УДК 519.72

МОДИФИЦИРОВАННЫЙ МЕТОД В. СИЗОВА НА СЛУЧАЙ НЕПЕРИОДИЧЕСКОЙ НЕОГРАНИЧЕННОЙ ФУНКЦИИ

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

В статье рассматривается усовершенствованный алгоритм метода шифрования текстовых данных Владимира Сизова.

Введение. Шифрование— обратимое преобразование информации в целях сокрытия от неавторизированных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Защищенность данных пользователей в современном мире очень актуальна. Взять как самый простой пример - пароли от интернет-банкингов. Пароли не просто так даны, они необходимы для защиты. Но также необходимо защищать и свои текстовые данные.

Основная часть. В данной работе рассмотрим модифицированный метод В. Сизова на случай непериодической неограниченной функции. Функция представляет собой сумму дробно-степенных функций. Аргумент функции один и тот же, представляет собой аффинное преобразование порядкового номера шифруемого символа

$$Z(i) = (i + w_0)t + fi$$

где Z – аргумент функции;
i – порядковый номер в шифруемой фразе;
w0– параметр частотной модуляции или сдвиг порядковых номеров;
t – момент времени;
fi– начальная фаза.

За исключением порядкового номера i, все остальные параметры – параметры ключа действительные числа двойной точности.

Функция шифрования имеет вид

$$Y = [X + F] \bmod P. \tag{3}$$

Функция дешифрования имеет вид

$$X = [Y - F] \bmod P, \tag{4}$$

где
$$F(i, a_1, a_2, a_3, b_1, b_2, b_3, w_0, t, fi) =$$
$$= a_1(Z)^{b_1} + a_2(Z)^{b_2} + a_3(Z)^{b_3} = \tag{5}$$
$$= a_1((i + w_0)t + fi)^{b_1} + a_2((i + w_0)t + fi)^{b_2} + a_3((i + w_0)t + fi)^{b_3}.$$

Функция F имеет 9 ключей: a_1, a_2, a_3 – амплитуды, b_1, b_2, b_3 – показатели дробно-степенных функций, w_0 – параметр частоты модуляции, t – момент времени, fi – начальная фаза.

Корректность формулы шифрования (3) и дешифрования (4) обсуждались с заведующим кафедры высшей математики, доцентом, кандидатом физ.-мат. наук А.А. Козловым.

Алгоритм шифрования можно разделить на несколько шагов:

– Исходный текст заносится в символьный массив массив char str[m+1]. Порядковый номер каждого символа в ASCII [4] заносится в baza[i];

– Согласно алгоритму применяется формула Сизова

$baza2[i] = baza[i] + 0{,}5(double)$ (действ. 2-й точности);

– $baza1[i] = [baza2[i] + F(Z)] mod F$ (целая переменная).

Особенностью выработанного алгоритма является следующая модификация метода:

Если $baza1[i] < 0$, то baza1[i] =baza1[i]+p-1.

Шифрованный текст хранится в массиве чисел baza1[i]

Алгоритм дешифрования:

1. Извлекаем из массива baza1[i] целое число – шифрованный символ.
2. Образуем действительное число из значения baza1[i] по формуле s2=baza[i]+0,5 (действ. 2-й точности) (данная часть алгоритма совпадает с алгоритмом Сизова).
3. Вычисляем функцию Z(i) (действ.2-й точности).
4. Составляем разность: $s3 = [s2 - s1] mod F$, что соответствует массиву baza3[i] (целая переменная), так как $s2 = x + F(Z), s1 = F(Z)$, $s3 = x$ (целая переменная), s3 – целочисленный массив поскольку от действительной разности $s2 - s1$ взята целая часть, затем остаток по $mod F$.
5. Применяем модернизированный алгоритм Сизова:

Если $baza3[i] < 0$,то $baza3[i] = baza3[i] + p - 1$.

Получим векторный массив, в котором число элементов m (число символов сообщения) должно совпадать с исходным массивом baza[i].

6. На конечном этапе можно обратить порядковый номер каждого символа фразы по таблице ASCII в сам символ.

Исходя из вышеперечисленных вариантов можно сделать вывод, что каждый алгоритм имеет свои плюсы или минусы. Все вышеперечисленные алгоритмы были изучены и запрограммированы, но чтобы добиться надежного шифрования текстовых данных, необходимо привнести новизну в существующие алгоритмы. Таким образом был выбран метод шифрования Владимира Сизова. Но метод был усовершенствован апериодической неограниченной функцией, то есть обобщенным степенным рядом Фробениуса

Заключение. В ходе данного изучения метода шифрования был усовершенствован алгоритм шифрования по методу В. Сизова, что привело данный алгоритм к большей защищенности от несанкционированных атак.

ЛИТЕРАТУРА

1. Сизов, В.П. Криптографические алгоритмы на остнове тригонометрических функций [Электронный ресурс]. – URL: https://www.ruscrypto.ru/accocuation/archive/rc2005.html. - Дата доступа: 22.09.2019.
2. Каминский, Л.П. Информационные технологии / Л.П. Каминский, В.А. Степанов // Тригонометрическая криптография. – Красноярск : Сибирский федеральный университет, 2005. – С. 38–41. – Дата доступа: 23.09.2018.
1.