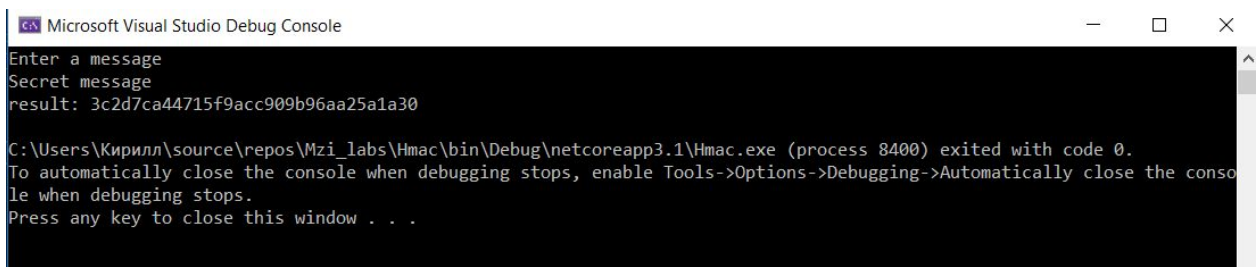


Рис.1 Блок-схема алгоритма

The image shows a screenshot of the Microsoft Visual Studio Debug Console window. The window has a title bar with the Visual Studio logo and the text "Microsoft Visual Studio Debug Console". The console output is as follows:
Enter a message
Secret message
result: 3c2d7ca44715f9acc909b96aa25a1a30

C:\Users\Кирилл\source\repos\Mzi_labs\Hmac\bin\Debug\netcoreapp3.1\Hmac.exe (process 8400) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .

Рис.2 Результат ввода данных и исполнения программы

Вывод

Полученный код аутентичности позволяет убедиться в том, что данные не изменялись каким бы то ни было способом с тех пор, как они были созданы, переданы или сохранены доверенным источником. Для такого рода проверки необходимо, чтобы, например, две доверяющие друг другу стороны заранее договорились об использовании секретного ключа, который известен только им. Тем самым гарантируется аутентичность источника и сообщения. Недостаток такого подхода очевиден — необходимо наличие двух доверяющих друг другу сторон.

Безопасность любой функции МАС на основе встроенных хеш-функций зависит от криптостойкости базовой хеш-функции. Привлекательность НМАС — в том, что его создатели смогли доказать точное соотношение между стойкостью встроенных хеш-функций и стойкостью НМАС.