УДК 681.3
С.Н. Фисун, доцент, канд. техн. наук,
О.И. Куржеевская, магистрант
Севастопольский национальный технический университет
ул. Университетская, д.33, г. Севастополь, Украина, 99053
E-mail:fserg48@mail.ru

КОМБИНИРОВАННЫЙ АЛГОРИТМ ВЕРОЯТНОСТНОГО ШИФРОВАНИЯ

Предложен комбинированный алгоритм вероятностного шифрования, в котором блок зашифрованной информации формируется из случайного, но ограниченного, числа битов исходного текста и битов сгенерированных случайным образом. Полученные биты подвергаются стохастической перестановке для формирования блока шифртекста, таким образом, доля битов исходного текста и количество случайных битов, а также расположение исходных и случайных битов в каждом блоке зашифрованной информации является случайным процессом, зависящим от используемых генераторов псевдослучайных последовательностей и криптографических ключей. Полученная битовая последовательность шифруется затем по алгоритму Голдвассера - Микали.

Ключевые слова: *вероятностное шифрование, комбинированный алгоритм, стохастическое перемешивание, квадратичный вычет, алгоритм шифрования Голдвассера-Микали*

Идея вероятностного шифрования была предложена Шафи Голдвассером и Сильвио Микали [5]. Основной целью вероятностного шифрования является устранение утечки информации в криптографии с открытым ключом. Поскольку криптоаналитик всегда может зашифровать случайные сообщения открытым ключом, он может получить некоторую информацию. При условии, что у него есть шифртекст $C = E_k(M)$, где C – зашифрованный текст, E – функция шифрования на ключе k, а M – открытый текст и криптоаналитик пытается получить открытый текст M, он может выбрать случайное сообщение M' и зашифровать его в виде $C' = E_k(M')$. Если $C' = C$, то криптоаналитик угадал правильный открытый текст. В противном случае он делает следующую попытку. При вероятностном шифровании алгоритм шифрования является вероятностным, а не детерминированным. Другими словами, многие шифртексты при расшифровке дают данный открытый текст, и конкретный шифртекст, используемый в любом конкретном шифровании, выбирается случайным образом.

$$C_1 = E_k(M),\ C_2 = E_k(M),\ C_3 = E_k(M),\ \dots,\ C_i = E_k(M)$$
$$M = Dk(C1) = Dk(C2) = Dk(C3) = \dots = Dk(Ci),$$

где D – функция расшифрования на ключе k.

При вероятностном шифровании криптоаналитику не удается шифровать произвольные открытые тексты в поисках правильного шифртекста. Например, пусть у криптоаналитика есть шифртекст $C_i = E_k(M)$. Даже если он правильно угадает M, полученный при шифровании $E_k(M)$ результат будет совершенно другим шифртекстом C_j. Ему бесполезно сравнивать C_i и C_j, криптоаналитик не сможет узнать, была ли его догадка правильной. Даже если у криптоаналитика есть открытый ключ зашифрования, открытый текст и шифртекст, он не сможет без закрытого ключа расшифрования доказать, что шифртекст является результатом шифрования конкретного открытого текста. Даже выполнив полный перебор, криптоаналитик может доказать только, что каждый допустимый открытый текст является всего лишь возможным открытым текстом. В этой схеме шифртекст всегда будет длиннее открытого текста.

Целью работы является создание комбинированного алгоритма вероятностного шифрования, в котором блок зашифрованной информации формируется из случайного, но ограниченного, числа битов исходного текста и сгенерированных случайных битов, полученные биты подвергаются стохастической перестановке для формирования блока шифртекста. Доля битов исходного текста и количество случайных битов, а также расположение исходных и случайных битов в каждом блоке зашифрованной информации является случайным процессом, зависящим от используемых генераторов псевдослучайных последовательностей и криптографических ключей. Полученная таким образом битовая последовательность шифруется затем по алгоритму Голдвассера-Микали. Классическая задача криптографии это обеспечение обратимости преобразования некоторого исходного теста (открытого текста) в кажущуюся случайной последовательность знаков, называемую шифртекстом (закрытым текстом) или криптограммой. При этом шифртекст может содержать как новые знаки, так и уже имеющиеся в исходном сообщении. Количество знаков в криптограмме и в исходном тексте может различаться. Непременным требованием является возможность однозначного и в полном объеме

восстановления исходного текста, используя лишь некоторые логические действия с символами шифртекста. Выше сказанное можно выразить следующим образом.

Пусть X, K, Y – конечные множества возможных открытых текстов, ключей и шифрованных текстов соответственно [1], а $E_k : X \to Y$ – правило зашифрования на ключе $k \in K$. Множество $\{E_k : k \in K\}$ обозначим через E, а множество $\{E_k(x): x \in X\}$ – через $E_k(X)$. Пусть $D_k : E_k(X) \to X$ – правило расшифрования на ключе $k \in K$, и D – множество $\{D_k : k \in K\}$.

Далее будем предполагать, что если $k \in K$ представляется в виде $k = (k_з, k_р)$, где $k_з$ – ключ зашифрования, а $k_р$ – ключ расшифрования (причем в общем случае $k_з \neq k_р$), то E_k понимается как функция $E_{кз}$, а D_k как функция $D_{кр}$. Введем условное обозначение $\sum_A$ для алгебраической модели шифра.

Шифром (шифросистемой) называется совокупность введенных множеств,

$$\sum_A (X, K, Y, E, D), \tag{1}$$

для которых выполняются следующие свойства:

1) для любых $x \in X$ и $k \in K$ выполняется равенство $D_k(E_k(x)) = x$;

2) $Y = \bigcup_{k \in K} E_K(X)$.

Шифр – это совокупность множеств возможных открытых текстов (то, что шифруется), возможных ключей (то, с помощью чего шифруется), возможных шифр-текстов (то, во что шифруется), правил зашифрования и правил расшифрования.

Необходимо отметить, что первое условие отвечает требованию однозначности шифрования. Второе условие означает, что любой элемент $y \in Y$ может быть представлен в виде $E_k(x)$ для подходящих элементов $x \in X$ и $k \in K$.

Нетрудно проверить, что из первого условия следует свойство инъективности функции E_k. Другими словами, если $x_1, x_2 \in X$, причем $x_1 \neq x_2$, то при любом $k \in K$ выполняется неравенство $E_k(x_1) \neq E_k(x_2)$.

По сути дела, (1) вводит математическую модель, отражающую основные свойства реальных шифров. В силу этого реальный шифр отождествляют с его моделью $\sum_A$, которая называется алгебраической моделью шифра.

В большинстве случаев множества X и Y представляют собой объединения декартовых степеней некоторых множеств A и B соответственно, так что для некоторых натуральных L и L_1

$$X = \bigcup_{i=1}^{L} A^i, \quad Y = \bigcup_{i=1}^{L_1} B^i. \tag{2}$$

Множества A и B называют соответственно алфавитом открытого текста и алфавитом шифрованного текста. Другими словами, открытые и шифрованные тексты записываются привычным образом в виде последовательностей букв.

Введем шифр простой замены в алфавите A.

Пусть $X = Y = \bigcup_{i=1}^{L} A^i$, $K \subseteq S(A)$, где S(A) – симметричная группа подстановок множества A. Для любого ключа $k \in K$, открытого текста $x = (x_1, \ldots, x_l)$ и шифрованного текста $y = (y_1, \ldots, y_l)$ правила зашифрования и расшифрования шифра простой замены в алфавите A определяются формулами:

$$E_k(x) = (k(x_1), \ldots, k(x_l)); \quad D_k(y) = (k^{-1}(y_1), \ldots, k^{-1}(y_l)), \tag{3}$$

где k^{-1} – подстановка, обратная к k.

В более общей ситуации для шифра простой замены $X = \bigcup_{i=1}^{L} A^i$, $Y = \bigcup_{i=1}^{L} B^i$, причем $|A| = |B|$, а K представляет собой множество биекций множества A на множество B. Правила зашифрования и расшифрования определяются для $k \in K$, $x \in X$, $y \in Y$ (и обратной к k биекции k^{-1}) формулами (3).

Определим еще один шифр, называемый шифром перестановки.

Пусть $X=Y=A^L$ и пусть $K \subseteq S_L$, где S_L – симметрическая группа подстановок множества {1, 2,…, L}. Для любого ключа k, открытого текста $x=(x_1,\ldots,x_L)$ и шифрованного текста $y=(y_1,\ldots,y_L)$ правила зашифрования и расшифрования шифра перестановки определяются формулами:

$$E_k(x)=(x_{k(1)},\ldots,x_{k(L)}), \quad D_k(y)=(y_{k^{-1}(1)},\ldots,y_{k^{-1}(L)}), \tag{4}$$

где k^{-1} – подстановка, обратная к k.

Одним из перспективных способов повышения стойкости известных шифров является задание неопределенности хода шифрования информации, что может быть реализовано путем введения в преобразуемое сообщение случайных данных. Если в механизме шифрования используются операции или процедуры, зависящие от преобразуемых данных, тогда сами операции будут изменяться случайно. Идея введения элементов случайности в процедуру шифрования преследует цель затруднить использование общего принципа криптоанализа блочных шифров, основанного на попытках выявления статистических свойств алгоритма шифрования, например, путем подбора специальных исходных текстов или криптограмм. "Подмешивание" случайных данных к шифруемому сообщению позволяет задать вероятностный характер операций преобразования и тем самым повысить вычислительную стойкость криптосистемы.

Пусть E есть b-битовая функция шифрования, P есть p-битовый блок открытого текста и R – r-битовый случайный блок, где b = r + p. Подадим на вход шифрующей функции блок B = R||P, где знак "||" обозначает конкатенацию двоичных векторов R и P: $P \rightarrow B = R||P \rightarrow C = E(B,K)$, где K – ключ шифрования. Поскольку при шифровании размер входного блока увеличивается, то такое шифрование отображает данный блок открытого текста P на большое множество блоков шифртекста $\{C_1, C_2, \ldots, C_n\}$, где $n = 2^r$.

При дешифровании блока шифртекста законный пользователь, владеющий секретным ключом, восстанавливает блок B = R || P, после чего значение R отбрасывается и выделяется исходное сообщение P. Выбирая различные значения отношения b/p, можно регулировать степень усиления шифрования. Чем больше указанное отношение, тем больше усиление.

Отличие вероятностного шифрования от криптосхемы с частой сменой сеансовых ключей состоит в том, что она не приводит к существенному снижению скорости шифрования в случае использования шифров с этапом предвычислений, на котором формируется ключ шифрования под управлением сеансового ключа. Схема вероятностного шифрования позволяет регулировать степень уменьшения скорости преобразования. Если функция E имеет исходное значение скорости преобразования s_0, то при использовании вероятностного шифрования она составляет $s = s_0(b - r)/b$.

Шифры с простым вероятностным механизмом предоставляют следующие преимущества:

- стойкость известных блочных шифров может быть существенно повышена;
- в определенном смысле можно управлять стойкостью шифра путем выбора различных значений отношения r/b;
- вероятностная криптосхема позволяет использовать новые механизмы задания зависимости процедур шифрования от секретного ключа.

Плата за эти достоинства состоит в следующих недостатках:

- скорость уменьшается в r/b раз;
- блоки шифртекста имеют длину больше, чем блоки исходного текста.

Рассмотрим три [2, 4, 6] варианта вероятностного шифрования. В первом варианте используется недетерминированное перемешивание случайных и информационных битов, благодаря чему обеспечивается уменьшение отношения r/t при существенном повышении стойкости. Для реализации данной идеи в случайном двоичном векторе выделяются две части с заранее условленной длиной: $R = R_1 || R_2$. Затем до выполнения шифрующего преобразования двоичного вектора $R_2||T$ над ним выполняют перестановку битов в зависимости от случайного значения R_1, что задает случайное перемешивание битов сообщения T и битов случайного значения R_2. Для перемешивания битов могут быть использованы управляемые операционные блоки перестановок P. Выполняемая блоком P перестановка зависит от значения управляющего вектора V, который формируется в зависимости от R_1.

Последовательность преобразований в варианте со случайным объединением информационных и случайных битов имеет следующий вид:

$$T \rightarrow R_2||T \rightarrow P_V(R_2||T) \rightarrow R_1||P_V(R_2||T) \rightarrow E_k(R_1||P_V(R_2||T)).$$

Второй вариант усиления упрощенной схемы вероятностного шифрования связан с идеей предварительного шифрования исходного текста T по случайно генерируемому значению R, используемому в качестве разового ключа предварительного шифрования.

Последовательность преобразований имеет вид:

$$T \rightarrow E'_R(T) \rightarrow E''_k(R||E'_R(T)).$$

Эффект усиления достигается за счет дополнительных преобразований по ключу разового использования, вероятность повторения которого составляет порядка 2^{-r} при атаках на основе подобранных значений T и C (благодаря хорошим рассеивающим свойствам шифрующих процедур E"). При выполнении предварительного шифрования может быть применена исходная схема вероятностного шифрования, что приводит к следующей последовательности преобразований:

$$T \rightarrow R_2 \| T \rightarrow E'_{R1}(R_2 \| T) \rightarrow E''_k(R_1 \| E'_{R1}(R_2 \| T)).$$

Этот случай относится к третьему варианту усиления и является обобщением первого варианта, в котором перемешивание случайных и информационных битов может быть рассмотрено как частный случай шифрующего преобразования. Эффект усиления в рассмотренных вариантах связан с тем, что в соотношения, связывающие пары значений T и C, входит случайная (псевдослучайная) величина R при атаке на основе подобранных исходных сообщений T (подобранных шифртекстов C).

В рассмотренных вариантах вероятностного шифрования доля случайных битов может быть переменной величиной, но остается неизменной для каждого конкретного случая и перемешивание битов исходного текста и случайных битов осуществляется за счет функции шифрования E. Рассматривается следующая модификация алгоритма вероятностного шифрования на основе алгебраической модели шифра (1) и [3]. Пусть имеется исходная информация длиной n бит, а длина блока m. Стартовым значением первого генератора псевдослучайной последовательности (ГПСП N1), выходные данные которого берутся по mod m, является ключ k1, сгенерированная последовательность имеет вид: l_1, l_2, l_3, … ,lk. Считываем первые l_1 битов исходной информации, вычисляем число m-l_1 случайных бит, необходимых для заполнения блока. Далее с помощью другого генератора псевдослучайной последовательности ГПСП N2 с ключом k2 получаем m-l_1 случайных бит, затем используем стохастическое перемешивание согласно (4) исходных и случайных бит с помощью ГПСП N3 (с ключом k3), результаты которого также берем по mod m. Процесс стохастической перестановки контролируем с помощью вспомогательного одномерного массива, чтобы не допустить расстановки двух бит в одну ячейку формируемого блока зашифрованной информации. Со следующими l_2 битами исходного текста поступаем аналогичным образом, следует заметить, что для каждого формируемого блока зашифрованного текста доля случайных битов будет различной. Процесс продолжается до тех пор, пока не будут считаны все биты исходного текста.

Применим к полученной таким образом битовой последовательности, в которой стохастически перемешаны биты исходного текста и случайные биты, вероятностный алгоритм шифрования Голдвассера и Микали. Для этого генерируем два больших простых числа p и q, а также найдем произведение этих чисел $N = p*q$. В качестве открытого ключа выберем случайное число y, не являющееся квадратичным вычетом как по модулю p, так и по модулю q. Пара чисел (N, y) является открытой информацией пользователя, числа (p,q) секретной информацией. Чтобы зашифровать строку бит $m = b_1 b_2 \ldots b_l$ необходимо для каждого i-го бита выбрать случайное число x_i из множества вычетов по модулю N и если этот бит равен 0, то $c_i = x_i * x_i \pmod N$, иначе $c_i = y_*(x_i * x_i) \pmod N$, где c_i – элемент шифртекста, соответствующий b_i. Для дешифрования полученной информации проверяем, если элемент криптограммы c_i является квадратичным вычетом по модулю N, то $b_i = 0$, иначе $b_i = 1$. Алгоритм вероятностного шифрования реализован на языке C/C++ и представляется полезным для защиты информации от несанкционированного доступа.

Предложенный алгоритм вероятностного шифрования отличается от известных алгоритмов тем, что процесс получения каждого блока зашифрованной информации является стохастическим процессом, зависящим от используемых генераторов псевдослучайных последовательностей и криптографических ключей, при этом доля битов исходного текста и число случайных битов, а также расположение исходных и случайных битов в каждом блоке шифртекста является случайным. Данный алгоритм может использоваться как этап подготовки исходной информации для дальнейшего шифрования по методу Голдвассера и Микали, что, по мнению авторов, повысит криптостойкость такой комбинированной схемы шифрования.

Библиографический список

1. Бабаш А. В. Криптография / А.В. Бабаш, Г.П. Шанкин. — М.: Изд-во «СОЛОН-Р», 2002. — 512 с.

2. Криптография: скоростные шифры. / А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. — СПб.: Изд-во «БХВ – Петербург», 2002. — 496 с.

3. Куржеевский И.В. Вероятностный алгоритм шифрования / И.В. Куржеевский // Зб. наук. пр., Севастопольський військово-морський ордена Червоної Зірки інститут ім. П.С. Нахімова. — 2008. — Вип. 1 (14). — С. 107–111.

4 Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов. / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. — СПб.: БХВ – Петербург, 2004. — 448 с.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М.: Изд-во «ТРИУМФ», 2003. — 816 с.

Поступила в редакцию 10.06.2009 г.