УДК 519.7

ФИНИТНЫЕ ФУНКЦИИ В АЛГОРИТМАХ КРИПТОГРАФИИ

А. В. Щуренко, В. Л. Леонтьев

Ульяновский государственный университет, г. Ульяновск, Россия

Предлагается применять ортогональные финитные функции (ОФФ) в алгоритмах криптографии в том случае, когда ОФФ не обладают свойством ортогональности. При этом последовательность сеточных наборов ОФФ, утративших свойство ортогональности, по-прежнему является базисом в пространстве Соболева. Потеря свойства ортогональности придает ОФФ новое свойство — множественность вариантов задания параметра ОФФ, что позволяет создавать дополнительные ключи в криптографических алгоритмах. Предложен алгоритм шифрования, основанный на использовании ОФФ, утративших свойство ортогональности. Использование ОФФ, не имеющих свойства ортогональности, в алгоритмах криптографии предложено В. Л. Леонтьевым. Реализация алгоритма выполнена в основном А. В. Щуренко.

Ключевые слова: *ОФФ, финитные функции, криптография, шифрование.*

DOI 10.17223/20710410/36/6

COMPACTLY SUPPORTED FUNCTIONS IN CRYPTOGRAPHY ALGORITHMS

A. V. Shchurenko, V. L. Leontiev

Ulyanovsk State University, Ulyanovsk, Russia

E-mail: tshurens@yandex.ru

In the paper, we propose a new symmetric block cipher based on the orthogonal finite functions (OFF) in the Sobolev's space. To encrypt a plaintext $a = a_1 a_2 \dots a_n$, we first convert a to a polynomial $a(x) = a_1 + a_2 x + \dots .. + a_n x^{n-1}$, then approximate $a(x)$ by a linear combination $F(x) = \sum\limits_{i=1}^{n} r_i f_i(x)$, where $f = (f_1, f_2, \dots, f_n)$ is an OFF-basis not having the orthogonality property, and finally compute the ciphertext $b = b_1 b_2 \dots b_n$, where $b_i = F(k_i)$ for some values k_i of x, $i = 1, 2, \dots, n$. The numbers $k_1, \dots, k_n$ and some parameters of functions in f form the key of the cipher. To decrypt the ciphertext b, we first, given $b_1, \dots, b_n$ and key parameters in f, compute the approximation coefficients $r_1, \dots, r_n$, next, given $k_1, \dots, k_n$, compute $x'_1, \dots, x'_n$ such that $a(x'_i) = r_i$ for $i = 1, 2, \dots, n$, then construct $a(x)$ by the Lagrange method, and finally convert $a(x)$ to a.

Keywords: *OFF, finite functions, cryptography, encryption.*

В работе предлагается алгоритм симметричного шифрования, основанный на применении ортогональных финитных функций. Теория ОФФ-базисов и её применение в алгоритмах численных методов изложены в [1 – 3].

Основная идея предлагаемого алгоритма заключается в аппроксимации многочлена, содержащего в себе исходное сообщение, с использованием функций ОФФ-базиса,

не обладающих свойствами ортогональности. После представления блока информации в виде многочлена проводится его аппроксимация с помощью ОФФ-базиса в выбранных узлах сетки, затем вычисляются значения ОФФ-аппроксимации с учётом произвольно заданного значения ключа, после чего результат шифрования представляется в виде блока ОФФ-аппроксимации. Информация о координатах точек, в которых проводилась аппроксимация, и о дополнительном ключе позволяет восстановить исходный многочлен и содержащееся в нём сообщение.

Операции по получению коэффициентов аппроксимации проводятся в кольце многочленов степени, не превосходящей n, над кольцом наименьших неотрицательных вычетов $\mathbb{Z}_N$, элементы которого образуют полную систему вычетов по модулю N. При этом n — чётное число, равное длине сообщения, а N — простое число. Сообщение длины, большей n, при шифровании следует разбить на блоки длины n.

Количество функций в используемой части ОФФ-базиса должно быть не меньше n. Для выполнения этого требования на равномерной сетке $x_1 < x_2 < \ldots < x_l$, $l \geqslant n$, с целыми неотрицательными x_i и шагом h задаётся набор $t = (t_1, t_2, \ldots, t_n)$, состоящий из n точек $t_i = (x_i, y_i)$, где все x_i, $i = 1, \ldots, n$, попарно различны. При этом все y_i принадлежат $\mathbb{Z}_N$, но их точные значения вычисляются уже в процессе шифрования. Далее задаётся соответствующий набор ОФФ $f = (f_1, f_2, \ldots, f_n)$. В качестве примера берутся ОФФ, являющиеся частным случаем [1, с. 11]. При использовании равномерной сетки с шагом h каждому узлу сетки x_i ставится в соответствие сеточная функция вида

$$f_i(x) = \begin{cases} (x - x_{i-1})/h, & x \in [x_{i-1}, x_{i-1} + h_1] \cup [x_{i-1} + h_2, x_i], \\ -\alpha + 2(\alpha h + h_1)(x_{i-1} + d_n - x)/(h(h_2 - h_1)), & x \in [x_{i-1} + h_1, x_{i-1} + d_n], \\ -\alpha + 2(\alpha h + h_2)(x - x_{i-1} - d_n)/(h(h_2 - h_1)), & x \in [x_{i-1} + d_n, x_{i-1} + h_2], \\ (x_{i+1} - x)/h, & x \in [x_i, x_i + h_1] \cup [x_i + h_2, x_{i+1}], \\ \beta + 2(\beta h + h_1 - h)(x - x_i - d_n)/(h(h_2 - h_1)), & x \in [x_i + h_1, x_i + d_n], \\ \beta + 2(\beta h + h_2 - h)(x_i + d_n - x)/(h(h_2 - h_1)), & x \in [x_i + d_n, x_i + h_2], \\ 0, & x \notin [x_{i-1}, x_{i+1}], \end{cases} \quad (1)$$

где $d_n = (h_1 + h_2)/2$; $h_1 = H_1 h$; $h_2 = H_2 h$; $0 \leqslant h_1 < h_2 \leqslant h$; H_1, H_2, α, β — некоторые константы; $\alpha > 0$, $\beta > 1$. Каждая f_i представляет собой сумму B-сплайна первой степени с конечным носителем $[x_{i-1}, x_{i+1}]$ и двух B-сплайнов первой степени, взятых с разными знаками, с более компактными по сравнению с $[x_{i-1}, x_{i+1}]$ конечными носителями. За счёт двух дополнительных B-сплайнов и с помощью выбора значений α, β, h_1, h_2 достигается выполнение условий ортогональности: $(f_i, f_j) = 0$ для всех $i \neq j$. Функции $f_i(x)$, $i = 1, \ldots, n$, линейно независимы, а их аппроксимирующие свойства представлены следующей теоремой.

Теорема 1 [1]. Если $u(x) \in W_2^1(\mathbb{R})$ и $H_1 + H_2 = 1$ ($h_1 + h_2 = h$), а $\alpha = \beta - 1$, то существует функция $u^h = \sum\limits_{i=1}^{n} \alpha_i f_i \in M_n$ (α_i — некоторые постоянные), такая, что

$$||u - u^h||_{\mathbb{L}_2(\mathbb{R})} \leqslant ch||u||_{W_2^1(\mathbb{R})}, \quad \sum_{i=1}^{n} |a_i|^2 \leqslant c_1 ||u||^2_{\mathbb{L}_2(\mathbb{R})},$$

где M_n — линейная оболочка $f_i(x)$; постоянные c и c_1 не зависят от u и h; W_2^l — функциональные пространства Соболева; $L_2 = W_2^0$.

Основная идея алгоритма состоит в том, чтобы, отказавшись от выполнения условия [1] ортогональности финитных функций, имеющего, например, в случае $h_1 = 0$, $h_2 = h$ вид

$$4\alpha\beta + \alpha - \beta = 0,$$

подбирать ОФФ, исходя только из условия $\alpha = \beta - 1$ теоремы. При этом числовое значение параметра β может быть любым вещественным числом, большим единицы, что является основой дополнительного шага шифрования исходного сообщения, связанного не только с деталями алгоритма шифрования, но и с дополнительным произвольно задаваемым значением параметра β. В общем случае значения β могут быть разными на различных участках выбранной сетки с узлами x_i, что порождает множество дополнительных ключей и поэтому значительно повышает уровень защищённости передаваемого сообщения. Отказ от ортогональности ОФФ значительно расширяет область применения ОФФ, которые, не обладая уже свойством ортогональности, представляют собой особую часть исходного множества ОФФ. Функции (1) в случае $h_1 = 0, h_2 = h$ принимают следующий вид:

$$f_i(x) = \begin{cases} 2\alpha(x_{i-1} - x)/h, & x \in [x_{i-1}, x_{i-1} + h/2], \\ 2(\alpha+1)(x - x_i)/h + 1, & x \in [x_{i-1} + h/2, x_i], \\ 2(\beta-1)(x - x_i)/h + 1, & x \in [x_i, x_i + h/2], \\ 2\beta(x_{i+1} - x)/h, & x \in [x_i + h/2, x_{i+1}], \\ 0, & x \notin [x_{i-1}, x_{i+1}]. \end{cases} \tag{2}$$

Пусть A — множество всех открытых текстов; K — множество выбранных случайным образом векторов k; B — множество всех шифртекстов. Алфавитом A является множество $\mathbb{Z}_L$ $(1 < L \leqslant N)$, алфавитом K — множество $\mathbb{Z}_{x_l+1}$, алфавитом B — множество целых чисел от $(-\lfloor \beta L \rceil - 1)$ до $(\lfloor \beta L \rceil + 1)$, $h \in \mathbb{Z}_{x_l}$, $\beta \in \mathbb{R}$ $(\beta > 1)$. Используемые здесь и далее усечённые квадратные скобки означают операцию округления до ближайшего целого числа.

Запишем исходное сообщение $a \in A$ в векторном виде:

$$a = (a_1, a_2, \ldots, a_n).$$

Пусть также выбран вектор $k \in K$, $k = (k_1, k_2, \ldots, k_n)$, и значения β, h и x_1, связанные с используемой сеткой. При этом все компоненты k попарно различны и для всех $i = 1, \ldots, n/2$ имеет место

$$\begin{cases} k_m \in [x_{j_i}, x_{j_{i+1}}], & m = 2i-1, 2i, \\ k_m \notin [x_{j_{i-1}}, x_{j_{i+2}}], & m \neq 2i-1, 2i, \end{cases}$$

где x_{j_i} и $x_{j_{i+1}}$ $(j_i, j_{i+1} \in \mathbb{Z}_l)$ — узлы сетки, между которыми лежат k_{2i-1} и k_{2i}. Другими словами, каждая компонента k_i является координатой на оси Ox точки, лежащей между двумя соседними узлами сетки x_{j_i} и $x_{j_{i+1}}$. Кроме того, если k_{2i-1} и k_{2i} лежат в $[x_{j_i}, x_{j_{i+1}}]$, то в данном интервале и в соседних $[x_{j_{i-1}}, x_{j_i}]$, $[x_{j_{i+1}}, x_{j_{i+2}}]$ не лежит более ни одна из компонент k_l, отличная от k_{2i-1} и k_{2i}.

Для большей определённости в предлагаемом алгоритме пусть $k_{2i} \in [x_{j_i} + h/2, x_{j_{i+1}}]$, $k_{2i-1} \in [x_{j_i}, x_{j_i} + h/2]$. Вместе с тем возможны другие варианты расположения точек с координатами k_{2i-1}, k_{2i} и связанные с этим другие варианты алгоритма.

При $k_{2i-1} \in [x_{j_i}, x_{j_i} + h/2]$, $k_{2i} \in [x_{j_i} + h/2, x_{j_{i+1}}]$, для исключения многозначности результатов расшифрования, пусть

$$(\beta - 1)(k_{2i-1} - x_{j_i}) > \beta(x_{j_{i+1}} - k_{2i}). \tag{3}$$

В силу ограничений, наложенных на элементы k, целесообразно проводить их выбор в три этапа. На первом шаге выбирается конкретный участок $[x_{j_i}, x_{j_{i+1}}]$, на втором шаге — k_{2i-1}, на третьем шаге — значение k_{2i} с учётом условия (3):

$$k_{2i} > x_{j_{i+1}} - \frac{(\beta - 1)(k_{2i-1} - x_{j_i})}{\beta}. \tag{4}$$

При невозможности выбора k_{2i} второй и третий шаги повторяются.

При этом следует отметить, что условия выбора элементов вектора k не препятствуют использованию для их генерации криптографически стойких генераторов случайных чисел. На всех трёх этапах, а также при генерации значений β, h и x_1 возможно использование таких алгоритмов, как алгоритм Блюм — Блюма — Шуба или криптографически стойкая хэш-функция. Это сводит задачу генерации ключей к передаче начальных значений генераторов, что упрощает задачу генерации, рассылки и хранения ключей без ущерба для криптостойкости алгоритма.

Обозначим x' вектор узлов сетки, используемых при аппроксимации многочлена. При этом $x'_{2i-1} = x_{j_i}$, $x'_{2i} = x_{j_{i+1}}$ $(i = 1, \ldots, n/2)$. В качестве f возьмем набор $f = (f_1, f_2, \ldots, f_n)$, где каждая f_i — ОФФ-функция, соответствующая узлу x'_i. Вектор (k, β, h, x_1) является ключом, вектор $b \in B$, $b = (b_1, b_2, \ldots, b_n)$, — шифртекстом.

Алгоритм шифрования состоит из следующих четырёх шагов.

Ш а г 1. Вектору a сопоставляется многочлен

$$a(x) = a_1 + a_2 x + a_3 x^2 + \ldots + a_n x^{n-1}. \tag{5}$$

Ш а г 2. Проводится аппроксимация многочлена $a(x)$ с помощью функций f_i. При этом аппроксимирующая функция $F(x)$ является суммой произведений ОФФ-функций f_i и соответствующих коэффициентов аппроксимации r_i:

$$F(x) = \sum_{i=1}^{n} r_i f_i(x).$$

Так как $f_j(x'_i) = \delta_{ij}$, где δ_{ij} — символ Кронекера $(i, j \in \{1, \ldots, n\})$, коэффициент i-й ОФФ-функции равен значению многочлена в точке с координатой x'_i. Значения этих коэффициентов — неотрицательные целые числа. Таким образом, значения вектора коэффициентов аппроксимации $r = (r_1, r_2, \ldots, r_n)$ находятся по формуле

$$r_i = a(x'_i) \bmod N.$$

Ш а г 3. Формируется вектор $b = (b_1, b_2, \ldots, b_n)$, где b_i равно значению аппроксимирующей функции в точке с координатой по оси Ox равной k_i, то есть $b_i = F(k_i)$, $i = 1, \ldots, n$.

Поскольку для всех $i \in \{1, \ldots, n/2\}$ точки k_{2i-1} и k_{2i} лежат между узлами x'_{2i-1} и x'_{2i}, значения аппроксимирующей функции в данных точках равны линейным комбинациям соответствующих значений f_{2i-1} и f_{2i} функций (2):

$$F(k_{2i-1}) = r_{2i-1} f_{2i-1}(k_{2i-1}) + r_{2i} f_{2i}(k_{2i-1}),$$
$$F(k_{2i}) = r_{2i-1} f_{2i-1}(k_{2i}) + r_{2i} f_{2i}(k_{2i}).$$

Согласно (2),

$$f_{2i-1}(k_{2i-1}) = 2(\beta-1)(k_{2i-1} - x'_{2i-1})/h + 1,$$
$$f_{2i}(k_{2i-1}) = 2\alpha(x'_{2i-1} - k_{2i-1})/h,$$
$$f_{2i-1}(k_{2i}) = 2\beta(x'_{2i} - k_{2i})/h,$$
$$f_{2i}(k_{2i}) = 2(\alpha+1)(k_{2i} - x'_{2i})/h + 1.$$

Таким образом,

$$\begin{aligned} F(k_{2i-1}) &= r_{2i-1}\left(\frac{2(\beta-1)(k_{2i-1}-x'_{2i-1})}{h}+1\right) + r_{2i}\frac{2(\beta-1)(x'_{2i-1}-k_{2i-1})}{h} = \\ &= \frac{2(\beta-1)(k_{2i-1}-x'_{2i-1})}{h}(r_{2i-1}-r_{2i}) + r_{2i-1}, \\ F(k_{2i}) &= r_{2i-1}\frac{2\beta(x'_{2i}-k_{2i})}{h} + r_{2i}\left(\frac{2\beta(k_{2i}-x'_{2i})}{h}+1\right) = \\ &= \frac{2\beta(x'_{2i}-k_{2i})}{h}(r_{2i-1}-r_{2i}) + r_{2i}. \end{aligned} \tag{6}$$

Ш а г 4. Вектор b, являющийся шифртекстом, записывается в виде

$$b = (\lfloor F(k_1)\rceil, \lfloor F(k_2)\rceil, \ldots, \lfloor F(k_n)\rceil).$$

Алгоритм расшифрования заключается в нахождении коэффициентов исходного многочлена $a(x)$ на основе вектора шифртекста b, известных значений k и β, а также параметров сетки h и x_1. Запишем шифртекст $b \in B$ в векторном виде

$$b = (b_1, b_2, \ldots, b_n),$$

где n — чётное натуральное число. Пусть известен вектор $k \in K$, $k = (k_1, k_2, \ldots, k_n)$, использованный при шифровании, а также значения β, h и x_1. При этом все k_i попарно различны и все k_{2i-1} и k_{2i} $(i = 1, \ldots, n/2)$ являются координатами на оси Ox точек, лежащих между двумя соседними узлами сетки x'_{2i-1} и x'_{2i}.

Ш а г 1. Вектору a исходного сообщения при шифровании был сопоставлен многочлен (5). При проведении аппроксимации $a(x)$ с помощью ОФФ-функций f в точках x' получился вектор коэффициентов аппроксимации $r = (r_1, r_2, \ldots, r_n)$, компоненты которого находятся по формуле

$$r_i = a(x_i) \bmod N.$$

Для нахождения значений вектора r при расшифровании значения вектора b берутся парами и первый элемент в паре складывается с элементом, обратным второму, то есть определяются значения $b'_i = b_{2i-1} - b_{2i}$ $(i = 1, \ldots, n/2)$:

$$b'_i = \left(\frac{2(\beta-1)(k_{2i-1}-x'_{2i-1})}{h} - \frac{2\beta(x'_{2i}-k_{2i})}{h} + 1\right)(r_{2i-1}-r_{2i}).$$

Далее находятся значения $(r_{2i-1} - r_{2i})$ по формуле

$$(r_{2i-1}-r_{2i}) = \left\lfloor \frac{b'_i}{2(\beta-1)(k_{2i-1}-x'_{2i-1})/h - 2\beta(x'_{2i}-k_{2i})/h + 1} \right\rceil.$$

Ш а г 2. Вычисляются значения вектора r. Для этого используется формула (6)

$$b_{2i} = \lfloor F(k_{2i}) \rceil = \left\lfloor \frac{2\beta(x'_{2i} - k_{2i})}{h}(r_{2i-1} - r_{2i}) \right\rceil + r_{2i},$$

где $i = 1, \ldots, n/2$. Отсюда следует, что

$$r_{2i} = b_{2i} - \left\lfloor \frac{2\beta(x'_{2i} - k_{2i})}{h}(r_{2i-1} - r_{2i}) \right\rceil, \quad r_{2i-1} = (r_{2i-1} - r_{2i}) + r_{2i}.$$

Ш а г 3. Вектор коэффициентов аппроксимации r теперь известен, по значениям вектора k определяются все x'_i ($k_{2i} \in [x'_{2i-1}, x'_{2i}]$, $i = 1, \ldots, n/2$). Решение системы уравнений

$$\begin{cases} a(x'_1) = r_1, \\ a(x'_2) = r_2, \\ \ldots \\ a(x'_n) = r_n \end{cases} \tag{7}$$

даёт коэффициенты многочлена $a(x)$. Найти целочисленное решение данной системы можно, применив сеточные полиномы Лагранжа для набора точек $t = ((x'_1, r_1), (x'_2, r_2), \ldots, (x'_n, r_n))$. Тогда $a(x)$ имеет вид

$$a(x) = \sum_{i=1}^{n} r_i l_i(x),$$

где $l_i(x) = \prod\limits_{j=1, j\neq i}^{n} \dfrac{x - x'_j}{x'_i - x'_j}$ есть многочлены Лагранжа, связанные с узлами x'_i сетки.

Ш а г 4. По значениям коэффициентов многочлена $a(x)$ строится вектор a, являющийся исходным сообщением.

Пример 1. Пусть дана равномерная сетка, определяемая значениями $h = 10$, $x_1 = 0$, и задано значение параметра ОФФ $\beta = 3{,}75$. При этом ОФФ-функции $f_i(x)$ имеют следующий вид:

$$\begin{cases} 5{,}5(x_{i-1} - x)/10, & x \in [x_{i-1}, x_{i-1} + 5], \\ 7{,}5(x - x_i)/10 + 1, & x \in [x_{i-1} + 5, x_i], \\ 5{,}5(x - x_i)/10 + 1, & x \in [x_i, x_i + 5], \\ 7{,}5(x_{i+1} - x)/10, & x \in [x_i + 5, x_{i+1}], \\ 0, & x \in [x_{i-1}, x_{i+1}]. \end{cases}$$

Пусть также $N = 257$, $L = 256$, $l = 26$. Тогда $x_l = 250$, алфавит $A = \mathbb{Z}_{256}$, алфавит $K = \mathbb{Z}_{251}$, алфавит B — множество целых чисел от -961 до 961.

Шифрование. Пусть исходное сообщение имеет вид $a = (20, 13, 2, 4, 5, 1)$, то есть $n = 6$. Пусть заданы значения вектора $k = (14, 19, 33, 39, 53, 58)$. При этом для всех компонент k справедливо следующее условие: если k_{2i-1} и k_{2i} лежат в $[x_{j_i}, x_{j_{i+1}}]$, то в данном интервале и в соседних интервалах $[x_{j_{i-1}}, x_{j_i}]$, $[x_{j_{i+1}}, x_{j_{i+2}}]$ не лежит более ни одна из компонент k, отличная от k_{2i-1} и k_{2i}.

Проверка условия (4)

$$19 > 20 - \frac{(3{,}75-1)(14-10)}{3{,}75} = 17{,}07,$$
$$39 > 40 - \frac{(3{,}75-1)(33-30)}{3{,}75} = 37{,}8,$$
$$58 > 60 - \frac{(3{,}75-1)(53-50)}{3{,}75} = 57{,}8$$

показывает его выполнение.

Случайные величины x_1 и h получили в результате генерации значения $x_1 = 0$, $h = 10$, поэтому вектор координат узлов сетки имеет вид $x' = (10, 20, 30, 40, 50, 60)$.

Ш а г 1. Вектору a сопоставляется многочлен $a(x) = 20+13x+2x^2+4x^3+5x^4+x^5$.

Ш а г 2. Проводится аппроксимация $a(x)$ с помощью ОФФ-функций f. При этом используется значение $\beta = 3{,}75$. В результате получается вектор коэффициентов аппроксимации $r = (r_1, r_2, r_3, r_4, r_5, r_6)$:

$$r_1 = a(10) = 154350 \equiv 150 \pmod{257},$$
$$r_2 = a(20) = 4033080 \equiv 236 \pmod{257},$$
$$r_3 = a(30) = 28460210 \equiv 30 \pmod{257},$$
$$r_4 = a(40) = 115459740 \equiv 177 \pmod{257},$$
$$r_5 = a(50) = 344255670 \equiv 58 \pmod{257},$$
$$r_6 = a(60) = 843272000 \equiv 2 \pmod{257}.$$

Получился вектор $r = (150, 236, 30, 177, 58, 2)$.

Ш а г 3. Строится вектор b:

$$b_1 = \lfloor F(k_1) \rceil = \left\lfloor \frac{2(3{,}75-1)(14-10)}{10}(150-236)+150 \right\rceil = -39,$$
$$b_2 = \lfloor F(k_2) \rceil = \left\lfloor \frac{2\cdot 3{,}75(20-19)}{10}(150-236)+236 \right\rceil = 172,$$
$$b_3 = \lfloor F(k_3) \rceil = \left\lfloor \frac{2(3{,}75-1)(33-30)}{10}(30-177)+30 \right\rceil = -213,$$
$$b_4 = \lfloor F(k_4) \rceil = \left\lfloor \frac{2\cdot 3{,}75(40-39)}{10}(30-177)+177 \right\rceil = 67,$$
$$b_5 = \lfloor F(k_5) \rceil = \left\lfloor \frac{2(3{,}75-1)(53-50)}{10}(58-2)+58 \right\rceil = 150,$$
$$b_6 = \lfloor F(k_6) \rceil = \left\lfloor \frac{2\cdot 3{,}75(60-58)}{10}(58-2)+2 \right\rceil = 86,$$
$$b = (-39, 172, -213, 67, 150, 86).$$

Вектор b является шифртекстом.

Расшифрование. При расшифровании шифртекста $b = (-39, 172, -213, 67, 150, 86)$ используются сформированные при шифровании векторы и величины $k = (14, 19, 33, 39, 53, 58)$, $\beta = 3{,}75$, $h = 10$, $x_1 = 0$, $x' = (10, 20, 30, 40, 50, 60)$, определяющие ключ.

Ш а г 1. Находятся значения выражений $(r_{2i-1} - r_{2i})$, $i = 1, \ldots, n/2$:

$$b'_1 = \left(\frac{2(\beta-1)(k_1 - x'_1)}{h} - \frac{2\beta(x'_2 - k_2)}{h} + 1\right)(r_1 - r_2) = -39 - 172 = -211,$$

$$r_1 - r_2 = \left\lfloor \frac{-211}{(2(\beta-1)(k_1 - x'_1)/h - 2\beta(x'_2 - k_2)/h + 1)} \right\rceil = \left\lfloor \frac{-211}{2{,}2 - 0{,}75 + 1} \right\rceil = -86,$$

$$b'_2 = \left(\frac{2(\beta-1)(k_3 - x'_3)}{h} - \frac{2\beta(x'_4 - k_4)}{h} + 1\right)(r_3 - r_4) = -213 - 67 = -280,$$

$$r_3 - r_4 = \left\lfloor \frac{-280}{2(\beta-1)(k_3 - x'_3)/h - 2\beta(x'_4 - k_4)/h + 1} \right\rceil = \left\lfloor \frac{-280}{1{,}65 - 0{,}75 + 1} \right\rceil = -147,$$

$$b'_3 = \left(\frac{2(\beta-1)(k_5 - x'_5)}{h} - \frac{2\beta(x'_6 - k_6)}{h} + 1\right)(r_5 - r_6) = 150 - 86 = 64,$$

$$r_5 - r_6 = \left\lfloor \frac{64}{2(\beta-1)(k_5 - x'_5)/h - 2\beta(x'_6 - k_6)/h + 1} \right\rceil = \left\lfloor \frac{64}{1{,}65 - 1{,}5 + 1} \right\rceil = 56.$$

Ш а г 2. Для определения значений компонент вектора r вычисляются

$$b_2 = \left\lfloor \frac{2 \cdot 3{,}75(20-19)}{10} \cdot (-86) \right\rceil + r_2 = -64 + r_2 = 172,$$

$$r_2 = 172 + 64 = 236, \quad r_1 = (r_1 - r_2) + r_2 = -86 + 236 = 150,$$

$$b_4 = \left\lfloor \frac{2 \cdot 3{,}75(40-39)}{10} \cdot (-147) \right\rceil + r_4 = -110 + r_4 = 67,$$

$$r_4 = 67 + 110 = 177, \quad r_3 = (r_3 - r_4) + r_4 = -147 + 177 = 30,$$

$$b_6 = \left\lfloor \frac{2 \cdot 3{,}75(60-58)}{10} \cdot 56 \right\rceil + r_6 = 84 + r_6 = 86,$$

$$r_6 = 86 - 84 = 2, \quad r_5 = (r_5 - r_6) + r_6 = 56 + 2 = 58.$$

Поэтому $r = (150, 236, 30, 177, 58, 2)$.

Ш а г 3. Решается система уравнений вида (7):

$$\begin{cases} a(10) = 150 \pmod{257}, \\ a(20) = 236 \pmod{257}, \\ a(30) = 30 \pmod{257}, \\ a(40) = 177 \pmod{257}, \\ a(50) = 58 \pmod{257}, \\ a(60) = 2 \pmod{257}. \end{cases}$$

В итоге получается многочлен $a(x) = 20 + 13x + 2x^2 + 4x^3 + 5x^4 + x^5$.

Ш а г 4. По значениям коэффициентов многочлена $a(x)$ строится вектор $a = (20, 13, 2, 4, 5, 1)$, являющийся исходным сообщением.

Замечание 1. Для обоснования выбора простого N запишем систему (7) в матричной форме:

$$\begin{pmatrix} 1 & x'_1 & \ldots & (x'_1)^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & x'_n & \ldots & (x'_n)^{n-1} \end{pmatrix} \begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix} = \begin{pmatrix} r_1 \\ \ldots \\ r_n \end{pmatrix}.$$

Если N простое и все точки x'_i, $i = 1, \ldots, n$, различны, то основная матрица системы невырожденная и, следовательно, система имеет единственное решение.

Замечание 2. В рассмотренном примере показано использование алгоритма в режиме простой замены, однако в практических реализациях, за исключением случаев шифрования коротких сообщений, целесообразно использование иных режимов. При этом разницу в объёмах блоков открытого текста и шифртекста можно компенсировать, заменяя в процессе шифрования очередной блок открытого текста x на результат обратимой функции $g(x)$, по объёму равный блоку шифртекста.

Поскольку алгоритм оперирует с блоками текста фиксированной длины n, уместно его сравнение с алгоритмами блочного шифрования. К достоинствам предложенного алгоритма относится динамическая длина ключа, что упрощает переход на версии алгоритма с большей длиной n блока текста. Более того, значения N и L также не фиксированы, что позволяет алгоритму шифрования на основе ОФФ оперировать с множествами A, K и B, имеющими алфавит любой длины, а также задавать сетки с любым максимальным значением x_l.

Параметр β может принимать любые вещественные значения больше единицы, однако в практических реализациях алгоритма целесообразно взять некоторую конечную область значений β, разбить её на интервалы, например длины $1/N$, и выбрать значения β, лежащие на концах данных интервалов. При этом поскольку число возможных значений β на каждом участке $[i, i+1]$, $i = 0, \ldots, N-1$, зависит от N, при увеличении N расширяется множество допустимых значений β. Значительно увеличивается преимущество алгоритма в стойкости шифрования при использовании любых вещественных значений β по сравнению с целыми значениями. Увеличение максимального значения β расширяет множество допустимых значений ключа, однако вместе с тем значительно возрастает объём шифртекста по сравнению с открытым текстом. В связи с этим в практических реализациях алгоритма рекомендуется ограничивать максимальное значение β, находя баланс между возрастающим объёмом шифртекста и количеством допустимых значений ключа.

Сравним алгоритм с поточным шифром гаммирования. При многократном использовании ключа существенно повышается стойкость шифрования в предложенном алгоритме по сравнению с шифром гаммирования к таким видам криптоанализа, как атаки на основе шифртекста, известного открытого текста, выбранного открытого текста и выбранного шифртекста. При шифровании гаммированием знание открытого текста и шифртекста позволяет определить точное значение гаммы, что исключает многократное использование одного и того же ключа. В случае шифрования предложенным методом знание двух сообщений a и b не позволяет однозначно подобрать параметры (k, β, h, x_1). Изменение любого из них, при соответствующих изменениях других параметров, приведёт к тому, что данному открытому тексту a будет соответствовать тот же шифртекст b.

Уровень сложности дешифрования в предложенном алгоритме характеризуется необходимостью перебора возможных значений параметров h и x_1 и решения со всеми возможными парами (h, x_1) уравнений (6) с неизвестными β, r_{2i-1} и r_{2i}, а также необходимостью решения системы (7).

Увеличение n приводит к увеличению мощности множества допустимых значений ключа, вместе с тем растёт сложность шифрования и расшифрования, поскольку максимальная степень многочлена (5), а также количество уравнений (7) зависят от n.

Пусть, например, $N = 65537$, $h = 4$, $n = 30$, $x_l = 65536$, а максимальное допустимое значение β равно 256. Пусть также $x_1 = 0$. Тогда сетка разбивается на $65536/(2h) = 8192$ различных участка, каждому из которых могут принадлежать две компоненты вектора k. С учётом условия (4), каждому участку $[x'_{2i-1}, x'_{2i+1}]$ могут соответствовать

16 допустимых значений пар (k_{2i}, k_{2i-1}). Общее число допустимых значений компонент вектора k в таком случае равно

$$|K| = A_{8192}^{15} \cdot 8 = \frac{8192!}{(8192-15)!} \cdot 8 \approx 3{,}2 \cdot 10^{63}.$$

Разобьём область допустимых значений β ($\beta > 1$) на интервалы длины $1/N$. Таким образом, для каждого возможного значения вектора k существует $255 \cdot 65536 - 1 = 16711679$ допустимых значений β.

Множество допустимых значений ключа содержит $3{,}2 \cdot 10^{63} \cdot 16711679 \approx 5{,}3 \cdot 10^{70}$ элементов, что даже при многократном использовании ключа делает абсурдными задачи полного перебора либо записи всех подобранных сочетаний (k, β, h, x_1) с целью вскрытия следующего шифртекста перебором лишь записанных заранее значений. При этом следует учесть, что в практических реализациях алгоритма возможно разделение области допустимых значений β на интервалы длины меньше $1/N$, а также нефиксированное значение x_1, что дополнительно расширяет множество допустимых значений ключа.

Вместе с тем при уменьшении n распределение символов шифртекста становится все более схожим с распределением символов открытого текста, что значительно упрощает задачу дешифрования без знания ключа.

В дальнейшем предполагается более подробное исследование стойкости предложенных алгоритмов к различным атакам в зависимости от выбранных параметров и ключа.

Методы использования базисов в криптографических алгоритмах развиваются и в других работах [4, 5], новизна предложенного здесь алгоритма шифрования заключается в использовании принципиально иных базисных функций — ОФФ, не обладающих свойством ортогональности.

ЛИТЕРАТУРА

1. *Леонтьев В. Л.* Ортогональные финитные функции и численные методы. Ульяновск: Изд-во УлГУ, 2003. 178 с.
2. *Леонтьев В. Л., Лукашенец Н. Ч.* Сеточные базисы ортогональных финитных функций // Журн. вычисл. матем. и матем. физ. 1999. Т. 39. № 7. С. 1158–1168.
3. *Леонтьев В. Л.* Ортогональные сплайны и вариационно-сеточный метод // Математическое моделирование. 2002. Т. 14. № 3. С. 117–127.
4. *Лукомский Д. С., Лукомский С. Ф.* Всплесковые базисы и криптография // Математика. Механика. 2011. № 13. С. 55–58.
5. *Левина А. Б.* Сплайн-вэйвлеты и их некоторые применения: дис. ... канд. физ.-мат. наук. СПб., 2009. 214 с.

REFERENCES

1. *Leont'ev V. L.* Ortogonal'nye finitnye funktsii i chislennye metody [Orthogonal finite functions and numerical methods]. Ul'yanovsk, UlSU Publ., 2003. 178 p. (in Russian)
2. *Leont'ev V. L., Lukashenets N. Ch.* Setochnye bazisy ortogonal'nykh finitnykh funktsiy [Grid bases of orthogonal compactly supported functions]. Zh. Vychisl. Mat. Mat. Fiz., 1999, vol. 39, no. 7, pp. 1158–1168. (in Russian)
3. *Leont'ev V. L.* Ortogonal'nye splayny i variatsionno-setochnyy metod [Orthogonal splines and variational-grid method]. Matem. Mod., 2002, vol. 14, no. 3, pp. 117–127. (in Russian)

4. *Lukomskiy D. S., Lukomskiy S. F.* Vspleskovye bazisy i kriptografiya [Splash bases and cryptography]. Matematika. Mekhanika, 2011, no. 13, pp. 55–58. (in Russian)
5. *Levina A. B.* Splayn-veyvlety i ikh nekotorye primeneniya [Spline-Wavelets and some their Applications]. PhD Thesis. SPb., 2009. 214 p. (in Russian)