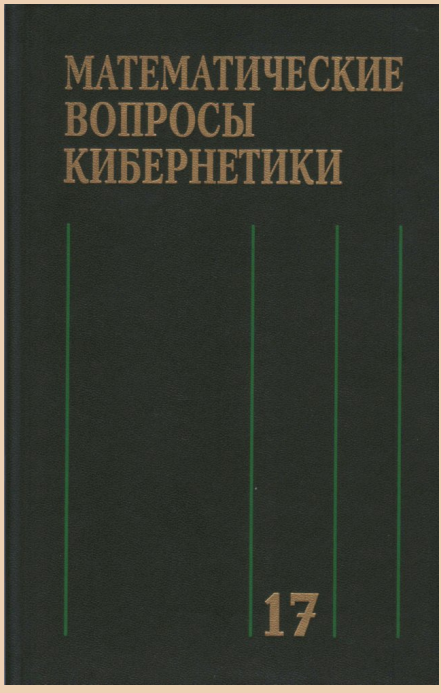
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 17



**М. П. Минеев,
В. Н. Чубариков**

Об арифметическом подходе к построению шифра Виженера

Рекомендуемая форма библиографической ссылки: Минеев М. П., Чубариков В. Н. Об арифметическом подходе к построению шифра Виженера // Математические вопросы кибернетики. Вып. 17. — М.: ФИЗМАТЛИТ, 2008. — С. 263–264. URL: http://library.keldysh.ru/mvk.asp?id=2008-263

КРАТКИЕ СООБЩЕНИЯ

ОБ АРИФМЕТИЧЕСКОМ ПОДХОДЕ К ПОСТРОЕНИЮ ШИФРА ВИЖЕНЕРА*)

М. П. МИНЕЕВ, В. Н. ЧУБАРИКОВ

(МОСКВА)

В настоящей статье продолжено построение шифров на основе теоретико-числовых алгоритмов [6–8]. Здесь дан арифметический подход к подобному конструированию шифра Виженера, рассматриваемого как шифр гаммирования с периодической гаммой (см. [1, с. 151–152]; [2, с. 11]).

Пусть количество символов алфавита равно n, причем $n > 2$. Каждому символу α_k, $k = 1, \ldots, n$, алфавита присваивается некоторый вычет a_k по модулю n, причем различным символам отвечают различные вычеты.

Перейдем к первому способу шифрования.

1. При некотором натуральном числе t имеем $2^{2t-2} < n \leqslant 2^{2t}$. Следовательно, $\sqrt{n} \leqslant 2^t < 2\sqrt{n}$. Представим каждое число a_k в виде $a_k = 2^t b_k + c_k$, где b_k, c_k будем записывать как t-значные числа в двоичной системе счисления (например, при $t = 3$ имеем $\overline{000} = 0$; $\overline{001} = 1$ и т. д.)

Составим две таблицы Виженера, отвечающие «полубуквам» b_k, c_k, где $k = 1, \ldots, n$. Имеем

$a_1, a_2, \ldots, a_{n-1}, a_n$
$b_1, b_2, \ldots, b_{n-1}, b_n$
$b_2, b_3, \ldots, b_n, b_1$
$\ldots\ \ldots\ \ldots\ldots\ldots$
$b_n, b_1, \ldots, b_{n-2}, b_{n-1}$

$a_1, a_2, \ldots, a_{n-1}, a_n$
$c_1, c_2, \ldots, c_{n-1}, c_n$
$c_2, c_3, \ldots, c_n, c_1$
$\ldots\ \ldots\ \ldots\ldots\ldots$
$c_n, c_1, \ldots, c_{n-2}, c_{n-1}$

Для каждой из этих таблиц при некоторых натуральных числах l, m с условиями $1 < l, m \leqslant \sqrt{n}, (l, m) = 1, lm \geqslant n$, возьмем свой ключ: $k = (k_1, k_2, \ldots, k_l)$ для первой таблицы и соответственно $s = (s_1, s_2, \ldots, s_m)$ для второй таблицы. Над каждой буквой первой строки первой таблицы выписываем в строку символы ключа k в количестве n символов следующим образом $k_1, k_2, \ldots k_l, k_1, k_2, \ldots$. Аналогично выписываем ключ s над второй таблицей.

Переходим к процедуре шифрования открытого текста $a_{q_1} a_{q_2} \ldots a_{q_r}$. Номер q_1 определяет номер столбца и в первой и во второй таблицах Виженера. Далее, делим число q_1 с остатком на l и на m. Получим

$$q_1 = lu + p_1, \quad 0 \leqslant p_1 < q_1, \qquad q_1 = mv + d_1, \quad 0 \leqslant d_1 < q_1.$$

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 04–01–00566а).

Пусть на пересечении q_1-го столбца и p_1-й строки в первой таблице находится символ x_1, а на пересечении q_1-го столбца и d_1-й строки находится символ y_1. Повторим эту процедуру для следующего символа a_{q_2} и т. д. Получим шифрованный текст $x_1y_1x_2y_2\ldots x_ry_r$ или два шифрованных текста $x_1x_2\ldots x_r$ и $y_1y_2\ldots y_r$, которые могут быть переданы по каналу связи последовательно.

Для расшифрования шифрограммы воспользуемся китайской теоремой об остатках. Действительно, номер столбца q_s, где $s=1,\ldots,r$, единственным образом восстанавливается из системы сравнений

$$\begin{cases} q_s \equiv p_s \pmod{l}, \\ q_s \equiv d_s \pmod{m}. \end{cases}$$

2. Дадим еще один способ построения шифра Виженера.

Пусть, как и раньше, количество символов алфавита равно n, $2^{h-1} < n \leqslant 2^h$, причем $n > 2$, и каждому символу α_k, $k=1,\ldots,n$, алфавита присваивается некоторый вычет a_k по модулю n, причем различным символам отвечают различные вычеты. Представим каждое число a_k в виде $a_k = 2b_k + \varepsilon_k$, где b_k будем записывать как h-значные числа в двоичной системе счисления, а ε_k будут принимать всего два значения, либо 0, либо 1.

Как и раньше, для набора $(b_1, b_2, \ldots, b_n)$ составим таблицу Виженера, и по ней, используя ключ $(k_1,\ldots,k_l)$, где $(l,2)=1$, $l \geqslant n/2$, зашифруем открытый текст $a_{q_1}, a_{q_2}, \ldots, a_{q_r}$. Рассмотрим в двоичной системе счисления число $m = \overline{\varepsilon_{q_1}\varepsilon_{q_2}\ldots\varepsilon_{q_r}}$. Передадим его по открытому каналу связи с использованием секретных ключей, используя криптографическую схему А. Шамира (см., например, [6–8]).

Используя китайскую теорему об остатках для определения при $s=1,\ldots,r$ номера столбца q_s из системы сравнений

$$\begin{cases} q_s \equiv p_s \pmod{l}, \\ q_s \equiv \varepsilon_{q_s} \pmod{2}, \end{cases}$$

получим расшифрование шифрованного текста.

Для построения шифров нами использованы руководства [3–5, 9, 10].

СПИСОК ЛИТЕРАТУРЫ

1. Бабаш А. В., Шанкин Г. П. Криптография. — М.: СОЛОН-ПРЕСС, 2007.
2. Баричев С. Криптография без секретов. — http://www.artelecom.ru/library/books/swos/index/html — 44 с.
3. Виноградов И. М. Основы теории чисел. — М.: Наука, 1983.
4. Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Наука, 1996.
5. Коблиц Н. Курс теории чисел и криптографии. — М.: Научное изд-во ТВП, 2001.
6. Минеев М. П., Чубариков В. Н. Задача об искажении частоты появления знаков в шифре простой замены // Математические вопросы кибернетики. Вып. 16.— М.: Физматлит, 2007. — С. 242–245.
7. Минеев М. П., Чубариков В. Н. Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН. — 2008. — Т. 420, № 6. — С. 736–738.
8. Минеев М. П., Чубариков В. Н. К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН. — 2009. — Т. 426, № 1. — С. 6–8.
9. Нечаев В. И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов. — М.: Высш. шк., 1999.
10. Чубариков В. Н. Элементы арифметики. — М.: Изд-во Механико-математического ф-та МГУ, 2007.

Поступило в редакцию 14 X 2008