Математические структуры и моделирование
2008, вып. 18, с. 95–97

УДК 536.763/764

ШИФРОВАНИЕ СООБЩЕНИЙ НА ОСНОВЕ СОБСТВЕННЫХ ФУНКЦИЙ ОПЕРАТОРОВ

С.В. Белим, С.Ю. Белим

Предложена схема шифрования, основанная на кодировании с использованием собственных функций эрмитовых операторов. Проведено исследование полученного шифра для некоторых простых операторов.

1. Схема шифрования

Будем считать, что существует взаимно однозначное отображение используемого алфавита A на конечное множество целых чисел $Kod : A \to 1, ..., N$, где N – мощность используемого алфавита $|A| = N$. Рассмотрим линейный оператор K на множестве действительных бесконечно дифференцируемых функций одной переменной, обладающий следующими свойствами:

(i1) оператор K обладает дискретным спектром собственных значений.

(i2) все собственные значения невырождены, то есть каждой собственной функции соответствует свое собственное значение.

Введем на множестве рассматриваемых функций скалярное произведение

$$\langle \Psi, \Phi \rangle = \int\limits_{-\infty}^{+\infty} \Psi \Phi dx,$$

тогда третье условие на оператор имеет вид:

(i3) оператор K эрмитов, и, как следствие, множество собственных функций ортонормированно

$$\langle \Psi_n, \Psi_m \rangle = \delta_{nm},$$

где δ_{nm} – символ Кронекера:

$$\delta_{nm} = \begin{cases} 1, n = m, \\ 0, n \neq m. \end{cases}$$

Рассматривая оператор K в качестве ключа, введем следующую схему симметричного шифрования:

1. Вычислим собственные функции оператора $K\Psi_n = k_n \Psi_n$.

Омский государственный университет.
E-mail: belim@univer.omsk.su

2. Сопоставим каждому символу t_i, входящему в открытый текст T, собственную функцию Ψ_s, где $s = Kod(t_i)$. Если символ t_i повторяется, то его m-ому вхождению сопоставляется собственная функция с номером

$$k = Kod(t) + (m-1)N.$$

3. Построим «функцию сообщения»

$$\Psi = \sum_{t_i \in T} c_k \Psi_k \mid_{k=Kod(ti)}.$$

Здесь $c_i = i/\sum\limits_{i=1}^{nt} i^2$, nt – количество символов в сообщении.

4. По каналу связи передается «функция сообщения» Ψ. Таким образом, все символы передаются одновременно.

Алгоритм расшифрования состоит из следующих шагов:

1. Последовательное вычисление собственных функций Ψ_s.

2. Для каждой собственной функции вычисление скалярного произведения

$$\langle \Psi, \Psi_s \rangle = \begin{cases} c_s, t_i \in T, \\ 0, t_i \notin T. \end{cases}$$

.

3. Восстановление символов сообщения $t_i = Kod^{-1}(s)$.

4. Упорядочивание символов по возрастанию c_s.

2. Экспериментальное исследование шифра

В качестве примера, для экспериментальной проверки шифра, возьмем ключевой оператор в виде:

$$K = -\frac{d^2}{dx^2} + U(x).$$

Функцию $U(x)$ определим следующим образом:

$$U(x) = \begin{cases} 0, & 0 < x < a, \\ \infty, & x \le 0, \quad x \ge a. \end{cases}$$

Общую структуру оператора будем считать известной, в качестве ключа шифрования будет выступать параметр a.

Собственные функции оператора K могут быть легко найдены путем решения дифференциального уравнения на трех отрезках числовой прямой и последующей сшивки решений:

$$\Psi_n(x) = \sqrt{\frac{2}{a}} \sin\left(\frac{\pi n}{a} x\right).$$

Отображение Kod зададим таблицей

	а	б	в	г	д	е	ж	з	и	к
1	2	3	4	5	6	7	8	9	10	11
л	м	н	о	п	р	с	т	у	ф	х
12	13	14	15	16	17	18	19	20	21	22
ц	ч	ш	щ	ь,ъ	ы	э	ю	я		
23	24	25	26	27	28	29	30	31		

Соответственно $|A| = 31$. Зашифруем сообщение $M =$«мама мыла раму», ключом шифрования $a = 1$. Функция сообщения в этом случае примет вид:

$$\Psi(M) = 0.1\Psi_{13} + 0.2\Psi_{2} + 0.3\Psi_{44} + 0.4\Psi_{33} + 0.5\Psi_{1} + 0.6\Psi_{75} + 0.7\Psi_{28} \quad (1)$$
$$+0.8\Psi_{12} + 0.9\Psi_{63} + 1.0\Psi_{32} + 1.1\Psi_{17} + 1.2\Psi_{95} + 1.3\Psi_{106} + 1.4\Psi_{20}.$$

Для проверки устойчивости шифра к взлому прямым перебором рассмотрим процесс расшифрования с ключом $a = 1.01$. Отбирая целые значения скалярного произведения с точностью до 0.1, получим фразу «бяюммнамфэса ныалрбну». Как легко видеть, изменились не только сами символы, но и количество символов.

3. Заключение

Рассмотренный пример в полной мере демонстрирует возможности представленного алгоритма шифрования. Однако предложенный ключевой оператор K не является достаточно стойким. Например, расшифрование с ключом $a = 1.001$ позволяет прочесть зашифрованное сообщение. Поэтому необходимы дальнейшие исследования в направлении доказательства существования «хороших» ключевых операторов и поиск их вида.