УДК 681.322

К ВОПРОСУ О СОЗДАНИИ КРИПТОСИСТЕМ С НЕСКОЛЬКИМИ ШИФРУЮЩИМИ ПРЕОБРАЗОВАНИЯМИ

С.Ю. Гавриленко, М.И. Главчев, А.М. Филоненко
(представил д.т.н., проф. А.И. Овчаренко)

Рассматриваются методологические подходы к шифрованию информации при использовании нескольких шифрующих алгоритмов и способы объединения этих алгоритмов, отражены преимущества таких систем и проблемы создания.

Современные криптографические системы представляют собой алгоритм, состоящий из совокупности преобразований и проверенный на криптостойкость профессиональными аналитиками и математиками. Ключевая последовательность используется для управления шифрованием путем установления параметров для осуществления преобразований. При проведении криптоатаки на данные, зашифрованные известным алгоритмом, оценка стойкости определяется путем перебора вариантов ключа (слабые криптоалгоритмы, естественно, не рассматриваются для создания качественных криптосистем).

В отличие от этих систем, сложность расшифрования информации которых зависит от выбранного ключа, возможно создание систем, в которых ключом устанавливаются не только параметры преобразований, но и выбирается сам алгоритм шифрования данных. Можно сказать, будет получена система с неопределенным или недетерминированным алгоритмом шифрования. При таком представлении для расшифрования данных требуется знание не только ключа, но и алгоритма, применяемого для конкретного сообщения. Понятно, что алгоритмическая неопределенность вводит существенную качественную особенность, которая усложняет использование аналитических выражений при криптоанализе, и использование средств вычислительной техники не увеличит относительное время раскрытия зашифрованного сообщения. Так как определение параметрических характеристик преобразований возможно с помощью криптоанализа, то применение различных алгоритмов значительно усложняет этот процесс даже в случае известного шифрованного и исходного текстов.

Рассмотрим различные подходы создания недетерминированных криптографических систем на основе симметричных шифров. В самом простом представлении разрабатывается несколько шифрующих преобразований $\mathbf{E}_1$, $\mathbf{E}_2$, $\mathbf{E}_3$, … $\mathbf{E}_n$ и объединяется в общую систему. Выбор

конкретного шифрующего преобразования выполняется на основе установленного пользователем ключа, который также участвует в процессе шифрования. Преобразование шифрования определяется на основании характеристик исходного сообщения (в частности, применение хэш-функций) и ключа, что в определенной степени усложняет процедуру криптоанализа зашифрованного сообщения.

Следующим методом является использование последовательно нескольких шифрующих преобразований $\mathbf{E_1}$, $\mathbf{E_2}$, $\mathbf{E_3}$, … $\mathbf{E_n}$ над исходным сообщением, т.е. зависимость получаемого результата определяется очередностью преобразований, построенной на основе ключа. Число всевозможных очередностей определяется как $\mathbf{N = n!}$. Например, при $\mathbf{n = 14}$ получим $\mathbf{N > 10^{10}}$.

В рассмотренных выше методах выбор преобразования или последовательности преобразований шифрования рекомендуется осуществлять на основе применения необратимых преобразований ключевой последовательности, которая приводится к определенному значению, равному количеству задействованных в криптосистеме алгоритмов.

Наиболее перспективными представляются недетерминированные криптосистемы с неопределенным количеством используемых преобразований. Если имеется библиотека программ шифрования $\mathbf{E_1}$, $\mathbf{E_2}$, ..., $\mathbf{E_n}$ и соответствующих им программ дешифрования $\mathbf{D_1}$, $\mathbf{D_2}$, ..., $\mathbf{D_n}$, то для задания алгоритма шифрования можно рассмотреть реализацию различных вариантов процедуры шифрования, которые состоят из выполнения последовательных **m** процедур, выбираемых из множества $\mathbf{\{E_1, E_2,..., E_n, D_1, D_2, ..., D_n\}}$, т. е. результирующее шифрование будет иметь вид

$$\mathbf{E(t) = P_{im}\,(P_{im-1}\,\ldots(P_{i2}\,(P_{i1}\,(t)))\ldots)},$$

где **t** – исходное сообщение, **P** – функция преобразования $\mathbf{P \in \{E, D\}}$, **i** – преобразования, выбранные для конкретного сеанса, $\mathbf{i \in \{1, 2, ..., n\}}$.

Необходимо обратить внимание на то, что, если выполнение следующих друг за другом процедур шифрования **E** и дешифрования **D** с одинаковыми индексами не изменяет исходного сообщения, то требуется наложить запрет на модификации результирующей функции шифрования, соответствующие таким случаям.

В качестве $\mathbf{P_{i1}}$ может быть выбран любой из **2n** элементов множества $\mathbf{\{E_1, E_2, ..., E_n, D_1, D_2, ..., D_n\}}$, а в качестве $\mathbf{P_{i2}}$, $\mathbf{P_{i3}}$, … $\mathbf{P_{im}}$ — один из **2n - 1** элементов.

Учитывая это уточнение, связанное с использованием неэффективной последовательности преобразований, можно подсчитать количество возможных модификаций **N** результирующей функции шифрования: $\mathbf{N = 2n\,(2n\text{-}l)^{m-1}}$. Например, при $\mathbf{n \in [5, 14]}$ и $\mathbf{m \in [5, 14]}$ получим **N** (табл.1). Следует учесть, что полученные значения не учитывают количественную вариантность с использованием ключа, т.е. рассмотрено только

функциональное многообразие результирующих функций.

Таблица 1

Количество различных вариантов функции шифрования

n \ m	5	6	7	8	9	10	11	12	13	14
5	$6{,}5\cdot10^{4}$	$5{,}9\cdot10^{5}$	$5{,}3\cdot10^{6}$	$4{,}7\cdot10^{7}$	$4{,}3\cdot10^{8}$	$3{,}8\cdot10^{9}$	$3{,}4\cdot10^{10}$	$3{,}1\cdot10^{11}$	$2{,}8\cdot10^{12}$	$2{,}5\cdot10^{13}$
6	$1{,}8\cdot10^{5}$	$1{,}9\cdot10^{6}$	$2{,}1\cdot10^{7}$	$2{,}3\cdot10^{8}$	$2{,}5\cdot10^{9}$	$2{,}8\cdot10^{10}$	$3{,}1\cdot10^{11}$	$3{,}4\cdot10^{12}$	$3{,}7\cdot10^{13}$	$4{,}1\cdot10^{14}$
7	$4{,}0\cdot10^{5}$	$5{,}2\cdot10^{6}$	$6{,}7\cdot10^{7}$	$8{,}8\cdot10^{8}$	$1{,}1\cdot10^{10}$	$1{,}5\cdot10^{11}$	$1{,}9\cdot10^{12}$	$2{,}5\cdot10^{13}$	$3{,}2\cdot10^{14}$	$4{,}2\cdot10^{15}$
8	$8{,}1\cdot10^{5}$	$1{,}2\cdot10^{7}$	$1{,}8\cdot10^{8}$	$2{,}7\cdot10^{9}$	$4{,}1\cdot10^{10}$	$6{,}1\cdot10^{11}$	$9{,}2\cdot10^{12}$	$1{,}4\cdot10^{14}$	$2{,}1\cdot10^{15}$	$3{,}1\cdot10^{16}$
9	$1{,}5\cdot10^{6}$	$2{,}6\cdot10^{7}$	$4{,}3\cdot10^{8}$	$7{,}4\cdot10^{9}$	$1{,}3\cdot10^{11}$	$2{,}1\cdot10^{12}$	$3{,}6\cdot10^{13}$	$6{,}1\cdot10^{14}$	$1{,}0\cdot10^{16}$	$1{,}8\cdot10^{17}$
10	$2{,}6\cdot10^{6}$	$4{,}9\cdot10^{7}$	$9{,}4\cdot10^{8}$	$1{,}8\cdot10^{10}$	$3{,}4\cdot10^{11}$	$6{,}5\cdot10^{12}$	$1{,}2\cdot10^{14}$	$2{,}3\cdot10^{15}$	$4{,}4\cdot10^{16}$	$8{,}4\cdot10^{17}$
11	$4{,}2\cdot10^{6}$	$8{,}9\cdot10^{7}$	$1{,}8\cdot10^{9}$	$3{,}9\cdot10^{10}$	$8{,}3\cdot10^{11}$	$1{,}7\cdot10^{13}$	$3{,}6\cdot10^{14}$	$7{,}7\cdot10^{15}$	$1{,}6\cdot10^{17}$	$3{,}3\cdot10^{18}$
12	$6{,}7\cdot10^{6}$	$1{,}5\cdot10^{8}$	$3{,}5\cdot10^{9}$	$8{,}1\cdot10^{10}$	$1{,}8\cdot10^{12}$	$4{,}3\cdot10^{13}$	$9{,}9\cdot10^{14}$	$2{,}2\cdot10^{16}$	$5{,}2\cdot10^{17}$	$1{,}2\cdot10^{19}$
13	$1{,}0\cdot10^{7}$	$2{,}5\cdot10^{8}$	$6{,}3\cdot10^{9}$	$1{,}5\cdot10^{11}$	$3{,}9\cdot10^{12}$	$9{,}9\cdot10^{13}$	$2{,}4\cdot10^{15}$	$6{,}1\cdot10^{16}$	$1{,}5\cdot10^{18}$	$3{,}8\cdot10^{19}$
14	$1{,}4\cdot10^{7}$	$4{,}0\cdot10^{9}$	$1{,}0\cdot10^{10}$	$2{,}9\cdot10^{11}$	$7{,}9\cdot10^{12}$	$2{,}1\cdot10^{14}$	$5{,}7\cdot10^{15}$	$1{,}5\cdot10^{17}$	$4{,}2\cdot10^{18}$	$1{,}1\cdot10^{20}$

Как предлагалось выше, возможно построение шифров на базе процедур и операций преобразования, которые зависят от преобразуемых данных. В этих шифрах на некотором шаге шифрования конкретный вид выполняемой операции (или процедуры) зависит от значения преобразуемого текста. При описании алгоритма шифрования на основе стандартных операций набор этих операций изменяется от одного входного текста к другому. Алгоритм преобразования в шифрах с операциями, зависящими от преобразуемых данных, является фиксированным, поскольку известно правило выбора конкретного вида операции от текущего значения преобразуемых данных. Использование шифрующих процедур с операциями, зависящими от входного сообщения, весьма перспективно для построения скоростных шифров, обладающих высокой криптостойкостью.

Недетерминированные системы шифрования имеют ряд преимуществ перед системами с определенными алгоритмами. Выделим следующие:

– вероятность генерации слабого алгоритма очень мала и резко падает при использовании разнотипных приемов задания недетерминированности процедур. Можно отметить как следствие, что при использование систем с различными криптоалгоритмами допустимо также применение преобразований шифрования с невысоким уровнем стойкости к криптоанализу;

– криптосистема может наряду с шифрующими преобразованиями выполнять в результирующей функции и функцию контроля (например, проверка равновероятности появления букв и биграмм), а затем и корректировать при необходимости;

– в системах с неопределенным количеством используемых преобразований в качестве одного или нескольких из составных алгоритмов шифрования можно использовать известные криптоалгоритмы и схемы, которые допускают оценку их стойкости по отработанным методикам.

В качестве проблем недетерминированных криптосистем видится следующее:

– существует определенная вероятность, что результирующая шифрующая функция будет иметь более низкую устойчивость к атакам на сообщение, чем составляющие эту функцию преобразования. Необходимо разработать математический аппарат, способный оценить результирующий алгоритм, или, как предлагалось выше, дополнить систему контролирующими функциями;

– для полноценного функционирования недетерминированной системы необходимо большое число используемых преобразований и эти преобразования не должны быть обратные или эквивалентные;

– осуществление равновероятностного выбора преобразований из определенного множества;

– проверка результирующих функций шифрования на чтение без использования ключа, как параметра этих преобразований.

В заключение отметим, что при создании недетерминированных криптосистем видится наиболее эффективным комбинированное использование вариантов преобразований и ключа – как параметра этих преобразований. Первые задают логическую трудность, а вторые — количественную. Основной смысл такого комбинирования заключается в том, чтобы обойти трудность задания высокого уровня неопределенности шифрующего алгоритма.

ЛИТЕРАТУРА

1. Андреев Н.Н. О некоторых направлениях исследований в области защиты информации. // Международная конференция «Безопасность информации». – М. – 1997. – С. 94 - 97.

2. Молдовян А.А., Молдовян Н.А. Новый принцип построения криптографических модулей в системах защиты ЭВМ // Кибернетика и системный анализ. – 1993. – № 5. – С. 42 - 49.

Поступила в редколлегию 15.10.2001