11 класс

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ИМЕНИ И.Я. ВЕРЧЕНКО ПО ИНФОРМАТИКЕ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

2018 год

ВАРИАНТ 1

Задача 1. Шифр

Сотруднику для анализа был предоставлен перехваченный фрагмент зашифрованного текста. Известно, что некоторые предложения исходного текста начинаются с фразы «устроить атаку» (регистр не учитывается). Каждый символ исходного текста закодирован тремя цифрами, а точка имеет код «200», после точки пробел не ставится.

```
020012021102101002021112000111002211212102012002210210200002022120002011001212100
212200220221211210101212111010020111001112212121202111222011022010221200201002120
111222201011011102202102101001022221220112202201220210220112200020012021102101002
021112000111002211212102012002210122122101121010012010011201012010200020012021102
101002021112000111002211212102012002210220212122022012222221101220011200100020200
220022121210100021210202102100212221200210102000200011211110212121010022211022121
012212000122100120122110001001120200001201022012022021112122100111100002102122002
000221010100211222110102000222120020202200012210001111100110021001100202021200222
011112121011200211100200111221200100111210201220221211020111220121102110220122010
000112111222221020022112021020202120200020012021102101002021112000202021202121020
202212200101100121201120202221200020012021102101002021112000111002211212102012002
210212120010100100211222120111021002022012012002100001200020012021102101002021112
000202021202121020212010202212210100121100120022012200020012021102101002021112000
111002211212102012002210201210020020221102211011121202101121201222010200020012021
102101002021112000202021202121020200122001122101112200222002000200201100121022211
221010001122211121001201112201020011012212100111201111212122200020012021102101002
021112000111002211212102012002210112222012022201120222220210212200020012021102101
002021112000202021202121020022001101102122220111021100001001202020211220211200020
012021102101002021112000202021202121020000112001001120111000001001201122022120002
012021102101002021112000202021202121020201012210201011010110002102221200210102021
210122122012012201212022210021201012022112022100022111112020000122200212121101201
211022200111022210222001201202110111021210100122120121122112002200011210000212121
111112122212012022211111120121210002211200122212221001022002120212000201222002020
000220121101211210102020212201121200010111212121102002102100122121111122201002021 1
220211212102200020012021102101002021112000111002211212102012002210022100120022110
002010212211212120120022111022222010200
```

Определите, как будет записано слово «СКОРОСТЬ» с использованием представленного шифра.

Задача 2. Удаленный файл

Для организации файловой системы на сервере компании используется структура хранения данных, включающая в себя три последовательно расположенных основных секции:

Таблица 1 (288 байт)	Таблица 2 (510 байтов)	Данные

Каждый файл разбивается на блоки размером не более 10 байт, информация о которых хранится в секции «*Таблица 2*», содержащей *N* ячеек и имеющей следующую структуру:

Ячейка с индексом 1			Ячейка с индексом N	
Адрес блока данных (1 байт)	Индекс следующей ячейки (1 байт)	…	Адрес блока данных (1 байт)	Индекс следующей ячейки (1 байт)

где «*Адрес блока данных*» – смещение блока данных файла в секции «*Данные*» относительно ее начала; «*Индекс следующей ячейки*» – порядковый номер ячейки (в секции «*Таблица 2*»), содержащей информацию о следующем блоке данных файла, либо `0x00`, если достигнут конец файла.

Для задания начала каждого файла используется секция «*Таблица 1*», содержащая *M* ячеек и имеющая следующую структуру:

Ячейка с индексом 1			Ячейка с индексом M	
Имя файла (8 байт)	Индекс первой ячейки (1 байт)	…	Имя файла (8 байт)	Индекс первой ячейки (1 байта)

где «*Имя файла*» – имя файла; «*Индекс первой ячейки*»» – индекс ячейки (в секции «*Таблица 2*»), содержащей информацию о первом блоке данных файла.

Все неиспользуемые ячейки секции «*Таблица 1*» заполнены байтами `0x00`. Для повышения скорости работы с файловой системой при удалении файла обнуляются (заполняются байтами `0x00`) только соответствующие ему ячейки секции «*Таблица 1*».

В результате ошибки администратора с сервера был удален один текстовый файл. Предложите алгоритм восстановления и приведите содержимое удаленного файла, имея в распоряжении файл *DiskImage.bin*, являющийся полной копией содержания и структуры файловой системы и данных, находящихся на диске, с которого был удален файл.

К задаче прилагается: файл DiskImage.bin.

Задача 3. Скрытое сообщение

Алексей получил электронное почтовое сообщение со следующим содержимым: «*Отправляю тебе мое кодовое слово. С уважением, Сергей*». К сообщению были прикреплены файлы *FirstFile.bmp*, *SecondFile.bmp*. Помогите Алексею определить полученное от Сергея кодовое слово.

К задаче прилагается: файлы FirstFile.bmp, SecondFile.bmp.

Задача 4. Гамма

Текстовое сообщение было зашифровано методом «двоичного гаммирования», т.е. путем выполнения операции «побитового исключающего ИЛИ» между байтами исходного сообщения и ключа длиной 2 байта. После применения операции «побитового исключающего ИЛИ» к байтам ключа и первым двум байтам сообщения, ключ сдвигается на 1 бит вправо относительно исходного текста, и операция выполняется повторно. Результат выполнения операции «побитового исключающего ИЛИ» сохраняется в соответствующих разрядах зашифрованного текста. Шифрование заканчивается, когда операция применяется к двум последним байтам сообщения.

```
35 17 1E 1A 0F 1E 1A 18 11 10 1F 0E 12 11 0E 0D 03 DF 10 0F 1A 1D 04 07 1A
DF 1D 0E 1A 70 43
```

Определите исходное сообщение и значение ключа, если известно, что сообщение может содержать только буквы, цифры, пробелы и знаки препинания.

Задача 5. Ключи

Взаимодействие между агентами осуществляется по каналу связи, позволяющему последовательно передавать несколько ключей шифрования произвольной длины. Длина каждого ключа кратна байту. В ходе осуществления очередного сеанса связи было отправлено 3 ключа шифрования:

```
44 41 54 4B 42 4A 41 43 4C 41 50 4C 56 58 4B 46 56 4C 41 50 41 54 4A 4C 44
4A
```

Для возможности однозначного определения длин всех ключей шифрования агенту на приемной стороне дополнительно (по некоторому другому каналу связи) сообщили значение, равное произведению их длин, и тот факт, что ключ наибольшей длины содержит последовательность байтов `0x41544A`. Помогите агенту восстановить каждый из трех полученных ключей.