РЕШЕНИЯ

Решение задачи №1.

Недостаток способа Ватсона состоит в том, что, перехватив сообщение $(A, E_B(m))$, злоумышленник может заменить его на $(C, E_B(m))$, получив которое B воспринимает его как первый шаг протокола передачи с уведомлением от C. Вычислив m, B затем уведомляет C о получении, посылая ему сообщение $(B, E_C(m))$. Из него C извлекает искомое m, и от имени B уведомляет A о получении, посылая ему сообщение $(B, E_A(m))$.

Способ Холмса не позволяет злоумышленнику получить секретное сообщение m. В самом деле, получить его C может либо из перехваченных сообщений $E_B(A,m)$, $E_B(B,m)$, либо из направленного к нему сообщения $E_C(B,m)$. По $E_B(A,m)$ и $E_B(B,m)$ злоумышленнику невозможно найти m, поскольку для этого ему нужно решить сложную задачу обращения E_A или E_B. Исключая возможность сговора между B и C, B "добровольно" не пошлет к C сообщение $E_C(B,m)$. Значит такое сообщение попадет в C от B лишь в качестве уведомления о получении им сообщения $E_B(C,m)$. Такое сообщение к B может попасть лишь от C, который заменяет $E_B(A,m)$ на это $E_B(C,m)$. По условию этого C также сделать не в состоянии.

Решение задачи №2.

Ключом шифра служит систематически перемешанный алфавит, записанный в квадратную таблицу. Такие алфавиты широко использовались в криптографии. Первые буквы алфавита составляли легко запоминаемое ключевое слово (в условии данной задачи это слово CODE), остальные же буквы следовали в их естественном порядке. Такое мнемоническое правило позволяло быстро восстановить ключ, и произвести зашифрование или расшифрование.

	1	2	3	4	5
1	C	O	D	E	A
2	B	F	G	H	I
3	K	L	M	N	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Правило зашифрования шифра Bifid состоит в следующем. Строки и столбцы квадратной таблицы пронумеруем числами от 1 до 5, как показано на рисунке. Теперь каждая буква алфавита имеет свой номер, состоящий из пары чисел $\binom{i}{j}$ где i — номер строки, а j — номер столбца. Например, буква S имеет номер $\binom{4}{3}$ Выпишем буквы открытого текста в строку, разделяя пробелом каждую пятерку букв, а под ней — номера соответствующих букв. Фраза, взятая из условия задачи, запишется в виде

S	I	X	T	Y		E	I	G	H	T		M	I	L	E	S
4	2	5	4	5		1	2	2	2	4		3	2	3	1	4
3	5	3	4	4		4	5	3	4	4		3	5	2	4	3

Затем заменим номера букв. Для этого выпишем две строчки из пяти цифр под каждой пятеркой в одну строку из десяти цифр. Например, для второй пятерки получается строка 1222445344. В получившейся строке каждая последовательная пара цифр и будет новыми номерами букв пятерки, которые выпишем под соответствующими буквами. Так, для букв второй пятерки получаем новые номера:

E	I	G	H	T
1	2	4	5	4
2	2	4	3	4
O	F	T	X	T

Наконец, заменяем буквы открытого текста буквами, номера которых в квадратной таблице указаны теперь под соответствующими буквами. В результате этой замены получаем шифрованный текст. Например, пятерка EIGHT будет зашифрована в пятерку OFTXT.

Зашифруем на том же ключе фразу ENTER OTHER LEVEL, заполнив следующую таблицу:

E	N	T	E	R	O	T	H	E	R	L	E	V	E	L
1	3	4	1	4	1	4	2	1	4	3	1	5	1	3
4	4	4	4	2	2	4	4	4	2	2	4	1	4	2
1	4	4	4	4	1	2	4	4	4	3	5	3	4	4
3	1	4	4	2	4	1	2	4	2	1	1	2	1	2
D	Q	T	T	R	E	B	R	T	T	K	V	L	Q	R

Ответ: DQTTR EBRTT KVLQR.

решение задачи № 3

Цифры пароля будем подбирать последовательно. Свяжемся с банком и наберем цифру 0. Если связь не оборвалась, то первая цифра пароля 0. Если связь прервана, то первая цифра отлична от 0 и, связываясь заново с банком, пробуем набрать 1 и так далее. Не позднее чем через девять звонков мы будем точно знать, какая цифра стоит на первом месте в пароле, и сможем перейти к подбору второй цифры и т.д.

Общее количество звонков, которое понадобится для выяснения пароля, не более 7*9=63. Еще один звонок может понадобиться для получения доступа после полного выяснения пароля.

Заметим, что если бы решение о доступе или отказе принималось только после ввода *всего* пароля, то система защиты была бы гораздо надежнее - последовательный подбор был бы невозможен и потенциально пришлось бы перебирать все 10^7 вариантов пароля.

решение задачи № 4 Подходы участников олимпиады к решению этой задачи были весьма разнообразны. Предлагалось, например, решать эту задачу перебором, вырезав из бумаги три полосы, соответствующие первым трем строкам таблицы. Были попытки “увидеть” в зашифрованном тексте какое-либо слово, имеющее отношение к геометрической тематике, например, *прямая, точка* и т.п. Немаловажную роль в решении сыграло то естественное соображение, что круг слов, используемых в геометрических текстах, существенно ограничен.

В определенном смысле операции *сдвига букв в столбцах* и *отражение столбца относительно средней линии* перестановочны. (Действительно, сдвинуть столбец на одну позицию вверх и затем отразить – это все равно что столбец сначала отразить, а затем сдвинуть вверх на девять позиций.) Поэтому можно считать, что сначала Криптоша передвигал буквы в столбцах, а затем может быть один раз отразил таблицу относительно средней линии. Рассмотрим букву **я** в предпоследнем столбце. Перед ней могут стоять буквы **о, п, н, р,с,ы, в.** Сочетание **оя** встречается в математических текстах в слове пост**оя**нная, но необходимой буквы **т** в седьмом столбце нет. Сочетание **ря** может быть частью слова п**ря**мая, но в седьмом столбце нет **р**. Сочетание **ся** (касающих**ся**, пересекающих**ся** и т.д.) представляется наиболее вероятным, и присутствие буквы **щ** в пятом столбце тому подтверждение. После того как столбцы с пятого по девятый выстроены так, чтобы прочитывалось **щихся**, получение ответа становится совсем простым делом.

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

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

Мы не будем останавливаться здесь на доказательстве этого геометрического утверждения. Отметим только (большинством решавших это было упущено), что утверждение верно и в том случае, когда прямые не лежат в плоскости. Поворот осуществляется относительно прямой, перпендикулярной двум данным прямым и проходящей через точку их пересечения.

решение задачи № 5

При решении этой задачи участники широко использовали двоичное представление чисел. Например, 105=1101001. Известно, что в двоичном представлении степеней двойки присутствует лишь одна единица: 2^0=1, 2^1=10, 2^2=100, ..., 2^8=100000000. Видим, что в двоичной записи числа 105 единицы стоят в 1-ой, 4-ой, 6-ой и 7-ой позициях (считаем слева направо). Значит $105=2^0+2^3+2^5+2^6$. Поскольку двоичное число 111111111 (девять единиц) равно 511>300, заключаем, что девяти чисел 1,2,4,8,16,32,64,128,256 вполне достаточно для представления любого натурального числа от 1 до 300 (и даже до 511).

Отметим, что использование двоичной системы записи не является ключевым при решении этой задачи. Например, участниками были предложены следующие девять чисел 1,2,3,7,14,28,56,112,224.

Лишь в очень немногих работах присутствовало доказательство того, что искомый набор не может содержать менее девяти чисел. Действительно, пусть у нас есть восемь чисел, и любое число от 1 до 300 представимо в виде суммы разных чисел из этого набора. Используя наш набор, мы можем *закодировать* любое число от 1 до 300: пусть, например, число *a* равно сумме первого и третьего чисел нашего набора, тогда будем писать *a*=(1,0,1,0,0,0,0,0). Итак, число *a* получило свой код -- строку из восьми символов, каждый символ или 0 или 1. Но нам надо закодировать триста чисел, а строк длины 8, как нетрудно видеть, всего 256. Значит восьми чисел недостаточно.

решение задачи № 6.

Обозначим $a=x_1$, $b=x_2$, $c=x_3$. Так как эти числа соответствуют буквам в таблице, то они принимают значания от 0 до 30. Из соотношения

$$x_{k=3} = x_k + x_{k+2}$$

последовательно получим

x_1 = a
x_2 = b
x_3 = c
x_4 = a + c
x_5 = a+ b+ c
x_6 = a+ b+ 2c
x_7 = 2a+ b+ 3c
x_8 = 3a+ 2b+ 4c
x_9 = 4a+ 3b+ 6c
x_{10} = 6a+ 4b+ 9c

и так далее.

При дальнейшем построении этой последовательности используем следующие правила:

1. Для построения следующей строки последнюю строку складываем с предпредпоследней;
2. Легко заметить, что столбцы чисел отличаются сдвигом по вертикали, оэтому сначала можно определить только коэффициенты при c;
3. Так как нас интересуют только остатки от деления на 31, то например, 41c =31c+10c можно заменить на 10c.

Продолжая аналогично, получим.

x_{11} = 13
x_{12} = 19
x_{13} = 28
x_{14} = 10
x_{15} = 29
x_{16} = 26

$x_{17} =$ 5
$x_{18} =$ 3
$x_{19} =$ 29
$x_{20} =$ 3
$x_{21} =$ 6
$x_{22} = 6a + 3b + 4c$
$x_{23} = 4a + 6b + 7c$
$x_{24} = 7a + 4b + 13c$
$x_{25} = 13a + 7b + 17c$
$x_{26} = 17a + 13b + 24c$

Используя сдвиги столбцов получили значения x_{22}, x_{23}, x_{24}, x_{25}, x_{26}. Продолжая аналогично, получим последние пять значений x_{46}, x_{47}, x_{48}, x_{49}, x_{50}.

$x_{27} =$ 6
$x_{28} =$ 23
$x_{29} =$ 16
$x_{30} =$ 22
$x_{31} =$ 14
$x_{32} =$ 30
$x_{33} =$ 21
$x_{34} =$ 4
$x_{35} =$ 3
$x_{36} =$ 24
$x_{37} =$ 28
$x_{38} =$ 0
$x_{39} =$ 24
$x_{40} =$ 21
$x_{41} =$ 21
$x_{42} =$ 14
$x_{43} =$ 4
$x_{44} =$ 25
$x_{45} =$ 8
$x_{46} = 8a + 25b + 12c$
$x_{47} = 12a + 8b + 6c$
$x_{48} = 6a + 12b + 14c$
$x_{49} = 14a + 6b + 26c$
$x_{50} = 26a + 14b + 1c$

Итак, получено выражение чисел x_{22}, x_{23}, x_{24}, x_{25}, x_{26} и чисел x_{46}, x_{47}, x_{48}, x_{49}, x_{50} через a,b,c. Обозначим через $О_i$, $Ш_i$ - числа, соответствующие i-ым буквам стихотворения и полученного шифрованного текста. Тогда, числа $О_{22} + x_{22}$ и $Ш_{22}$ имеют одинаковые остатки от деления на 31. Тоже самое и с числами $О_{46} + x_{46}$ и $Ш_{46}$.

А так как $О_{22}$ и $О_{46}$ одинаковые, то, рассмотрев разности соответствующих частей, получим, что

$$x_{46} - x_{22} \text{ и } Ш_{46} - Ш_{22} \qquad (*)$$

дают одинаковые остатки от деления на 31.

Последним пяти буквам первой строки шифрованного текста соответствуют числа $Ш_i$:

Б, Ш, Ь, Е, Ю – 1,23,27,5,29

второй строки –

В, Ы, Ю, И, Д – 2,26,29,8,4.

Подставляя эти значения в (*) и выражая x_i через a, b, c, получаем систему

$$\begin{cases} 2a - 9b + 8c = 1 \\ 8a + 2b - c = 3 \\ -a + 8b + c = 2 \\ a - b + 9c = 3 \\ 9a + b + 8c = 6 \end{cases}$$

где равенство означает равенство остатков от деления на 31. При этом использовали правило 3, например, в первом уравнении +22b заменили на –9b. Осталось решить полученную систему. Складывая второе и третье, четвертое и пятое, третье и четвертое уравнения получим

$$\begin{cases} 7a + 10b = 5 \\ 10a + 17c = 9 \\ 7b + 10c = 5 \end{cases} \qquad (**)$$

Выразим b и c через a и подставим в первое уравнение

$$b = \frac{5 - 7a}{10}, \qquad c = \frac{9 - 10a}{17},$$

$$2a - 9\frac{5 - 7a}{10} + 8\left(\frac{9 - 10a}{17}\right) = 1$$

$$340a - 9 \cdot 17(5 - 7a) + 80(9 - 10a) = 170$$

$$611a = 215$$

$$22a = 29$$

Последнее уравнение можно решить методом подбора и обнаружить, что $22 \cdot 14$ и 29 дают одинаковые остатки от деления на 31. Итак

a=14.

Из системы (**) находим, что
10b=0 и 10c=5 , откуда

b=0

c=16.

Зная a, b, c можно последовательно найти все x_i и из соотношения $O_i = Ш_i - x_i$ получить стихотворение:

ВЕЧОРТЫПОМНИШЬВЬЮГАЗЛИЛАСЬ
НАМУТНОМНЕБЕМГЛАНОСИЛАСЬ