УДК 004.056.55

РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМОВ КУБИКА РУБИКА

И.Е. ИВАНЕНКО
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается проектирование алгоритма шифрования на основе алгоритмов кубика Рубика. Приведён обобщённый алгоритм решения задачи.

Введение. Алгоритмы шифрования и дешифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом в них является условие, что передатчик и приемник заранее знают алгоритм шифрования, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

Алгоритм шифрования на основе кубика Рубика является шифром перестановки. Метод перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов, т.е. преобразования приводят к изменению только порядка следования символов исходного сообщения.

В 1991 г. В.М. Кузьмич предложил схему перестановки, основанной на кубике Рубика. Согласно этой схеме открытый текст записывается в ячейки граней куба по строкам. После осуществления заданного числа заданных поворотов слоев куба считывание шифртекста осуществляется по столбикам. Сложность дешифрования в этом случае определяется количеством ячеек на гранях куба и сложностью выполненных поворотов слоев. Перестановка, основанная на кубике Рубика, получила название объемной (многомерной) перестановки [1].

Данный алгоритм шифрования на основе алгоритма кубика Рубика был изменен для работы не с символами шифруемого текста, а с массивом байт, который получается путем преобразования шифруемого текста. Данный алгоритм является симметричным алгоритмом шифрования.

Алгоритм шифрования на основе алгоритма кубика Рубика работает с ключами шифрования различной длины. Для работы алгоритма могут быть использованы ключи 16 байт (128 бит), 32 байта (256 бит), 64 байта (512 бит), 128 байт (1024 бита) и 256 байт (2048 бит). Длина ключа определяет количество раундов, которое будет использовано для шифрования или дешифрования символов исходного сообщения.

Обобщенный алгоритм решения задачи.

Алгоритм шифрования включает в себя следующие этапы:

1. Для алгоритма генерируется или задается ключ шифрования необходимой длины.
2. Символов исходного сообщения преобразуются в массив байт.
3. Из полученного ключа генерируется массива раундовых ключей.
4. Массив данных разбивается на блоки по 6 байт (48 бит). Если данных недостаточно для формирования целого блока, то блок дополняется «0».
5. Каждый байт из блока данных заменяется на соответствующей ему из константной таблицы, представленной на рисунке 1.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Рисунок 1 – Константная таблица замен

6. Блок данных преобразуется в матрицу бит размером 6 на 8.
7. Полученная матрица перемешивается по алгоритму «кубика Рубика».
8. Полученная после перемешивания матрица складывается по модулю два с раундовым ключом.
9. Каждый блок сдвигается на 1 байт влево.

Раундовые ключи вырабатываются из ключа шифра K с помощью процедуры расширения ключа, в результате чего формируется массив раундовых ключей, из которого затем непосредственно выбирается необходимый раундовый ключ.

Каждый раундовый ключ имеет длину 128 бит (или 4 четырехбайтовых слова w_i, w_{i+1}, wi_{+2}, wi_{+3}, а длина в битах всех раундовых ключей равна 128 бит). Первые четыре слова w_i, w_{i+1}, wi_{+2}, wi_{+3} в ключевом массиве заполнены ключом шифра, из остальных выработанных 44 слов выбираются по 4 слова для ключа раунда. Выбор слов прост: первые четыре слова (они совпадают с ключом шифра) являются ключом с номером 0, следующие четыре слова w_4, w_5, w_6, w_7 – раундовым ключом для первого полного раунда и т.д.

Новые слова w_{i+4}, w_{i+5}, w_{i+6}, w_{i+7} следующего раундового ключа определяются из слов w_i, w_{i+1}, wi_{+2}, wi_{+3} предыдущего ключа на основе уравнений:

– $w_{i+5} = w_{i+4} \oplus w_{i+1}$;

– $w_{i+6} = w_{i+5} \oplus w_{i+2}$;

– $w_{i+7} = w_{i+6} \oplus w_{i+3}$.

Первое слово w_{i+4} в каждом раундовом ключе изменяется по- другому:

– $w_{i+4} = w_i \oplus g(w_{i+3})$.

Здесь действие функции g сводится к последовательному выполнению трех шагов, отображающих слово в слово:

1 Циклический сдвиг четырехбайтового слова влево на один байт.

2 Замена каждого байта слова, полученного на шаге 10, в соответствии с таблицей константных замен, используемой при шифровании.

3 Суммирование по mod 2 байтов, полученных на шаге 2, с раундовой постоянной $R_{con}[i]$ = (RC[i],0,0,0), несекретной и уникальной для каждого раундового ключа. Три самые правые байты этой константы – нулевые, а ненулевой левый байт меняется по известному закону рекурсии: RC[1] =1, RC [i] = 2 * RC[i-1], i = 1,2,...11.

Цель суммирования с раундовыми константами – разрушить любую симметрию, что может возникнуть на разных этапах разворачивания ключа и привести к появлению слабых ключей, как в алгоритме DES.

Работа алгоритма расширения ключа продемонстрирована на рисунке 2.

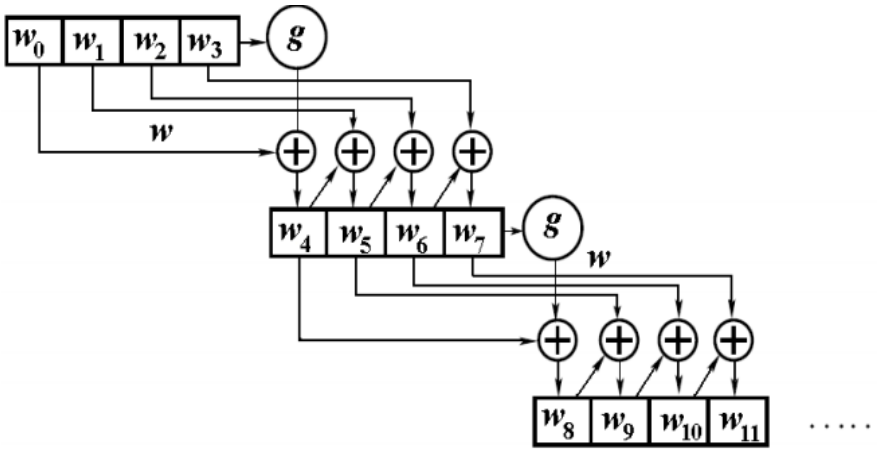

Рисунок 2. – Алгоритм расширения ключа

Заключение. В ходе данного исследования был спроектирован алгоритм шифрования на основе алгоритма кубика Рубика. При этом разработанный алгоритм оставляет возможность для доработки и введения дополнительных средств защиты.

ЛИТЕРАТУРА

1. Материал из StudFiles — файловый архив студентов. Шифры перестановки [Электронный ресурс]. – Режим доступа: https://studfiles.net/preview/5470123/page:8/. – Дата доступа: 20.09.2018.
2. Птицын, Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – М. : МГТУ им. Н.Э. Баумана, 2002. – 80 с.
3. Гатчин, Ю.А. Основы криптографических алгоритмов : учеб. пособие / Ю.А. Гатчин, А.Г. Коробейников. – СПб. : ГИТМО (ТУ), 2002. – 29 с.
4. Жданов, О.Н. Актуальные проблемы безопасности информационных технологий / О.Н. Жданов. – Красноярск : Сиб. гос. аэрокосмич. ун-т., 2009. – 144 с.