

# «Мир информатики»

Журнал для тех, у кого информатика – любимый школьный предмет

Выпуск № 44, апрель 2020 г.

011000100010101001001111100100011001001000101001001001011

Криптография

## Простейшие методы шифрования текста. Часть 2 «Перестановочные шифры»<sup>1</sup>

Мы продолжаем описывать простейшие методы шифрования текстов.

*Шифрование перестановкой* заключается в том, что текста переставляются по определенному правилу. Простейшим примером перестановочного шифра являются так называемые «маршрутные перестановки», использующие некоторую геометрическую фигуру (плоскую или объемную). Шифрование заключается в том, что текст записывается в такую фигуру по некоторой траектории, а выписывается по другой траектории. Пример — маршрутные шифры перестановки, основанные на прямоугольниках (таблицах). Шифруемое сообщение в этом случае записывается в прямоугольную таблицу по маршруту: по горизонтали, начиная с верхнего левого угла, поочередно слева направо.

П	Р	И	М	Е	Р	М
А	Р	Ш	Р	У	Т	Н
О	Й	П	Е	Р	Е	С
Т	А	Н	О	В	К	И

Шифрованное сообщение записывается, например, по маршруту: по вертикалям, начиная с верхнего левого угла<sup>2</sup>, поочередно сверху вниз:

ПАОТРРЙАИШПНМРЕОЕУРВРТЕКМНСИ

Пример использования описанного метода шифрования — шифрование с помощью так называемой «скиталы». Скитала или скитала (от греч. σκῆταλη — «жезл») представляла собой палочка цилиндрической формы и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг палочки по спирали. Античные греки и спартанцы, предположительно, использовали этот шифр для обмена сообщениями во время военных кампаний, поэтому его называют также «шифр Древней Спарты».

Пергаментная лента наматывалась на палочку так, чтобы не было ни просветов, ни нахлестов. Написание сообщения производилось по намотанной пергаментной ленте вдоль палочки. После написания «строки», палочка поворачивалась на часть оборота и написание

<sup>1</sup> Часть 1 – см. журнал «Мир информатики», выпуск № 41, январь 2020 г.

<sup>2</sup> Можно и с правого верхнего угла.

сообщения продолжалось. После разматывания ленты на ней оказывалось зашифрованное сообщение. Расшифровка выполнялась с использованием палочки таких же размеров.



Скитала является официальным символом Американской ассоциации криптограмм



Например, если использовалась палочка, по длине окружности которой помещается 4 символа, а исходный текст для шифрования «ВСТРЕЧАОТМЕНЯЕТСЯ», то сначала на ленте вдоль палочки писали 5 букв: ВСТРЕ (почему в данном случае именно 5 букв – обсудим ниже), потом ниже (также вдоль) – еще 5 букв: ЧАОТМ, еще ниже – ЕНЯЕТ и затем оставшиеся буквы С и Я. В результате на ленте после её снятия с палочки будет написано:

ВЧЕССАНЯТОЯ\_РТЕ\_ЕМТ

(символ «\_» у нас соответствует «пробелу», одной пустой позиции).

Соответствующую «скиталу» можно схематически изобразить в виде таблицы с четырьмя строками и пятью столбцами:

В	С	Т	Р	Е
Ч	А	О	Т	М
Е	Н	Я	Е	Т
С	Я			

### Задание для самостоятельной работы

Зашифруйте методом Древней Спарты текст МНЕСРОЧНОНУЖЕНРАДИСТ, учитывая, что по длине окружности скиталы размещаются 5 букв.

Для шифрования текста с помощью программы или в среде электронной таблицы нам и надо научиться получать таблицу из букв исходного текста, аналогичную только что приведенной. Чем и займемся ☺.

Пронумеруем каждую букву шифруемого текста:

В	С	Т	Р	Е	Ч	А	О	Т	М	Е	Н	Я	Е	Т	С	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

а также строки и столбцы таблицы:

	1	2	3	4	5
1	В	С	Т	Р	Е
2	Ч	А	О	Т	М
3	Е	Н	Я	Е	Т
4	С	Я			

Запишем в полученную таблицу вместо букв их порядковые номера в шифруемом тексте:

	1	2	3	4	5
1	1	2	3	4	5
2	6	7	8	9	10
3	11	12	13	14	15
4	16	17			

Как записать перечисленные номера не «вручную», а с помощью одной формулы? Для этого надо получить зависимость номера буквы от номера строки *str* и номера столбца *stol*. Она такая:

$$n = (str - 1) \times 5 + stol \quad (1)$$

(Убедитесь в справедливости приведенной зависимости.)

А теперь по указанным номерам можно получить нужные буквы:

	1	2	3	4	5
1	В	С	Т	Р	Е
2	Ч	А	О	Т	М
3	Е	Н	Я	Е	Т
4	С	Я			

Именно такая методика заполнения таблицы будет использована при шифровании в статьях в рубриках «Школа программирования» и «Microsoft Excel углубленно».

Книжная полка

## Книга для подготовки к ЕГЭ по информатике

В издательстве ДМК-Пресс вышла книга Д.М. Златопольского «Подготовка к ЕГЭ по информатике в 2020 году. Решение задач по программированию».



Книга предназначена для подготовки учащихся к Единому государственному экзамену по информатике и ИКТ в части решения задач по программированию. Рассмотрена методика решения основных типовых задач, а также заданий из демонстрационных вариантов ЕГЭ (в том числе варианта 2020 года) и из пособий, написанных разработчиками контрольно-измерительных материалов по информатике.

Издание будет полезно также студентам вузов и колледжей, преподавателям информатики и другим читателям при изучении программирования вне связи с ЕГЭ.

С оглавлением книги и содержанием первой главы можно ознакомиться по адресу:

<https://dmkpress.com/files/PDF/978-5-97060-829-6.pdf>

## Ответы, решения, разъяснения

к заданиям, опубликованным в журнале «Мир информатики» № 40  
(декабрь 2019 г.)

### Задача «Четыре цепочки»

Напомним условие: «Четырем школьникам было дано задание сформировать цепочку из трех букв по следующим правилам. В конце цепочки может стоять одна из букв А, В или С, на первом месте — одна из букв С, D или Е, которой нет в середине, а в середине — одна из букв А, В, Е или D, не стоящая на последнем месте.

Мария составила такую цепочку АВА, Ренат — ССС, Татьяна — DAC, Арам — CDE. Кто из ребят составил цепочку, соответствующую все правилам?»

*Ответ:* Всем правилам соответствует цепочка DAC, то есть правильно задачу решила Татьяна.

### Четыре непростых ребуса с непростыми терминами

*Ответы*

Ребус № 1. ИСПОЛНИТЕЛЬ. Ребус № 2. ФОРМАЛИЗАЦИЯ. Ребус № 3. РЕКУРСИЯ.  
Ребус № 4. КОНКАТЕНАЦИЯ.

### Задание «Вопросы, вопросы...» (рубрика «Поиск информации»)

*Ответы*

1. Известная картина художника-реалиста XIX века Гюстава Курбе «Происхождение мира», которая больше века не показывалась публике, сейчас выставлена в музее Орсе.

2. Ювелирная фирма, создавшая бриллиантовое кольцо с рубином весом 8,24 карата, которое Элизабет Тейлор подарил на Рождество ее муж Ричард Бартон, — «Van Cleef & Arpels».

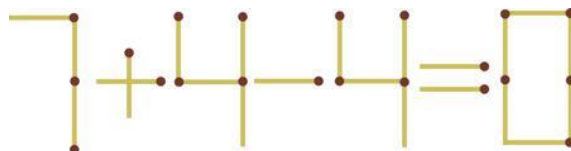
3. Американский киноактер Том Круз был лишь трижды номинирован (выдвинут) на премию «Оскар», но ни раз не был ею награжден.

4. Должность директора-распорядителя Международного валютного фонда с 2011 года занимала Кристин Лагард.

5. Десерт «Тарт Татен» назван так, в честь сестёр-француженок Стефани и Каролины Татен, придумавших рецепт его приготовления.

### Задача «Получить верное равенство»

Напомним, что требовалось, переложив всего одну спичку, сделать так, чтобы приведенное на рисунке ниже равенство стало верным.



*Решение*

Спичку из последней четверки переставить так, чтобы получилось число 11 — получим равенство  $7 + 4 - 11 = 0$ .

### Задача «Перестановка двойки»

Напомним условие: «Некоторое число оканчивается на 2. Если эту цифру перенести в начало числа, то оно удвоится. Найдите наименьшее такое число».

*Решение*

Так как при перестановке двойки в начало число удваивается, то последняя цифра полученного числа равна 4. В исходном числе цифра 4 — предпоследняя, а заканчивается оно на 42, то есть в числе после перестановки последние две цифры — 84. Дальнейшие расчеты удобно проводить с помощью такой таблицы:

Исходное число имеет вид	Число после перестановки имеет вид
*2	*4
*42	*84
*842	*684
*6842	*3684
...	...
*157894736842	*215789473684

где символом обозначена некоторая последовательность цифр.

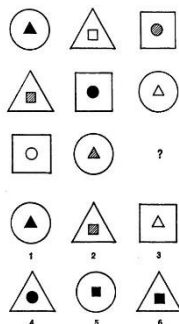
**Внимание!** Получено число, начинающееся с двойки. Означает ли это, что искомое число 157894736842 и надо прекратить расчеты? Или следует их продолжить?

...	...
*5263157894736842	*10526315789473684
105263157894736842	210526315789473684

Какое из чисел — 157894736842 или 105263157894736842 — является искомым?

### Головоломка «Выбрать фигуру»

Напомним, что требовалось из шести пронумерованных фигур выбрать ту, которая должна стоять на месте вопросительного знака:



*Решение*

Фигуры на рисунке состоят из двух частей: «внешней» и «внутренней», каждая из которых является окружностью, треугольником или квадратом, и при этом «внутренняя» часть может иметь 3 вида заливки. В каждой из фигур в каждом ряду эти характеристики фигур не совпадают.

Это значит, что на месте вопросительного знака должна быть фигура, которой:

- 1) «внешняя» часть — треугольник;
  - 2) «внутренняя» часть — квадрат, заливка которого должна быть сплошной черной.
- Из пронумерованных такими свойствами обладает фигура 6.

### Задача «Волейбольный турнир»

Напомним условие: «Команды четырех школ участвовали в турнире по волейболу. Болельщики поделились своими прогнозами:

- 1) 1-й болельщик: «Победит 556-я школа, а 450-я будет второй»;

- 2) 2-й болельщик: «Нет, 556-я будет последней», а победит 324-я»;
- 3) 3-й болельщик: «Уверен, что первой будет 445-я школа», а 450-я будет третьей».

Когда соревнования закончились, выяснилось, что каждый болельщик был неправ в одном из своих прогнозов. Какое место заняла каждая из команд?»

*Решение*

Допустим, что прогноз 1-го болельщика: «Победит 556-я школа» — верный. Тогда получается, что оба прогноза 2-го болельщика — ошибочные, чего быть не может. Значит, верным является второй прогноз 1-го болельщика, то есть второе место заняла команда школы № 450.

После этого анализ прогнозов 3-го болельщика показывает, что его первый прогноз — верный, то есть в турнире победила команда школы № 445, а анализ прогнозов 2-го болельщика — что школа № 556 в итоге действительно оказалась последней.

Третье место заняла команда школы № 324.

**Задача «Перекодировка»**

Напомним условие: «Автоматическое устройство осуществило перекодировку двух информационных сообщений равной длины из 8-битной кодировки ASCII в одно общее в 16-битной кодировке Unicode. Информационный объем нового сообщения в результате стал больше общего объема исходных на 240 байт. Какова длина каждого из исходных сообщений в символах?»

*Решение*

Пусть искомая длина каждого из исходных сообщений в символах равна  $x$ . Их общая длина —  $2x$ . При 8-битной кодировке общий информационный объем исходных сообщений составлял  $2x \cdot 8/8 = 2x$  байт, а информационный объем нового сообщения при 16-битной кодировке —  $2x \cdot 16/8 = 4x$ , то есть увеличился на  $2x$  байт. По условию соответствующее увеличение равно 240 байт. Это значит, что  $x = 120$ .

*Ответ:* 120 символов.

**Числовые ребусы в пятеричной системе счисления. Часть 3**

*Ответы*

<i>Ребус № 7</i>	$\begin{array}{r} 2\ 2 \\ +\ 3\ 3 \\ \hline 1\ 1\ 0 \end{array}$
<i>Ребус № 8</i>	$\begin{array}{r} 2\ 2 \\ +\ 4\ 4 \\ \hline 1\ 2\ 1 \end{array}$
<i>Ребус № 9</i>	$\begin{array}{r} 4\ 4 \\ +\ 3\ 3 \\ \hline 1\ 3\ 2 \end{array}$

**Задания, предложенные для самостоятельной работы в статье «Задания 21 ЕГЭ по информатике»**

Напомним, что были предложены задания, связанные с определением таких значений аргумента трех функций, при которых последние имеют минимум:

- 1) функции  $F = 16(x - 8)(x - 8)$  на отрезке  $a := 10; b := 10$
- 2) функции  $F = 2(x^2 - 25)(x^2 - 25) + 5$  на отрезке  $a := 11; b := 11$
- 3) функции  $F = \text{abs}(\text{abs}(x - 1) + \text{abs}(x + 1) - 10) + 25$  на отрезке  $a := -15; b := 15$

### Решение

Проанализируем заданные функции.

В первой функции её значения представляют собой квадраты некоторых значений, увеличенные в 16 раз. Так как квадрат числа не может быть отрицательным, то минимум функции может быть нулевым или положительным. Проверим сначала на равенство минимума нулю. Это может быть при  $x = 8$ . Значит, искомое значение аргумента равно 8.

Аналогично для второй функции минимальное значение достигается при аргументах  $x$ , при которых  $(x^2 - 25)^2 = 0$ . Таких значений — два:  $-5$  и  $5$ . Если в программе указано строгое неравенство, то ответом является минимальное значение аргумента ( $-5$ ), если нестрогое — максимальное ( $5$ ).

анализе третьей функции следует учесть, что абсолютная величина выражения не может быть отрицательной. Следовательно, функция имеет минимумы при тех значениях  $x$ , при которых справедливо неравенство  $|x - 1| + |x + 1| - 10 \geq 0$ .

Исследование равенства  $|x - 1| + |x + 1| - 10 = 0$  показывает, что оно возможно при  $x = -5$  и при  $x = 5$  (значение функции, которое также используется в ответе, в обоих случаях равно 25). Итак, ответ:

— при строгом неравенстве в программе:  $-5 + 25 = 20$ ;

— при нестрогом неравенстве:  $5 + 25 = 30$ .

### Шестеро друзей в буфете

Напомним условие: «Шестеро друзей в ожидании электрички зашли в буфет. Маша взяла то же, что и Егор, и вдобавок ещё бутерброд с сыром. Аня купила, то же, что и Саша, но не стала покупать шоколадное печенье. Кирилл ел то же, что и Мила, но без луковых чипсов. Егор завтракал тем же что и Аня, но бутерброду с котлетой предпочел картофельные чипсы. Саша ел то же, что и Мила, но вместо молочного коктейля пил лимонад. Из чего состоял завтрак каждого из друзей?»

*Ответ* (задача решается табличным методом):

Аня – ела луковые чипсы, лимонад и бутерброд с котлетой;

Егор – луковые чипсы, лимонад и картофельные чипсы;

Кирилл – шоколадное печенье, молочный коктейль и бутерброд с котлетой;

Маша – бутерброд с сыром, луковые чипсы, лимонад и картофельные чипсы;

Мила – шоколадное печенье, луковые чипсы, молочный коктейль и бутерброд с котлетой.

Саша – шоколадное печенье, луковые чипсы, лимонад и бутерброд с котлетой;

### Задача «Фальшивая гирька»

Напомним условие: «Имеются 6 гирек массой 1, 2, 3, 4, 5 и 6 г. На них нанесена соответствующая маркировка. Однако есть основания считать, что при маркировке гирь допущена одна ошибка. Как при помощи двух взвешиваний на чашечных весах, на которых можно сравнить веса любых групп гирь, определить, верна ли имеющаяся на гирях маркировка?»

### Решение

На одну чашу весов кладем гири, маркированные 1 и 6 г, а на другую — 2 и 5 г. Если весы не будут в равновесии, то маркировка на гирьках — неверна («фальшивая» гирька — среди четырех рассмотренных). Если же весы окажутся в равновесии, то возможная «фальшивая» гирька — среди двух оставшихся.

Вторым взвешиванием сравниваем две оставшиеся гирьки (на одной чаше весов) и, например, гири, маркированные 1 и 6 г. Если весы будут в равновесии — маркировка правильная, если нет, то неправильная.

## Более сложная задача

Имеются 6 гирек массой 1, 2, 3, 4, 5 и 6 г. На них нанесена соответствующая маркировка, но по виду они все одинаковые. Есть основания считать, что при маркировке гирь допущена одна ошибка. За какое минимальное число взвешиваний на чашечных весах, на которых можно сравнить веса любых групп гирь, можно определить, верна ли имеющаяся на гирях маркировка и, если неверна, установить, какая из гирек маркирована неправильно?

### Ответы и решения представили:

— Абдувахидова Алина, Абдувахидова Софья, Камышанская Анастасия, Куклева Анастасия, Куклева Лидия, Лебедев Сергей, Лефтеров Влад, Смирнова Полина и Хозин Марат, Владимирская обл., г. Струнино, школа № 11, учитель **Волков Ю.П.**;

— Борисов Сергей (ученик 5-го класса!), Деревницкий Никита, Приезжева Ирина и Свинаярева Маргарита, г. Рязань, школа № 44, учитель **Марцинкевич Е.Е.**;

— Боровиков Иван, Костюк Максим, Кравец Сергей и Фунтиков Роман, г. Пенза, школа № 73, учитель **Диков А.В.**;

— Великородных Светлана и Королёва Марина, средняя школа села Восточное Нижегородской обл., учитель **Долгова Г.А.**;

— Германов Данил, Республика Карелия, Сегежский р-н, поселок Надвоицы, школа № 1, учитель **Каликина Т.В.**;

— Серякова Елена, Фомин Никита и Шаяхметов Булат, Республика Башкортостан, г. Стерлитамак, гимназия № 4, учитель **Орлова Е.В.**;

— Торопов Александр, Филимонова Надежда и Юмашев Сергей, средняя школа деревни Муравьево, Вологодская обл., учитель **Муравьева О.В.**

Читатели, приславшие наибольшее число правильных ответов, будут награждены дипломами. Поздравляем всех!

Решение задач и головоломок, опубликованных в ноябрьском выпуске журнала «Мир информатики», прислали также учащиеся школы № 44 г. Рязани (учитель **Марцинкевич Е.Е.**):

— Агапкин Владимир и Ионов Александр (решение задач «На катке» и «Расположить ребят по росту»);

— Приезжева Ирина и Свинаярева Маргарита (решение ребусов).

Данил Германов, Республика Карелия, Сегежский р-н, поселок Надвоицы, школа № 1, (учитель **Каликина Т.В.**) прислал также ответы на задания на поиск информации, предложенные в ноябрьском выпуске журнала «Мир информатики».

---

## Двоичное число

Про некоторое двоичное число известно, что в нем:

1) не более 40 цифр;

2) цифры чередуются;

3) количество одной из цифр составляет ровно 52% общего числа цифр.

Найдите это число и его десятичный эквивалент.

В части нахождения двоичного числа задачу целесообразно решить методом рассуждений. В виде исключения допускается также использование электронной таблицы Microsoft Excel или подобной программы.



## Исполнитель У2П1<sup>3</sup>

В системе команд исполнителя У2П1 две команды:

1. Умножь на 2.
2. Прибавь 1.

Сколько возможно вариантов программы решения задачи получения числа 10 из числа 1?

В каком из них меньше всего команд?

В какой программе ровно 7 команд?

## Задача “Четыре девочки”<sup>4</sup>

На улице, став в кружок, беседуют Аня, Валя, Галя и Надя. Девочка в зелёном платье (не Аня и не Валя) стоит между девочкой в голубом платье и Надей. Девочка в белом платье стоит между девочкой в розовом платье и Валею. Какое платье носит каждая из девочек?”

Для эрудитов

## Викторина “Рыба, триатлон и динозавры”

Выберите один правильный ответ из трех предложенных к каждому вопросу.

1. Китайские кулинары придумали способ избавлять свежую рыбу от запахов ила. Для начала они промывают тушку рыбы ледяной водой, а после, вытерев ее насухо, кладут ей на брюхо на пару часов особую начинку. Какую?

- А. Имбирь.
- Б. Лимон.
- В. Киви.

2. Первенство по триатлону “Железный человек” впервые разыграли на Гавайях в 1978 году. Каждый из его участников должен был проплыть 4 км, проехать на мотоцикле 180 км и пробежать определенную дистанцию. Какова была дистанция?

- А. 10 км.
- Б. Марафон.
- В. 30 км.

3. Девять видов динозавров из фильма “Парк Юрского периода” с ревом и топотом пронеслись по экранам мира в 90-х годах прошлого века. Сделанные из губчатой резины, они выглядели абсолютно реалистично. Один из них стал самым большим роботом, когда-либо созданным для съемок фильма. Что это за ящер?

- А. Раптор.
- Б. Тираннозавр
- В. Дилофозавр.

По материалам “Российской газеты”

Ответы (можно не на все вопросы присылайте в редакцию).

<sup>3</sup> Эта задача была опубликована в декабрьском выпуске нашего журнала. На один из заданных в ней вопросов ответ представил Деревницкий Никита, г. Рязань, школа № 44, учитель **Марцинкевич Е.Е.**

<sup>4</sup> Задача предназначена для учащихся 1–7-х классов.

## Шифруем текст методом перестановки, разработав программу

Опишем методику разработки программ для шифрования текста методом маршрутной перестановки, описанным в рубрике «Криптография» в этом выпуске журнала.

Основные этапы алгоритма шифрования:

1. Ввод текста для шифрования
2. Заполнение таблицы с буквами исходного текста
3. Формирование шифротекста (зашифрованного сообщения)
3. Вывод шифротекста

Примем для простоты, что шифруется текст из 20 символов, а ключ шифрования (количество строк в таблице с буквами) равен 4. Это значит, что двумерный массив для хранения отдельных символов исходного текста (пусть его имя — `таблица`) описывается так:

```
таблица[1 : 4, 1 : 5]
```

Используем в программе также следующие переменные величины:

`текст` — исходный текст;

`шифр_текст` — зашифрованный текст;

`номер_буквы` — номер буквы исходного текста, записываемый в тот или иной элемент массива `таблица`;

`стр` — номер строки массива `таблица`;

`стол` — то же, столбца.

Прежде чем представлять программу, напомним, что:

1) обратиться к отдельному символу величины строкового типа (в нашем случае — заданного текста) можно, указав имя величины и в квадратных скобках — номер соответствующего символа;

2) обратиться к значению элемента двумерного массива строкового типа (в нашем случае — массива `таблица`) можно, указав имя массива и в квадратных скобках — номер строки и номер столбца, в которых находится данный элемент;

3) величины строкового типа, в том числе отдельные символы можно «склеивать» («сцеплять») друг с другом с помощью знака `+`.

Итак, программа:

**алг**

**нач лит** `текст`, `шифр_текст`, **сим таб** `таблица`[1 : 4, 1 : 5]

**цел** `стр`, `стол`, `номер_буквы`

**вывод нс**, "Введите текст для шифрования "

**ввод** `текст`

| Заполняем таблицу

**нц для** `стр` **от** 1 **до** 4 | Для каждой строки,

**нц для** `стол` **от** 1 **до** 5 | а в ней — для каждого столбца

| Определяем номер буквы,

| которая будет записана в данную ячейку таблицы

| (см. первую статью данного выпуска журнала)

`номер_буквы` := (`стр` - 1) \* 5 + `стол`

| Записываем соответствующую букву исходного текста

`таблица`[`стр`, `стол`] := `текст`[`номер_буквы`]

**кц**

**кц**

```

| Выводим таблицу
| (только при отладке – для контроля правильности программы)
нц для стр от 1 до 4
  вывод нс
  нц для стол от 1 до 5
    вывод таблица[стр, стол]
  кц
кц
| Формируем шифровку
шифр_текст := "" | Начальное значение
нц для стол от 1 до 5 | Здесь сначала перебираем все столбцы,
  нц для стр от 1 до 4 | а затем – строки
    шифр_текст := шифр_текст + таблица[стр, стол]
  кц
кц
| Выводим её
вывод нс, шифр_текст
кон

```

### Задания для самостоятельной работы

1. Разработайте программы (на языке программирования, который изучаете) для шифрования текста методом маршрутной перестановки и зашифруйте с её помощью текст:

МИРИНФОРМАТИКИЭТООЧЕНЬХОРОШИЙЖУРНАЛ

Ключ шифрования (количество строк в таблице с буквами) примите равным 5.

2. Опишите алгоритм расшифровки текста, зашифрованного описанным в статье методом, или/и разработайте соответствующую программу. При этом примите, что длина зашифрованного текста кратна ключу шифрования.

Книжная полка

## Сборник задач по программированию

В издательстве ДМК-Пресс вышла книга Д.М. Златопольского «1400 задач по программированию».



В книге приведено более 1400 задач по программированию. Задачи имеют разный уровень сложности и охватывают большой круг тем. Они не привязаны к конкретному языку программирования и могут быть решены в программе на любом языке (Паскаль, Python, Си, школьном алгоритмическом языке и т. д.).

Издание будет полезно как читателям, изучающим программирование самостоятельно, так и преподавателям школ, колледжей и вузов. В последнем случае задачи могут быть использованы при объяснении нового материала, для организации самостоятельной работы учащихся и проведения контрольных мероприятий. Ряд задач предназначен для внутришкольных олимпиад, для использования в кружках по программированию и т. п.

## Четыре ребуса

Решите, пожалуйста, ребусы.

Ребус № 1



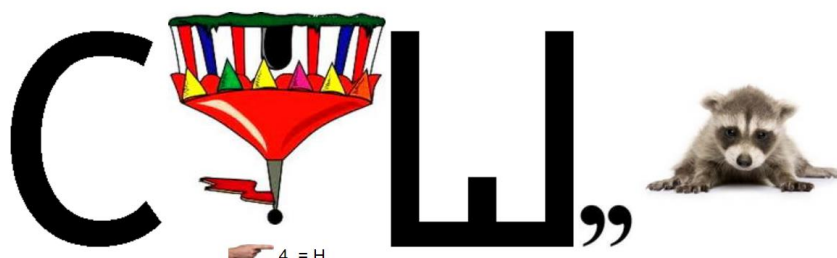
Ребус № 2



Ребус № 3



Ребус № 4



## Числовые ребусы в пятеричной системе счисления. Часть 6

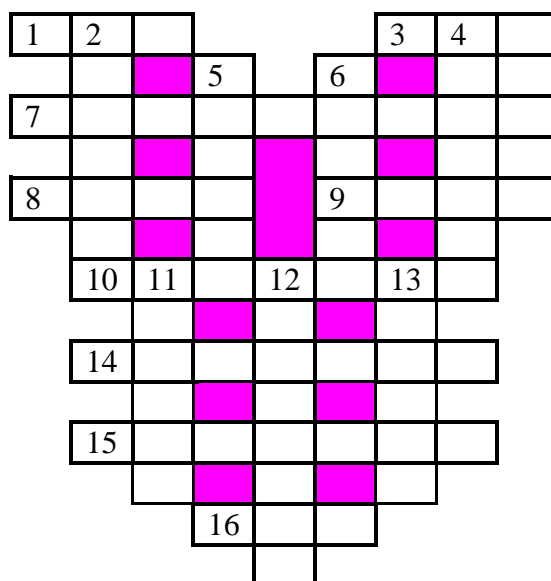
Решите ребусы с числами, записанными в пятеричной системе счисления (редакция использует сквозную нумерацию ребусов).

Ребус № 16	$\begin{array}{r} + \quad Y \quad Y \\ \quad X \quad Y \\ \hline Z \quad Z \quad Z \end{array}$	Ребус № 17	$\begin{array}{r} + \quad A \quad A \\ \quad B \quad A \\ \hline C \quad B \quad D \end{array}$	Ребус № 18	$\begin{array}{r} + \quad E \quad E \\ \quad F \quad E \\ \hline * \quad F \quad F \end{array}$
------------	---	------------	---	------------	---

Как обычно принято в таких головоломках, одинаковые цифры представлены одинаковыми буквами, а различные цифры — разными буквами. В разных ребусах одна и та же буква может соответствовать разным цифрам. Звездочка (\*) может быть любой цифрой.

## Кроссворд

Решите, пожалуйста, кроссворд. При необходимости найдите требуемую информацию в Интернете или по другим источникам.



### *По горизонтали*

1. Цифра пятеричной системы счисления.
3. Название буквы древнерусского алфавита, напоминающей твердый знак.
7. Создание резервных копий файла.
8. Знак препинания.
9. Первый отечественный электронный калькулятор.
10. Устройство, осуществляющее преобразование представления и скорости передачи информации между ЭВМ и внешним устройством.
14. Листок бумаги с записью, коротенькое письмо.
15. Место расположения символа на экране.
16. В программировании — характеристика величины, определяющая множество её допустимых значений и применимых к ней операций.

### *По вертикали*

2. Точка графа или место в стеке.
4. Электронная схема, применяемая в регистрах компьютера для запоминания одного бита информации.
5. Символ, знак.
6. Использование ресурсов одним процессом с запрещением обращений к нему из других процессов.
11. Форма взаимодействия пользователя с компьютером.
12. Так называют простейший графический объект, например, линию, эллипс и т.п.
13. Дневнегреческий математик, автор алгоритма нахождения наибольшего общего делителя двух натуральных чисел.

## Кто на каком инструменте играет?

Два мальчика умеют играть на гитаре, а еще один — на балалайке. На чем играет Андрей, если Максим и Павел играют на разных инструментах, а Павел и Андрей — тоже?

Задача предназначена для учеников начальной школы.

### **Литература**

1. Богомолова О.Б. Логические задачи. М. БИНОМ. Лаборатория знаний, 2005.

## Шифруем текст в среде электронной таблицы. Часть 2 «Перестановочный шифр»<sup>5</sup>

Д.М. Златопольский

Опишем методику шифрования текста методом, рассмотренным в рубрике «Криптография», с помощью электронной таблицы Microsoft Excel.

Для этого нам понадобится ряд функций, которые имеются в программе.

### Функция ЕСЛИ

Она используется, когда в ячейке могут быть выведены два значения в зависимости от некоторого условия: первое значение, если указанное в ней условие истинное, и второе — если ложное. Например, функция:

ЕСЛИ(A1>10, "Больше 10", "10 или меньше")

возвращает строку "Больше 10", если значение в ячейке A1 больше 10, и "10 или меньше", если оно меньше или равно 10.

Общий вид функции:

ЕСЛИ(<условие>; <значение\_1>; <значение\_2>)

В простейшем случае аргумент <условие> — это сравнение конкретных значений (чисел, текста и др.), адресов ячеек и выражений с использованием знаков "=", ">", ">=", "<", "<=" и "<>".

A10 = 100  
B12 < B11  
B12 + B13 <> 0  
C44 = "яблоки"  
D10 + D11 <= E10 + E11

Если <условие> — истинное, то в ячейке с функцией ЕСЛИ будет отображен второй аргумент (<значение\_1>) если ложное — третий аргумент (<значение\_2>).

В качестве второго и/или третьего аргумента, в свою очередь, может быть также записана функция ЕСЛИ:

=ЕСЛИ(B1>B2,"Больше первое число",ЕСЛИ(B1<B2;"Больше второе число";"Числа равны))

### Функция И

Эта функция возвращает результат проверки двух условий:

И(<условие1>; <условие2>)

Примеры

И(D12>F12; A15<0)  
И(\$N\$12>M\$12; P15<=Q15)

Результат определяется по правилам определения результата операции конъюнкции.

<sup>5</sup> Часть 1 – см. журнал «Мир информатики», выпуск № 41, январь 2020 г.

## Функция ПСТР<sup>6</sup>

Эта функция возвращает заданное число знаков из текстовой строки, начиная с указанной позиции. Ее общий вид:

ПСТР(<текст>;<начальная\_позиция>;<число\_символов>)

Аргумент <текст> это текстовая строка, содержащая символы, которые требуется получить. Это может быть конкретный текст, адрес ячейки с текстом, функция, возвращающая текст или указанные элементы, соединенные знаком «склейки» &.

Аргумент <начальная\_позиция> это номер первого из символов, которые нужно получить символы (первый знак в тексте имеет номер 1 и так далее).

Аргумент <число\_символов> указывает, сколько символов должна вернуть функция ПСТР.

Двумя последними аргументами могут быть конкретные числа, адреса ячеек с числами и т.п.

Значения всех трех аргументов должны быть обязательно указаны.

Например, если в ячейке записано слово «Информатика», то для получения в ячейке слова «форма»:

A	B	C
1	Информатика	
2		
3		

в ней следует записать:

=ПСТР(B1; 3; 5)

Конечно, можно получить и один символ.

## Функция ПОИСК

Ее общий вид:

ПОИСК(<что\_ищем>;<где\_ищем>)

Эта функция находит одну текстовую строку (<что\_ищем>) в другой (<где\_ищем>) и возвращают начальную позицию первой текстовой строки (считая от первого символа второй текстовой строки). Например, чтобы определить позицию буквы "н" в слове "принтер", следует так оформить функцию:

=ПОИСК("н";"принтер")

Функция вернет значение 4, так как "н" является четвертым символом в слове "принтер".

Обратим внимание на одну особенность (странную! — ☺) функции ПОИСК. Если в качестве искомой строки (<что\_ищем>) указать «пустой» символ (""), которого, естественно, в заданной строке нет, то функция вернет ... 1 (!?).

Напомним также о так называемых «относительной», «абсолютной» и «смешанной/комбинированной» ссылках, используемых в формулах.

Если в формуле адрес ячейки с нужным значением записан в виде B13 (буква столбца и номер строки), то такая ссылка на значение называется «относительной». При копировании этой формулы в ячейку выше или ниже номер строки в ссылке увеличится или уменьшится на

---

<sup>6</sup> Имя функции происходит от слова «подстрока» — часть строки символов.

соответствующее «смещение». Аналогично при копировании формулы в ячейку правее или левее соответствующим образом изменится буква столбца. Конечно, могут меняться обе «координаты» адреса.

Но часто нужно, чтобы при копировании адрес используемой ячейки не менялся. В таких случаях в формуле записывается абсолютная ссылка. Она выглядит так:  $\$B\$13$ .

Кроме того, возможны случаи, когда при копировании буква столбца менялась, а номер строки — нет. Для этого записывается так называемая «смешанная» (или «комбинированная») ссылка:  $B\$13$ .

Такой вариант «смешанной» ссылки:  $\$B13$  — обеспечивает изменение только номера строки адреса<sup>7</sup>.

И ещё. Для «сложения», «склейки» двух и более текстов (в том числе отдельных символов) в электронных таблицах используется знак «&»:

$=B33&B34$

$=A3+"Д"$

Теперь можем приступить к оформлению листа для шифрования.

Сначала примем, что размер таблицы, с помощью которой происходит шифрование (см. рубрику «Криптография»), известен. Пусть её размеры — 4 строки и 5 столбцов. Маршрут шифрования примем таким, как в статье.

Верхняя часть листа показана ниже:

	A	B	C	D	E	F	G	...
1	<b>Шифрование текста маршрутной перестановкой</b>							
2	Исходный текст							
3	Ключ шифрования (кол-во строк таблицы)	4						
4	Зашифрованный текст							
5								

Шифруемый текст вводится в ячейку B2, зашифрованный — выводится в ячейке B4. В ячейке B3 запишем ключ шифрования<sup>8</sup>, в качестве которого примем количество строк таблицы.

Пусть текст для шифрования такой: МНЕСРОЧНОНУЖЕНРАДИСТ.

Напомним, что для шифрования надо получить таблицу из букв исходного текста:

М	Н	Е	С	Р
О	Ч	Н	О	Н
У	Ж	Е	Н	Р
А	Д	И	С	Т

О том, как это сделать, рассказано в первой статье данного выпуска.

<sup>7</sup> Можно запомнить такое правило: символ «\$» в адресе как бы фиксирует «координату» адреса, перед которой он стоит.

<sup>8</sup> Ключ шифрования — число или текст, знание которого позволяет провести шифрование или/шифрование.



Все вспомогательные расчеты проведем вне зоны видимости листа:

1) в ячейку B52 запишем количество столбцов (в данном случае оно известно):

	A	B	C	D	E	F	G	...
...								
52	Количество столбцов	5						
53								

2) в таблицу 4 на 5 записываются номера букв шифруемого текста:

	A	B	C	D	E	F	G	...
...								
54		Номер столбца						
55	Номер строки	1	2	3	4	5		
56	1	1	2	3	4	5	Номера	
57	2	6	7	8	9	10	букв	
58	3	11	12	13	14	15	исходного	
59	4	16	17	18	19	20	текста	
60								

Их можно получить по формуле (1). При этом в формуле не забудьте использовать абсолютную и комбинированную (смешанную) ссылки.

3) определяются соответствующие буквы:

	A	B	C	D	E	F	G	...
...								
61		М	Н	Е	С	Р		
62		О	Ч	Н	О	Н		
63		У	Ж	Е	Н	Р		
64		А	Д	И	С	Т		
65								

Здесь используется функция ПСТР.

4) формируется текст в каждом из пяти столбцов (с использованием знака &):

	A	B	C	D	E	F	G	...
...								
63		У	Ж	Е	Н	Р		
64		А	Д	И	С	Т		
65								
66	Текст в столбце	МОУА	НЧЖД	ЕНЕИ	СОНС	РНРТ		
67								

Зашифрованный текст в ячейке B4 также получается с использованием указанного знака.

### Задание для самостоятельной работы

Оформите листы электронной таблицы:

- 1) для шифрования текста описанным методом с использованием таблицы из четырех строк и пяти столбцов при длине текста — 20 букв;
- 2) для расшифровки текста, зашифрованного этим методом;

3) для шифрования текста описанным методом с использованием таблицы из шести строк и четырех столбцов при длине текста 24 буквы.

Указания по выполнению задания 2

1. В верхней части листа указывается все тот же ключ шифрования:

	A	B	C	D	E	F	G	...
1	<b>Расшифровка текста (маршрутная перестановка)</b>							
2	Зашифрованный текст	МОУАНЧЖДЕНЕИСОНСРНРТ						
3	Ключ шифрования (кол-во строк таблицы)	4						
4	Исходный текст	МНЕСРОЧНОНУЖЕНРАДИСТ						
5								

2. Таблицы со вспомогательными расчетами должны быть такими

	A	B	C	D	E	F
...						
52	Количество строк в таблице расшифровки	5				
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						

*Номер столбца*

<i>Номер строки</i>	1	2	3	4
1	1	2	3	4
2	5	6	7	8
3	9	10	11	12
4	13	14	15	16
5	17	18	19	20

М	О	У	А
Н	Ч	Ж	Д
Е	Н	Е	И
С	О	Н	С
Р	Н	Р	Т

МНЕСР ОЧНОН УЖЕНР АДИСТ

то есть количество строк (в ячейке B52) и количество столбцов в них представляют собой значения, соответственно, количество столбцов и количество строк таблицы, использовавшейся при шифровании.

Внимательный читатель, конечно, обнаружил, что в приведенных примерах общее количество букв в шифруемом тексте равно произведению количества строк на количество столбцов в используемой таблице.

Теперь рассмотрим вариант, когда это не так:

	A	B	C	D	E	F	G	...
1	<b>Шифрование текста маршрутной перестановкой</b>							
2	Исходный текст	СРОЧНОНУЖЕНРАДИСТ						
3	Ключ шифрования (кол-во строк таблицы)	4						
4	Зашифрованный текст							
5								



Для этого в формуле надо использовать функцию ЕСЛИ (условие в ней установите самостоятельно).

В результате шифрованный текст примет вид:

	A	B	C	D	E	F	G	...	
1	<b>Шифрование текста маршрутной перестановкой</b>								
2	Исходный текст	СРОЧНОНУЖЕНРАДИСТ							
3	Ключ шифрования (кол-во строк таблицы)	4							
4	Зашифрованный текст	СОНСРНРТОУА ЧЖД НЕИ							
5									

а его расшифровка даст правильный результат.

### Небольшое отступление

В ряде книг по криптографии (например, в [2]) говорится о том, что заполнять последнюю строку таблицы пробелами (или другими символами) нецелесообразно. В качестве довода указывается, что, если противник получит в свое распоряжение такой зашифрованный текст, это даст ему информацию о размере ключа для расшифровки. В самом деле, в этом случае длину ключа следует искать среди делителей общей длины сообщения. Но такой подбор ключа можно сделать в любом случае, что мы покажем ниже.

### Задание для самостоятельной работы

Оформите листы электронной таблицы:

- 1) для шифрования текста описанным методом с использованием таблицы из четырех строк и пяти столбцов при длине текста — не более 20 букв;
- 2) для расшифровки текста, зашифрованного этим методом.

Мы описали лист для варианта шифрования, при котором длина ключа заранее известна. Давайте обсудим общий случай, когда она вводится на лист в момент шифрования.

	A	B	C	D	E	F	G	...
1	<b>Шифрование текста маршрутной перестановкой</b>							
2	Исходный текст							
3	Ключ шифрования (кол-во строк таблицы)							
4	Зашифрованный текст							
5								

Примем, что размер ключа шифрования (количество строк) и количество столбцов используемой таблицы не превышает 10.

Алгоритм действий следующий.

1. В ячейку B52 записывается количество столбцов:

	A	B	C	D	E	F	G	...
...								
52	Количество столбцов							
53								

В данном случае оно неизвестно и зависит от общего числа букв в сообщении и от количества строк. Но как?

Вспомним таблицу, которая уже использовалась:

	1	2	3	4	5
1	1	2	3	4	5
2	6	7	8	9	10

3	11	12	13	14	15
4	16	17	18	19	20

На её основе можно составить такую:

Общее число букв в шифруемом текст, $V$	Количество столбцов, $S$
8	2
9	3
10	3
11	3
12	3
13	4
14	4
15	4
16	4
17	5

А из неё можно такую установить зависимость количества столбцов  $S$  от общего числа букв в шифруемом тексте  $V$  (для четырех строк таблицы):

$$S = [(V - 1)/4] + 1$$

или

$$S = [(V + 3)/4]$$

где  $[]$  – соответствует целой части частного (убедитесь и в этом!).

Это для случая, когда в таблице 4 строки.

В общем случае, когда количество строк таблицы (ключ шифрования) равно  $k$ , количество столбцов равно:

$$S = [(V - 1)/k] + 1 \quad (2)$$

или

$$S = [(V + k - 1)/k] \quad (3)$$

Одна из таких формул и записывается в ячейку B52. Напомним, что в программе Microsoft Excel целочисленное частное можно получить с помощью функции ЦЕЛОЕ.

2. В таблицу размером 10 на 10 записываются номера строк и столбцов:

	A	B	C	D	...	K	L	
...								
54		<i>Номер столбца</i>						
55	<i>Номер строки</i>	1	2	3	...	10		
56	1	1	2	3				
57	2	4	5	6				
...								
65	10							
60								

3. В ячейки диапазона B56:K65 записываются номера букв шифруемого текста, но только в те, для которых номера строки и столбца не превышают количество строк в ячейках B3 и B52, соответственно. То есть в функции ЕСЛИ условие для записи номера такое:

$$\text{И}(\$A65 \leq \$B\$3; K\$55 \leq \$B\$52)$$

(Сами номера, как и ранее, рассчитываются по формуле (1).) Если указанное условие не соблюдается, записывается «пустой» символ.

4. Записываются отдельные буквы сообщения:

	A	B	C	D	...	K
...						
67	1	С	Р	О		
68	2	Ч	Н	О		
69	3	Н	У	Ж		
70	4	Е	Н	Р		
71	5	А	Д	И		
72	6	С	Т			
73	7					
...						
76	10					

Здесь логика такая:

**если** номер строки не больше значения в ячейке В3  
и номер столбца не больше значения в ячейке В52  
**то** | Записываем либо букву, либо пробел

...

**иначе**

записываем «пустой» символ

**все**

Это означает, что «базовая» для копирования на 100 ячеек формула в ячейке В56 такая:

=ЕСЛИ(И(\$A56<=\$B\$3;B\$55<=\$B\$52); ЕСЛИ(B56<=ДЛСТР(\$B\$2); ПСТР(\$B\$2;B56;1);" ");"")

Дальнейшие действия по шифрованию определите самостоятельно. При этом имейте в виду, что в каждом из 10 столбцов следует «склеивать» 10 значений (от 67-й строки до 76-й), а все зашифрованное сообщение получается путем «склейки» значений (в том числе возможных «пустых») в столбцах от В до К.

### Задание для самостоятельной работы

Оформите листы электронной таблицы:

- 1) для шифрования текста описанным методом с использованием таблицы из 10 строк и 10 столбцов при длине текста — не более 100 букв;
- 2) для расшифровки текста, зашифрованного этим методом;

Указания по выполнению задания 2

1. В верхней части листа ключ шифрования может быть любым (не более 10):

	A	B	C	D	E	F	G	...
1	<b>Расшифровка текста (маршрутная перестановка)</b>							
2	Зашифрованный текст							
3	Ключ шифрования (кол-во строк таблицы)							
4	Исходный текст							
5								

2. Количество строк в таблице расшифровки (в ячейке В52) определяется по формуле:

=ЦЕЛОЕ((ДЛСТР(В2)-1)/В3)+1

Используйте также особенности расшифровки для текста длиной 20 букв и для шифрования в общем случае.

Если вы разработаете соответствующий вариант расшифровки, то сможете убедиться, что, даже не зная размер ключа шифрования, текст можно расшифровать. Для этого надо перебирать возможные значения ключа до тех пор, когда расшифрованный текст станет осмысленным.

### Задание для самостоятельной работы

Расшифруйте, подобрав ключ шифрования перебором, следующую шифрограмму<sup>9</sup>:

МФТЧОЙАИОИЕРЖЛРРКНОУ ИМИЬШР НАОХИН

### Литература

1. Шифр Цезаря и три письма. // «Мир информатики», № 16 (октябрь 2017 г.).
2. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин. Основы криптографии. — Гелиос АРВ, 2002.

## Крепкий орешек

Как всегда, в этой рубрике редакция проводит разбор задач, решение которых вызвало трудности.

### Числовой ребус «Чему равны три ТРЕТИ»

Напомним, что было предложено решить числовой ребус:

$$\text{ТРЕТЬ} + \text{ТРЕТЬ} + \text{ТРЕТЬ} = \text{ЦЕЛОЕ}$$

Приведем начало решения.

Запишем ребус «в столбик»:

	Т	Р	Е	Т	Ь
+	Т	Р	Е	Т	Ь
	Т	Р	Е	Т	Ь
	Ц	Е	Л	О	Е

Исследуем возможные значения **Ь** и соответствующие значения **Е** (по последнему справа разряду), **Л** (по разряду сотен) и **Р** (по разряду тысяч):

Ь	Е	Л	При этом в «уме» из разряда сотен переходит	Р	Допустим ли вариант?
1	3	9	0	1	
2	6	8			
3	9	7			
4	2	6			
5	5				
6	8	4			
7	1	3			
8	4	2			
9	7	1			

Четвертый и пятый столбцы таблицы заполните самостоятельно, после чего ответьте на вопрос в последнем столбце. В результате вы найдете решения ребуса (их — больше одного<sup>10</sup>). Ответы присылайте в редакцию.

<sup>9</sup> Шифрограмма, шифротекст, шифртекст — результат операции шифрования. Часто также используется вместо термина «криптограмма».

<sup>10</sup> Одно из решений нашел Марат Хозин, Владимирская обл., г. Струнино, школа № 11, учитель Волков Ю.П.

## Переливания молока

Есть три бидона емкостью 14, 9 и 5 литров. В большом — 14 литров молока, остальные пусты. Как с помощью этих сосудов разлить 14 литров пополам?



Решение, пожалуйста, оформите в виде таблицы:

		Бидон емкостью 14 л	Бидон емкостью 9	Бидон емкостью 5 л
0	Исходное состояние	14	0	0
1	Перелить из 14 л в 5 л	9	0	5
2	...	...	...	...

## Система числовых ребусов

Решите, пожалуйста, систему из двух числовых ребусов:

$$\begin{cases} MA \cdot MA = МИР \\ AM \cdot AM = РИМ \end{cases}$$

В них, как обычно в таких головоломках, одинаковым буквам соответствуют одинаковые цифры, разным буквам — разные цифры.

## Страшный сон

Вернувшийся из Китая английский офицер заснул в церкви во время службы. Ему приснилось, что к нему приближается палач, чтобы отрубить голову, и в тот самый момент, как сабля опускалась на шею несчастного офицера, его жена, желая разбудить заснувшего, слегка дотронулась до его шеи веером. Потрясение было столь велико, что офицер тут же упал замертво.

Что-то в рассказе неладно. Что именно?

## Внимание! Конкурс!

### Конкурс № 27

В качестве задания этого конкурса редакция предлагает выполнить задания, предложенные для самостоятельной работы в рубрике «Школа программирования».

Срок представления программ не ограничен (не ☺).

### Конкурс № 28

В качестве задания этого конкурса редакция предлагает выполнить задания, предложенные для самостоятельной работы в статье «Шифруем текст в среде электронной таблицы».

Срок представления файлов — см. конкурс № 27.