Условия задач заключительного этапа

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.

```
020012021102101002021112000111002211212102012002210210200002022120
002011001212100212200220221211210101212111010020111001112212121202
111222011022010221200201002120111222201011011102202102101001022221
220112202201220210220112200020012021102101002021112000111002211212
102012002210122122101121010012010011201012010200020012021102101002
021112000111002211212102012002210220212122022012222221101220011200
100020200220022121210100021210202102100212221200210102000200011211
110212121010022211022121012212000122100120122110001001120200001201
022012022021112122100111100021021220020002210101002112221101020000
222120020202200012210001111100110021001100202021200222011112121011
200211100200111221200000111210201220221211020111220121102110220122
010000112111222221020022112021020202120200020012021102101002021112
000202021202121020202212200101100121201120202221200020012021102101
002021112000111002211212102012002210212120010100100211222120111021
002022012012002100001200020012021102101002021112000202021202121020
212010202212210100121100120022012200020012021102102100202111200011 1
002211212102012002210201210020020221102211011121202101121201222010
200020012021102101002021112000202021202121020200122001122101112200
222002000200201100121022211221010001122211121001201112201020011012
212100111201111212122200020012021102101002021112000111002211212102
012002210112222012022011202222202102122000200120211021010020211112
000202021202121020022001101102122220111021100001001202020211220211
200020012021102101002021112000202021202121020001120010011201110000
010012011220221200020012021102101002021112000202021202121020201012
210201011010110002102221200210102021210122122012012201212022210021
201012022112022100022111112020001222002121211012012110222001110 22
210222001201202110111021210100122120121122112002200011210000212121
111112122212012022211111120121210002211200122212221001022002120212
000001222002020000220121101211210102020212201121200010112121211020
021021001221211111222010020211220211212102200020012021102101002021
112000111002211212102012002210022100120022110002010212211212120120
022111022222010200
```

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

Решение:

Первым шагом необходимо разбить фрагмент на предложения (код точки – «200»). Необходимо учитывать, что длина предложения должна быть кратна трем. Для удобства разобьем весь фрагмент на группы по 3 цифры (символы).

020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002
210 210 **200**
002 022 120 002 011 001 212 100 212 **200**
220 221 211 210 101 212 111 010 020 111 001 112 212 121 202 111
222 011 022 010 221 **200**
201 002 120 111 222 201 011 011 102 202 102 101 001 022 221 220
112 202 201 220 210 220 112 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002
210 122 122 101 121 010 012 010 011 201 012 010 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002
210 220 212 122 022 012 222 221 101 220 011 **200**
100 020 **200**
220 022 121 210 100 021 210 202 102 100 212 221 **200**
210 102 000 **200**
011 211 110 212 121 010 022 211 022 121 012 212 000 122 100 120
122 110 001 001 120 **200**
001 201 022 012 022 021 112 122 100 111 100 002 102 122 002 000
221 010 100 211 222 110 102 000 222 120 020 202 **200**
012 210 001 111 100 110 021 001 100 202 021 **200**
222 011 112 121 011 **200**
211 100 **200**
111 221 **200** 000 111 210 201 220 221 211 020 111 220 121 102 110
220 122 010 000 112 111 222 221 020 022 112 021 020 202 120 **200**
020 012 021 102 101 002 021 112 000 202 021 202 121 020 202 212
200
101 100 121 201 120 202 221 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002
210 212 120 010 100 100 211 222 120 111 021 002 022 012 012 002
100 001 **200**
020 012 021 102 101 002 021 112 000 202 021 202 121 020 212 010
202 212 210 100 121 100 120 022 012 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002
210 201 210 020 020 221 102 211 011 121 202 101 121 201 222 010
200
020 012 021 102 101 002 021 112 000 202 021 202 121 020 **200**
122 001 122 101 112 **200**
222 002 000 **200**
201 100 121 022 211 221 010 001 122 211 121 001 201 112 201 020
011 012 212 100 111 201 111 212 122 **200**
...

В условии сказано, что фраза «УСТРОИТЬ АТАКУ» встречается больше одного раза. Эта фраза состоит из 14-ти символов (включая пробел) и должна быть закодирована 42-мя цифрами (по 3 на символ). Необходимо найти повторяющиеся фрагменты в началах предложений, длиной 14 символов (42 цифры). Такие повторяющиеся фрагменты есть.

020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210 210 **200**
002 022 120 002 011 001 212 100 212 **200**
220 221 211 210 101 212 111 010 020 111 001 112 212 121 202 111
222 011 022 010 221 **200**
201 002 120 111 222 201 011 011 102 202 102 101 001 022 221 220
112 202 201 220 210 220 112 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210 122 122 101 121 010 012 010 011 201 012 010 **200**

020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210 220 212 122 022 012 222 221 101 220 011 **200**
100 020 **200**
220 022 121 210 100 021 210 202 102 100 212 221 **200**
210 102 000 **200**
011 211 110 212 121 010 022 211 022 121 012 212 000 122 100 120 122 110 001 001 120 **200**
001 201 022 012 022 021 112 122 100 111 100 002 102 122 002 000 221 010 100 211 222 110 102 000 222 120 020 202 **200**
012 210 001 111 100 110 021 001 100 202 021 **200**
222 011 112 121 011 **200**
211 100 **200**
111 221 **200** 000 111 210 201 220 221 211 020 111 220 121 102 110 220 122 010 000 112 111 222 221 020 022 112 021 020 202 120 **200**
020 012 021 102 101 002 021 112 000 202 021 202 121 020 202 212 **200**
101 100 121 201 120 202 221 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210 212 120 010 100 100 211 222 120 111 021 002 022 012 012 002 100 001 **200**
020 012 021 102 101 002 021 112 000 202 021 202 121 020 212 010 202 212 210 100 121 100 120 022 012 **200**
020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210 201 210 020 020 221 102 211 011 121 202 101 121 201 222 010 **200**
020 012 021 102 101 002 021 112 000 202 021 202 121 020 **200**
122 001 122 101 112 **200**
222 002 000 **200**
201 100 121 022 211 221 010 001 122 211 121 001 201 112 201 020 011 012 212 100 111 201 111 212 122 **200**
...

Найдено 2 повторяющихся фрагмента:

020 012 021 102 101 002 021 112 000 111 002 211 212 102 012 002 210

И

020 012 021 102 101 002 021 112 000 202 021 202 121 020

По длине фрагмента и коду можно определить, что во втором фрагменте закодирована фраза «УСТРОИТЬ АТАКУ». Из него можно извлечь коды для букв, входящих в эту фразу:

Символ	**Код**
У	020
С	012
Т	021
Р	102
О	101
И	002
Ь	112
ПРОБЕЛ	000

А	202
К	121

Слово «СКОРОСТЬ» состоит из букв, для которых известен код, поэтому ответ написать не составит труда.

Ответ: 012 121 101 102 101 012 021 112

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.

Решение:

Исходя из структуры таблиц, для решения задачи необходимо найти все ячейки в «Таблице 2», ссылок на которые нет из других ячеек «Таблицы 2» (продолжение файла) и из «Таблицы 1» (начало файла). Для упрощения задачи поиска таких ячеек необходимо написать программу автоматизирующую соответствующие операции. Так как был удален только 1 файл, то такая ячейка будет единственной. В дальнейшем необходимо определить все блоки данных, которые соответствуют файлу путем считывания индексов всех ячеек до момента, пока не будет достигнут конец файла (значение индекса следующей ячейки будет равно `0x00`).

Ответ: Был удален файл ls.txt

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.

Электронные материалы: файлы FirstFile.bmp, SecondFile.bmp.
(http://v-olymp.ru/olmp_it/docs/2018/tasks/11/3/files.rar).

Решение

Визуально файлы не различимы. Стоит проанализировать содержимое файлов в бинарном формате.

Сравнив содержимое файлов, можно увидеть, что отличаются 64 байта:

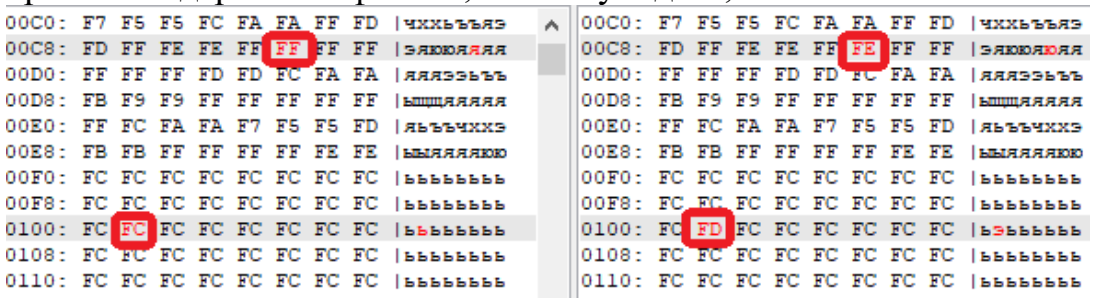

Рисунок 1 – Различия в файлах

Байты отличаются только последним разрядом: **FF → FE**, **FC → FD**. В первом байте последний бит поменяли с «1» на «0», во втором «0» → «1».

Можно сделать предположение, что измененный бит содержит информацию, каждый измененный байт несёт 1 бит информации. Учитывая, что измененных байтов 64, можно сделать вывод, что сообщение состоит из 8-ми байт.

Собирая измененные байты по порядку их появления от начала файла и извлекая модифицированные биты, можно собрать 8 байт информации.

Логично предположить, что информация является сообщением, и каждый байт представляет собой символ в ASCII-формате, то есть значение байта - это код символа в ASCII-таблице.

Получив значение 8-ми байт и сверившись с ASCII-таблицей можно получить ответ.

Ответ: Security

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.

Решение:

Первым делом необходимо понять схему шифрования: каждый раз 2-байтный ключ сдвигается относительно текста на 1 разряд вправо. Это означает, что начиная с 3-го байта текста, все остальные, кроме последних двух байтов, складывается по модулю 2 со всеми разрядами ключа. То есть каждый разряд байта текста последовательно складывается со всеми разрядами ключа. Это означает, что все разряды текста складываются с одним и тем же значением, равным сумме по модулю 2 всех разрядов ключа.

Если сумма по модулю 2 всех разрядов ключа равна 0 – результат сложения не изменится. Если сумма по модулю 2 всех разрядов ключа равна 1 – результат сложения будет инверсией исходного текста.

Если попытаться декодировать сообщение по ASCII-таблице, смысловой текст не получится. Значит необходимо инвертировать разряды зашифрованного текста:

```
CA E8 E1 E5 F0 E1 E5 E7 EE EF E0 F1 ED EE F1 F2 FC 20 EF
F0 E5 E2 FB F8 E5 20 E2 F1 E5 8F BC
```

Инвертированный фрагмент можно преобразовать в текст с использованием ASCII-таблицы:

«Кибербезопасность превыше всеЏj»

Как видно, последние 2 байта не являются буквами. Это так, поскольку последние 2 байта складывались с ключом ровно 1 раз, причем каждый разряд текста складывался по модулю 2 с соответствующим разрядом ключа.

Из смыслового содержания сообщения можно предположить, что последние 2 байта – это буквы «*г*» и «*о*».

При известном исходном тексте и известном зашифрованном тексте (70 43) не составляет труда найти ключ. Для этого необходимо сложить по модулю 2 исходный текст (ASCII-код букв «*г*» и «*о*») и зашифрованный текст:

```
E3 EE
70 43
-----
93 AD
```

Ответ: сообщение «*Кибербезопасность превыше всего*», ключ шифрования – `93 AD`.

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.

Решение:

Исходя из того, что предоставленных данных о сумме (26) и произведении размеров пакетов недостаточно, можно сделать вывод – существует несколько наборов значений, соответствующих размерам сообщений, имеющих одинаковую сумму и произведение. Под такие критерии подпадают следующие наборы:

288 = 18 * 4 * 4 = 12 * 12 * 2
270 = 18 * 5 * 3 = 15 * 9 * 2
126 = 21 * 3 * 2 = 18 * 7 * 1

Наличие информации о содержимом самого большого сообщения позволяет однозначно определить размеры переданных сообщений только для случая, когда произведение размеров равно 288, где встречаются 2 сообщения имеющих одинаковую длину. Для других ситуаций данная информация не устраняет неопределенность (для 270 – «самое короткое сообщение имеет длину 3 или 2?», и то и другое могут поместиться с 24 по 26 байты; для 126 - аналогично). Следовательно, с учетом информации о наличии сообщения, обладающего максимальной длинной, можно сделать вывод - размеры переданных сообщений равны 18, 4 и 4 байтов.

Далее необходимо определить, где начинается самое длинное сообщение. Так как `0x41544A` начинается с 21 байта и заканчивается 23 байтом, то расположение сообщений в зависимости от их длины в потоке данных может быть только следующим: 4, 4, 18.

Ответ: Были переданы следующие ключи:

```
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
```

Критерии оценивания заданий

Каждая задача заключительного этапа олимпиады при проверке работ оценивается по системе: «–», «∓», «±», «+»:

«–» — отсутствует решение задачи;

«∓» — отсутствует логически законченное решение задачи (решено менее половины задачи);

«±» — логически законченное решение с неточностями (ответ может быть неправильным);

«+» — полностью правильное решение задачи и правильный ответ.

Затем, с учётом сложности задач, осуществляется перевод результатов проверки в баллы. Для каждой параллели классов (8-10 и 11) разработана своя система баллов (см. Таблицы 1, 2) и критерии определения победителей и призеров (см. Таблицу 3), принятые на заседании жюри олимпиады.

Таблица 1

Критерии оценивания задач олимпиады для 8-10 классов

	1 задача	2 задача	3 задача	4 задача	5 задача
–	0	0	0	0	0
∓	1	2	2	2	2
±	2	3	4	3	3
+	3	4	5	4	4

Максимальное количество балов за работу – 20.

Таблица 2

Критерии оценивания задач олимпиады для 11 класса

	1 задача	2 задача	3 задача	4 задача	5 задача
–	0	0	0	0	0
∓	1	1	2	2	2
±	3	2	3	4	5
+	4	4	5	5	6

Максимальное количество балов за работу – 23.

Таблица 3

Критерии определения победителей и призеров олимпиады

Возрастная категория	**1 место**	**2 место**	**3 место**
11 класс	16 баллов и более	13-14 баллов	10-12 баллов
10 класс	15 баллов и более	12-13 баллов	9-11 баллов
9 класс	15 баллов и более	12-13 баллов	9-11 баллов
8 класс	15 баллов и более	12-13 баллов	9-11 баллов