МОДИФИКАЦИЯ ТАБЛИЦ ПЕРЕСТАНОВОК АЛГОРИТМА ШИФРОВАНИЯ MV2

Е. Г. Шалёв
Кафедра интеллектуальных информационных технологий, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: evheny.shaliov@tut.by

Приведены результаты исследования изменения параметров алгоритма шифрования MV2. Предложены меры усиления защищённости алгоритма.
Ключевые слова: криптография, шифрование, алгоритм шифрования MV2, таблица перестановок.

Введение

Одним из последних достижений в криптографии является алгоритм шифрования MV2[1]. Алгоритм зашифрования с помощью алгоритма MV2 представлен ниже.

1. На вход подаётся исходный текст (T), ключ (K) для выполнения процедуры забеливания текста, а также генерируется 32 таблицы замены (ТЗ) с длиной слова 8.
2. С помощью таблиц замен бинарное представление забелённого текста преобразуется в текущие остаток и флаги. К флагам добавляется блок служебной информации о текущем шаге: номер использованной таблицы (0-31) и результат остатка от деления длины текущего остатка на длину слова в таблице замен, а именно — 8. Таким образом, для указания номера использованной таблицы необходимо выделение 5 бит ($log_2(32)$) в служебной области, для указания остатка от деления — 3 бита ($log_2(8)$). Текущие остаток и флаги добавляются к результирующим флагам и ядру.
3. Предыдущий шаг повторяется несколько раз. Вместо забелённого текста передаются текущие флаги.

На выходе алгоритма получаем следующие данные, необходимые для восстановления исходного текста:

1. результирующие флаги,
2. результирующее ядро,
3. 32 таблицы замен,
4. ключ, необходимый для забеливания[1].

В этой работе выполнен анализ реализаций алгоритма MV2, выполненных с помощью изменения различных параметров алгоритма, и предложены меры для усиления криптостойкости алгоритма.

Анализ характеристик алгоритма MV2

Для анализа криптостойкости алгоритма MV2 сделаем допущения, позволяющие упростить процедуру взлома алгоритма:

1. после процедуры забеливания текст не изменяется,
2. в таблице перестановок содержатся такие записи, согласно которым перестановки не совершаются,
3. криптоаналитику известны флаги и ядро, но неизвестна таблица перестановок,
4. криптоаналитику известен алгоритм шифрования,
5. минимально допустимый ключ имеет длину 128 бит[2].

Пусть таблица перестановок содержит записи по n бит. Тогда количество возможных комбинаций (k) в таблице можно рассчитать по формуле

$$k(n) = n! * 2^n.$$

Очевидно, при построении таблицы перестановок нужно учитывать количество и объём (p) всех записей. Это значение вычисляется по формуле

$$p(n) = n * 2^{n+1}.$$

Поскольку минимальные длины ключей большинства современных алгоритмов симметричного шифрования равны 128 битам, а также учитывая, что алгоритм MV2 является симметричным алгоритмом шифрования, предположим, что минимально допустимый размер ключа будет равен 128 битам. Таким образом, минимальное количество раундов (r), необходимых для достижения длины ключа в 128 бит, рассчитывается по формуле

$$r(n, k(n)) = 128/log_2(k(n)).$$

Очевидно, что после каждого раунда скрывается как минимум 1 бит блока данных. Таким образом, после n раундов отношение объёма данных флагов к объёму данных исходного текста (h), который можно рассчитать по формуле

$$h(n, r(n, k(n))) = (1 - ((n-1)/n)^{r(n)}) * 100.$$

Результаты вычислений количества возможных комбинаций (k), объёма (p) всех записей в таблице перестановок, минимальное количество раундов шифрования (r), отношение объёма данных флагов к объёму данных исходного текста (h) для длины слова от 1 до 32 бит представлены в таблице 1.

Таблица 1 – Результаты вычислений характеристик алгоритма MV2 в зависимости от длины слова

n (бит)	k	p	r	h
1	1	0,5(б)	128	100
2	3	2(б)	43	100
3	5	6(б)	26	99,9974
4	8	16(б)	16	99,9977
5	11	40(б)	12	93,13
6	15	96(б)	9	80,62
7	19	224(б)	7	66,01
8	23	512(б)	6	55,12
9	27	1,125(Кб)	5	44,51
10	31	2,5(Кб)	5	40,95
11	36	5,5(Кб)	4	31,7
12	40	12(Кб)	4	29,39
13	45	26(Кб)	3	21,35
14	50	56(Кб)	3	19,93
15	55	120(Кб)	3	18,7
16	60	256(Кб)	3	17,61
17	65	544(Кб)	2	11,42
18	70	1,125(Мб)	2	10,80
19	75	2,375(Мб)	2	10,25
20	81	5(Мб)	2	9,75
21	86	10,5(Мб)	2	9,3
22	91	22(Мб)	2	8,88
23	97	46(Мб)	2	8,51
24	103	96(Мб)	2	8,16
25	108	200(Мб)	2	7,84
26	114	416(Мб)	2	7,54
27	120	864(Мб)	2	7,27
28	125	1,75(Гб)	2	7,02
29	131	3,625(Гб)	1	3,45
30	137	7,5(Гб)	1	3,33
31	143	15,5(Гб)	1	3,24
32	149	32(Гб)	1	3,13

Заключение

Дальнейшие исследования перспективны при использовании длины слова в таблице перестановок от 12 до 28 бит. При этом отношение объёма данных флагов к объёму данных исходного текста — от 7% до 35%. Достаточное количество раундов шифрования данных — от 2 до 5 в зависимости от длины слова.

Перспективным направлением может быть разработка переменной длины заменяемых слов в зависимости от раунда. Другими словами в первом раунде происходит замена слов, например, длиной 16 бит, на втором раунде — 22 бита, и т. д. Таким образом, при использовании слов с длиной от n до m бит при r раундах, длина ключа будет увеличена до значения, которое может быть рассчитано по формуле:

$$r * (m - n) * ((log_2(n!) + log_2(m!))/2).$$

Другими словами, количество раундов умноженное на арифметическую прогрессию перестановок для каждой из длин слов.

На основании проведённых теоретических исследований сделаны следующие предположения.

1. Для повышения криптостойкости алгоритма можно использовать переменную длину слова в таблице перестановок.
2. Минимально допустимым числом раундов шифрования алгоритмом MV2 является 2.
3. Также для повышения криптостойкости алгоритма и уменьшения количества раундов можно использовать длину слова в таблице перестановок от 12 до 24 бит.
4. В случае передачи таблицы перестановок по закрытому каналу длина слова в таблице перестановок ограничивается 20 битами, поскольку большее количество бит в слове существенно увеличивает объём передаваемых данных.

В таком случае ожидаемый результат может быть следующим.

1. Отношение объёма данных флагов к объёму данных исходного текста составит от 12% до 17,6%.
2. Улучшение криптостойкости при применении грубой силы – при тех же затратах количество вариантов ключа возрастает до

$$3 * 8 * ((log_2(16!) + log_2(24!))/2) = 1480(bit).$$

Для подтверждения или опровержения перечисленных гипотез необходимы дальнейшие исследования модификаций таблиц перестановок, алгоритма MV2 и шифртекста.

1. Мищенко, В. А. Ущербные тексты и многоканальная криптография / В. А. Мищенко, Ю. В. Виланский. - Минск: Энциклопедикс, 2007. – 292 с.
2. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.