10. *Алексейчук А.Н.*, *Ковальчук Л.В.*, *Скрынник Е.В.*, *Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника. – 2008. – Т. 7. – № 3. – С. 203 – 209.

11. *Шевцов А.С.* Оцінки ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(15). – Київ, 2007. – С. 76 – 81.

12. *Олексійчук А.М.*, *Шевцов А.С.* Аналітична оцінка ймовірності білінійної апроксимації композиції перетворень заміни та зсуву за модулем 2^m // Вісник ДУІКТ. – 2008. – № 1. – С. 5 – 11.

13. *Алексейчук А.Н.*, *Ковальчук Л.В.*, *Скрыпник Л.В.*, *Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительного разностного, линейного и билинейного методов криптоанализа // Материалы Четвертой международной конференции по проблемам безопасности и противодействию терроризму. МГУ им. М.В. Ломоносова. 30 – 31 октября 2008 г. Том. 2. Материалы Седьмой общероссийской научной конференции "Математика и безопасность информационных технологий" (МаБИТ-2008). – М.: МЦНМО, 2009. – С. 15 – 20.

14. *Алексейчук А.Н.*, *Шевцов А.С.* Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров // Кибернетика и системный анализ. – 2010. – № 3 (в печати).

15. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

16. *Горбенко І.Д.*, *Долгов В.І.*, *Олійников Р.В.*, *Руженцев В.І.*, *Михайленко М.С.*, *Горбенко Ю.І.*, *Тоцький О.С.*, *Казьміна С.В.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 195 – 208.

17. *Шевцов А.С.* Оцінки ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(15). – Київ, 2007. – С. 76 – 81.

18. *Растовцев А.Г., Маховенко Е.Б.* Введение в теорию итерированых шифров. – Спб.: НПО "Мир и Семья", 2003. – 302 с.

Получены верхние оценки параметров, характеризующих способность раундовых функций шифров ГОСТ 28147-89 и "Калина" противостоять билинейному методу криптоанализа. Результаты проведенных исследований свидетельствуют в пользу предположения о практической стойкости указанных шифров к известным в настоящее время билинейным атакам.

Ключевые слова: криптоанализ, билинейный метод, шифры, противостояние криптоанализу.

Отримані верхні оцінки параметрів, що характеризують здатність раундових функцій шифрів ГОСТ 28147-89 та "Калина" протистояти білінійному методу криптоаналізу. Результати проведених досліджень свідчать на користь припущення про практичну стійкість вказаних шифрів відносно відомих в наступний час білінійних атак.

Ключові слова: критоаналіз, білінійний метод, шифри, протистояння криптоаналізу.

In the article upper bounds of parameters that define the capability of round functions of State Standard 28147-89 and "Kalyna" ciphers to resist a bilinear method of cryptoanalysis.

Key words: cryptoanalysis, bilinear method, ciphers, resistance to cryptoanalysis.

Поступила 11.01.2010

УДК 681.3.07

д.т.н., проф. Белецкий А.Я., Аксентий Е.А.
(Национальный авиационный университет)

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ ТИПА НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

Введение и постановка задачи

Современные методы защиты информации (*шифрование*) в компьютерных сетях представляют собой математические преобразования (алгоритмы), в которых сообщения рассматриваются как числа или алгебраические элементы в некотором пространстве [1]. С позиций теории сигналов и процессов *зашифрование* исходного (коррелированного,

избыточного, сжимаемого) текста состоит в его «*отбеливании*», т.е. обращении в некоррелированную последовательность символов (элементов) шифрограммы (практически несжимаемой) с плотностью распределения вероятностей элементов выходного алфавита максимально близкой к равномерной.

Криптостойкие системы могут быть построены путем многократного применения относительно простых криптографических преобразований (примитивов), в качестве которых К.Шенон предложил [2] использовать подстановки (Substitution) и перестановки (Permutation). Схемы, реализующие эти преобразования, называются *SP-сетями*. Часто используемыми криптографическими примитивами являются также преобразования типа циклический сдвиг (круговая прокрутка блоков), гаммирование и ряд других.

Типовая схема нелинейной подстановки (замены) байтов (используемая, в частности, в принятом в качестве международного стандарта шифрования *AES – Advanced Encryption Standard* [1]) построена из композиции таких двух преобразований данных, выполняемых независимо с каждым шифруемым байтом x:

1) получение обратного элемента x^{-1} относительно умножения в поле $GF(2^8)$, нулевой элемент '00' переходит сам в себя;

2) применением аффинного преобразования над $GF(2)$, определяемого следующим образом:

$$y = x^{-1} \otimes A \oplus \beta \ , \qquad (1)$$

где матрица

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

и аддитивный вектор

$$\beta = 11000110.$$

Следует отметить, что нелинейность преобразования (1) обеспечивается исключительно нелинейностью инверсии x^{-1} над полиномом $\varphi(x)$, в качестве которого в AES выбран полином

$$\varphi(x) = x^8 + x^4 + x^3 + x + 1 \ ,$$

являющийся *неприводимым полиномом* (многочленом) показателя 51.

В данной работе ставится задача разработки универсального программного стенда, обеспечивающего возможность оценки статистических свойств обобщенного криптографического примитива нелинейной подстановки:

$$y = (x \oplus \alpha)_{\varphi}^{-1} \otimes A \oplus \beta \ , \qquad (2)$$

в котором аддитивные компоненты α и β, а также невырожденная по mod 2 квадратная (0, 1)-матрица A и неприводимый полином φ, являются вариативными параметрами преобразования (2). Значения всех параметров преобразования, а именно, размеры векторов, порядок матрицы и степень неприводимого полинома (НП) выбраны равными восьми.

Базовый интерфейс программного комплекса. Интерфейс базового моделирующего комплекса изображен на рис. 1.

Система окон, показанных на рис.1, позволяет параметризовать характеристики неприводимого полинома φ и образующего элемента ω поля $GF(2^8)$ над выбранным НП, аддитивных составляющих α и β соотношения (2), а также матрицы преобразования, которая обозначена как матрица *G*. Резидентно в качестве матрицы *G* в программу ведена единичная матрица восьмого порядка. Окна < СКГ > и < из файла > дают возможность ввести в квадрат *G* матрицу, отвечающую произвольному составному коду Грея (СКГ) [3], или заполнить этот квадрат, считывая его из заранее подготовленного файла. В последнем случае следует предварительно нажать на кнопку активации, стоящую справа от окошка. Интерфейс допускает возможность полного или частичного ввода матрицы *G* в ручном режиме. Частичный режим ручного ввода означает корректировку элементов матрицы, ранее введенной из окон < СКГ > или < из файла >. Естественно, что при этом следует проверить матрицу на невырожденность. Такая проверка осуществляется нажатием на кнопку ПУСК. Если матрица невырождена, то в окошке «невырожденность» появляется знак +, в противном случае –.

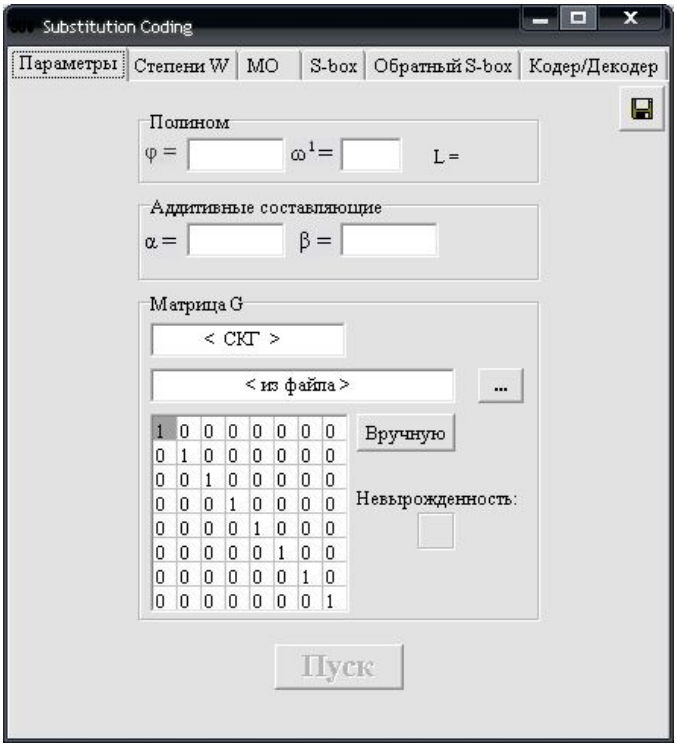

Рис.1. Базовый интерфейс моделирующего комплекса

После ввода значений φ и ω можно, нажав кнопку ПУСК, вычислить *порядок L образующего элемента* ω. Порядком образующего элемента ω называют то минимальное (но не равное нулю) значение L, которое обращает $\omega^L \bmod \varphi$ в единицу. Если окно ω оставить пустым, то программа вычислит и выведет значение минимального *примитивного* образующего элемента ω, порядок которого составляет величину $L = 255$.

В табл. 1 сведены показатели ряда образующих элементов для всех 30-ти неприводимых полиномов восьмой степени.

Как следует из табл. 1, только 16 из 30-ти НП восьмой степени являются *примитивными*, т.е. такими, для которых образующий элемент 10 обладает максимальным порядком, равным 255. Минимальный примитивный образующий элемент 255-го порядка 14-го неприводимого многочлена 101111011 равен 1001.

Выберем параметры преобразования (2) такими, которые указаны в окнах интерфейса на рис. 2.

Таким образом, согласно рис. 2, для последующих пояснений процесса преобразований по алгоритму (2) нами выбран пятый НП из табл. 1, которому отвечает примитивный образующий полином $\omega = 11$. В качестве матрицы преобразования A остановимся на матрице, соответствующей СКГ $G = 13$.

Таблица 1. Порядок образующих элементов двоичных неприводимых многочленов восьмой степени

Номер полинома	Неприводимый полином	Образующий элемент					
		10	11	100	101	110	111
1	100011011	51	255	51	255	255	85
2	100011101	255	51	255	51	255	85
3	100101011	255	85	255	85	255	255
4	100101101	255	17	255	17	255	255
5	100111001	17	255	17	255	255	255
6	100111111	85	255	85	255	255	255
7	101001101	255	255	255	255	85	255
8	101011111	255	255	255	255	85	255
9	101100011	255	255	255	255	85	85
10	101100101	255	255	255	255	85	85
11	101101001	255	255	255	255	15	5
12	101110001	255	85	255	85	255	255
13	101110111	85	255	85	255	255	255
14-1001	101111011	85	85	85	85	5	15
15	110000111	255	85	255	85	51	255
16	110001011	85	51	85	51	255	17
17	110001101	255	255	255	255	17	255
18	110011111	51	255	51	255	255	51
19	110100011	85	85	85	255	255	85
20	110101001	255	255	255	255	255	255
21	110110001	51	85	51	85	255	255
22	110111101	85	17	85	17	85	255
23	111000011	255	255	255	255	255	255
24	111001111	255	85	255	85	255	85
25	111010111	17	85	17	85	85	255
26	111011101	85	51	85	51	255	255
27	111100111	255	51	255	51	255	51
28	111110011	51	85	51	85	255	17
29	111110101	255	255	255	255	17	255
30	111111001	85	255	85	255	51	255

Степени примитивного образующего элемента. Полное множество ненулевых элементов поля $GF(2^n)$ над неприводимым полиномом φ может быть представлено в виде степеней ω^k примитивного элемента ω**,** вычисляемых по mod φ. Это означает, в частности, что ненулевые компоненты $GF(2^n)$ образуют циклическую абелеву группу относительно операции умножения.

Пусть $L = 2^n - 1$. Тогда имеет место соотношение

$$\omega^L \bmod \varphi \equiv 1. \qquad (3)$$

Рассмотрим методику вычисления степеней образующего элемента $\omega = 11$ по заданному модулю неприводимого многочлена $\varphi = 100111001$. Имеем $\omega^0 = 1$, $\omega^1 = 11$.

Последующие k – е степени, $k \geq 2$, элемента ω будем формировать по правилу

$$\omega^k = \omega^{k-1} \cdot \omega^1. \tag{4}$$

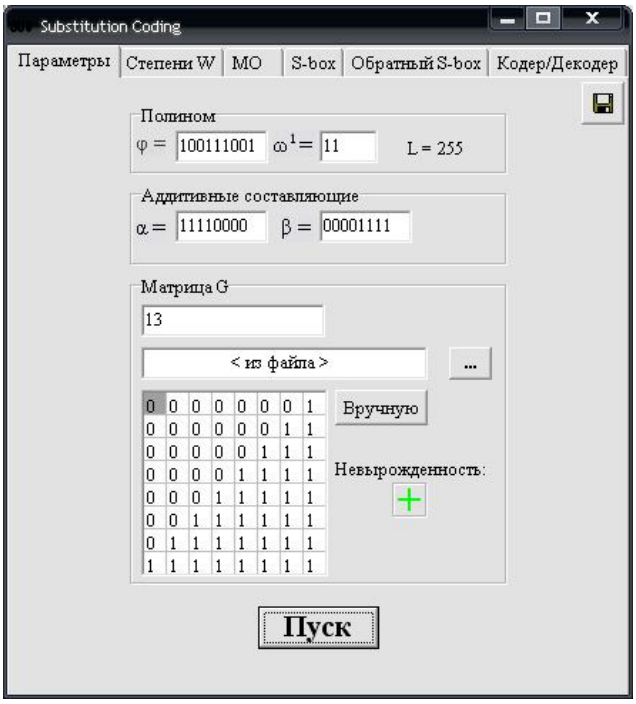

Рис. 2. Параметризация нелинейной подстановки (2)

Вычисления в соотношении (4) для $\omega = 11$ сводятся к поразрядному сложению по mod 2 многочлена ω^{k-1} и его копии, сдвинутой на один разряд влево. Следуя данному алгоритму, получим

$$\omega^2 = 101,$$
$$\omega^3 = 1111,$$
$$\omega^4 = 10001,$$
$$\omega^5 = 110011,$$
$$\omega^6 = 1010101,$$
$$\omega^7 = 11111111.$$

Восьмая степень (ω^8) примитивного образующего элемента $\omega = 11$, равная 100000001, оказывается девятиразрядной и, следовательно, должна быть приведена к остатку по модулю φ. В двоичной модулярной арифметике операция поразрядного вычитания, которая появляется на этапе вычисления остатков, эквивалентна операции поразрядного сложения. Таким образом,

$$\begin{aligned} (\omega^8) \bmod \varphi \;=\; (\omega^8) \oplus \varphi \;&=\; 100000001 \\ &\oplus \\ &\underline{100111001} \\ &\quad 111000 \;=\; \omega^8. \end{aligned} \tag{5}$$

Продолжая вычисления (2) степеней элемента ω по модулю выбранного НП φ, приходим (определяя, в случае необходимости, остатки по формуле (5)) к результатам, которые представлены на рис. 3.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	03	05	0F	11	33	55	FF	38	48	D8	51	F3	2C	74	9C
1	9D	9E	9B	94	85	B6	E3	1C	24	6C	B4	E5	16	3A	4E	D2
2	4F	D1	4A	DE	5B	ED	0E	12	36	5A	EE	0B	1D	27	69	BB
3	F4	25	6F	B1	EA	07	09	1B	2D	77	99	92	8F	A8	C1	7A
4	8E	AB	C4	75	9F	98	91	8A	A7	D0	49	DB	54	FC	3D	47
5	C9	62	A6	D3	4C	D4	45	CF	68	B8	F1	2A	7E	82	BF	F8
6	31	53	F5	26	6A	BE	FB	34	5C	E4	15	3F	41	C3	7C	84
7	B5	E6	13	35	5F	E1	1A	2E	72	96	83	BC	FD	3E	42	C6
8	73	95	86	B3	EC	0D	17	39	4B	DD	5E	E2	1F	21	63	A5
9	D6	43	C5	76	9A	97	80	B9	F2	2F	71	93	8C	AD	CE	6B
A	BD	FE	3B	4D	D7	40	C0	79	8B	A4	D5	46	CA	67	A9	C2
B	7F	81	BA	F7	20	60	A0	D9	52	F6	23	65	AF	C8	61	A3
C	DC	5D	E7	10	30	50	F0	29	7B	8D	AE	CB	64	AC	CD	6E
D	B2	EF	08	18	28	78	88	A1	DA	57	F9	32	56	FA	37	59
E	EB	04	0C	14	3C	44	CC	6D	B7	E0	19	2B	7D	87	B0	E9
F	02	06	0A	1E	22	66	AA	C7	70	90	89	A2	DF	58	E8	01

Рис. 3. Таблица степеней $\omega = 11$ по mod φ = 100111001

Таблица, показанная на рис. 3, выводится на экран монитора при нажатии на клавишу СТЕПЕНИ W. Степени k полинома ω (восьмиразрядные двоичные числа) представляются конкатенацией двух 16-ричных чисел k_1 и k_2, т.е. $k = k_2 \circ k_1$, где $\circ$ – знак конкатенации. Роль осей координат таблицы выполняют ее затененные верхняя строка и левый столбец. На оси абсцисс отложены значения младших четырех двоичных разрядов k_1, а на оси ординат - старшие разряды k_2 восьмибитных входных величин k. Компоненты k_1 и k_2, как и отвечающие им значения $\omega^k \bmod \varphi$, находящиеся на пересечении соответствующих столбцов и строк таблицы, представлены в 16-ричной системе счисления.

Мультипликативно обратные элементы поля $GF(2^8)$. Соотношение (3) приводит нас к достаточно простому алгоритму вычисления мультипликативно обратных (МО или просто – обратных или инверсных) величин (рис. 4). В самом деле, согласно (3), для восьмибитных элементов, образующих поле $GF(2^8)$,

$$(\omega^k \cdot \omega^l) \bmod \varphi = 1, \qquad \text{если только } k + l = 255. \tag{6}$$

Следовательно, ω^k и ω^l являются МО величинами (многочленами или двоичными векторами) при соблюдении условия, приведенного в (6). Указанные свойства элементов $GF(2^n)$ позволяют достаточно просто выполнять инверсии в полях Галуа. Алгоритм определения МО элементов поля сводится к выполнению таких двух этапов. На первом этапе следует провести инверсию последовательности степеней ω, расположив инверсный столбец справа от исходного столбца. Тогда в строках столбцов $k-$й степени элемента ω левого столбца будет отвечать $l-$я степень элемента ω правого столбца; при этом выполняются условия (6), т.е. соседние элементы становятся инверсными. На втором этапе

необходимо ранжировать векторы первого столбца, придав им естественную форму двоичной последовательности. Естественно, что синхронно с перестановками элементов первого столбца необходимо переставлять и элементы второго (инверсного) столбца.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	9C	E8	4E	58	74	AE	27	8D	2C	28	3A	83	57	DF
1	8F	A2	DA	21	16	97	14	96	1D	B6	DD	7B	B7	18	F3	35
2	DB	13	51	98	6D	CD	8C	08	0B	2D	D7	85	0A	29	4B	FB
3	92	6B	5B	89	F2	1F	A1	D1	C7	72	0C	82	E5	81	86	9A
4	F1	76	95	7C	B4	A4	4C	7F	AA	60	FA	2E	46	7E	04	59
5	99	22	8A	CE	F7	90	DE	0E	05	4F	88	32	B9	C1	E1	E2
6	49	AB	A9	E6	B1	9F	D8	A6	79	EF	93	31	CC	24	F4	AC
7	FF	BE	39	C6	06	AF	41	F0	EE	68	DC	1B	43	94	4D	47
8	E4	3D	3B	0D	D6	2B	3E	9B	5A	33	52	CF	26	09	A3	10
9	55	F6	30	6A	7D	42	17	15	23	50	3F	87	02	E9	B0	65
A	D0	36	11	8E	45	B5	67	D9	E7	62	48	61	6F	F5	07	75
B	9E	64	BB	FD	44	A5	19	1C	C0	5C	FC	B2	EC	F8	71	FE
C	B8	5D	C9	C5	C8	C3	73	38	C4	C2	D3	EA	6C	25	53	8B
D	A0	37	EB	CA	D5	D4	84	2A	66	A7	12	20	7A	1A	56	0F
E	E3	5E	5F	E0	80	3C	63	A8	03	9D	CB	D2	BC	F9	78	69
F	77	40	34	1E	6E	AD	91	54	BD	ED	4A	2F	BA	B3	BF	70

Рис. 4. Таблица MO элементов поля $GF(2^8)$ над НП $\varphi = 100111001$

Впрочем, второй этап преобразований можно исключить, непосредственно заполняя квадратную таблицу 16-ричными MO величинами.

Таблица, изображенная на рис. 4, выводится на экран монитора при нажатии на кнопку MO базового интерфейса. Также как и в таблице степеней ω (рис. 3) роль осей координат таблицы обратных элементов (рис. 4) выполняют ее затененные верхняя строка и левый столбец. На оси абсцисс отложены значения младших четырех двоичных разрядов x_1, а на оси ординат - старшие разряды x_2 восьмибитных входных величин $x = x_2 \circ x_1$.

Формирование S-бокса и обратного S-бокса. Блок нелинейной подстановки (S-box) реализует преобразование, заданное в общем случае соотношением (2). Проследим за последовательностью этапов вычисления операнда y, начиная с простейшего варианта, в котором аддитивные компоненты α и β выражения (2) равны нулю. Для такого варианта подстановки

$$y = x_{\varphi}^{-1} \otimes A, \tag{7}$$

где НП $\varphi = 100111001$, а матрица A восьмого порядка показана на рис. 2 и отвечает составному коду Грея $G = 13$.

Двухразрядные 16-ричные числа, соответствующие значениям x_{φ}^{-1}, сведены в таблицу на рис. 4. Умножим элементы этой таблицы, предварительно преобразованные в восьмибитные числа, на матрицу A. Результат преобразования (S-box), показан на рис. 5.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	FF	2E	1A	5C	13	34	59	B8	DE	27	18	68	81	B3	AD
1	A1	79	6D	F8	4F	B1	30	4E	D0	49	D2	94	B6	10	8A	C8
2	92	8F	F3	11	DB	DD	21	1F	9F	D8	B2	C1	60	E7	9C	95
3	71	9B	93	E1	75	AF	F9	F2	BD	74	20	7E	C5	FE	41	6E
4	F5	4B	CE	2B	36	39	23	AB	66	04	6A	58	43	54	3F	EC
5	EE	78	61	5D	B5	0E	52	5F	C0	A3	1E	77	E9	FD	FA	7A
6	E3	99	E6	45	F6	AE	12	46	EB	A5	8E	F7	22	38	35	26
7	AA	56	E8	42	40	A6	FC	0A	5A	1B	2D	90	83	31	DC	BC
8	3A	D7	97	DF	4D	98	57	91	6C	88	73	A2	47	E0	86	0F
9	CC	4A	08	64	D4	7C	B0	CF	87	0C	A8	BE	7F	E5	09	C4
A	0D	48	F0	5E	C3	C9	BB	ED	BA	7B	1C	FB	A4	CA	BF	CB
B	51	3B	96	D5	3C	C6	EF	2F	02	2C	2A	76	25	15	F4	55
C	16	D3	E2	C2	1D	82	8B	17	3D	7D	8D	65	24	C7	8C	9E
D	06	B7	9A	62	CD	32	3E	67	44	B9	70	07	6B	6F	4C	A0
E	85	53	AC	05	01	28	84	19	80	D1	9D	72	29	EA	14	E4
F	B4	03	37	50	5B	D9	F1	33	D6	DA	63	A7	69	89	A9	0B

Рис. 5. Таблица S-бокса, отвечающая преобразованию (7)

Рассмотрим пример перевода элементов таблицы из рис. 4 в соответствующие элементы таблицы на рис. 5. Выберем (на рис. 4) 16-ричный элемент 1C (равный двоичному вектору 00011100), который расположен на пересечении строки B (1011) и столбца 7 (0111). Проверим сначала, действительно ли операнд $y = 1\mathrm{C}$ является обратным (по mod $\varphi = 100111001$) входному операнду $x = \mathrm{B7}$ (равному двоичному вектору 10110111). Перемножив (в кольце вычетов по mod 2) двоичные векторы x и y, получим

$$
\begin{array}{rl}
 & 10110111 \quad = x \\
\otimes & \\
 & \underline{\quad\quad 11100} \quad = y \\
 & 1011011100 \\
\oplus & 10110111 \\
 & \underline{10110111\quad\quad} \\
 & 110000010100 \quad = z
\end{array}
$$

Приведем произведение $z = x \otimes y$ к остатку по mod $\varphi = 100111001$. Имеем

$$
\begin{array}{rl}
 & 110000010100 \\
\oplus & \\
 & \underline{100111001} \\
 & 10111011100 \\
\oplus & \\
 & \underline{100111001} \\
 & 100111000 \quad = w
\end{array}
$$

Векторы w и φ различаются значениями лишь в младших разрядах, а это означает что $z \bmod \varphi = 1$ и, следовательно, x и y - взаимно инверсные величины, что и требовалось подтвердить.

Перемножив, в соответствии с (7), байты x_{φ}^{-1}, являющиеся элементами таблицы из рис. 5, на матрицу преобразования

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \qquad (8)$$

приходим к S-боксу, показанному на рис. 5.

Проиллюстрируем приведенный алгоритм вычислений на примере. Выберем элемент x_{φ}^{-1} = 88 = 10001000, расположенный на пересечении пятой строки и 10-го столбца (т.е. столбца A) таблицы на рис. 4. Умножение вектора 10001000 на матрицу A эквивалентно поразрядному сложению по mod 2 первой (считая сверху вниз) и пятой строк матрицы (8). Имеем

$$\begin{array}{r} 00000001 \\ \oplus \\ \underline{00011111} \\ 00011110 \end{array} = 1E,$$

что совпадает со значением соответствующего (5A) элемента таблицы на рис. 5.

А теперь, сохраняя аддитивную компоненту β в преобразовании (2) нулевой, придадим некоторое (отличное от нуля) значение компоненте α, т.е. построим S-box

$$y = (x \oplus \alpha)_{\varphi}^{-1} \otimes A . \qquad (9)$$

Из сопоставления соотношений (7) и (9) следует, что в ячейку x (элемент таблицы) с координатами x_2 (номер строки) и x_1 (номер столбца) S-бокса на рис. 5 следует переписать содержимое ячейки $x' = x \oplus \alpha$ с координатами x_2' и x_1' того же S-бокса.

На рис. 6 показана таблица S-бокса (9) с компонентой $\alpha = 11110000$ такой же, которая выбрана для интерфейса, представленного на рис. 2. Вполне очевидно, что данное значение параметра α приводит к инверсии строк S-бокса (7), изображенного на рис. 5.

Переходим к обсуждению алгоритма составления S-бокса, осуществляющего преобразование по формуле (2) при условии, что компонента β отлична от нуля. Реализация алгоритма (2) достаточно проста. С этой целью необходимо все элементы S-бокса, соответствующие преобразованию (9), поразрядно просуммировать с байтом компоненты β.

Обратный S-box, используемый на этапе расшифрования (декодирования) криптограммы, также достаточно прост в реализации. В самом деле, пусть $x = x_2 \circ x_1$ есть некоторый байт, обратное значение которого (обозначим его через $y = y_2 \circ y_1$) расположено в таблице S-бокса с координатами x_2 и x_1. В обратном S-боксе координаты таблицы образуют оси $ó_2$ и y_1, отвечающие строкам и столбцам таблицы соответственно. На

пересечении строки $\acute{o}_2$ и столбца y_1 таблицы обратного S-бокса как раз и следует поместить 16-ричное представление байта x.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B4	03	37	50	5B	D9	F1	33	D6	DA	63	A7	69	89	A9	0B
1	85	53	AC	05	01	28	84	19	80	D1	9D	72	29	EA	14	E4
2	06	B7	9A	62	CD	32	3E	67	44	B9	70	07	6B	6F	4C	A0
3	16	D3	E2	C2	1D	82	8B	17	3D	7D	8D	65	24	C7	8C	9E
4	51	3B	96	D5	3C	C6	EF	2F	02	2C	2A	76	25	15	F4	55
5	0D	48	F0	5E	C3	C9	BB	ED	BA	7B	1C	FB	A4	CA	BF	CB
6	CC	4A	08	64	D4	7C	B0	CF	87	0C	A8	BE	7F	E5	09	C4
7	3A	D7	97	DF	4D	98	57	91	6C	88	73	A2	47	E0	86	0F
8	AA	56	E8	42	40	A6	FC	0A	5A	1B	2D	90	83	31	DC	BC
9	E3	99	E6	45	F6	AE	12	46	EB	A5	8E	F7	22	38	35	26
A	EE	78	61	5D	B5	0E	52	5F	C0	A3	1E	77	E9	FD	FA	7A
B	F5	4B	CE	2B	36	39	23	AB	66	04	6A	58	43	54	3F	EC
C	71	9B	93	E1	75	AF	F9	F2	BD	74	20	7E	C5	FE	41	6E
D	92	8F	F3	11	DB	DD	21	1F	9F	D8	B2	C1	60	E7	9C	95
E	A1	79	6D	F8	4F	B1	30	4E	D0	49	D2	94	B6	10	8A	C8
F	00	FF	2E	1A	5C	13	34	59	B8	DE	27	18	68	81	B3	AD

Рис. 6. Таблица S-бокса, отвечающая преобразованию (9)

Функция Кодер/Декодер. С помощью данной функции осуществляется зашифрование (кодирование) и расшифрование (декодирование) текстов с любым расширением. Под зашифрованием понимается замена (подстановка) каждого байта открытого текста байтом закрытого текста (шифрограммы). Расшифрование является процессом, обратным зашифрованию, т.е. восстановлением открытого текста из шифрограммы.

Качество зашифрования оценивается различными статистическими характеристиками [4]. Простейшей из них является энтропия сообщения (открытого текста или шифрограммы) H, рассчитываемая по формуле

$$H = -\sum_{i=0}^{L-1} p_i \cdot \log_2 p_i,$$

где L – число элементов (символов) входного или выходного алфавита, а p_i – частота i – го символа в тексте.

Примем за основу построения открытого текста и шифрограммы байт, образующий 256 двоичных символов. Множество 256 символов текста удобно отображать в виде гистограммы, преобразованной в таблицу, содержащую восемь столбцов и 32 строки. Частоту символа x_i, отвечающего индексу $i = 0$ $(x_0 = 00000000)$, будем размещать в левом верхнем углу таблицы, а частоту символа, отвечающего индексу $i = 255$ $(x_{255} = 11111111)$ – в правом нижнем углу таблицы. Для эксперимента был выбран русскоязычный текст объемом 208 Кбайт. Ниже в табл. 2 приведена гистограмма частот этого текста.

Таблица 2. Пример гистограммы открытого текста

00000000
00389000389000
00000000
00000000
427203528400002
44403513333625382
810574253
41218419000148
02140011
20003201
30103001
00000000
073241014
8120095418
617410813
12000000
00000000
00000000
00000000
00000000
00000000
02000000
00000000
00000000
3266329035118931871
203011736173288355202
41601213525341939
000038542157
11931234463683041465812105148425 33
10340142447877369460896311673038 77
56828008101694524731411604257 3
13545922827673416403104433 07

Энтропия входного текста, распределение частот символов которого представлено в табл. 2, составляет 4,64228. Зашифруем выбранный текст криптографическим примитивом (2) с параметрами преобразования, которые отображены на интерфейсе, показанным на рис.2. Распределение частот символов шифрограммы сведено в табл. 3.

Таблица 3. Гистограмма частот символов шифрограммы

003120043
042720000205682
390400452402767
382014110529631
110169000000
28030009117
00402600
0006040001484
465825331025380714240
0004003550
000730025730
10100000
3336202636813513003416
201923890003
93612100023440
001180003264
6010184051673038902
8000024030
01480426328408
7115773692904130
930330700000
000020119312
0020300041354
3546080010440121051
40000003877
00173183700
459241053000
1044104787010340
10100000
8505005350
80082880000183041
00002137101

Из сопоставления данных табл. 2 и 3 следует, что криптопримитив нелинейной подстановки осуществляет простую замену символов входного текста на символы выходного текста. Энтропия зашифрованного текста совпадает с энтропией исходного текста, что, впрочем, так и должно быть.

Заключение

Разработанная на языке C++ программа моделирования криптографических примитивов типа нелинейной подстановки (2) предоставляет возможность проводить статистические исследования S-боксов в широком диапазоне изменения параметров бокса. В качестве таких параметров выступают неприводимые полиномы восьмой степени φ, невырожденные (0, 1)-матрицы преобразования $\grave{A}$ и аддитивные компоненты преобразования α и β. Интерфейс S-бокса достаточно прост и удобен не только для выполнения научных исследований, но и с успехом может быть использован в учебных целях.

Список литературы

1. *Мао В*. Современная криптография. Теория и практика. – М.: «Вильямс», 2005. – 768с.
2. *Шеннон К.Е.* Работы по теории информации и кибернетики.– М.: ИЛ, 1963. – 829 с.
3. *Белецкий А.Я.* Преобразования Грея. / Белецкий А.Я., Белецкий А.А., Белецкий Е.А. Т. 1. Основы теории. – К.: Кн. Изд-во НАУ, 2007. – 412с.
4. Random Number Generation and Testing. http: www.csrc.nist.gov/rng/

Разработан на алгоритмическом языке C++ программный продукт, обеспечивающий возможность комплексной оценки статистических характеристик обобщенных криптографических примитивов типа нелинейной подстановки (S-боксов)

Ключевые слова: программный комплекс, криптографический примитив, нелинейная подстановка

Розроблений на алгоритмічній мові C++ програмний продукт, що забезпечує можливість комплексної оцінки статистичних характеристик узагальнених криптографічних примітивів типу нелінійної підстановки (S-боксів)

Ключові слова: програмний комплекс, криптографічний примітив, нелінійна підстановка

Developed at the algorithmic language C + + software product? that provides the possibility of a comprehensive assessment of the statistical characteristics of generalized cryptographic primitives such as nonlinear substitutions (S-boxes).

Keywords: software system, cryptographic primitive, non-linear substitution.

Поступила 10.02.2010