ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА АУТЕНТИФИКАЦИИ СООБЩЕНИЙ HMAC

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мишулков А. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

В настоящее время проблема аутентификации сообщений, обрабатываемых системами, находящимися в незащищенных сетях является очень важной, поскольку передаваемая информация общедоступна для просмотра, а значит и легко уязвима для изменения и подделки. Одним из наиболее широко используемых механизмов решения данной задачи является HMAC (hash-based message authentication code).

Данный вариант аутентификации сообщений реализуются на основе использования функций хеширования и не предусматривает применения алгоритмов шифрования. Его работа описывается следующим выражением:

$$HMAC = H\left[\left(K_0 \oplus opad\right) \cup H\left[\left(K_0 \oplus ipad\right) \cup M\right]\right],$$

где H – встроенная функция хеширования (например, SHA1), M – подаваемое на вход HMAC сообщение (включая биты заполнителя, требуемые встроенной функцией хеширования), K_0 – секретный ключ, расширенный до размера хеш-значения путем добавления нулей слева; $ipad$ – шестнадцатеричное 363636…36, повторенное до заполнения K_0, $opad$ – шестнадцатеричное 5C5C5C…5C, повторенное до заполнения K_0.

Время выполнения алгоритма HMAC должно быть практически одинаковым со временем выполнения используемой хеш-функции для длинных сообщений. HMAC добавляет три выполнения хеш-преобразований – для блоков $K \oplus opad$ и $K \oplus ipad$, а также для полученного путем первого выполнения функции хеширования блока. Однако для коротких сообщений разница во времени выполнения может быть существенной. Поэтому предлагается эффективная реализация алгоритма HMAC (рисунок 1).

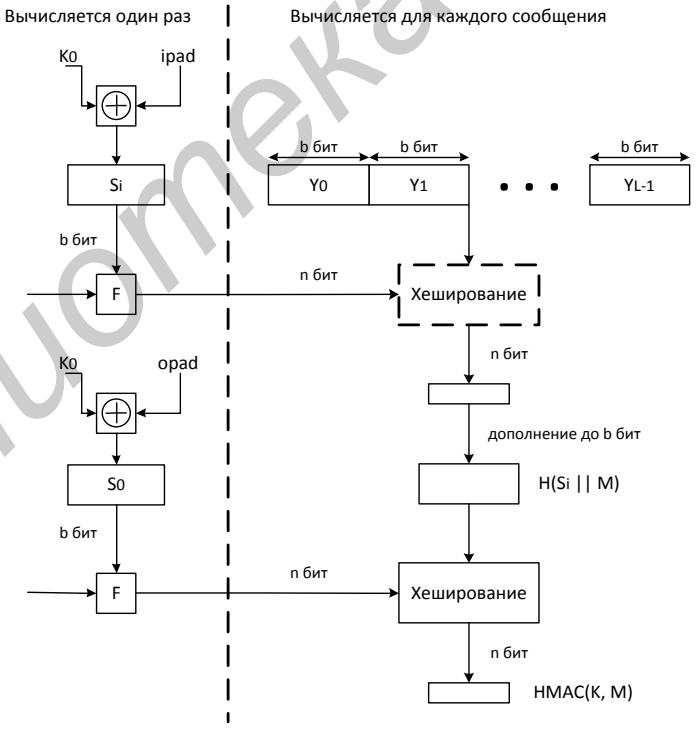

Рис. 1 – Эффективная реализации алгоритма HMAC

Улучшение алгоритма состоит в использовании функции сжатия *F*, которая принимает на вход блок длины *b* и возвращает сжатый блок длины *n*, где *n* – длина результирующего хеш-значения.

Результат функции сжатия используется в качестве вектора инициализации начальных состояний для алгоритма функции хеширования. Таким образом, в данной реализации алгоритма генерации хеш-кодов сообщений выполняется лишь одно дополнительное хеш-преобразование. Это реализация особенно целесообразна, если большинство сообщений, для которых вычисляется MAC, короткие. Также следует отметить, что функцию сжатия необходимо выполнить только в самом начале и каждый раз, когда ключ

изменяется.

На рисунке 2 представлены результаты экспериментальных сравнений обычной и эффективной реализаций алгоритма HMAC.

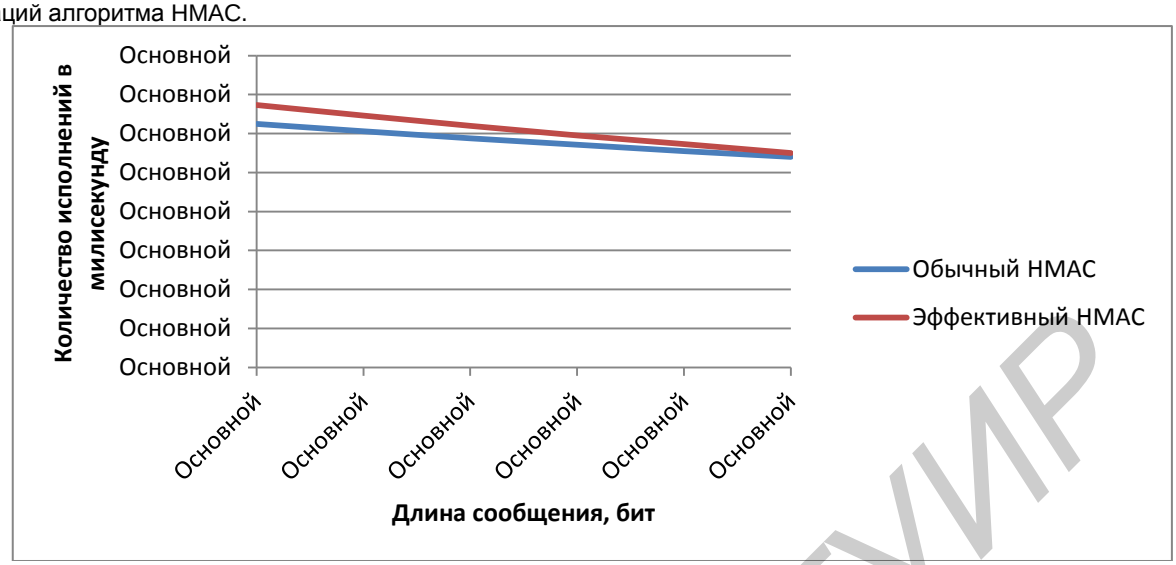

Рис. 2 – Сравнение производительности обычной и эффективной реализаций алгоритма аутентификации сообщений HMAC

Экспериментальное сравнение алгоритмов показало, что предлагаемая реализация HMAC действительно превосходит в эффективности обычную реализацию алгоритма. Данное превосходство наблюдается для коротких сообщений с длиной до 400 байт. Для сообщений большей длины разница в производительности сглаживается, т.к. количество хеш-преобразований при генерировании кодов аутентичности намного больше числа преобразований, удавшееся сократить в эффективной версии алгоритма.

Список использованных источников:

1. Stallings, W. Cryptography and Network Security Principles and Practices, Fourth Edition / W. Stallings. – Prentice Hall, Ca, 2005.
2. Ярмолик, В. Н. Теория информации / В. Н. Ярмолик // Уч. метод. пособие для студентов специальности I – 40 01 01 "Программное обеспечение информационных технологий" дневной и дистанционной форм обучения. – Минск: БГУИР, 2004. – 118 с.: ил.
3. Занкович, А. П. Защита информации: практикум для студентов специальности I – 40 01 01 «Программное обеспечение информационных технологий» дневной и дистанционной форм обучения / А. П. Занкович. – Мн.: БГУИР, 2006. – 39 с.: ил.

ВНЕДРЕНИЕ СТЕГАНОГРАФИЧЕСКОГО СООБЩЕНИЯ В ИЗОБРАЖЕНИЯ ФОРМАТА JPEG

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Герман Н. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

В современном обществе очень популярен обмен изображениями, гигабайты графической информации ежедневно проходят через социальные сети и средства личного общения. Таким образом, с использованием стеганографии можно передавать значительное количество информации, факт передачи которой является предметом сокрытия.

Стеганографические системы предназначены для передачи по открытым каналам связи таким образом, что сторонний наблюдатель не может обнаружить передачу секретной информации помимо открытой информации. Безусловно, наибольшую вместимость будут иметь форматы сжатия без потерь, однако их применение на сегодняшний день крайне ограничено, в то время как обмен изображениями в формате JPEG распространён довольно широко. Это делает JPEG изображения логичным выбором в качестве стеганографического контейнера.

Существует возможность помещения секретного сообщения в области, предназначенные для метаинформации и неиспользуемые при декодировании изображения области. Однако, такие техники не заслуживают внимания в связи с тем, что их применение легко обнаружить. Другие техники внедрения секретного сообщения связаны с алгоритмом сжатия формата JPEG. Преобразование изображения в формат JPEG происходит в несколько этапов: