УДК 621. 391:519.2:519.7

КОМБИНАТОРНЫЕ СВОЙСТВА УМЕНЬШЕННОЙ ВЕРСИИ ШИФРА «КАЛИНА»

В.И. РУЖЕНЦЕВ, С.В. ЧИЧМАРЬ, Д.И. САВИН

Приводятся результаты исследования комбинаторных свойств мини версии шифра «Калина», одного из претендентов на национальный стандарт блочного симметричного шифрования Украины. Подтверждается, что законы распределения циклов, возрастаний и инверсий мини-шифра, рассматриваемого как подстановочное преобразование, повторяют свойства законов распределения вероятностей, характерные случайным подстановкам.

Ключевые слова: криптоанализ, шифр «Калина».

ВВЕДЕНИЕ

При выборе алгоритма шифрования нужно быть уверенным в том, что он будет обеспечивать необходимую стойкость защиты информации, а также будет иметь высокую скорость преобразований. Но всесторонний анализ криптографических алгоритмов требует больших вычислительных мощностей, а некоторые его аспекты вообще неосуществимы на данный момент. Для преодоления трудностей криптоанализа больших шифров на кафедре БИТ развивается подход, ориентированный на использование результатов анализа уменьшенных версий прототипов, для которых уже удается построить вычислительные эксперименты.

Важность развития работ в этом направлении определяется тем, что сейчас в Украине проходит конкурс по отбору претендентов на национальный стандарт блочного симметричного шифрования Украины и необходимы подходы, позволяющие ускорить процесс экспертизы представленных решений. Одних из предложений, рассматриваемых на этом конкурсе, является шифр «Калина».

Сегодня уже имеются результаты исследования циклических свойств шифрующих преобразований ряда мини версий шифров, представленных на Украинский конкурс [1]. Настоящая работа посвящена дальнейшему совершенствованию методики исследования комбинаторных свойств уменьшенных моделей шифров. В этой работе предлагаются построенные в ходе статистического эксперимента законы распределения инверсий, возрастаний и циклов уменьшенной модели шифра «Калина». Показывается, что полученные законы являются близкими к асимптотическим законам распределения, свойственным случайным подстановкам.

1. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ИНВЕРСИЙ

В этом случае для каждого ключа зашифрования из полного множества всех ключей путем последовательных зашифрований (на одном и том же ключе) создаётся массив всех возможных вариантов зашифрованных блоков данных, начиная с зашифрования нулевого значения блока данных, и так последовательно до последнего значения входного блока данных (равного 2^{16}–1). Тем самым в массиве данных запоминается вторая строка нормализованного представления подстановки (шифрующего преобразования). Затем на основе последовательного просмотра и сравнения значений элементов массива с текущим, выбранным для анализа, выполняется подсчет числа инверсий, соответствующего рассматриваемому элементу массива (числа превышений значения текущего рассматриваемого элемента множества значений просмотренных элементов, стоящих в массиве правее рассматриваемого). Результат подсчета числа инверсий для каждого из последовательно выбранных элементов массива нижней строки подстановки отсылается в накапливающий счетчик, фиксирующий общее число инверсий, соответствующее текущей подстановке. Естественно, что потребуется использовать 2^{16} накапливающих счетчиков, чтобы затем построить, по данным счетчиков, закон распределения вероятностей для числа инверсий.

2. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ЦИКЛОВ

В этом случае для каждого ключа зашифрования из полного множества ключей производится подсчет числа циклов подстановки, соответствующей каждому ключу. Поиск циклов и подсчет их числа производиться следующим образом. Создаётся массив всех возможных вариантов зашифрованных текстов, подобно тому, как это было сделано при анализе числа инверсий. Затем, начиная с нулевого значения элемента верхней строки подстановки (нулевого для зашифрования значения входного блока данных), выполняется зашифрование с последующим выполнением функции зашифрования к блокам данных, получающихся в результате зашифрования на текущем шаге. Значения результатов зашифрования фиксируются в исходном (запомненном) массиве путем исключения из него (или маркирования) появившихся в результате зашифрований значений. Эта операция выполняется до тех пор, пока в результате зашифрования не появится блок данных с нулевым значением (начальный блок

данных серии последовательных зашифрований). После этого выбирается наименьший по значению из оставшихся элементов массива (не попавший в предыдущий цикл), и строится новый цикл, начинающийся от нового значения, с запоминанием (″вычеркиванием″ или маркированием) пройденных (состоявшихся) зашифрованных значений. И эта процедура повторяется до тех пор, пока не будут пройдены (″вычеркнуты″) все элементы исходного массива. Параллельно с поиском циклов выполняется подсчет их числа с помощью соответствующего накапливающего счетчика. Для последующего построения закона распределения вероятностей для числа циклов используются дополнительный набор счетчиков, в которых подсчитывается число счетчиков, имеющих одинаковое заполнение, т.е. фиксирующих число подстановок (ключей зашифрования) с одним и тем же числом циклов.

3. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ВОЗРАСТАНИЙ

И в этом случае создаётся массив всех возможных вариантов зашифрованных текстов (строится вторая строка нормализованного представления подстановки). Для подсчета числа возрастаний для каждого элемента массива производится подсчет числа элементов массива, имеющих следующий элемент массива больший по значению текущего. Число превышений (возрастаний), полученных для каждой подстановки, фиксируется соответствующим накапливающим счетчиком.

4. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ КОМБИНАТОРНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

Результаты исследования комбинаторных свойств, выполненные в соответствии с изложенными выше методиками, иллюстрируют таблица 1 и графические зависимости, представленные на рис. 1 и рис. 2. В табл.1 приведен закон распределении числа циклов шифра мини-Калина.

На рис. 1 и рис. 2 приведены графические зависимости, отражающие законы распределения вероятностей для числа инверсий и числа возрастаний шифра мини-Калина.

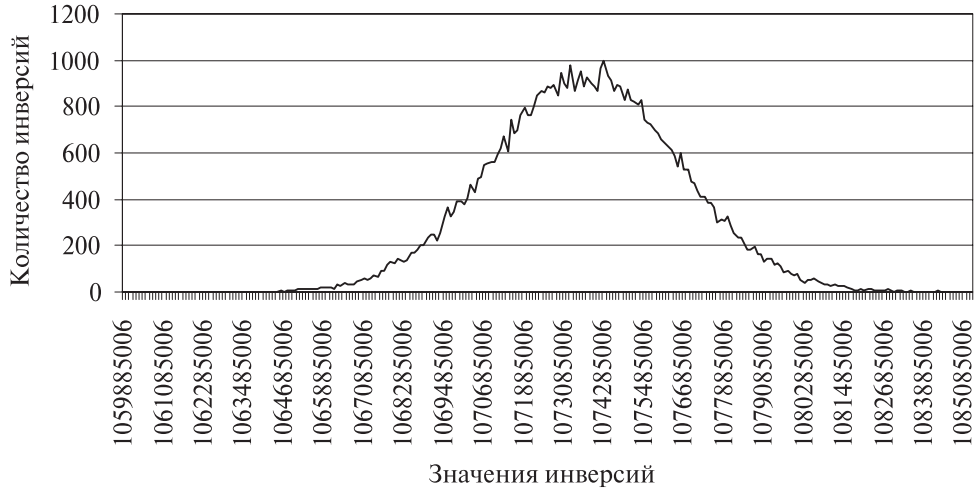

Рис. 1. Закон распределения числа инверсий для шифра мини-Калина

Рис. 2. Закон распределения числа возрастаний для шифра мини-Калина

Таблица 1

Закон распределения числа циклов шифра мини-Калина

Циклы	Количество
2	27
4	507
6	3234
8	9482
10	15318
12	16054
14	11524
16	6052
18	2407
20	706
22	186
24	34
26	5
28	1

ЗАКЛЮЧЕНИЕ

Представленные результаты свидетельствуют, что законы распределения числа циклов, возрастаний и инверсий шифра мини-Калина являются весьма близкими к нормальным, т.е. повторяют свойства, характерные для случайных подстановок [2]. Для определения числовых значений этих распределений можно пользоваться формулами для асимптотических законов распределения случайных подстановок.

Литература.

[1] *Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев Ф.В., Дробатько Е.В.* Криптографические свойства уменьшенной версии шифра "Калина" // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010, Т. 9, № 3. – С. 349-354.

[2] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. – Т. 6, № 2 – С. 257-263.

Поступила в редколлегию 2.07.2010.

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ, ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Чичмарь Сергей Владимирович, сотрудник кафедры БИТ ХНУРЕ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Савин Дмитрий Игоревич, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптография, системы защиты информации.

УДК 621. 391:519.2:519.7

Комбінаторні властивості зменшеної версії шифру «Калина» / В.І. Руженцев, С.В. Чичмар, Д.І. Савін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 346-348.

Наводяться результати дослідження комбінаторних властивостей міні версії шифру «Калина», одного з претендентів на національний стандарт блокового симетричного шифрування України. Підтверджується, що закони розподілу циклів, зростання та інверсій мінішифру, що розглядається як підстановлювальне перетворення, повторюють властивості законів розподілу ймовірностей, характерні випадковим підстановкам.

Ключові слова: криптоаналіз, шифр «Калина».

Табл. 01. Іл.02. Бібліогр.: 2 найм.

UDC 621. 391:519.2:519.7

Combinatorial properties of reduced cipher «Kalina» / V.I. Ruzhentsev, S.V. Chichmar', D.I. Savin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 346-348.

The paper presents results of researching combinatorial properties of mini versions of the cipher «Kalina», one of the pretenders to the national standard of block symmetric encryption of Ukraine. It is confirmed that the laws of distributing cycles, increases and inversions of a mini-cipher, considered as a substitution transformation, follow properties of the laws of distributing probabilities which are characteristic of random substitutions.

Key words: cryptanalysis, cipher «Kalina».

Tab. 01. Fig. 02. Ref.: 02 items.