УДК 518.6+681.3

©2008. **В.В. Скобелев**

РАЗРУШЕНИЕ ЧАСТОТ БУКВ НА ОСНОВЕ РЕГУЛЯРНЫХ КОМБИНАТОРНЫХ СТРУКТУР

Разработан аксиоматический подход, предназначенный для решения задачи разрушения частот букв в словах исходного языка, основанный на использовании регулярных комбинаторных структур. Доказана корректность предложенного подхода. Оценена асимптотическая временная и емкостная сложность дискретного преобразователя, предназначенного для решения задачи разрушения частот букв в словах исходного языка, и построенного в соответствии с предложенным подходом.

Введение. Одной из типичных атак на шифры является частотный анализ, т.е. использование статистических свойств применяемого естественного языка и поиск слов с характерной структурой [1]. Этот тип атак является основным при наличии у криптоаналитика только шифртекста, т.е. в наихудшей для криптоаналитика ситуации. Шифры неустойчивые к таким атакам принято считать абсолютно неустойчивыми шифрами [2]. Поэтому разработка моделей и методов, обеспечивающих стойкость шифра к частотному анализу, является актуальной задачей при построении любых вычислительно стойких коммерческих шифров. В [3] сформулированы требования, предъявляемые к комбинаторным структурам, предназначенным для решения рассматриваемой задачи и показано, что этим требованиям удовлетворяют шары и грани единичного куба.

Основной целью настоящей работы является построение и анализ дискретного преобразователя, построенного на основе регулярных комбинаторных структур, и предназначенного для решения задачи разрушения частот букв в словах исходного языка.

1. Основные понятия и определения. Снабдив схему шифрования дискретным преобразователем, осуществляющим разрушение частот букв на этапе предвычислений, мы естественно приходим к схеме, представленной на рис.1.

Рис. 1. Положение дискретного преобразователя, разрушающего частоты в схеме шифрования.

Побуквенное кодирование исходного текста двоичной последовательностью осу-

ществляется обычным образом и укладывается в рамки следующей модели.

Пусть исходные сообщения образуют бесконечный язык $L \subseteq \Sigma^+$. Длину слова u обозначим через $d(u)$. Предположим, что каждая буква алфавита Σ встречается, по крайней мере, в одном слове $u \in L$. Положим

$$l_1 = \lceil \log |\Sigma| \rceil.$$

Зафиксируем инъекцию $cdng : \Sigma \to \mathbf{E}^{l_1}$ (где $\mathbf{E} = \{0, 1\}$) и расширим ее на множество Σ^+ в соответствии с равенством

$$cdng(\sigma_1 \dots \sigma_n) = cdng(\sigma_1) \dots cdng(\sigma_1).$$

Ясно, что язык $cdng(L) = \{cdng(u) | u \in L\}$ представляет собой такой язык в алфавите $cdng(\Sigma) = \{cdng(\sigma) | \sigma \in \Sigma\}$, что:

1) $d(cdng(u) = l_1 \cdot d(u)$ $(u \in L)$;

2) $d_{cdng(\Sigma)}(cdng(u)) = d(u)$ для любого слова $u \in L$, где $d_{cdng(\Sigma)}(cdng(u))$ – это длина слова $cdng(u)$ в алфавите $cdng(\Sigma)$.

Под алгоритмом побуквенного кодирования исходного текста двоичными последовательностями принято понимать любой алгоритм, осуществляющий вычисление значений $cdng(\sigma)$ $(\sigma \in \Sigma)$ с временной и емкостной сложностью, соответственно, равной $T = O(\lceil \log |\Sigma| \rceil)$ $(|\Sigma| \to \infty)$ и $V = O(\lceil |\Sigma| \cdot \log |\Sigma| \rceil)$ $(|\Sigma| \to \infty)$.

Эффективность представленной на рис. 1 схемы шифрования для легальных пользователей и ее стойкость к криптоанализу существенно зависят от комбинаторных структур, применяемых в процессе разрушения частот букв. Поэтому важными характеристиками являются возможность компактного представления используемой комбинаторной структуры в неявном виде и существование быстрого алгоритма порождения элементов этой структуры одного за другим в явном виде. Комбинаторные структуры, обладающие этими двумя свойствами, назовем регулярными комбинаторными структурами.

2. Регулярные комбинаторные структуры. Пусть $n(u, \sigma)$ $(u \in \Sigma^+, \sigma \in \Sigma)$ – число вхождений буквы σ в слово u. Ясно, что

$$\sum_{\sigma \in \Sigma} n(u, \sigma) = d(u)$$

и

$$n(cdng(u), cdng(\sigma)) = n(u, \sigma)$$

для всех $u \in \Sigma^+$ и $\sigma \in \Sigma$.

Положим

$$L(k) = \{u \in L | d(u) \le k\} \ \ (k \in \mathbf{N})$$

и

$$\nu(L(k), \sigma) = \frac{\sum\limits_{u \in L(k)} n(u, \sigma)}{\sum\limits_{u \in L(k)} d(u)} \ \ (k \in \mathbf{N}, \sigma \in \Sigma).$$

Тогда

$$\sum_{\sigma\in\Sigma}\nu(L(k),\sigma)=1$$

и

$$\nu(cdng(L(k)),cdng(\sigma))=\nu(L(k),\sigma)\ \ (k\in\mathbf{N},\sigma\in\Sigma).$$

Предположим, что для каждого $\sigma\in\Sigma$ существует предел

$$\lim_{k\to\infty}\nu(L(k),\sigma)=a(\sigma)>0.$$

Тогда для любого фиксированного числа $\varepsilon>0$ для каждого $\sigma\in\Sigma$ существует такое число $k_0(\sigma,\varepsilon)\in\mathbf{N}$, что

$$|\nu(L(k),\sigma)-a(\sigma)|<\varepsilon$$

для всех $k\geq k_0(\sigma,\varepsilon)$ $(k\in\mathbf{N})$.

Зафиксируем такое достаточно малое число $\varepsilon>0$, что $a(\sigma)-\varepsilon>0$ $(\sigma\in\Sigma)$. Пусть

$$k_0(\varepsilon)=\max\{k_0(\sigma,\varepsilon)|\sigma\in\Sigma\}.$$

Назовем относительной частотой появления буквы $\sigma\in\Sigma$ в словах языка L число

$$frqnc(L,\sigma)=\nu(L(k_0(\varepsilon)),\sigma).$$

Отметим, что $frqnc(L,\sigma)>0$ для всех $\sigma\in\Sigma$.

В дальнейшем предполагается, что числа $frqnc(L,\sigma)$ $(\sigma\in\Sigma)$ представлены двоичными дробями и вычислены с точностью до 2^{-r} $(r\in\mathbf{N})$, причем

$$\sum_{\sigma\in\Sigma}frqnc(L,\sigma)=1.$$

Так как

$$frqnc(cdng(L),cdng(\sigma))=frqnc(L,\sigma)\ \ (\sigma\in\Sigma),$$

то построение комбинаторных структур в терминах языка $cdng(L)$ и относительных частот $frqnc(L,\sigma)$ корректно. Для краткости записи относительную частоту $frqnc(L,\sigma)$ $(\sigma\in\Sigma)$ будем обозначать $frqnc(\sigma)$.

Зафиксируем число $h\in\mathbf{N}$ $(h\geq r)$ и такое число $l_2\in\mathbf{N}$, что $l_2\geq l_1+h$.

Регулярной комбинаторной структурой для языка L назовем бинарное отношение $\Delta\subseteq\mathbf{E}^{l_1}\times\mathbf{E}^{l_2}$, удовлетворяющее следующим пяти условиям.

Условие 1. $pr_1\Delta=cdng(\Sigma)$.

Условие 2. $|\Delta(cdng(\sigma))|=2^r\cdot frqnc(\sigma)$ $(\sigma\in\Sigma)$.

Условие 3. $\Delta(cdng(\sigma_1))\bigcap\Delta(cdng(\sigma_2))=\emptyset$ для всех $\sigma_1,\sigma_2\in\Sigma$ $(\sigma_1\neq\sigma_2)$.

Условие 4. Емкостная сложность представления в неявном виде каждого множества $\Delta(cdng(\sigma))$ $(\sigma\in\Sigma)$ равна $O(l_2)$ $(|\Sigma|\to\infty)$.

Условие 5. Существует алгоритм A, который при фиксированной начинающейся с нуля нумерации элементов любого множества $\Delta(cdng(\sigma))$ $(\sigma\in\Sigma)$ с временной и емкостной сложностью, равной $O(l_2)$ $(l_2\to\infty)$, порождает: а) 0-й элемент множества

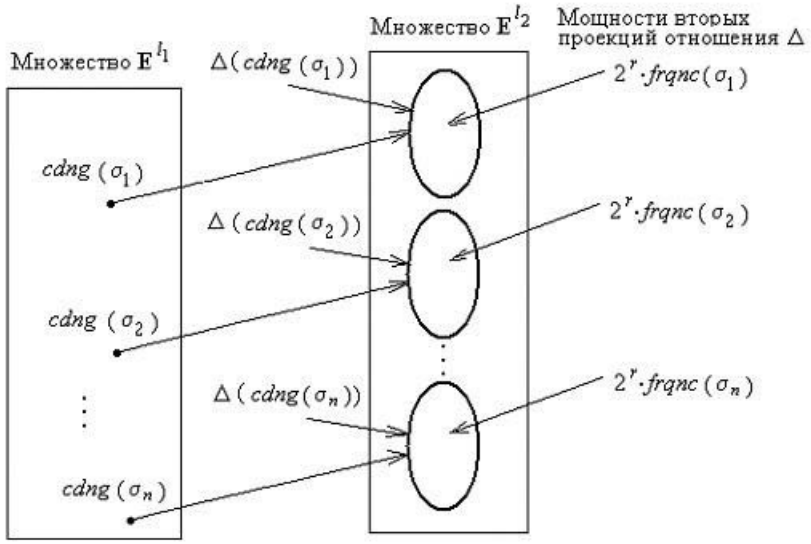

Рис. 2. Схематическое представление регулярной комбинаторной структуры.

$\Delta(cdng(\sigma))$; б)по j-му элементу ($j = 0, 1, \ldots, |\Delta(cdng(\sigma))|-1$) множества $\Delta(cdng(\sigma))$ порождает $(j+1)$ (mod $|\Delta(cdng(\sigma))|$)-й элемент множества $\Delta(cdng(\sigma))$.

Регулярная комбинаторная структура Δ схематически изображена на рис. 2.

Теорема 1. *Множество регулярных комбинаторных структур для языка L – непустое множество.*

Доказательство. Достаточно показать, что существует регулярная комбинаторная структура в случае, когда $l_2 = l_1 + h$.

Пусть $S_{\sigma,h}$ ($\sigma \in \Sigma$) – множество всех таких слов $\alpha_\sigma \uparrow\uparrow 0^{h-r} \in \mathbf{E}^h$ ($\alpha_\sigma \in \mathbf{E}^r$), что α_σ – двоичное представление числа, принадлежащего множеству $\mathbf{Z}_{2^r \cdot frqnc(\sigma)-1}$. Определим бинарное отношение $\Delta_h \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$ равенством

$$\Delta_h = \bigcup_{\sigma\in\Sigma} \{(cdng(\sigma), cdng(\sigma) \uparrow\uparrow \alpha_\sigma \uparrow\uparrow 0^{h-r}) \mid \alpha_\sigma \uparrow\uparrow 0^{h-r} \in S_{\sigma,h}\}.$$

Так как

$$pr_1\Delta_h = cdng(\Sigma)$$

и

$$|\Delta_h(cdng(\sigma))| = 2^r \cdot frqnc(\sigma) \ (\sigma \in \Sigma),$$

то для бинарного отношения Δ_h выполнены условия 1 и 2.

А так как $cdng$ – инъекция, то для всех $\sigma_1, \sigma_2 \in \Sigma$ ($\sigma_1 \neq \sigma_2$)

$$(cdng(\sigma_1), cdng(\sigma_1) \uparrow\uparrow \alpha_{\sigma_1} \uparrow\uparrow 0^{h-r}) \neq (cdng(\sigma_2), cdng(\sigma_2) \uparrow\uparrow \alpha_{\sigma_2} \uparrow\uparrow 0^{h-r}),$$

т.е.

$$\Delta_h(cdng(\sigma_1)) \bigcap \Delta_h(cdng(\sigma_2)) = \emptyset \ (\sigma_1, \sigma_2 \in \Sigma, \sigma_1 \neq \sigma_2)$$

и, следовательно, для бинарного отношения Δ_h выполнено условие 3.

Представлением каждого множества $\Delta_h(cdng(\sigma))$ $(\sigma \in \Sigma)$ в неявном виде является упорядоченная тройка $(cdng(\sigma), 2^r \cdot frqnc(\sigma), h-r)$, т.е. емкостная сложность представления каждого множества $\Delta_h(cdng(\sigma))$ в неявном виде равна $O(l_2)$ $(|\Sigma| \to \infty)$. Это означает, что для бинарного отношения Δ_h выполнено условие 4.

Зафиксируем такую нумерацию элементов множества $\Delta_h(cdng(\sigma))$ $(\sigma \in \Sigma)$, что номер каждого элемента $cdng(\sigma) \uparrow\uparrow \alpha_\sigma \uparrow\uparrow 0^{h-r} \in \Delta_h(cdng(\sigma))$ $(\alpha_\sigma \uparrow\uparrow 0^{h-r} \in S_{\sigma,h})$ совпадает с тем двоичным числом, которое представляет α. Отсюда вытекает, что для бинарного отношения Δ_h выполнено условие 5. $\square$

Отметим, что для любой регулярной комбинаторной структуры $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$ истинно равенство

$$pr_2\Delta = 2^r.$$

3. Анализ математической модели дискретного преобразователя. Построим математическую модель дискретного преобразователя, осуществляющего разрушение частот букв в словах языка $cdng(L)$, и основанного на использовании регулярной комбинаторной структуры $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$.

Пусть $A(\sigma, j)$ $(\sigma \in \Sigma, j \in \mathbf{Z}_{|\Delta(cdng(\sigma))|})$ – j-й элемент множества $\Delta(cdng(\sigma))$, порождаемый алгоритмом A, а $CNTR$ – одномерный массив длины $|\Sigma|$, элементы которого занумерованы элементами множества $cdng(\Sigma)$. Положим

$$\mathtt{Q} = \{CNTR \mid 0 \le CNTR(cdng(\sigma)) \le |\Delta(cdng(\sigma))| \ (\sigma \in \Sigma)\}.$$

Массив $CNTR \in \mathtt{Q}$ предназначен для подсчета (по $\mod |\Delta(cdng(\sigma))|$) числа вхождений каждой буквы $cdng(\sigma) \in cdng(\Sigma)$ в слово $cdng(u) \in cdng(L)$.

Обозначим через $GNRT(\mathtt{Q})$ псевдослучайный выбор элемента $CNTR \in \mathtt{Q}$.

Рассмотрим следующий алгоритм преобразования слова

$$cdng(u) = cdng(\sigma_1) \dots cdng(\sigma_n) \in cdng(L)$$

в слово в алфавите $pr_2\Delta$.

Шаг 1. $result := \Lambda$, $CNTR := GNRT(\mathtt{Q})$, $i := 1$.

Шаг 2. $CNTR(cdng(\sigma_i)) := (CNTR(cdng(\sigma_i)) + 1) \ (\mod |\Delta(cdng(\sigma_i))|)$.

Шаг 3. $b_i := A(\sigma_i, CNTR(cdng(\sigma_i)))$.

Шаг 4. $result := result \uparrow\uparrow b_i$, $i := i + 1$.

Шаг 5. Если $i \le n$, то переход к шагу 2, иначе конец.

Обозначим через $\mathtt{B}(cdng(u))$ слово в алфавите $pr_2\Delta$, в которое предложенный алгоритм переводит слово $cdng(u) \in cdng(L)$. Положим

$$\mathtt{L} = \{\mathtt{B}(cdng(u)) \mid u \in L\}.$$

Отметим, что предложенный алгоритм осуществляет инъекцию языка $cdng(L)$ в язык $\mathtt{L}$. При этом, для любого слова $cdng(u) \in cdng(L)$

$$d_{pr_2\Delta}(\mathtt{B}(cdng(u))) = d(u),$$

где $d_{pr_2\Delta}(\mathtt{B}(cdng(u)))$ – длина слова $\mathtt{B}(cdng(u))$ в алфавите $pr_2\Delta$.

Теорема 2. *Относительная частота появления каждой буквы $x \in pr_2\Delta$ в словах языка $\mathtt{L}$ равна 2^{-r}.*

Доказательство. Так как

$$\nu(\mathtt{L}(k), x) = \frac{\sum\limits_{u \in L(k)} n(\mathtt{B}(cdng(u)), x)}{\sum\limits_{u \in L(k)} d(u)} \ (k \in \mathbf{N}, x \in pr_2\Delta)$$

и

$$\sum_{x \in pr_2\Delta} \nu(\mathtt{L}(k), x) = 1 \ (k \in \mathbf{N}),$$

то

$$\lim_{k \to \infty} \sum_{x \in pr_2\Delta} \nu(\mathtt{L}(k), x) = 1,$$

т.е.

$$\sum_{x \in pr_2\Delta} frqnc(\mathtt{L}, x) = 1.$$

Из шагов 2–4 предложенного алгоритма вытекает, что

$$n(\mathtt{B}(cdng(u)), x) \le \frac{n(u, \sigma)}{|\Delta(cdng(\sigma))|} + 1 \ (x \in \Delta(cdng(\sigma)))$$

для любого слова $cdng(u) \in cdng(L)$.

Следовательно, для всех $x \in \Delta(cdng(\sigma))$

$$\nu(\mathtt{L}(k), x) \le \frac{\sum\limits_{u \in L(k)} \left(\frac{n(u,\sigma)}{|\Delta(cdng(\sigma))|} \right) + 1}{\sum\limits_{u \in L(k)} d(u)} =$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot \frac{\sum\limits_{u \in L(k)} n(u, \sigma)}{\sum\limits_{u \in L(k)} d(u)} + \frac{\sum\limits_{u \in L(k)} 1}{\sum\limits_{u \in L(k)} d(u)} =$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot \frac{\sum\limits_{u \in L(k)} n(u, \sigma)}{\sum\limits_{u \in L(k)} d(u)} + \frac{|\mathtt{L}(k)|}{\sum\limits_{u \in L(k)} d(u)}.$$

Отсюда вытекает, что для всех $x \in \Delta(cdng(\sigma))$

$$frqnc(\mathtt{L}, x) = \lim_{k \to \infty} frqnc(\mathtt{L}, x) \le$$

$$\leq \lim_{k\to\infty}\left(\frac{1}{|\Delta(cdng(\sigma))|}\cdot\frac{\sum\limits_{u\in L(k)} n(u,\sigma)}{\sum\limits_{u\in L(k)} d(u)}+\frac{|\mathtt{L}(k)|}{\sum\limits_{u\in L(k)} d(u)}\right)=$$

$$=\frac{1}{|\Delta(cdng(\sigma))|}\cdot frqnc(L,\sigma)+\lim_{k\to\infty}\frac{|\mathtt{L}(k)|}{\sum\limits_{u\in L(k)} d(u)}.$$

Так как L – бесконечный язык, то

$$\lim_{k\to\infty}\frac{|\mathtt{L}(k)|}{\sum\limits_{u\in L(k)} d(u)}=0.$$

Следовательно,

$$frqnc(\mathtt{L},x)\leq\frac{1}{|\Delta(cdng(\sigma))|}\cdot frqnc(L,\sigma)=\frac{1}{2^r\cdot frqnc(L,\sigma)}=2^{-r}.$$

Предположим, что существует такое $x\in\Delta(cdng(\sigma))$, что $frqnc(\mathtt{L},x)<2^{-r}$. Тогда

$$1=\sum_{x\in pr_2\Delta} frqnc(\mathtt{L},x)<\sum_{x\in pr_2\Delta}2^{-r}=2^r\cdot 2^{-r}=1.$$

Получено противоречие. Следовательно, предположение – ложное. Отсюда вытекает, что $frqnc(\mathtt{L},x)=1$ для всех $x\in\Delta(cdng(\sigma))$. □

Теорема 3. *Временная и емкостная сложность преобразования слова*

$$cdng(u)=cdng(\sigma_1)\ldots cdng(\sigma_n)\in cdng(L)$$

в слово в алфавите $pr_2\Delta$ равна, соответственно,

$$T(n)=O(T_{GNRT}(|\Sigma|)+n\cdot l_2\cdot 2^r)\ \ (|\Sigma|\to\infty) \tag{1}$$

и

$$V(n)=O(V_{GNRT}(|\Sigma|)+l_2\cdot|\Sigma|+n\cdot l_2)\ \ (|\Sigma|\to\infty), \tag{2}$$

где $T_{GNRT}(|\Sigma|)$ и $V_{GNRT}(|\Sigma|)$ – соответственно, временная и емкостная сложность заполнения массива $CNTR$ при помощи псевдослучайного генератора такими числами, что $0\leq CNTR(cdng(\sigma))\leq|\Delta(cdng(\sigma))|$ $(\sigma\in\Sigma)$.

Доказательство. Временная сложность шага 1 предложенного алгоритма равна

$$T_1=O(T_{GNRT}(|\Sigma|)\ \ (|\Sigma|\to\infty). \tag{3}$$

Оценим временную сложность цикла, определяемого шагами 2–5.

Временная сложность выполнения как шага 2, так и шага 4, равна

$$T_2=O(l_2)\ \ (|\Sigma|\to\infty). \tag{4}$$

Временная сложность 1-го исполнения шага 3 равна

$$T_3^{(1)} = O(l_2 \cdot 2^r) \ (|\Sigma| \to \infty), \tag{5}$$

а для каждого последующего исполнения шага 2

$$T_3^{(2)} = O(l_2) \ (|\Sigma| \to \infty). \tag{6}$$

Временная сложность выполнения шага 5 равна

$$T_4 = O(1) \ (|\Sigma| \to \infty). \tag{7}$$

Из (3)–(7) вытекает (1).

Емкостная сложность шага 1 предложенного алгоритма равна

$$V_1 = O(V_{GNRT}(|\Sigma|) \ (|\Sigma| \to \infty). \tag{8}$$

Оценим объем памяти, необходимой для реализации цикла, определяемого шагами 2–5.

Для хранения текущего значения $A(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ необходим объем памяти, равный

$$V_2 = O(l_2 \cdot |\Sigma|) \ (|\Sigma| \to \infty). \tag{9}$$

Объем памяти, необходимой для реализации как шага 2, так и шага 3, равен

$$V_3 = O(l_2) \ (|\Sigma| \to \infty). \tag{10}$$

Объем памяти, необходимой для реализации шага 4, равен

$$V_4 = O(n \cdot l_2) \ (|\Sigma| \to \infty). \tag{11}$$

Объем памяти, необходимой для реализации шага 5, равен

$$V_5 = O(n) \ (|\Sigma| \to \infty). \tag{12}$$

Из (8)–(12) вытекает (2). □

Секретным сеансовым ключом для предложенного алгоритма является настройка псевдослучайного генератора $GNRT$. Из (1),(3),(5) и (6) вытекает, что временная сложность во многом определяется именно исполнением шага 1 и первым исполнением шага 3.

Ни массив $GNRT(\mathtt{Q})$, ни исходные значения $A(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ не зависят от слова $cdng(u) \in cdng(L)$, преобразуемого алгоритмом. Следовательно, если процесс разворачивания ключа, т.е. вычисление массива $GNRT(\mathtt{Q})$ и массива $A(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ вынести за рамки предложенного алгоритма (т.е. на этап предвычислений), то асимптотическая временная сложность станет равной $O(n \cdot l_2)$ $(|\Sigma| \to \infty)$, т.е. полное разрушение частот букв исходного сообщения будет осуществляться с линейным замедлением.

Несложно показать, что предложенный алгоритм, рассматриваемый как поточный шифр, является неустойчивым шифром по отношению к атаке, осуществляемой на основе заранее выбранного исходного текста и является вычислительно устойчивым шифром по отношению к атаке, осуществляемой на основе только шифртекста.

Заключение. В настоящей работе построена и исследована математическая модель дискретного преобразователя, построенного на основе регулярной комбинаторной структуры и предназначенного для решения задачи разрушения частот букв в словах исходного языка.

Рассмотренный в работе подход допускает следующее обобщение. Пусть в неявном виде задано семейство регулярных комбинаторных структур

$$S = \{\Delta_i \mid i = 1, \ldots, n\},$$

а в процессе реализации предложенного алгоритма выбор бинарного отношения $\Delta_i \in S$ в очередном фрагменте преобразуемого слова осуществляется с помощью псевдослучайного генератора Г чисел, принадлежащих множеству $\mathbf{N}_n$. Будем считать, что инициализация генератора Г является частью секретного сеансового ключа. В результате мы приходим к нестационарному поточному шифру, который является устойчивым шифром по отношению к атаке, осуществляемой на основе заранее выбранного исходного текста.

Отметим, что неявно заданное семейство регулярных комбинаторных структур S представляет собой естественное обобщение парадигмы управляемой подстановочной операции, применяемой при построении высокоскоростных блочных шифров. Такое обобщение получается за счет перехода от отображений к бинарным отношениям.

1. *Алферов А.П. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480с.
2. *Диффи У., Хеллмен М.Е.* Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. – 1979. – Т.67. – №3. – С.71-109.
3. *Скобелев В.В.* Построение стойких к частотному анализу криптосистем на основе регулярных комбинаторных структур // Искусственный интеллект. – 2004. – №1. – С.88-96.

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 19.05.08