Задачи XIII олимпиады (2003 год)

1. Пользователи сети связи для обеспечения секретности сообщений выбирают (независимо друг от друга) пары преобразований *(E,D)*, одно из которых, *E* (открытый ключ), публикуют в справочнике, а второе, *D* (личный ключ), держат в секрете. Известно, что значения *E(m)* и *D(n)* легко вычислить для любых сообщений *m* и *n*, причем из равенства *E(m)=n* следует, что *D(n)=m*. В то же время, нахождение *m* по *E(m)* является сложной задачей, которую невозможно решить (любыми средствами) за реальное время, если неизвестно *D*. Если пользователь *A* хочет послать *B* сообщение *m,* он берет из справочника открытый ключ E_B пользователя *B,* вычисляет $n=E_B(m)$, и посылает *n* к *B*. Получив *n, B* вычисляет $D_B(n)=m$. Злоумышленник, перехвативший *n,* не сможет вычислить *m*. Это гарантирует секретность информации.

Ватсон предложил Холмсу способ передачи секретных сообщений с уведомлением о получении: *A* передает *B* сообщение $\boldsymbol{(A,E_B(m))}$; *B,* получив сообщение, вычисляет *m* и направляет *A* уведомление $\boldsymbol{(B,E_A(m))}$. Холмс возразил Ватсону, что этот способ не обеспечивает секретности информации от любого пользователя, который может перехватывать сообщения и как угодно их изменять. Дополнительно потребовав, чтобы для каждого преобразования *E* было бы сложно подобрать пару *(m,n),* для которой *E(m)=E(n),* Холмс предложил Ватсону свой способ: *A* передает *B* сообщение $\boldsymbol{E_B(A,m)}$; *B,* получив сообщение, находит *m* и направляет *A* уведомление $\boldsymbol{E_A(B,m)}$. Объясните, почему способ Холмса лучше способа Ватсона.

C	**O**	**D**	**E**	**A**
B	**F**	**G**	**H**	**I**
K	**L**	**M**	**N**	**P**
Q	**R**	**S**	**T**	**U**
V	**W**	**X**	**Y**	**Z**

2. Шифр Bifid, имеющий простое правило зашифрования, использует в качестве ключа квадратную таблицу, в которую в некотором порядке записаны буквы английского алфавита (буквы **I** и **J** отождествлены). Результатом зашифрования фразы **SIXTY EIGHT MILES** на приведенном ключе является «фраза» **RYXXT OFTXT LKSWS**. Зашифруйте на том же ключе фразу **ENTER OTHER LEVEL**.

3. Для доступа к управлению параметрами своего счета, клиенту Зазеркального банка необходимо связаться по телефону с банком и набрать семизначный пароль. После первой же неправильно набранной цифры пароля банк прерывает телефонное соединение. Как надо действовать, чтобы за наименьшее число попыток подобрать пароль?

4. Формулировка некоторого геометрического утверждения вписана в клетки таблицы 10×а10 построчно слева направо, начиная с верхней левой клетки. Знак переноса на следующую строку не ставился, но между соседними словами одной строки помещалась пустая клетка. Криптоша решил переставлять буквы в отдельных столбцах сдвигая их все на одну позицию вверх и перенося самую верхнюю букву вниз (при этом пустую клетку он также считал буквой). Иногда он менял местами сразу все строки, симметричные относительно средней линии, а именно:
1-ю с 10-й, 2-ю с 9-ой и так далее. После чего снова брался за передвижение букв в столбцах. В результате таблица приняла представленный на рисунке вид. Прочитайте исходное геометрическое утверждение

а	**л**	**п**	**н**	**в**	**и**		**в**	**т**	**р**
е	**о**	**с**	**н**	**л**	**я**		**о**	**л**	**т**
п		**я**	**л**	**ы**	**е**	**о**	**ы**	**т**	**у**
е	**о**	**а**	**о**	**щ**	**д**	**р**	**р**	**а**	**е**
н	**р**	**у**	**и**		**о**	**н**	**с**	**т**	**в**
п	**к**	**и**	**м**	**е**	**ь**		**р**		
е	**в**	**о**	**ю**	**т**	**х**	**х**	**н**	**а**	**с**
д	**с**	**е**	**х**	**и**	**и**	**е**	**о**	**я**	
о	**к**	**ь**	**т**	**ы**	**п**	**ь**	**п**	**е**	**н**
с	**ж**	**с**	**с**	**е**	**л**		**о**	**о**	**о**

5. Какое наименьшее количество натуральных чисел надо взять, чтобы любое число от **1** до **300** можно было представить в виде суммы подходящего набора различных указанных натуральных чисел.

6. Для зашифрования сообщения используют последовательность неотрицательных целых чисел $x_1, x_2, \ldots$, удовлетворяющую соотношению $x_{k+3} = x_k + x_{k+2}$, $k = 1, 2, \ldots$ Две строки известного стихотворения, последние **5** букв которых совпадают, зашифровали следующим образом. Первую букву заменили числом согласно 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	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

и сложили с x_1, вторую заменили и сложили с x_2 и так далее. Затем все суммы заменили остатками от деления на **31**, а остатки заменили буквами согласно таблице. Получили текст

СЕЗНПБКЬЛЧЕЮЩЦТНИЭЛЬЩБШЬЕЮ
ЛУАЕЧЖЪЭШЭЛЪШЩХЧШДЮВЫЮИД.

Восстановите три буквы, соответствующие в таблице числам x_1, x_2, x_3, и прочитайте двустишие.