Секція 2. Захист інформації в комп'ютерних системах

УДК 004.432

А.Я. Белецкий, А.А. Белецкий

Национальный авиационный университет, Киев

БЛОЧНЫЙ КРИПТОАЛГОРИТМ С ДИНАМИЧЕСКИМ УПРАВЛЕНИЕМ ПАРАМЕТРАМИ ШИФРОВАНИЯ

Введение и постановка задачи

Современные методы защиты информации (шифрование) в компьютерных сетях представляют собой математические преобразования, в которых сообщения рассматриваются как числа или алгебраические элементы в некотором пространстве [1, 2]. С позиции теории сигналов и процессов зашифрование исходного текста (коррелированного, избыточного, сжимаемого) состоит в его отбеливании, т.е. обращении в некоррелированную последовательность символов (элементов) практически несжимаемой шифрограммы с плотностью распределения вероятностей элементов выходного алфавита максимально близкой к равномерной.

Несмотря на многообразие существующих промышленных образцов блочных криптографических систем, все еще сохраняет актуальность разработка новых более гибких алгоритмов шифрования.

В данном докладе предлагается симметричный блочный криптоалгоритм, названный RSB-32 шифром. Аббревиатура RSB происходит от ключевых слов Round, Step, Blok – подчеркивая тем самым, что основными для криптоалгоритма являются раундовые преобразования, разбитые на определенное число шагов, а действие алгоритма осуществляется над блоками открытого или закрытого текстов. Отличительная особенность RSB алгоритма состоит в том, что в нем используется оригинальный криптографический примитив скользящего кодирования, который обеспечивает не только глубокое перемешивание открытого текста, но и участвует в формировании блочного раундового ключа для очередного шифруемого блока. Тем самым все преобразования, выполняемые криптоалгоритмом, становятся зависимыми не только от секретного ключа, но и от шифруемых данных, т.е. относятся к классу «управляемых криптопреобразований» [3, 4].

Общая характеристика алгоритма

Предлагаемый RSB алгоритм шифрования закладывает основу создания принципиально новой технологии симметричной блочной криптографической защиты информации, не имеющей аналогов в мировой практике. Реализация алгоритма позволяет существенно повысить криптостойкость систем шифрования по сравнению с уже существующими продуктами и в то же время сохраняет высокую скорость криптопреобразования.

Достижение первого заявляемого качества (криптостойкости) базируется на таких предпосылках. В сложившейся мировой практике построения симметричных блочных криптографических алгоритмов в пределах раунда все блоки шифруемого текста подвергаются одинаковым преобразованиям. С одной стороны это обеспечивает возможность параллельной обработки информации, что повышает скорость шифрования. Вместе с тем, такая технология шифрования облегчает работу криптоаналитиков. В самом деле, если в открытом тексте присутствуют одинаковые блоки, то одинаковыми будут также эти блоки после зашифрования.

Отмеченный недостаток классических блочных шифраторов устраняется в RSB алгоритме за счет применения двунаправленного скользящего кодирования, посредством которого каждый шифруемый блок текста становится управляемым своим индивидуальным блочным раундовым ключом, зависящим не только от базового раундового ключа, но и всего текста, предшествующего преобразуемому блоку. Тем самым интуитивно становится понятным, что RSB технология значительно усложняет работу криптоаналитика (что эквивалентно повышению криптостойкости шифра), поскольку опыт, приобретенный на этапе взлома одной шифрограммы, может оказаться малополезным для взлома другой шифрограммы (за счет различия исходных текстов).

Высокую скорость шифрования в RSB технологии можно обеспечить за счет табличных и параллельных способов выполнения основных алгебраических преобразований, а также за счет аппаратной реализации на платформах с 32-х разрядными шинами.

Согласно литературным источникам до настоящего времени управляемые криптографические примитивы еще не получили сколько-нибудь заметного применения в шифраторах. Мы можем лишь отметить такие шифры, как MARS, RC5 и RC6 (США), которые можно отнести к модифицированным шифрам Фейстеля. В этих шифрах используется операция циклического «прокручивания» блоков на число разрядов, изменяющихся в зависимости от шифруемых данных и секретного ключа. Несмотря на крайнюю простоту построения, шифр RC5 оказался весьма стойким к линейному и дифференциальному анализу, что считается достойным качеством криптосистемы.

Теоретические исследования показали, как отмечают российские криптографы А.А. Молдавян и Н.А. Молдавян [5, 6], что применение оператора стохастической прокрутки блока, зависящего от преобразуемых данных, является эффективным средством противодействия этим двум важнейшим типам атак. Благодаря своей эффективности циклический сдвиг, управляемый преобразуемыми данными, нашел применение в новых шифрах – RC6 и MARS, вошедших в состав финалистов международного конкурса по разработке нового стандарта криптографической защиты – Advanced Encryption Standard (AES).

Если операция прокрутки блока с фиксированным параметром сдвига является линейной, то задание ее зависимой от преобразуемых данных приводит к построению новой нелинейной операции с хорошими криптографическими свойствами [5].

Кроме операции циклического сдвига, зависящей от преобразуемых данных, в RSB алгоритме реализованы и другие виды управляемых операций шифрования, как размер общего секретного ключа и число шагов (а, следовательно, и раундов) криптографических преобразований.

Выводы

1. RSB алгоритм допускает динамичное управление в широком диапазоне такими параметрами

2. Криптографические преобразования в каждом блоке осуществляются под управлением индивидуальных раундовых ключей, зависящих не только от значения секретного базового раундового ключа, но и всего текста, предшествующего преобразуемому блоку.

3. Основные выполняемые в RSB шифре криптографические преобразования (круговой сдвиг блока, скользящее кодирование 32-битных элементов, нелинейная подстановка и перестановка байтов в блоках) относятся к классу стохастически управляемых операций шифрования.

4. Стохастичность операций шифрования обеспечивается не только выбором случайных базовых раундовых ключей, но и домешиванием в блочные раундовые ключи криптографически преобразуемых (в силу чего приобретающих стохастические свойства) 32-битных элементов шифруемого текста.

5. RSB алгоритм допускает аппаратную реализацию на платформах с 32-разрядной шиной, причем возможно распараллеливание операций нелинейных подстановок и перестановок байтов в шифруемых блоках.

Список литературы

1. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.

2. Венбо Мао. Современная криптография: теория и практика / Мао Венбо. – М.: Вильямс, 2005. – 768 с.

3. Белецкий А.Я. Симметричный блочный криптоалгоритм / А.Я. Белецкий, А.А. Белецкий // Захист інформації. – 2006. – № 2 (29). – С. 42-51.

4. Белецкий А.Я. Семейство симметричных блочних криптографических алгоритмов с динамически управляемыми параметрами шифрования / А.Я. Белецкий, А.А. Белецкий, А.А. Кузнецов // Електроніка та системи управління. – К.: НАУ, 2007. – № 1 (11). – С. 5-16.

5. Молдаван Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдаван, А.А. Молдаван, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.

6. Молдаван Н.А. Криптография: скоростные шифры / Н.А. Молдаван, А.А. Молдаван, Н.Д. Гуц, Б.В. Изотов. – СПб.: БХВ-Петербург, 2002. – 496 с.