Иванова Н.Ю.

ИССЛЕДОВАНИЕ МЕТОДА ВАРИАНТНОГО ШИФРОВАНИЯ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Метод вариантного шифрования основан на том, что сообщение шифруется несколькими алгоритмами шифрования (функциями) последовательно, то есть набором из n алгоритмов, который выбирается из множества возможных сочетаний (списка наборов). Выходная криптограмма очередного алгоритма является сообщением для последующего алгоритма. Наборы составляются путем комбинирования алгоритмов (функций) входящих в метод. Количество наборов шифрующих функций определяется:

$$m = C_t^n = \frac{t!}{(t-n)!}\ , \qquad (1)$$

где t – количество используемых алгоритмов в системе, n – количество алгоритмов в данном наборе.

Сообщение M, зашифрованное одним из наборов (i-тый набор), то есть криптограмма A_i описывается из :

$$A_i = f_n(f_{n-1}(f_{n-2}(....f_1(M, K_1),....), K_{n-2}), K_{n-1}), K_n)\ , \qquad (2)$$

где f_1 – первая шифрующая функция в наборе i,…, f_n – n – ая шифрующая функция в наборе i, M – сообщение (открытый текст), K_1 – ключ первой шифрующей функции в наборе i,…, K_n – ключ n – ой шифрующей функции в наборе i.

Для шифрования сообщения выбирается набор алгоритмов из списка с соответствующими ключами, таким образом получается криптограмма S:

$$S = \sum_{i=1}^{m} d_i A_i\ , \qquad (3)$$

где S – криптограмма, m – количество наборов шифрующих функций, A_i – i-ая криптограмма, d_i – весовой коэффициент однозначно определяющий выбор единственного A_i из m возможных.

Затем происходит построение контекста безопасности. Контекст безопасности содержит информацию необходимую для расшифровки сообщения на принимающей стороне. К полученной криптограмме S добавляется контекст безопасности.

$$Q = con \rightarrow S \qquad , \qquad (4)$$

где «→» – конкатенация, Q – выходное сообщение.

Распределение ключей является основной проблемой в криптографии. Для решения данной задачи предлагается на этапе установления соединения использовать криптографический алгоритм с открытым ключом для передачи контекста безопасности. Таким образом, конечная криптограмма W, которую получат на принимающей стороне описывается:

$$W = R(Q,K) \quad , \qquad (5)$$

где R – криптографический алгоритм с открытым ключом.

Из (2), (3), (4), (5) получим

$$W = R(con \rightarrow \sum_{i=1}^{m} d_i f_{i,n}(f_{i,n-1}(f_{i,n-2}(....f_{i,1}(M, K_{i,1}),....), K_{i,n-2}), K_{i,n-1}), K_{i,n}), K)$$

На рисунке 1 представлена схема метода вариантного шифрования на этапе установления соединения.

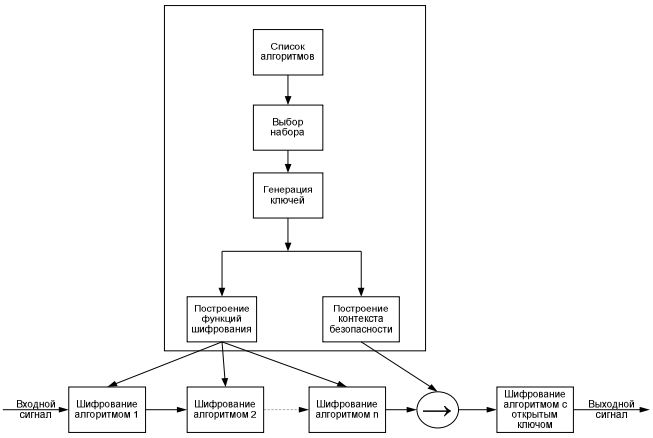

Рисунок 1. Метод вариантного шифрования (этап шифрования).

Процесс дешифрования представлен на рисунке 2. Входной сигнал дешифруется, используя алгоритм с открытым ключом. Из полученных данных выделяется контекст безопасности, на его основе происходит составление набора используемых функций, а также генерация ключей для используемых криптографических алгоритмов. Далее на основе полученных данных составляется функция дешифрования непосредственно с уже сгенерированными ключами. Происходит процесс дешифрования полученного сообщения с последовательным использованием функций криптографических алгоритмов. В результате этих преобразований на выходе получается исходное сообщение.

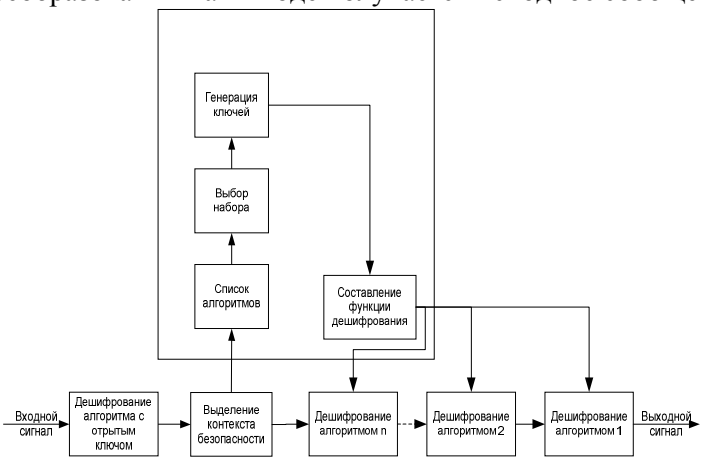

Рисунок 2.3. Метод вариантного шифрования (этап дешифрования).

В классическом криптоанализе предполагается, что злоумышленнику известен алгоритм шифрования. Криптостойкость алгоритма определяется необходимым количеством переборов для определения ключа (взлом грубой силой):

$$Z = 2^K,$$

где Z – количество необходимых переборов для вскрытия алгоритма, K – длина ключа алгоритма.

Таким образом, криптостойкость последовательности алгоритмов составляющих A_i:

$$Z_A = \prod_{j=1}^{n} 2^{K_j} = 2^{\sum_{j=1}^{n} K_j}, \quad (6)$$

где, Z_A – количество необходимых переборов для вскрытия последовательности алгоритмов, K_j – длина ключа j-ого алгоритма.

Следовательно, из (6), количество переборов необходимых для вскрытия S:

$$Z_S = \sum_{i=1}^{m} 2^{\sum_{j=1}^{n} K_{i,j}}, \quad (7)$$

где, $K_{i,j}$ – длина ключа j-ого алгоритма i-го набора алгоритмов.

Метод вариантного шифрования позволяет создать криптосистему на базе существующих алгоритмов шифрования. Определим показатель V который показывает, во сколько раз увеличится число переборов необходимых для вскрытия криптограммы зашифрованной методом вариантного шифрования по сравнению с криптограммой зашифрованной одиночным алгоритмом:

$$V = \frac{Z_S}{Z} = \sum_{j=1}^{m} 2^{\sum_{i=1}^{n} K_{i,j} - K} \quad (8)$$

Для получения системы более криптостойкой чем одиночный алгоритм с максимальной длиной ключа K необходимо выполнение условия:

$$\sum_{i=1}^{n} K_{i,j} + \log_2(m) > K$$

На основе описанного метода был разработан алгоритм вариантного шифрования, в котором используются блочные (DES, IDEA, RC5, LOKI91, GOST, BLOWFISH, 3 WAY,) и потоковые (RC4, A5, SEAL) алгоритмы. По мнению Б. Шнайера именно эти алгоритмы просты для программно-аппаратной реализации. Общее количество алгоритмов в алгоритме вариантного шифрования равно 10.

Для выбора приемлемого количества алгоритмов в наборе n вычислили из (8) показатель V при различных n . Одиночный алгоритм был взят с ключом 256 бит. Вычислили объем необходимой памяти вычислительного устройства P для хранения кодовой книги при различных n. Объем памяти P рассчитывался:

$$P = (n + l) * m, \quad (9)$$

где l – количество байт необходимых для хранения в памяти числа m. Показатель $YV(n)$ показывает динамику изменения показателя V в зависимости от n.

$$YV(n) = \frac{V(n)}{V(n\text{-}1)}$$

Показатель $YP(n)$ показывает динамику изменения показателя P в зависимости от n.

$$YP(n) = \frac{P(n)}{P(n\text{-}1)}$$

Полученные данные представлены и на рисунке 3.

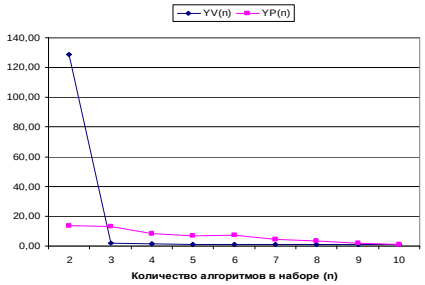

Рисунок 3. Значения показателей YP и YV

Из рисунка 3. видно, что точкой пересечения графиков является точка n=3. Следовательно, количество алгоритмов в наборе возьмем равным трем. В этом случае число возможных наборов достаточно большое m=720 (в соответствии с (1)), криптостойкость алгоритма вариантного шифрования достаточно высока $Z_s \approx 2^{770}$(в

соответствии с (7)) и объем требуемой памяти достаточно низок P=3600 бит(в соответствии с (9)). Общая схема алгоритма вариантного шифрования представлена на рисунке 4.

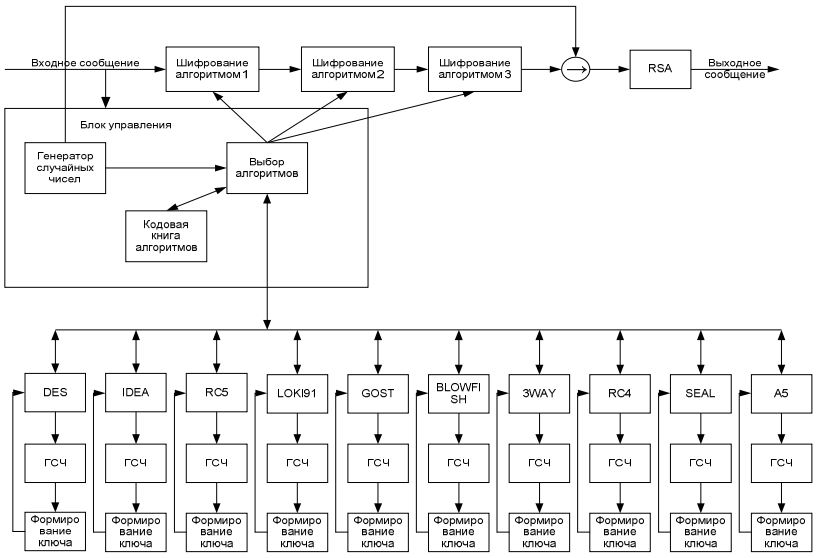

Рисунок 4. Алгоритм вариантного шифрования.

В кодовой книге алгоритмов содержится 720 записей. Кодовая книга алгоритмов представляет собой двухмерную таблицу, которая содержит порядковые номера записей и наборы алгоритмов. В качестве шифрующей функции для передачи контекста безопасности используется алгоритм с открытым ключом RSA.

При поступлении сигнала на вход устройства, передается сигнал блоку управления. Блок управления генерирует случайное число в диапазоне от 1 до 720 (номер набора в кодовой книге алгоритмов). Сгенерированное случайное число включается в контекст безопасности.

Для выбранного набора алгоритмов генерируются ключи на основе случайных чисел (они включаются в контекст безопасности). В алгоритме вариантного шифрования предлагается получение различных ключей в зависимости от четности случайного числа. Входной сигнал шифруется последовательно всеми тремя функциями из набора. К полученной криптограмме добавляется контекст безопасности. Выходное сообщение шифруется алгоритмом RSA.

После процесса установления соединения нет необходимости создавать ключи и список алгоритмов, следовательно, можно исключить алгоритм RSA для минимизации времени задержки вносимой в канал связи.

Криптостойкость некоторых сочетаний алгоритмов находится ниже уровня 2^{256}, то есть ниже, чем криптостойкость одного алгоритма, такого, как ГОСТ, RC4 или BLOWFISH. Следовательно, при составлении кодовой книги алгоритмов необходимо обеспечить выполнение условия: криптостойкость последовательности алгоритмов должна быть больше 2^{256}. В этом случае число сочетаний алгоритмов составит 667.

Произведем сравнение, во сколько раз увеличится число переборов необходимых для вскрытия криптограммы зашифрованной алгоритмом вариантного шифрования по сравнению с криптограммой зашифрованной алгоритмом с максимально допустимой длиной ключа среди выбранных одиночных алгоритмов - 256 бит. По (8) имеем:

$$V = \frac{Z_S}{Z} = \frac{\sum_{i=1}^{667} 2^{\sum_{j=1}^{3} K_{i,j}}}{2^{256}} \approx \frac{2^{770}}{2^{256}} \approx 2^{514}$$

Таким образом, криптостойкость разработанного алгоритма является существенно выше криптостойкости одиночных алгоритмов с максимально допустимой длиной ключа-256 бит.

Так же преимуществом алгоритма вариантного шифрования является модульность, и как следствие простая замена и добавление новых одиночных алгоритмов шифрования. При замене даже одного алгоритма произойдет переформирование всей таблицы, что существенно усложнит задачу взлома.

Разработанный алгоритм был реализован на цифровых сигнальных процессорах семейства TMS320C64x. Время выполнения каждого алгоритма представлено на рисунке 5.

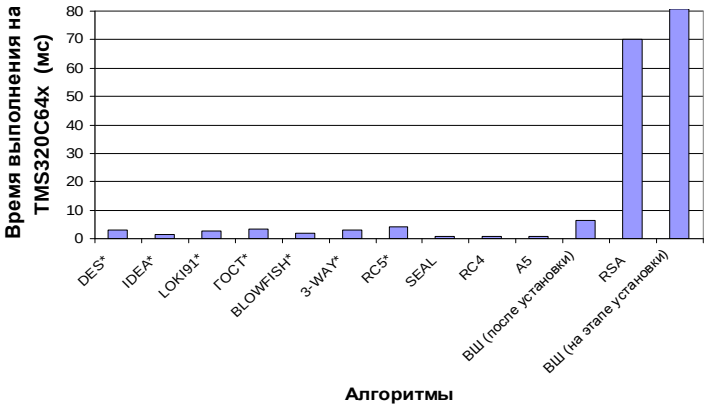

Рисунок 5 Время выполнения алгоритмов.

Для оценки работы алгоритма вариантного шифрования определили критерий *J*, показывающий отношение криптостойкости алгоритма к времени задержки вносимой в канал связи. Полученные данные представлены и на рисунке 6. Критерий *J* показал, что алгоритм вариантного шифрования является наилучшим алгоритмом по соотношению криптостойкость/время выполнения.

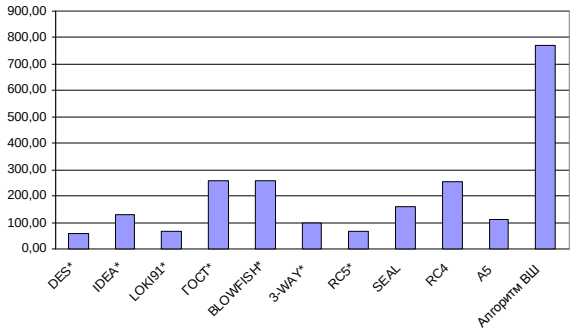

Рисунок 6. Отношение криптостойкости алгоритма к времени задержки вносимой в канал связи.

Разработанный на основе метода вариантного шифрования алгоритм применим для создания надежных систем защиты информации от несанкционированного доступа в телекоммуникационных сетях.