УДК 681.322

И.В. Лысенко, Т.А. Исиченко

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

МОДЕЛИ ОБНАРУЖЕНИЯ МОДИФИКАЦИЙ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СИММЕТРИЧНОЙ КРИПТОГРАФИИ НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Проведен анализ возможности использования принципа диверсности (многоверсионности) для решения задачи обеспечения целостности данных с использованием методов криптографии. Предложены модели обеспечения целостности сообщений на основе межсеансовой и внутрисеансовой диверсности.

принцип диверсности, целостность данных, целостность сообщений

Введение

Постановка проблемы. В последнее время с быстрым развитием компьютерных сетей и внедрением их во все сферы деятельности человека актуализировалась проблема защиты передаваемой по компьютерным сетям информации. Одной из наиболее важных задач, решением которой призвана заниматься криптография, является обеспечение целостности информации, что обеспечивается за счет обнаружения факта модификаций передаваемых данных. Задача обеспечения целостности и аутентичности сообщений, передаваемых по компьютерным сетям, традиционно решается путем разработки новых и совершенствования существующих криптографических методов [1]. Существуют различные подходы к решению данной задачи, воплощенные в конкретные средства, использующие криптографические методы. В рамках несимметричной криптографии практически единственным механизмом обнаружения факта изменения целостности данных является цифровая подпись. Что касается симметричной криптографии, то здесь наиболее традиционным методом решения этой задачи является выработка кода аутентификации сообщений на основе стандартных криптографических алгоритмов. В то же время, на наш взгляд, для решения указанной выше задачи может быть использован многоверсионный подход (принцип диверсности), который традиционно используется для успешного решения задачи обеспечения заданного уровня надежности и гарантоспособности компьютерных и компьютеризированных систем [2].

Целью статьи является анализ возможности использования принципа диверсности для обеспечения целостности сообщений.

Принцип диверсности и проблема обеспечения целостности передаваемых сообщений

В рамках современной криптографии существуют два наиболее распространенных подхода к обеспечению целостности информации, основанных соответственно на симметричной и несимметричной криптографии.

В области несимметричной криптографии традиционным является подход, основанный на использовании цифровой подписи (ЦП).

Общая идея технологии ее применения состоит в вычислении хэш-значения подписываемого документа M и шифрования его секретным ключом отправителя. Что касается симметричной криптографии, то здесь можно выделить метод, основанный на выработке КАС (код аутентификации сообщения), или в английской версии – MAC (message autentification code). Выработка кода аутентификации сообщений с использованием процедуры криптографического преобразования данных официально или полуофициально закреплена во многих стандартах на алгоритмы шифрования. Этот подход заключается в том, что контрольная сумма вычисляется с использованием секретного ключа с помощью некоторого блочного шифра. Важно, что на основе любого такого шифра можно создать алгоритм вычисления КАС для массивов данных произвольного размера.

Из всех режимов работы криптографических алгоритмов, при помощи которых производится выработка КАС, для обеспечения функции целостности данных подходят только 3, а именно: CBC (Cipher Block Chaining) – режим сцепления блоков шифрованного текста, CFB (Cipher Feedback) – режим обратной связи по шифрованному тексту и IGE (Infinite Garble Extension) – режим неограниченного размножения ошибки.

Сущность диверсного подхода применительно к решению задачи обеспечения конфиденциальности сообщений подробно рассмотрена в [3, 4], где были рассмотрены 2 модели:

– на основе целостной диверсности, в которой используется принцип комбинирования симметричных и несимметричных криптоалгоритмов для шифрования сообщения и ключа шифрования сообщения соответственно;

– на основе блочной диверсности, где используется принцип шифрования каждого блока сооб-

щения с использованием различных криптоалгоритмов с применением различных ключей, которые выбираются определенным образом.

Базируясь на предложенных в [3, 4] идеях, представляется целесообразным разработка моделей межсеансовой и внутрисеансовой диверсности применительно к услуге целостности.

Модель обеспечения целостности сообщений на основе межсеансовой диверсности. Суть данной модели состоит в том, что исходное сообщение разбивается на блоки определенной длины (равной размеру ключа сеанса), каждый из которых шифруется с помощью криптоалгоритма E_{ci} с использованием ключа K_m в режиме R_j. Суть его состоит в том, что КАС формируется на основе определенного алгоритма и режима шифрования, которые могут выбираться пользователями из заданного их множества в соответствии с некоторым правилом, остающимся неизвестным для криптоаналитика.

В результате сформированный КАС добавляется к исходному тексту и отправляется по открытому каналу; на стороне получателя КАС отделяется от основного текста и получатель формирует КАС по тому же алгоритму, что и на стороне отправителя. В завершении КАС (отправителя) сравнивается с КАС, рассчитанным получателем, после чего делается вывод о норме или не норме целостности отправленных данных. Выбранный алгоритм и режим шифрования, а также ключ сеанса определяются по результатам вычисления трех функций, сконструированных определенным образом. А именно, $f_1 = (K_i \oplus K_{i+1}) \bmod n$ (для вычисления криптоалгоритма), где K_i – ключ текущего сеанса, K_{i+1} – ключ следующего сеанса, n – количество используемых алгоритмов; $f_2 = \overline{(K_i \oplus K_{i+1})} \bmod m$ (для вычисления режима работы алгоритма), где m – количество используемых режимов; $f_1 = K_i \bmod p$ (для вычисления процедуры модификации ключа текущего сеанса, на основе которой будет получен ключ для следующего сеанса), где p – количество процедур модификаций ключа.

Алгоритм работы данной модели представлен на рис. 1.

Модель обеспечения целостности сообщений на основе внутрисеансовой диверсности. Отличие данной модели от предыдущей состоит в том, что исходное сообщение разбивается на блоки определенной длины m_i (равной размеру ключа сеанса), каждый из которых шифруется с помощью криптоалгоритма, выбранного из множества $ME_к$ (ключ при этом используется один и тот же – K_i).

При этом выбор криптоалгоритма для шифрования каждого i-го блока m_i исходного сообщения осуществляется по какому-либо правилу (данное правило выбора криптоалгоритма должно быть заранее известно двум сторонам).

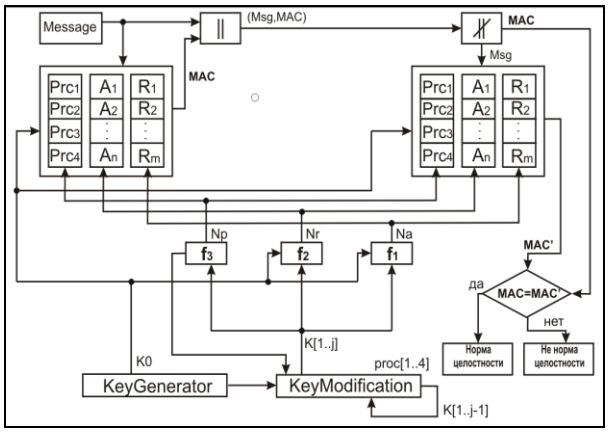

Рис. 1. Модель обеспечения целостности сообщений на основе межсеансовой диверсности

Как и в модели на основе межсеансовой диверсности выработка КАС происходит с использованием одного из трех режимов работы блочного шифра.

На выход криптосистемы поступает блок фиксированной длины, который собственно и является кодом аутентификации сообщения.

Примером такой модели может служить модель на основе режима CBC, где каждый блок шифруется одним из трех криптоалгоритмов множества $ME_к$ = {DES, IDEA, ГОСТ}, которые выбираются в порядке очереди циклически, т.е. после 3-го по порядку номера идет 1-й и т.д. Визуально данная модель представлена на рис. 2.

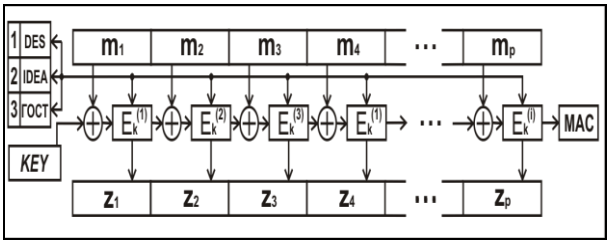

Рис. 2. Модель обеспечения целостности сообщений на основе внутрисеансовой диверсности

Следует отметить, что на основе моделей, представленных на рис. 1 и 2, может быть реализована комбинированная система. Разумеется, такого рода комбинирование значительно усложнит систему, что приведет к увеличению времени криптопреобразований из-за дополнительных вычислений, связанных с выбором алгоритма шифрования для каждого блока. Однако, на наш взгляд, это позволит увеличить криптостойкость системы.

Заключение

Ожидается, что использование данного подхода усложнит задачу криптоанализа, поскольку криптоаналитик сталкивается с необходимостью узнать, какой именно криптоалгоритм и какой режим шифрования использовался в каждом сеансе, помимо того, что ему необходимо узнать ключ сеанса.

Направлением дальнейшей работы будет являться программная реализация представленных моделей и оценка их эффективности.

Список литературы

1. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 815 с.

2. Харченко В.С. и др. Многоверсионные системы, технологии и проекты / Под ред. В.С. Харченко. – Х.: Мин. образования и науки Украины, 2003. – 528 с.

3. Лысенко И.В., Филиппов Д.А. Модели обеспечения конфиденциальности сообщений средствами криптографии на основе принципа диверсности // Системи обробки інформації. – Х.: ХУПС, 2006. – Вип. 2 (51). – С. 76-80.

4. Лысенко И.В. Использование принципа диверсности для обеспечения конфиденциальности сообщений в рамках современной криптографии // Радіоелектронні і комп'ютерні системи. – 2006. – Вип. 5 (17). – С. 118-121.

Поступила в редколлегию 1.12.2006

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.