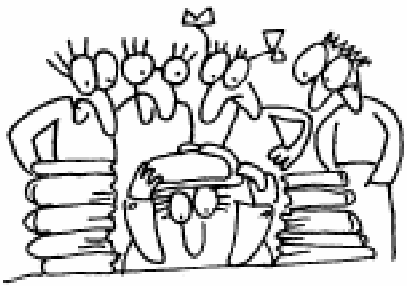
Миронов Илья Лазаревич
Черкасова Полина Геннадьевна

ЗАДАЧИ

Задача 1.

Уровень 1. Вспомните школьников, которые выясняли среднее значение IQ в своем классе. У приведенного алгоритма есть один существенный недостаток: если два соседа одного школьника сговорятся, то они смогут определить его IQ. Как следует модифицировать этот алгоритм, чтобы для определения IQ одного школьника был необходим сговор всех остальных?



Это количество, как можно заметить, является и наилучшим возможным значением для количества школьников, необходимых для раскрытия тайны своего одноклассника. Действительно, если все школьники без одного выяснят свой средний IQ, то по этому числу и по среднему IQ класса они смогут выяснить интеллектуальный коэффициент выставленного за дверь одноклассника. Таким образом, алгоритм, который вам предлагается придумать, предоставляет своим участникам самую высокую возможную защиту.

Задача 2.

Уровень 1. Пусть в группе из нескольких человек одному известна некая тайна. Он хочет ее сообщить все остальным,

но хочет, чтобы его личность не была раскрыта. Предложите такой алгоритм, при котором все узнают это анонимное сообщение, но пославший его ничем не будет рисковать.

Задача 3.

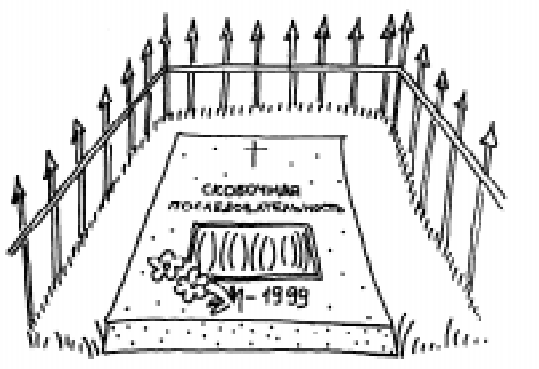
Уровень 1. Считается, что секрет приготовления «Кока-колы» закрыт в сейфе, который могут открыть члены совета директоров компании, только собравшись вместе. Руководители компании ведут активный образ жизни, часто летают на самолетах и отдыхают на лыжных курортах. Поэтому следует учесть вероятность того, что в промежутке между заседаниями совета директоров с кем-нибудь из них может случиться несчастный случай. Чтобы обезопасить компанию от безвозвратной утраты секрета, было принято решение, что отныне сейф можно открыть на собрании совета директоров, на котором присутствуют все, кроме, может быть, одного (любого!) его члена. Предложите конструкцию такого сейфа с N замками, в котором было бы как можно меньше движущихся деталей, а открывался бы он любым набором из N-1 ключа. Постарайтесь не использовать сложные механизмы с рычагами и блоками, ведь, как известно, чем проще конструкция, тем она надежнее.

Задача 4.

Жила-была правильная скобочная последовательность из круглых скобок. Некто взял и написал под каждой открывающейся скобкой число скобок, которые содержатся между ней и соответствующей закрывающейся. После этого некто стер скобочную последовательность. Сможете ли вы ее восстановить по тем числам, которые написал некто?

Уровень 1. Изложите алгоритм для восстановления скобочной последовательности

Уровень 2. Напишите программу, которая находит скобочную последовательность.



Формат ввода:

Количество чисел M

Первое число

...

M-е число

Формат вывода:

Скобочная последовательность.

Пример:

Ввод:

6

0

8

0

4

0

0

Вывод:

()(()(()()))

Задача 5.

Шпионам из племени Мумба-Юмба требуется переслать секретный шифр, состоящий из чисел от 1 до 100. Сначала они хотели прибавлять ко всем числам одно и то же задуманное секретное число – ключ (тоже от 1 до 100). Но потом решили, что сложение – это слишком простое действие, а умножение гораздо сложнее и таинственнее. Поэтому они стали умножать все числа на ключевое число.

Агенты из племени Юмба-Мумба перехватили донесение и пронюхали, что

шпионы кодируют донесение с помощью умножения на одно и то же число. Помогите им найти все возможные ключи.

Уровень 1. Опишите алгоритм, с помощью которого, зная донесение, можно найти все варианты ключей, которыми могут пользоваться шпионы.

Уровень 2. Напишите программу, которая решает эту задачу.

Формат ввода:

Длина донесения M
Первое число
...
M-е число

Формат вывода:

Количество возможных ключей N
Первый ключ
...
N – й ключ

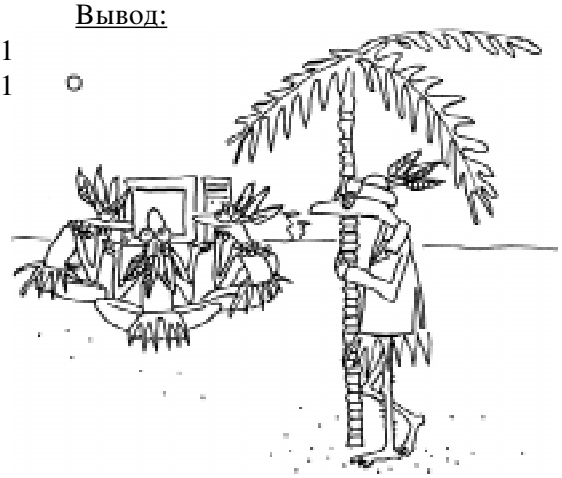
Пример:

Ввод:

3
1
3
4

Вывод:

1
1



Задача 6.

Расшифруйте текст, который закодирован при помощи шифра, аналогичного описанному в рассказе Эдгара По «Золотой жук». Зашифрован отрывок из литературного произведения, из которого были удалены все знаки препинания. Что это за произведение?

G@[U A[GGIA[?WR[@S X Q[G@[U DCY R G[EF YH YGV[@AWR[U XPUYHW YPH[ODHHZD EZB[HWDV YGDHW W G IYVY\WJ G@[AYCY G[EYRHWL[PDADOHY WB FLF@ZR[U @DIUYM GYUYVYM UWKY DCY WQYPA[O[UY GIYLYMG@RWD QEYAYRSD W EYPAYEF?WD YH VHD YPA[EYR[UGX W G@[U A[GGIA[?WR[@S YP FO[GHZB IAYWG?DG@RWXB LYWV X PZU GRWED@DUS X A[GGL[Q[U DVF RGD G@[AWL GUF?[U VDHX GY RHWV[HWDV W VDOEF @DV Y@ADQZR[U GFBWD RD@RW PDEHZM VWAYHYR GL[Q[U YH LYCE[X LYHNWU GRYJ IDN[USHFJ IYRDG@S O[US DCY BYAY?WM PZU

YTWKDA

Задача 7.

Муха ползет по квадратной проволочной сетке размером N*N (N < 30) из одного угла (точка (0, 0)) в противоположный (точка (N, N)). Два паука сидят по краям сетки (слева и снизу) и наблюдают за мухой. Каждый из них записывает, сколько клеток проползла муха, прежде чем повернуться спиной к пауку (при каждом повороте муха поворачивается спиной к одному из пауков).

После этого пауки встречаются и по полученным данным вычисляют путь, по которому ползла муха. (Ведь обратно она поползет тем же путем и пауки смогут устроить засаду.)

Комарик хочет спасти муху. Но для этого ему тоже нужно знать путь мухи. Он подсмотрел записи пауков. Помогите ему.

Уровень 1. Опишите, как нарисовать путь мухи, если известны записи пауков.

Уровень 2. Напишите программу, которая это делает. Программа должна выводить координаты всех узлов (включая первый, последний и все промежуточные) сетки, которые проползла муха

Формат ввода:

Сторона квадрата N
Количество чисел в записи первого паука M1
Первое число
...
M1-е число
Количество чисел в записи второго паука M2
Первое число
...
M2-е число

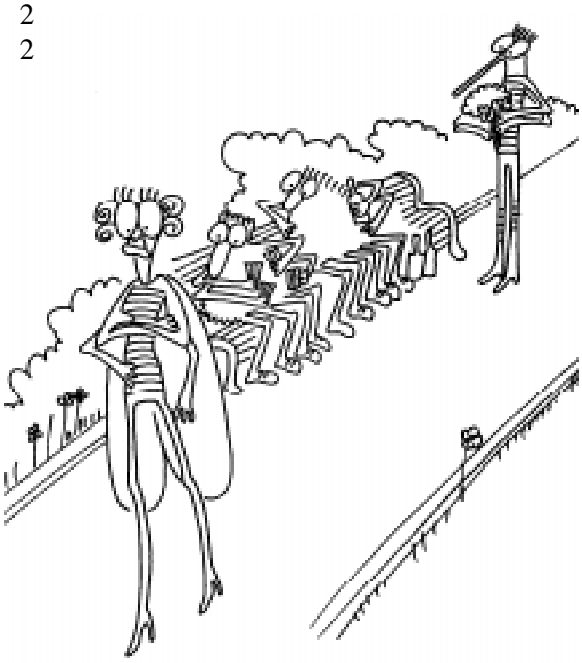
Формат вывода:

Число узлов, которые проползла муха.
Координаты первого узла (через пробел)
...
Координаты последнего узла

Пример:

Ввод:

```
3
2
2
1
2
2
1
```



Вывод:

```
7
0 0
1 0
2 0
2 1
2 2
3 2
3 3
```

Задача 8.

Винни-Пух и Пятачок занимаются поисками древнего клада. И чтобы Тигра не раскрыл их планов, они обмениваются зашифрованными записками.

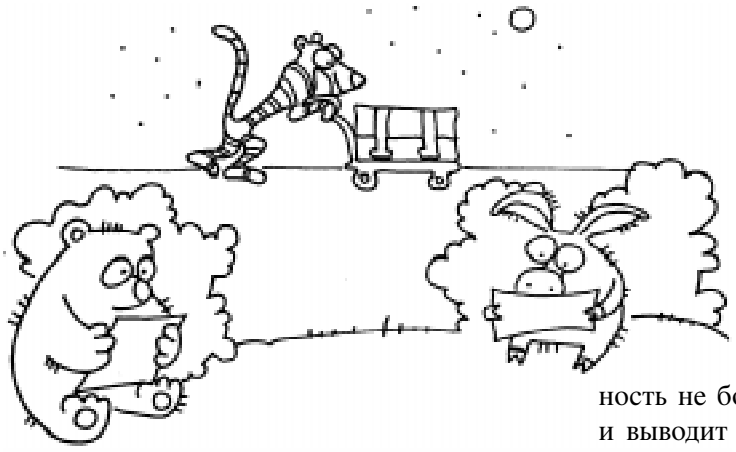
В их шифре используются числа Фибоначчи. Они устроены следующим образом: Первые два числа равны единице. А каждое следующее число равняется сумме двух предыдущих: 1, 1, 2, 3, 5, 8, 13, 21, 34, ... Обозначим их f1, f2, f3, ...

Шифр следующий: вместо первой буквы сообщения пишем следующую по алфавиту. Вместо второй – тоже следующую. А дальше вместо каждой буквы пишем букву, увеличенную на очередное число Фибоначчи. То есть вместо четвертой буквы «q» мы пишем «q» + f4 = «q» + 3 = «t».

Если мы уперлись в конец алфавита, то нужно перейти в начало и отсчитывать дальше (напоминаю, что английский алфавит состоит из 26 букв). Пробелы и знаки препинания так и пишутся. Ввиду важности события сообщения пишутся только заглавными буквами.

Но записки у Вини-Пуха и Пятачка были очень длинные. А числа Фибоначчи растут очень быстро. Поэтому все время у друзей уходило на вычисление чисел и отсчитывание букв, а на поиски клада совсем ничего не оставалось. Заменить шифр они не могли, потому что Тигра усилил бдительность, и у них не было возможности обговорить новый шифр.

Уровень 1. Попробуйте придумать способ упростить расчеты так, чтобы времени на зашифровку текста тратилось как можно меньше. Изложите алгоритм такой оптимизации. Зашифруйте текст «ISN'T



IT FUNNY HOW A BEAR LIKES HONEY?».

Уровень 2. Напишите программу, которая зашифровывает таким образом текст. Программа должна брать текст из файла IN.TXT и записывать зашифрованный текст в файл OUT.TXT.

Формат ввода:

Исходный текст

Формат вывода:

Зашифрованный текст.

Пример:

Ввод:

WINNIE-THE-POOH

Вывод:

XJPQNM-GCM-SZCG

Задача 9.

Уровень 1. Злой Карабас-Барабас посадил в два темных подвала Буратино и Мальвину. Он разрешает им обмениваться письмами, но читает их, поскольку опасается, что они договорятся о побеге. К несчастью для Карабаса, пленники заранее договорились о способе передачи секретных сообщений. Чтобы зашифровать сообщение из нулей и единиц пленники составляют письмо на правильном русском языке, в котором нулям из секретного сообщения соответствуют слова четной длины, а единицам - нечетной. Знаки препинания (точки, запятые, тире, и т.п.) при дешифровке не учитываются. В зашифрованном тексте запрещается:

1. повторять предложения;
2. дважды использовать слово в одном предложении (использовать одно слово в разных предложениях не запрещается).

Напишите программу, которая вводит секретное сообщение — последовательность не более чем из 100 нулей и единиц и выводит его в зашифрованном виде. Зашифрованный текст должен быть составлен по правилам русского языка (т.е. не содержать орфографических, пунктуационных и синтаксических ошибок).

Исходные данные:

Файл содержит одну или несколько секретных последовательностей. Каждая последовательность состоит не более, чем из 100 нулей и единиц и записывается на отдельной строке. Файл исходных данных не содержит пробелов и пустых строк.

Выходные данные:

Для каждого секретного сообщения вывести в выходной файл его зашифрованный вариант. Сообщения в выходном файле должны разделяться пустой строкой. Сообщение не должно содержать пустых строк. Каждое зашифрованное сообщение может располагаться на несколь-

ких строках, переносить слова запрещается.

Пример:

Файл исходных данных INPUT.TXT:

1100010000010001110010111 0
0

Выходной файл OUTPUT.TXT:

Мороз и солнце: день чудесный!
Еще ты дремлешь, друг прелестный -
Пора, красавица, проснись:
Открой сомкнуты негой взоры
Навстречу северной Авроры,
Звездою севера явись!
А.С. Пушкин

Вечереет.

Примечание. Различные наборы исходных данных задают различные секретные сообщения, поэтому одно предложение может встречаться в разных зашифрованных текстах.

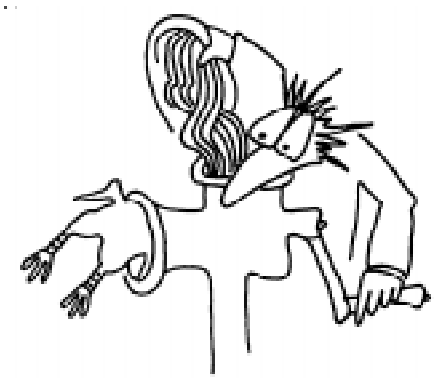
Задача 10.

Уровень 1. Придумайте симметричный шифр, то есть такой, чтобы один и тот же алгоритм зашифровывал и расшифровывал текст. То есть если на вход алгоритму дать им же зашифрованный текст, то он его расшифрует.

Уровень 2. Напишите программу, которая реализует этот алгоритм. Программа должна брать текст из файла IN.TXT и записывать зашифрованный текст в файл OUT.TXT.

Формат ввода:

Исходный текст



Формат вывода:

Зашифрованный текст.

Задача 11.

Уровень 1. Давайте устроим конкурс односторонних функций.

Требования к функции y = f(x) таковы:

- область определения и область значений функции (то есть диапазон изменения x и y) от 0 до 4294967295 (= 2^{32} - 1);
- функция не должна быть слишком сложной и громоздкой. По значению аргумента значение функции должно находиться быстро;
- функция должна быть односторонней, – то есть для того чтобы по значению функции найти значение аргумента, нужно просто перебрать все аргументы.

Мы опубликуем те функции, которые нам понравятся, и устроим проверку их односторонности следующим способом: если кто-нибудь из наших читателей сможет написать программу, которая будет быстро находить по значению функции значение аргумента неперебoрным методам, то функция не является односторонней. В обратном случае она прошла испытание.

Уровень 2. Будет хорошо, если, кроме письменного описания функции, вы пришлете программу, которая по значению x находит значение f(x).

Формат ввода:

Целочисленное значение аргумента

Формат вывода:

Целочисленное значение функции

Пример:

Ввод:

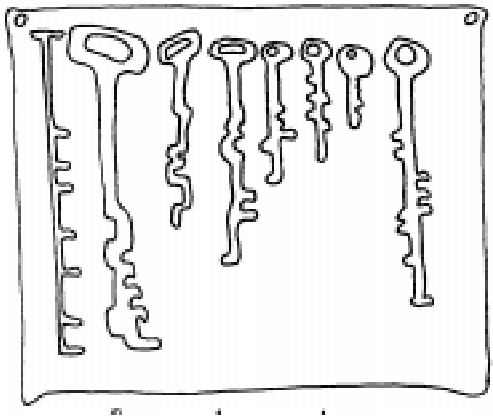
999990

Вывод:

12

Задача 12.

Уровень 1. Очень важным этапом проектирования любой криптостойкой системы является обоснованный и тщательно продуманный выбор длины ключа.



Для этого необходимо оценить стоимость и продолжительность атаки методом грубой силы, то есть взлома кода путем полного перебора всех возможных ключей. Представим себе, что в открытую продажу поступил чип (микросхема) стоимость 10 долларов, совершающий миллион операций шифрации одного блока в секунду. Оцените, сколько времени потребуется вашей младшей сестре, чтобы расшифровать ваше сообщение, если вы пользуетесь ключом длины 40 бит, а она готова потратить на это 100 долларов. А если длина ключа 56 бит? 168 бит? (40 бит – это максимальная длина ключа, которая допускается в программных и аппаратных средствах, разрешенных к импорту из США, 56 – длина ключа в обычном DES, 168 бит – длина ключа в троированном DES, то есть один текст шифруется трижды с разными ключами). А если вам противостоит крупная частная организация, которая в состоянии потратить 100 тысяч долларов, лишь бы взломать код? Теперь поставьте себя на место Джеймса Бонда, за которым охотится зловещая организация СПЕКТР. Сколько времени есть у него в запасе, прежде чем его код будет раскрыт, если на это может быть потрачено десять миллионов долларов?

Заполните таблицу, вписав в нее время, требуемое для атаки методом грубой силы с данной длиной ключа и в рамках заданного бюджета.

Как изменятся вычисленные значения через 5 и 15 лет? Для этого воспользуйтесь законом Мура, гласящим, что производительность процессоров удваивается каждые 18 месяцев.

Уровень 2. Выбрав длину ключа (см. предыдущую задачу), следует решить следующую проблему: откуда эти ключи брать?

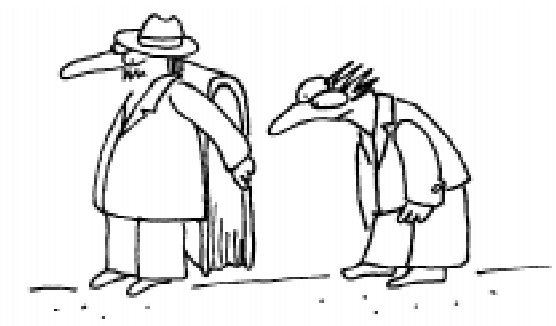
алгоритм	**импортированный из США алгоритм**	**DES**	**троированный DES**
длина ключа	40 бит	56 бит	168 бит
бюджет сестры ($100)			
бюджет банка ($100 тыс.)			
бюджет спецслужбы ($10 млн.)			

Если предлагать пользователю ввести пароль, то количество возможных ключей сильно сокращается. Если воспользоваться датчиком псевдослучайных чисел ис-

пользуемого языка программирования, то становится возможным поиск ключа с помощью перебора начальных значений этого датчика. Чтобы обойти эти трудности, попробуем извлечь из компьютера как можно больше «почти» случайных чисел, а потом используем их для построения ключа. Например, можно взять количество микросекунд, прошедших с начала секунды, последнюю цифру количества свободных байтов на диске и т.п. Найдите такие числа, их которых можно сформировать ключ длиной хотя бы 40 бит. Может быть, для этого вам потребуется помощь пользователя компьютера.

Задача 13.

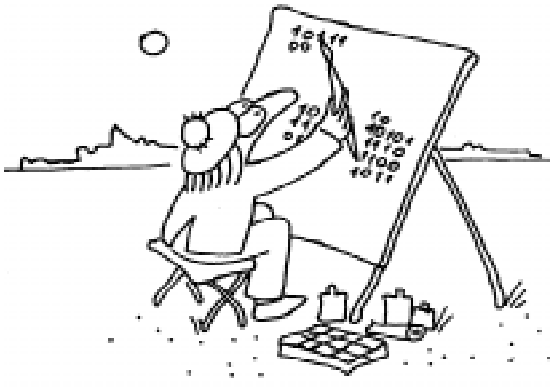
Уровень 1. Передать одноразовый блокнот для шифрации может оказаться нелегко. Еще труднее его спрятать, а уж обнаружение такого блокнота демаскирует его владельца полностью. Тем не менее, можно договориться использовать в качестве такого блокнота какую-нибудь книгу, одинаковое издание которой есть у разведчика и в центре. Непосредственное использование букв в книге является не очень удачной идеей, так как буквы в естественных текстах встречаются крайне неравномерно. Придумайте другой способ извлечь из книги абсолютно случайную последовательность.



Задача 14.

В занятии 2 прошлого номера было рассказано, что растровую двуцветную картинку можно закодировать с помощью нулей и единиц. В этой задаче предлагается закодировать 256-цветную картинку размером M*N. Причем это нужно сделать так, чтобы итоговый файл с картинкой оказался как можно меньше.

Уровень 1. Опишите алгоритм записи графического изображения.



Уровень 2.

А) Напишите программу, которая записывала бы картинку в придуманном вами формате. Исходные данные находятся в файле IN.TXT, а закодированную картинку следует записывать в файл PICTURE.PIC. Этот файл не обязательно должен иметь текстовый формат (ведь он занимает слишком много места). Будет хорошо (но не обязательно), если ваша программа быдет при этом показывать картинку на экране.

Формат ввода:

Высота рисунка N
Ширина рисунка M
Цвет первой точки в первом ряду
Цвет второй точки в первом ряду
...
Цвет M-й точки в первом ряду
...
...
Цвет первой точки в N-ом ряду
Цвет второй точки в N-ом ряду
...
Цвет M-й точки в N-ом ряду

Формат вывода:

Запись картинки в вашем формате.

Б) Напишите программу, которая показывала бы на экране картинку, которая записана в придуманном вами формате в файл PICTURE.PIC.