Многоалфавитные шифры замены с периодическим ключом
Содержание:

П.1 Многоалфавитные шифры замены с периодическим ключом

Ранее мы рассматривали шифры замены, в этой теме рассмотрим многоалфавитные шифры замены с периодическим ключом.

Рассмотрим 30-буквенный алфавит русского языка:

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ.

В этом алфавите отсутствуют буквы Ё, Й и Ъ, что практически не ограничивает возможностей по составлению открытых сообщений на русском языке. В самом деле, замена буквы Ё на букву Е, буквы Й — на букву И, а буквы Ъ — на букву Ь позволяет понять смысл открытого сообщения, написанного с использованием этого алфавита.

В алфавите любого естественного языка буквы следуют друг за другом в определенном порядке. Это дает возможность присвоить каждой букве алфавита ее естественный порядковый номер. Так, в приведенном алфавите букве А присваивается порядковый номер 1, букве О — порядковый номер 14, а букве Ы — порядковый номер 27. Если в открытом сообщении каждую букву заменить ее естественным порядковым номером в рассматриваемом алфавите, то преобразование числового сообщения в буквенное позволяет однозначно восстановить исходное открытое сообщение.

Например, числовое сообщение 1 11 20 1 3 9 18

преобразуется в буквенное сообщение: АЛФАВИТ.

Дополним естественный порядок букв в алфавите. Будем считать, что за последней буквой алфавита следует его первая буква. Такой порядок букв достигается, если расположить их на окружности в естественном порядке по часовой стрелке. При таком расположении можно каждой из букв присвоить порядковый номер относительно любой буквы алфавита.

Рис 1.

Такой номер назовем относительным порядковым номером. Заметим, что если число букв в алфавите равно z, то относительный порядковый номер данной буквы может принимать все значения от 0 до (z — 1) в зависимости от буквы, относительно которой он вычисляется. Для примера рассмотрим исходный 30-буквенный алфавит русского языка, расположенный на окружности (см. рис. 1). В этом случае порядковый номер буквы А относительно буквы А равен 0, относительно буквы Я он уже равен 1 и так далее, относительно буквы Б

порядковый номер А равен 29. Значения относительных порядковых номеров букв алфавита из z букв совпадают со значениями всевозможных остатков от деления целых чисел на натуральное число z. В следующем пункте мы рассмотрим математические основы этого утверждения.

П.2 Математические основы

Мы уже выяснили, что порядковый номер какой-либо буквы алфавита относительно другой буквы равен остатку от деления разности их естественных порядковых номеров на число букв в алфавите. Теперь остановимся более подробно на математическом значении данного утверждения.

Обозначим символами:

$D(N_1,N_2)$ — порядковый номер буквы с естественным порядковым номером N_1 относительно буквы с естественным порядковым номером N_2; $r_m(N)$— остаток от деления целого числа N на натуральное число m.

При этом справедливо равенство $D(N_1,N_2) = r_z(N_1- N_2)$, где z — число букв в алфавите.

Для удобства обозначим $N_1 \boxed{-} N_2 = r_2(N_1 – N_2)$, $N_1 \oplus N_2 = r_z(N_1+N_2)$. Тогда имеют место равенства:

$$D(N_1,N_2)=N_1 \boxed{-} N_2 \qquad \textbf{(1)}$$

$$N_1=N_2 \oplus D(N1,N2) \qquad \textbf{(2)}$$

Формула (2) непосредственно получается из (1) и ее можно использовать для замены буквы с естественным порядковым номером N_2 на букву с естественным порядковым номером N_1. Число $D(N_1, N_2)$ называется знаком гаммы.

Будем считать верными следующие факты:

1. Для любых целых N_1, N_2 и любого натурального z справедливо равенство:

$$D(N_1,N_2) = N_1-N_2-\left[(N_1-N_2) : z\right] *z ,$$

   где[X] — целая часть числа X (наибольшее целое число, не превосходящее числа X).

2. Верно равенство:

$$N_2=N_1 \boxed{-} D(N1,N2) \qquad \textbf{(3)}$$

Для зашифрования некоторого открытого сообщения, состоящего из N букв, с помощью указанной замены требуется N знаков гаммы: по одному на каждую букву сообщения. Последовательность знаков гаммы, необходимая для зашифрования открытого сообщения, является ключом данного шифра.

Если последовательность знаков гаммы имеет небольшой (по сравнению с длиной открытого текста) период, то соответствующий шифр называется ***шифром замены с периодическим ключом***.

Ключом такого шифра, по существу, является отрезок гаммы, равный по длине периоду.

Число отрезков некоторой длины T, состоящих из чисел от O до (z — 1) равно z^T, так как на каждой из T позиций отрезка может быть любое из z чисел (независимо от чисел, находящихся на других позициях). Для наглядности приведем значения z^T при z = 30 в зависимости от значений T:

Т	1	2	3	4	5	6	7
$зо^{т}$	30	900	27000	810000	24300000	$0,729*10^{9}$	$0,2187*10^{11}$

т	8	9	10
$зо^{т}$	$0,6561*10^{12}$	$0,19683*10^{14}$	$0, 59049 • 10^{15}$

Как видно из приведенной таблицы, число ключей рассматриваемого шифра замены с ключом периода 10, достаточно внушительно и составляет уже сотни триллионов. Это обстоятельство делает практически невозможным вскрытие шифра методом перебора всех его ключей даже при меньших значениях периода гаммы.

Для рассматриваемого шифра характерно то, что буквы открытого текста, зашифрованные одним и тем же знаком гаммы, по сути, зашифрованы одним и тем же шифром простой замены.

Например, ключевая таблица этого шифра простой замены при знаке гаммы, равном 1, имеет вид:

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА

Вторую строку этой ключевой таблицы называют алфавитом шифрования, соответствующим данному знаку гаммы.

П.3 Примеры

Поскольку в рассматриваемом шифре возможны все значения гаммы от 0 до 29, то данный шифр можно рассматривать как 30-алфавитный шифр замены. Если каждому из этих алфавитов поставить в соответствие его первую букву, то каждый знак гаммы можно заменить этой буквой. В этом случае ключ рассматриваемого шифра можно взаимнооднозначно заменить соответствующим словом в этом же алфавите.

Такой многоалфавитный шифр замены был описан в 1585 году французом Блезом де Виженером в его «Трактате о шифрах»:

ABCDEFGHIJKLMNQPQRSTUVWXYZ
BCDEFGHIJKLMHOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMHOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MHOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMHOPQRSTU
WXYZABCDEFGHIJKLMNDPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Все алфавиты шифрования относительно латинского алфавита были сведены им в таблицу, получившую впоследствии название ее автора. Выше приведена таблица Виженера для современного латинского алфавита, она состоит из списка 26 алфавитов шифрования. Способ зашифрования с помощью таблицы Виженера заключается в том, что первый из алфавитов соответствует алфавиту открытого текста, а букве ключевого слова соответствует алфавит шифрования из данного списка, начинающийся с этой буквы. Буква шифрованного текста находится в

алфавите шифрования на месте, соответствующем данной букве открытого текста. Простота построения таблицы Виженера делает эту систему привлекательной для практического использования.

Рассмотрим пример вскрытия многоалфавитного шифра замены с периодическим ключом, содержащийся в рассказе Жюля Верна «Жангада». Вот текст, который был получен с помощью такого типа шифра:

с	г	у	ч	п	в	э	л	л	з	й	р	т	е	п	н	л	н	ф	г	и	н	б	о	р	г	й	у		
г	л	ч	д	к	о	т	х	ж	г	у	у	м	з	д	х	р	ъ	с	г	с	ю	д	т	п	ъ	а	р		
в	й	г	г	и	щ	в	ч	э	е	ц	с	т	у	ж	в	с	е	в	х	а	х	я	ф	б	ь	б	е		
т	ф	з	с	э	ф	т	х	ж	з	б	з	ъ	г	ф	б	щ	и	х	х	р	и	п	ж	т	з	в	т		
ж	й	т	г	о	й	б	н	т	ф	ф	е	о	и	х	т	т	е	г	и	и	о	к	з	п	т	ф	л		
е	у	г	с	ф	и	п	т	ь	м	о	ф	о	к	с	х	м	г	б	т	ж	ф	ы	г	у	ч	о	ю		
н	ф	н	ш	з	г	э	л	л	ш	р	у	д	е	н	к	о	л	г	г	н	с	б	к	с	с	е	у		
п	н	ф	ц	е	е	е	г	г	с	ж	н	о	е	ы	и	о	н	р	с	и	т	к	ц	ь	е	д	б		
у	б	т	е	т	л	о	т	б	ф	ц	с	б	ю	й	п	м	п	з	т	ж	п	т	у	ф	к	д	г		

Догадавшись, что ключом является натуральное число, персонаж «Жангады», судья Жаррикес, объясняет сыну обвиняемого Маноэлю, как был зашифрован документ: —«Давайте возьмем фразу, все равно какую, ну хотя бы вот эту:

У СУДЬИ ЖАРРИКЕСА ПРОНИЦАТЕЛЬНЫЙ УМ

А теперь я возьму наудачу какое-нибудь число, чтобы сделать из этой фразы криптограмму. Предположим, что число состоит из трех цифр, например, 4, 2 и 3. Я подписываю число 423 под строчкой так, чтобы под каждой буквой стояла цифра, и повторяю число, пока не дойду до конца фразы. Вот что получится:

у	с	у	д	ь	и	ж	а	р	р	и	к	е	с	а	п	р	о	н	и	ц	и	а	т	е	л	ь	н	ы	й	у	м
2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	4

Будем заменять каждую букву нашей фразы той буквой, которая стоит после нее в алфавите

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

на месте, указанном цифрой. Например, если под буквой А стоит цифра 3, вы отсчитываете три буквы и заменяете ее буквой Г. Если буква находится в конце алфавита и к ней нельзя прибавить нужного числа букв, тогда отсчитывают недостающие буквы с начала алфавита.

Доведем до конца начатую криптограмму, построенную на числе 423, и исходная фраза заменится следующей:

ЧУЦИЮЛКВУФКНЙУГУТССКЩДФИПЮРЯЛЦР

Но как найти числовой ключ? Подсчет, проведенный Жаррикесом, показывает, что поиск ключа перебором всех возможных чисел, состоящих не более чем из 10 цифр, потребует более трехсот лет. Судья пытается наудачу отгадать заветное число. Наступает день казни. Обвиняемого Жоама Дакосту ведут на виселицу...

Но все заканчивается благополучно. Помог счастливый случай. Другу Жоама удается узнать, что автора криптограммы звали Ортега. Поставив буквы О, Р, Т, Е, Г, А над последними шестью буквами документа и подсчитав, на сколько эти буквы по алфавиту сдвинуты относительно букв криптограммы, судья, наконец, находит ключ к документу:

исходное сообщение	О	Р	Т	Е	Г	А
шифрованное сообщение	Т	У	Ф	К	Д	Г
относительный сдвиг букв	4	3	2	5	1	3

Г. А. Гуревич в статье «Криптограмма Жюля Верна» (журнал «Квант» №9, 1985 г.) обращает внимание на то, что судья прошел практически весь путь до отгадки. Будучи уверенным, что в документе упоминается имя Жоама Дакосты, судья строит предположение: «Если бы строчки были разделены на слова, то мы могли бы выделить слова, состоящие из семи букв, как и фамилия Дакоста, и, опробуя их одно за другим, может быть и отыскали бы число, являющееся ключом криптограммы». Маноэль, в свою очередь, поняв основную идею судьи, предлагает опробовать возможные расположения слова ДАКОСТА в исходном тексте. Поскольку текст состоит из 252 букв, то достаточно опробовать не более 246 вариантов. В один прекрасный момент, записав над фрагментом ЙБНТФФЕ слово ДАКОСТА, мы определили бы последовательность цифр 5134325. Естественно предположить, что последняя цифра 5 — начало следующего периода:

исходное сообщение	...	Д	А	К	О	С	Т	А	...
шифрованное сообщение	...	Й	Б	Н	Т	Ф	Ф	Е	...
относительный сдвиг букв	...	5	1	3	4	3	2	5	...

Вместо ключа 432513 мы нашли его циклическую перестановку 513432, что ни в коей мере не мешает расшифрованию текста. Для этого достаточно для каждой буквы шифрованного текста определить букву, относительно которой данная буква сдвинута на величину соответствующей цифры ключа:

С Г У Ч П В Э Л Л З Й Р Т Е П Н Л Н Ф Г И Н Б О Р
4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4
Н А С Т О Я Щ И Й В И Н О В Н И К К Р А Ж И А Л М

Г Й У Г Л Ч Д К О Т Х Ж Г У У М З Д Х Р Ъ С Г С Ю
3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3
А З О В И У Б И Й С Т В А С О Л Д А Т О Х Р А Н Ы

Д Т П Ъ А Р В Й Г Г И Щ В Ч Э Е Ц С Т У Ж В С Е В
2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2

В НОЧЬ НА ДВА ДЦ АТ ЬВТО РОЕ Я НВА

Х А Х Я Ф Б Ь Ь Б Е Т Ф З С Э Ф Т Х Ж З Б З Ъ Г Ф Б
5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5
Р Я Т Ы С Я Ч А В О С Е М Ь С О Т Д В А Д Ц А Т Ь

Щ И Х Х Р И П Ж Т З В Т Ж Й Т Г О Й Б Н Т Ф Ф Е О
1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1
Ш Е С Т О Г О Г О Д А Н Е Ж О А М Д А К О С Т А Н

И Х Т Т Е Г И И О К З П Т Ф Л Е У Г Б Ф И П Т Ь М
3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3
Е С П Р А В Е Д Л И В О П Р И Г О В О Р Е Н Н Ы Й

О Ф О К С Х М Г Б Т Ж Ф Ы Г У Ч О Ю Н Ф Н Ш З Г Э
4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4
К С М Е Р Т И А Я Н Е С Ч А С Т Н Ы Й С Л У Ж А Щ

Л Л Ш Р У Д Е Н К О Л Г Г Н С Б К С С Е П У Н Ф Ц
3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 1 5 3 4 3
И Й У П Р А В Л Е Н И Я А Л М А З Н О Г О О К Р У

Е Е Е Г Г С Ж Н О Е Ы И О Н Р С И Т К Ц Ь Е Д Б У
2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2
Г А Д А Я О Д И Н В Ч Е М И П О Д П И С Ы В А Ю С

Б Т Е Т Л О Т Б Ф Ц С Б Ю Й П М П З Т Ж П Т У Ф К
5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5
Ь С В О И М Н А С Т О Я Щ И М И М Е Н Е М О Р Т Е

Д Г
1 3
Г А

П.4 Еще немного теории

Итак, **первая** идея состоит в использовании вероятного слова, то есть слова, которое с большой вероятностью может содержаться в данном открытом тексте. Речь идет, в том числе и о словах, часто встречающихся в любых открытых текстах. К ним, например, относятся такие слова как КОТОРЫЙ, ТОГДА, ЧТО, ЕСЛИ, приставки ПРИ, ПРЕ, ПОД и т. п.

Вторая идея основана на том, что буквы открытого сообщения находятся в открытом тексте на вполне определенных позициях. Если разность номеров их позиций окажется кратной периоду гаммы, то стоящие на этих позициях буквы будут зашифрованы одним и тем же знаком гаммы. Это означает, что определенные части открытого текста окажутся зашифрованными шифром простой замены. Эту идею можно использовать для определения периода ключа многоалфавитного шифра замены.

Способы определения периода

Для определения периода гаммы могут быть применены два способа. Первый из них известен как тест Казизки, второй способ использует так называемый индекс совпадения.

- Тест Казизки был описан в 1863 году Фридрихом Казизки. Он основан на следующем наблюдении: два одинаковых отрезка открытого текста будут соответствовать двум одинаковым отрезкам шифрованного текста, если разность номеров позиций их начал кратна периоду гаммы. Следовательно, если мы обнаружим два одинаковых отрезка шифрованного текста, состоящих по крайней мере из трех букв, то с большой вероятностью им соответствуют одинаковые отрезки открытого текста (случайное совпадение маловероятно). Тест Казизки, по сути, заключается в том, что в шифрованном тексте надо найти пары одинаковых отрезков, вычислить разности номеров позиций их начал и определить общие делители найденных разностей. Как правило, один из этих общих делителей равен периоду гаммы.
- Для уточнения значения периода гаммы может быть использован индекс совпадения, предложенный в 1920 году Уильямом Фридманом. Для последовательности букв индекс совпадения представляет собой число, равное количеству всех пар номеров позиций последовательности, на которых находятся одинаковые буквы, деленному на общее количество всех пар номеров позиций этой последовательности, т. е. среднему числу пар, состоящих из одинаковых букв. Примечательно то, что при зашифровании последовательности с помощью шифра простой замены указанное число не меняется.

Для иллюстрации этого подхода рассмотрим тот же самый шифрованный текст, записанный в виде последовательности столбцов, содержащих по шесть подряд идущих букв текста в каждом (подряд идущие буквы текста располагаются в столбцах сверху вниз):

С Э Т Ф Р Ч Ж Д С А И Ц С Я Т Т Ъ Х Т Т Т Х И Ф Ф О М Ы Н Э Д Г С Ф Г Ы И Д Т Ц М Т

Г Л Е Г Г Д Г Х Ю Р Щ С Е Ф Ф Х Г Х З Г Ф Т О Л И Ф Г Г Ф Л Е Г С Ц С И Т Б Л С П У
У Л П И Й К У Р Д В В Т В Б З Ж Ф Р В О Ф Т К Е П О Б У Н Л Н Н Е Е Ж О К У О Б З Ф
Ч З Н Н У О У Ъ Т Й Ч У Х Ь С З Б И Т Й Е Е З У Т К Т Ч Ш Ш К С У Е Н Н Ц Б Т Ю Т К
П Й Л Б Г Т М С П Г Э Ж А Б Э Б Щ П Ж Б О Г П Т Ь С Ж О З Р О Б П Е О Р Ь Т Б Й Ж Д
В Р Н О Л Х З Г Ъ Г Е В Х Е Ф З И Ж Й Н И И Т С М Х Ф Ю Г У Л К Н Г Е С Е Е Ф П П Г

Составим для каждой из 6 получившихся строк соответствующий ей набор частот встречаемости букв в каждой из них:

	А	Б	В	Г	Д	Е	Ж	З	и	И	к	л	м	н	О	п
1 строка	1	0	0	2	3	0	1	0	3	0	0	0	2	1	1	0
2 строка	0	1	0	9	1	3	0	1	2	0	0	4	0	0	1	1
3 строка	0	3	4	0	1	3	2	2	1	1	3	2	0	3	4	2
4 строка	0	2	0	0	0	4	0	3	1	2	3	0	0	4	1	0
5 строка	1	6	0	4	1	1	4	1	0	2	0	0	1	0	4	5
6 строка	0	0	2	5	0	5	1	2	3	1	1	2	1	3	1	2

	Р	С	Т	У	ф	Х	Ц	Ч	ш	щ	ъ	ы	ь	Э	Ю	Я
1 строка	1	4	8	0	4	2	2	1	0	0	1	2	0	2	0	1
2 строка	1	4	2	1	5	3	1	0	0	1	0	0	0	0	1	0
3 строка	2	0	2	4	3	0	0	0	0	0	0	0	0	0	0	0
4 строка	0	2	6	4	0	1	1	3	2	0	1	0	1	0	1	0
5 строка	2	2	2	0	0	0	0	0	0	1	0	0	2	2	0	0
6 строка	1	2	1	1	3	3	0	0	0	0	1	0	0	0	1	0

По этой таблице частот встречаемости букв вычислим для каждой строки соответствующий ей индекс совпадения:

Номер строки	1	2	3	4	5	6
Индекс совпадения	0,060	0,077	0,045	0,053	0,057	0,057

Для всего шифрованного текста индекс совпадения равен 0,040, что заметно меньше, чем индекс совпадения для каждой из указанных строк. Это является хорошим подтверждением гипотезы о длине периода гаммы.

Другие идеи подходов к вскрытию рассматриваемых шифров основаны на тех или иных особенностях их построения и использования, мы же с Вами рассмотрели самые основные.

Задачи для самостоятельного решения

1. Реализуйте на одном из языков программирования следующую задачу. В адрес олимпиады пришло зашифрованное сообщение:
   Ф В М Е Ж Т И В Ф Ю.
   Найдите исходное сообщение, если известно, что шифропреобразование заключалось в следующем. Пусть x_1, x_2-корни трехчлена x^2+3x+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(x)=x^6+3x^5+x^4+x^3+4x^2+4x+3$, вычисленное либо при $x=x_1$, либо при $x=x_2$ (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.
2. Реализуйте на одном из языков программирования следующую задачу. Знаменитый математик Леонард Эйлер в 1759 г. нашел маршрут обхода всех клеток шахматной доски ходом коня ровно по одному разу. Прочтите текст, вписанный в клетки шахматной доски по такому маршруту (см. рис.1.). Начало в а4.

Д	Л	Р	И	Л	П	Н	Б
У	К	А	Л	Т	У	С	Т
О	О	О	А	Н	О	И	Р
Т	Б	Г	К	Т	Т	У	К
К	О	Е	О	Р	А	В	О
К	Д	Г	П	В	Л	Е	Т
Т	А	Н	Р	М	А	Г	О
Е	А	О	В	И	Д	У	Л

3. Реализуйте на одном из языков программирования следующую задачу. Клетки квадрата 4 х 4 пронумеровали так, что клетка в правом нижнем углу получила номер 1, а все остальные получили разные номера от 2 до 16. Оказалось, что суммы номеров клеток каждой строки, каждого столбца, а также каждой из двух диагоналей квадрата одинаковы («магический» квадрат). Клетки квадрата заполнили буквами некоторого сообщения так, что его первая буква попала в клетку с номером – 1, вторая - в клетку с номером 2 и т.д. В результате построчного выписывания букв заполненного квадрата (слева направо и сверху вниз) получилась последовательность букв Ы Р Е У С Т Е В Ь Т А Б Е В К П . Восстановите магический квадрат и исходное сообщение.
4. Реализуйте на одном из языков программирования следующую задачу. Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

   Для зашифрования полученного числового сообщения используется шифрующий отрезок последовательности A_1, A_2, … подходящей дины, начинающийся с A_{100}.

При зашифровании каждое число числового сообщения складывается с соответствующим числом шифрующего отрезка. Затем вычисляется остаток от деления полученной суммы на 30, который по данной таблице заменяется буквой. Восстановите сообщение КЕНЗЭРЕ, если шифрующий отрезок взят из последовательности, у которой $A_1=3$ и $A_{k+1}=A_k+3(k^2+k+1)$, для любого натурального k.

Список рекомендуемой литературы

1. Аршинов М.Н., Садовский Л.Е. Коды и математика, -М., Наука, 1983.
2. Кушниренко А.Г. Кодирование чисел //Информатика. Приложение к «1 сентября» №23 1997.
3. Нечаев В.И. Элементы криптографии (основы теории защиты информации): учебное пособие для университетов и педвузов./Под ред. В.А. Садовничевого. - М.: Высш.шк., 1999.
4. Новиков Ф.А. Дискретная математика для программистов,- СПб: Питер, 2001.
5. Цикоза В.А., Чурина Т.Г. Методы программирования. Ч-1,-Новосибирск 1999.
6. Ященко В.В. Введение в криптографию,- СПб: Питер, 2001г.