ИССЛЕДОВАНИЕ СВОЙСТВ АЛГОРИТМА MV2

В.В. Герасименок

Белорусский государственный университет,
пр-т Независимости 4, 220030 Минск, Беларусь

В [1] приведено описание алгоритма MV2 получения ущербных текстов. Суть алгоритма заключается в том, что исходный открытый текст преобразуется с использованием ключевых таблиц $T_1, T_2, \ldots, T_k$ в два – ядро текста и флаг текста. Ядро текста зашифровывается с использованием некоторого алгоритма шифрования. Флаг текста остается неизменным при его хранении.

В описании алгоритма жестко не установлено правило выбора таблиц $T_1, T_2, \ldots, T_k$, а также их количество. В докладе рассматривается возможность восстановления ключевой таблицы T_1 алгоритма MV2 по специально подобранным парам открытого и соответствующего ему шифрованного текста [2] для частного случая, когда во всех итерациях преобразования открытого текста используется таблица T_1.

Приведем краткое описание алгоритма восстановления таблицы T_1. Очевидно, если на вход алгоритма MV2 подать последовательность, состоящую из всех 256 символов ASCII в лексикографическом порядке $M = 00000000||00000001||\ldots||11111111$, и при этом рассмотреть первые 256 символов последовательности флагов

$$f_1(M) = f_1(00000000)||f_1(00000001)||\ldots||f_1(11111111),$$

то соответствующими значениями заполняется третий столбец таблицы T_1.

Для восстановления второго столбца таблицы на вход необходимо подавать последовательности вида *аааааааа*, где $a \in \{0,1\}^8$, и наблюдать флаги, полученные после второй итерации алгоритма. Размерность флагов может принимать значения: 7 (128 раз), 5 (32 раза), 3 (80 раз) и 1 (16 раз). Последовательно рассмотрим множество возможных вариантов замены второго столбца таблицы T_1 и сравним их с наблюдаемыми значениями. При их полном совпадении определяем заполнение второго столбца таблицы T_1 для конкретного значения. В том случае, если наблюдаемые последовательности совпадают между собой, таблица T_1 восстанавливается в вариантах.

Следующим шагом восстановления состояний является анализ криптоэквивалентных относительно первых двух шагов таблиц. Пусть значения $X = (x_1, x_2, \ldots, x_8)$, $X^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots, x_8^{(1)})$ неразличимы после двух итераций и длина флагов равна 1. Пусть $c(X) = (y_1, y_2, \ldots, y_7)$, $c(X^{(1)}) = (y_1^{(1)}, y_2^{(1)}, \ldots, y_7^{(1)})$ – значения ядра.

Рассмотрим следующие наборы: $Y_1 = (0, y_1, y_2, \ldots, y_7)$, $Y_2 = (1, y_1, y_2, \ldots, y_7)$, $Y_3 = (y_1, y_2, \ldots, y_7, 0)$, $Y_4 = (y_1, y_2, \ldots, y_7, 1)$ и $Y_1^{(1)} = (0, y_1^{(1)}, y_2^{(1)}, \ldots, y_7^{(1)})$, $Y_2^{(1)} = (1, y_1^{(1)}, y_2^{(1)}, \ldots, y_7^{(1)})$, $Y_3^{(1)} = (y_1^{(1)}, y_2^{(1)}, \ldots, y_7^{(1)}, 0)$, $Y_4^{(1)} = (y_1^{(1)}, y_2^{(1)}, \ldots, y_7^{(1)}, 1)$.

Если $f(Y_i) \neq f(Y_i^{(1)})$, хотя бы для одного $i \in \{1,2,3,4\}$, то значения второго столбца таблицы T_1 для значений X и $X^{(1)}$ становятся различимы и т.д.

В результате применения алгоритма таблица T_1 будет восстановлена. Для полного восстановления таблицы замены требуется не более 8 наборов открытый/шифрованный текст общей длины $\sim O(2000)$ байт.

Литература

1 *Мищенко В.А., Виланский Ю.В., Лепин В.В.* Криптографический алгоритм MV2. Мн.: Энциклопедикс 2007. 176 с.

2 *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. М.: Гелиос-АРВ. 2001. 480 с.