УДК 004.056.55

к.т.н. **Петров А.А.** (ВНУ им. В. Даля)
Каражанов Д.Ф. (ВНУ им. В. Даля)

АНАЛИЗ НЕДОСТАТКОВ ФИКСИРОВАННОГО РАЗМЕРА БЛОКА В БЛОЧНЫХ ШИФРАХ

У даній статті розглянута структура блокових алгоритмів шифрування. Запропонований метод для усунення виявлених недоліків і підвищення стійкості блокових алгоритмів до атаки повним перебором.

Ключові слова: блокові алгоритми, шифрування

В данной статье рассмотрена структура блочных алгоритмов шифрования. Предложен метод для устранения выявленных недостатков и повышения стойкости блочных алгоритмов к атаке полным перебором .

Ключевые слова: блочные алгоритмы, шифрование.

In this article the structure of block algorithms of enciphering is considered. The method for elimination of the revealed shortcomings and increase of firmness of block algorithms to attack by full search is offered.

Keywords: block algorithms, enciphering.

Введение. Блочный шифр – разновидность симметричного шифра. Блочный шифр обрабатывает открытый текст блоками по несколько байт за одну итерацию. Если исходный текст (или его остаток) меньше размера блока, перед шифрованием его дополняют (1).

Блочный шифр состоит из двух взаимосвязанных алгоритмов: алгоритм шифрования E и алгоритм дешифрования E−1. Входными данными служат блок размером n бит и k-битный ключ.

1. Выявление недостатков блочных шифров.

Размер блока n – это фиксированный (2) параметр блочного шифра, обычно равный 64 или 128 битам, хотя некоторые шифры допускают несколько различных значений.

Из предпосылки (1) сразу становится видно что блочные шифры обладают избыточностью. Из предпосылки (2) видно что злоумышленник заранее знает размер блока для начала криптоанализа.

Из этих утверждений можно сделать вывод о уязвимостях блочных шифров:

1. при дополнении блока открытого текста “не случайными значениями” злоумышленник имеет больше возможностей для анализа и взлома;
2. гораздо легче анализировать текст при знании размера блока - последовательно выбираются 8 (или 16) байт информации и проводится анализ.

2. Метод устранения выявленных недостатков.

От выявленных уязвимостей возможно избавится если производить шифрование блоков не фиксированного размера, а динамически формируемыми на каждой итерации шифрования, в зависимости от ключа.

Рассмотрим отношение длинны блока открытого текста к количеству вариантов размера блока. В качестве алгоритма с фиксированным размером блока выберем DES алгоритм. В таблице представлены данные сравнения количества вариантов блоков в соответствии с размером входных данных.

Таблица 1

Размер блока данных в байтах	Колличество вариантов для блока фиксированной длинны	Колличество вариантов для блока переменной длинны	Варианты размеров блока переменной длинны
1	1	1	1
2	1	2	2 1,1
3	1	4	3 2,1 1,2 1,1,1
4	1	8	4 3,1 1,3 2,2 2,1,1 1,2,1 1,1,2 1,1,1,1
5	1	16	5 4,1 1,4 3,1,1 1,3,1 1,1,3 3,2 2,3 2,2,1 2,1,2 1,2,2 2,1,1,1 1,2,1,1 1,1,2,1 1,1,1,2 1,1,1,1,1

При продолжении таблицы можно увидеть тенденция роста количество вариантов размера блока переменной длинны по формуле $y = x^{N-1}$ (3).

Исходя из (3) видно что для блока из 64 бит (8 байт) количество вариантов будет составлять $2^{8-1} = 2^7 = 128$ вариантов. Соответственно для блока из 128 бит (16 байт)—32768 вариантов.

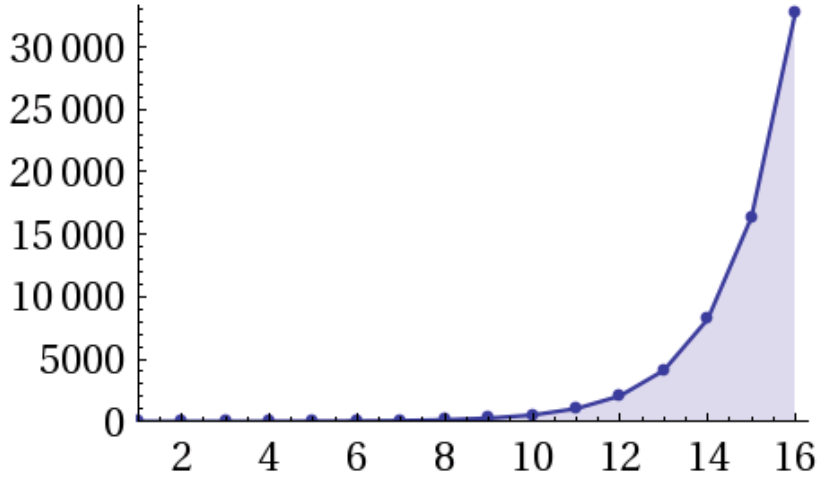

Рис. 1. График роста количества вариантов при увеличении размера блока разбиения

3. Доказательство повышенной стойкости алгоритма.

Количество вариантов начального фиксированного блока из 8 байт – $256^8 = 1.845*10^{19}$. Если в алгоритме шифрования используется ключ длинны 8 байт (латинские буквы + цифры) - тогда количество вариантов результирующего блока – $1.281*10^{14}$.

То есть при полном переборе ключей со скоростью 10^9 ключей в секунду для подбора ключа потребуется максимум 1,5 дня.

Большая проблема заключается в том что ротация ключей происходит между блоками, то есть для каждого блока из 8 байт используется 1 ключ.

При использовании предложенного подхода - количество ротаций ключа возрастет и для блока из 8 байт будет использоваться от 1 до 8 ключей.

Сравним стандартный алгоритм разбиения блока и предложенный.

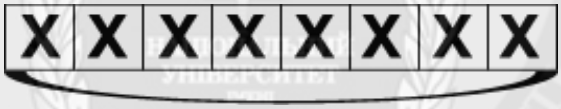

Рис. 2. Стандартный блок фиксированного размера (8 байт)

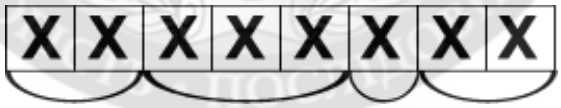

Рис. 3. 8 байт разбиты на 4 блока (2–3–1–2 байта соответственно)

Рассмотрим количество вариантов для полного перебора. На рис. 2 используется 1 ключ для шифрования всего блока. То есть для выявления ключа необходимо взять 8 байт шифрованного текста и сделать максимум X^8 попыток дешифровки.

Каждый символ X в ячейке – символ из 256 вариантов. Значит для дешифровки рис. 2 потребуется $256^8 = 1.845 * 10^{19}$ попыток.

Взлом рис. 3 потребует $256^2 * 256^3 * 256^1 * 256^2 = 256^8$ попыток. На первый взгляд сложность рис. 2 и рис. 3 одинаковая. Но это только если известно разбиение (2–3–1–2). Разбиение может быть известно только при знании ключа. Значит при не известном разбиении количество вариантов возрастет еще на количество вариантов разбиения (3) – $256^8 * 128 = 236.118 * 10^{19}$.

Выводы. В статье рассмотрена структура блочных алгоритмов шифрования. Были выявлены их уязвимости и слабые места. Предложен метод для устранения выявленных недостатков и повышения стойкости блочных алгоритмов к атаке полным перебором.

Из недостатков предложенного метода можно выявить невозможность либо крайнюю затруднительность применения его к существующим алгоритмам блочного шифрования.

ЛИТЕРАТУРА:

1. Анин Б. Ю. Защита компьютерной информации. − СПб.: БХВ Петербург, 2000.
2. Винокуров А.Ю. Как устроен блочный шифр?, Рукопись, 1995.
3. Девянин П.Н., Михальский О.О., Правиков Д.И. Теоретические основы компьютерной безопасности. − М., 2000.
4. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: − СПб ГИТМО (ТУ), 2002.
5. Кузнецов Г.В. та інші. Математичні основи криптографії: Навч. посібник. Дніпропетровськ: Національний гірничий університет, 2004. − Ч.1.
6. Петров А.А. Компьютерная безопасность: криптографические методы защиты. − М., 2000
7. Фергюсон Н., Шнаер Б. Практическая криптография. − М.: Вильямс, 2005. − 424 с.
8. Харин Ю.С. Математические основы криптологии: Учеб. Пособие. − Минск: БГУ, 1999. − 319 с.
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. − М., 2012

Рецензент: д.т.н., проф. Лєнков С.В.