УДК 004.056.55

КОНСТАНТЫ ДЛЯ АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ ЗАДАЧИ РАЗМЕЩЕНИЯ

Димитриев Александр Петрович

канд. тех. наук
Чувашский государственный университет им. И.Н. Ульянова, Чебоксары
author@apriori-journal.ru

Аннотация. Излагаются вопросы, касающиеся разработанной криптографической системы. Криптографическая система основана на вычислении хэш-функции, получаемой при решении задачи размещения. Цель работы – рассмотрение трех используемых таблиц констант, которые в принципе можно частично модифицировать на усмотрение программиста.

Ключевые слова: криптографическая система; шифрование; подстановочная последовательность; алгоритм.

CONSTANTS FOR THE ENCRYPTION ALGORITHM ON THE BASIS OF LOCATION PROBLEM

Dimitriev Alexander Petrivich

candidate of engineering
Chuvash State University named after I.N. Ulyanov, Cheboksary

Abstract. Outlines issues relating to developed a cryptographic system. The cryptographic system is based on the calculation of the hash function obtained by solving the location problem. The purpose of this paper is consideration of three used tables of constants, which in principle can be partially modified at the discretion of the programmer.

Key words: cryptographic system; cryptography; wildcard sequence; algorithm.

Введение

В настоящее время в мире активно ведутся исследования по информационной безопасности. В открытом доступе в Интернете существуют сотни статей на эту тему только на русском языке. Достаточно сделать соответствующие запросы на сайтах научной электронной библиотеки или ряда электронных изданий по информационным технологиям, чтобы в этом убедиться. Одним из ключевых аспектов защиты информации является шифрование [1].

Целью данной работы является представление таблиц констант для разработанного алгоритма шифрования, образующего первую часть криптографической системы.

Основополагающая идея данной криптографической системы выдвинута в итоговом отчете по гранту Российского фонда фундаментальных исследований 08-07-97003-р_поволжье_а «Разработка чувашско-русского автоматизированного переводчика на основе программно-концептуальной технологии создания переводчиков для неродственных языков». Криптографическая система основана на вычислении хэш-функции, получаемой при решении задачи размещения.

Алгоритм шифрования

В одном из пунктов алгоритма производится чтение блока из входного файла в *ms* и увеличение на 1 переменной «№ текущего блока». Далее скремблирование (чтобы избежать одинаковых выходных сочетаний символов на местах одинаковых входных) следующим образом. Для нечетных байтов массива *ms* выполнить для операцию «исключающее или» с числом 170, а для четных сначала поменять местами старшие и младшие 4 бита, затем выполнить операцию «исключающее или» (*xor*) с числом 15. Выполнить операции «исключающее или» (*xor*) с байтами массива *ms* согласно табл. 3. Следующие действия выполняются точно в последовательности, задаваемой табл. 1. При этом каждый раз с бай-

том-операндом в конце производится операция «исключающее или» с числом «номер текущего блока, взятый по модулю 253». Необходимо отметить, что в зависимости от программной реализации данные константы могут быть заменены на другие по некоторым правилам. Например, можно изменять количество циклических сдвигов в ту или иную сторону (целые числа в пределах от 1 до 4). Можно менять местами номера байтов в массиве *ms* как операнда. Важно, чтобы были задействованы почти все комбинации номеров элемента массива ms как источника и бита элемента как источника, эти комбинации можно менять местами. Так, в табл. 1 не задействована комбинация только 3-8.

Таблица 1

Последовательность действий по скремблированию

№	№ элемента массива *ms* как источника	№ бита элемента как источника	№ байта в массиве *ms* как операнда	Число циклических сдвигов байта (см. столбец 3) влево (при бите = 1)	Число циклических сдвигов байта (см. столбец 3) вправо (при бите = 0)
1.	1	1	4	1	1
2.	1	2	5	2	2
3.	1	3	6	3	3
4.	1	4	7	4	2
5.	3	7	8	1	1
6.	1	5	9	2	2
7.	1	6	10	3	3
8.	1	7	11	3	1
9.	1	8	12	2	4
10.	2	8	13	2	4
11.	2	7	14	4	2
12.	2	6	15	3	3
13.	2	5	16	4	1
14.	2	4	17	1	4
15.	2	3	18	2	3
16.	2	2	19	3	2
17.	2	1	20	4	3
18.	3	1	21	3	4
19.	3	2	22	2	4
20.	3	3	23	1	4
21.	3	4	24	3	1
22.	3	5	1	2	1
23.	3	6	2	3	1

В другом пункте алгоритма для каждого элемента выходного вектора перенумерации, в зависимости от хранимого в нем номера, выполняются циклические сдвиги по табл. 2.

Таблица 2

Параметры циклических сдвигов

№ из вектора	Номер координаты	Значение координаты	Индекс в массиве сдвигов
1.	1	1	1
2.	3	15	24
3.	3	10	20
4.	2	1	2
5.	3	1	3
6.	1	2	4
7.	3	13	23
8.	3	9	19
9.	2	2	5
10.	3	2	6
11.	1	3	7
12.	3	12	22
13.	3	8	18
14.	2	3	8
15.	3	3	9
16.	1	4	10
17.	3	11	21
18.	2	4	11
19.	3	4	12
20.	2	5	13
21.	3	5	14
22.	2	6	15
23.	3	6	16
24.	3	7	17

Следует заметить, что в зависимости от программной реализации приведенные константы могут быть заменены на другие, в соответствии с некоторым правилом. Например, можно менять местами индексы в массиве сдвигов. Можно изменить последовательность строк в таблице, от этого изменится результат. Можно менять местами пары «номер координаты – значение координаты». Можно вместо одного из значений координаты при номере координаты, равном 3, использовать число 14.

Еще в одном из пунктов, ближе к концу, для остатка входного файла, меньшего размера блока, выполняется поэлементная операция *XOR*

со строкой «*Russia Cheboxary ChuvGU*.». Это надо, чтобы, если все последние символы одинаковы, на глаз невозможно было это заметить в зашифрованном файле. Результат обозначен *ms2*.

Таблица 3

№ в *ms*	*XOR*	№ в *ms*	*XOR*	№ в *ms*	*XOR*	№ в *ms*	*XOR*
1	3	2	253	3	17	4	10
5	100	6	16	7	200	8	201
9	154	10	5	11	80	12	132
13	9	14	88	15	116	16	95
17	195	18	11	19	255	20	6
21	79	23	46	24	179	–	–

Основополагающий принцип данной криптографической системы развит в [2]. Разработан комплекс программ[1] для ЭВМ, в котором данный принцип использован для шифрования базы данных автоматизированного переводчика. К основным работам автора по машинному переводу относятся [2-4]. Итак, можно считать, что автоматизированный перевод является одной из востребованных областей применения такой сферы деятельности, как криптография.

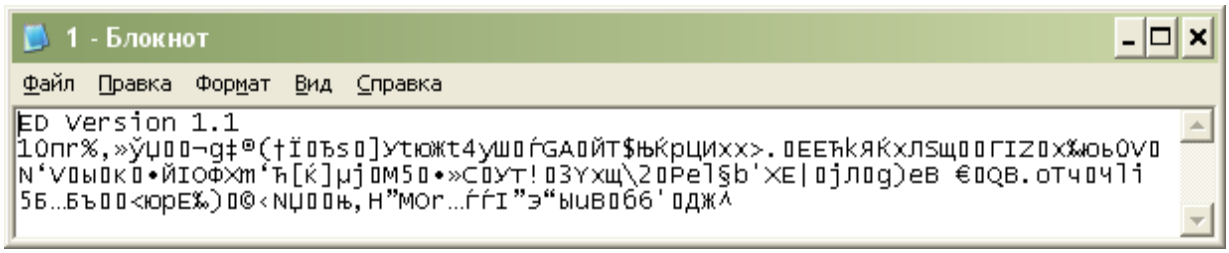
Результаты работы комплекса программ

Результаты работы комплекса программ можно представить в виде копий экрана (рис. 1).

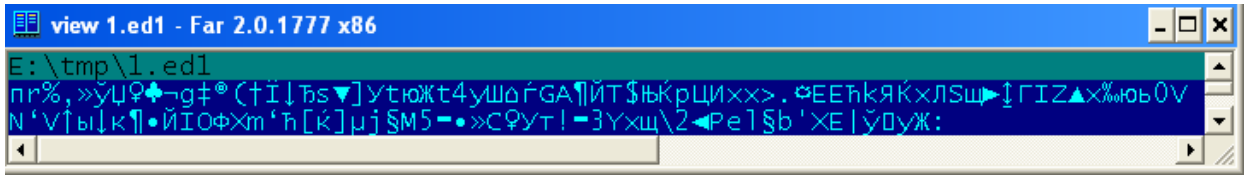
На рис. 1, а) представлен результат шифрования файла, содержащего 187 байт, из которых первые 181 – пробелы, а последние шесть – "123456". Для шифрования использован пароль, применяемый программой по умолчанию "123". Вначале виден заголовок. Необходимо иметь в виду, что заголовок представляет собой известные данные, если далее

[1] *Желтов П.В., Желтов В.П., Димитриев А.П. Автоматизированный чувашско-русский переводчик. Свидетельство № 2013618544 от 11 сентября 2013 г.*

все будет дополнительно шифроваться, например, архиватором W*inRar*. Такие известные данные могут послужить промежуточной ступенью при раскрытии шифра, поэтому разработана также версия программы, не формирующая заголовок. Результат ее работы представлен на рис. 1, б). В этом случае целевое сообщение для взлома результатов шифрования *WinRar*-ом не привязано к характерным наборам символов, что значительно затрудняет задачу злоумышленнику.



а)



б)

Рис. 1. Зашифрованный файл

Заключение

Алгоритмы криптографической системы реализованы в виде комплекса программ, успешно прошедшего тестирование. Программный комплекс шифрует компьютерные файлы с пользовательским паролем и расшифровывает ранее зашифрованные файлы. Программный комплекс в настоящее время реализован в качестве версии 1.1, которая отличается от версии 1.0 наличием скремблирования. Кроме того, устранена ошибка, заключавшаяся в том, что при определенных длинах файлов добавлялся лишний последний символ файла.

Список использованных источников

1. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. СПб. и др.: Питер, 2008. 668 с.
2. Димитриев А.П. Модели и алгоритмы составления расписаний учебных занятий: Ч. II. Чебоксары, 2014. 160 с.
3. Димитриев А.П. База данных, применяемая в программе чувашско-русского перевода // Мироновские чтения: сб. ст. Вып. I. Чебоксары: Изд-во Чуваш. ун-та, 2011. С. 45-51.
4. Димитриев А.П. Модели и алгоритмы в системах автоматизированного перевода текста // Прикладная информатика. 2013. № 6 (48). С. 45-59.
5. Димитриев А.П. Разработка базы данных чувашских слов // Подготовка квалифицированных специалистов как основа устойчивого развития экономики в современных условиях: матер. Всерос. науч.-практ. конф., посвящ. 15-летию Канашского филиала. Чебоксары: Изд-во Чуваш. ун-та, 2009. С. 124-129.
6. Димитриев А.П. Чувашско-русский переводчик: программная реализация // Прикладная информатика. 2011. № 6 (36). С. 43-46.