В последние десятилетия криптография стала объектом интенсивного математического изучения. Появляется множество криптоалгоритмов, ученые проводят их исследования, выявляют слабые стороны, на смену одним алгоритмам приходят другие.

В данной статье предложен алгоритм симметрического шифрования, основанный на применении базисов ортогональных финитных функций (ОФФ-базисов). Подробнее про ОФФ-базисы и про применение ортогональных финитных функций в численных методах изложено в [2] и [3].

Основная идея алгоритма заключается в манипуляции коэффициентами, полученными при использовании ОФФ-базисов. Представив блок информации в виде многочлена, мы можем аппроксимировать его с помощью заданных ОФФ-базисов, после чего произвольным образом изменить коэффициенты аппроксимации, а результат снова представить в виде многочлена.

Все операции будем проводить в кольце $\mathbb{Z}[X]/(X^N - 1)$ усеченных многочленов степени, не превосходящей $N - 1$. В нашем случае $N = 257$. Пусть дан исходный текст $A = (a_1, a_2, \dots, a_n)$ и ключ $K = (k_1, k_2, \dots, k_n)$. Вектором $B = (b_1, b_2, \dots, b_n)$ обозначим шифртекст.

Прежде всего, представим вектор A в виде многочлена:

$$A(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}.$$

Количество векторов в ОФФ-базисе должно быть не меньше количества элементов в исходном тексте. Зададим набор из n точек $P = (p_1, p_2, \dots, p_n)$, в которых будем проводить аппроксимацию многочлена, и набор из n простейших базисных функций $F = (f_1, f_2, \dots, f_n)$, где каждая функция f_i равна единице в точке p_i, принимает ненулевые значения в небольшой окрестности p_i и равна нулю во всех остальных точках. Аппроксимируя $A(x)$ с помощью данных функций, получаем вектор коэффициентов аппроксимации $R = (r_1, r_2, \dots, r_n)$, где $r_i = A(x_i) \bmod N \quad \forall i = \overline{1, n}$.

Далее выполняем непосредственно операцию шифрования: получаем новый вектор коэффициентов аппроксимации $R^* = (r_1^*, r_2^*, \dots, r_n^*)$, где $r_i^* = (r_i + k_i)\ mod\ N \quad \forall i = \overline{1,n}$.

Последний шаг – получение новых коэффициентов B из вектора R^*. Фактически, нам нужно решить систему уравнений по модулю N:

$$\begin{pmatrix} b_1 + b_2 p_1 + \cdots + b_n p_1^{n-1} \\ b_1 + b_2 a_2^* + \cdots + b_n p_2^{n-1} \\ \vdots \\ b_1 + b_2 p_n + \cdots + b_n p_n^{n-1} \end{pmatrix} = \begin{pmatrix} r_1^* \\ r_2^* \\ r_3^* \\ r_4^* \end{pmatrix}.$$

Значения $p_1, \dots, p_n$ и $r_1^*, \dots, r_n^*$ нам известны. Переведем данную систему уравнений в матричную форму:

$$\begin{pmatrix} 1 & p_1 & \cdots & p_1^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & p_1 & \cdots & p_n^{n-1} \end{pmatrix} = \begin{pmatrix} r_1^* \\ \vdots \\ r_n^* \end{pmatrix}.$$

Приведя ее к верхнетреугольному виду, в нижней строке получим уравнение вида $bx \equiv r\ (mod\ N)$, а уравнения во всех остальных строках сводятся к нему.

Согласно [1], данное уравнение имеет решение тогда и только тогда, когда $(b, N) \mid r$. Если в качестве N взять простое число, как в нашем случае, такое уравнение гарантированно будет иметь решение. К тому же, в случае простого N решение будет только одно.

Процесс расшифровки полностью аналогичен. Аппроксимируем многочлен B, отнимаем от коэффициентов аппроксимации соответствующие элементы ключа, а на основе получившихся новых коэффициентов аппроксимации вычисляем коэффициенты исходного многочлена A.

Сообщение длины, большей N, при шифровке нужно разбить на блоки длиной N. При одинаковом ключе такие блоки, очевидно, шифруются одинаково, независимо от положения в тексте.

Список литературы

1. *Акритас А*. Основы компьютерной алгебры с приложениями: Пер. с англ. — М., Мир, 1994. — 544 с.
2. *Леонтьев В. Л.* О СВОЙСТВАХ ОРТОГОНАЛЬНЫХ ФИНИТНЫХ ФУНКЦИЙ И ОБ ИХ ИСПОЛЬЗОВАНИИ В АЛГОРИТМАХ ЧИСЛЕННЫХ МЕТОДОВ // Фундаментальные исследования . 2012. №11-3. С.696-699.
3. *Леонтьев В.Л.* Ортогональные финитные функции и численные методы — Ульяновск, УлГУ, 2003. — 181 с.