Решения задач

Задача № 1

Квадрат натурального числа может оканчиваться только на цифры 0, 1, 4, 5, 6, 9. Число 0…0 натуральным не является. Число 5…5≠ n^2 , так как оно делится на 5, но не делится на 25. Аналогично 6…6 ≠ n^2, т.к. делится на 2, но не делится на 4. Числа 4…4 и 9…9 являются полными квадратами в том и только том случае, когда полным квадратом будет 1…1.

Докажем, что 1…≠ n^2. Предположим, что это не так: существует натуральное число n такое, что 1…1= n^2. Тогда n=10k ± 1 и следовательно $100k^2$± 20k=1…10 ⇔ $10k^2$± 2k=1…1. Получили противоречие: нечетное число равно четному.

Задача № 2.

Для решения этой задачи достаточно было заметить, что при указанном способе зашифрования количество различных букв в исходном тексте совпадает с числом различных пар в криптограмме. Первая из приведенных в условии задачи криптограмм содержит 23 различные пары, а вторая – 29. Так как латинский алфавит состоит из 26 букв, английскому исходному тексту может соответствовать только первая криптограмма.

Задача № 3.

Слово ПОДЪЕЗД состоит из семи букв, причем 3-я и 7-я совпадают. Найдем в тексте фрагменты длины семь с совпадающими парами в 3 и 7 позициях. Таких фрагментов получится семь:

36 72 97 92 70 73 97
74 76 97 34 79 78 97
70 76 74 72 74 73 74
73 74 76 70 70 97 76
74 37 39 75 97 70 39
71 74 98 35 94 90 98
98 35 94 90 98 97 94

Удалим из этого списка те, в которых есть другие повторы. Останется четыре варианта:

36 72 97 92 70 73 97
74 76 97 34 79 78 97
74 37 39 75 97 70 39
71 74 98 35 94 90 98.

Отметим для первого случая ставшие известными буквы текста

```
 Ъ  Д  П  О  Д  Ъ  Е  З  Д     Д
92 97 36 72 97 92 70 73 97 90 97
 О              Д            Д  Е  …
72 38 39 74 76 97 34 79 78 97 70  …
```

Видно, что уже в самом начале содержится «нечитаемая» последовательность букв. Отметим для остальных вариантов становящиеся известными буквы текста:

Второй:

```
      Д         Д           Д     Д
92 97 36 72 97 92 70 73 97 90 97
         П  О  Д  Ъ  Е  З  Д
72 38 39 74 76 97 34 79 78 97 70
     П     П     П  О        Д  О
76 74 72 74 73 74 76 70 70 97 76
 П     П           Д        П  Е
74 96 74 37 39 75 97 70 39 74 79
         П                    Д
39 37 71 74 98 35 94 90 98 97 94
     П     П  О  Д
96 74 98 74 76 97
```

Третий:

```
      Е         Е     З     Е     Е
92 97 36 72 97 92 70 73 97 90 97
        Д  П     Е           Е  З
72 38 39 74 76 97 34 79 78 97 70
     П     П     П     З  З  Е
76 74 72 74 73 74 76 70 70 97 76
 П     П  О  Д  Ъ  Е  З  Д  П
74 96 74 37 39 75 97 70 39 74 79
  Д  О     П                 Е
39 37 71 74 98 35 94 90 98 97 94
     П     П     Е
96 74 98 74 76 97
```

Четвертый:

```
                              З
92 97 36 72 97 92 70 73 97 90 97
         О
72 38 39 74 76 97 34 79 78 97 70
     О     О     О
76 74 72 74 73 74 76 70 70 97 76
 О     О                    О
74 96 74 37 39 75 97 70 39 74 79
        П  О  Д  Ъ  Е  З  Д     Е
39 37 71 74 98 35 94 90 98 97 94
     О     О
96 74 98 74 76 97
```

Предполагалось, что участники на этом остановятся. Все решения с указанными тремя вариантами признавались правильными. Тем не менее, двое участников пошли еще дальше – отсеяли еще по одному варианту исходя из соображений частот встречаемости букв в текстах (во втором и третьем вариантах слишком часто встречается буква П; кроме того, во втором варианте присутствует удвоение буквы З, что не характерно для обычных текстов).

Задача № 4.

Приведенный в задаче протокол работы брелка и замка был изобретен в ЮАР и практически без изменения использовался во многих известных противоугонных системах. Вызывает лишь удивление, что достаточно продолжительное время очевидная уязвимость этого протокола не была замечена (примечательно, что заметили и воспользовались ошибкой разработчиков непрофессионалы в области защиты информации).

Перейдем собственно к решению, пояснив предварительно одно из условий задачи. Пусть СБ=k и СЗ=m, где k не меньше m. Отметим, что в данной ситуации при нажатии на кнопку брелка и срабатывании замка, счетчик замка принимает значение не m+1 (как ошибочно считали некоторые участники олимпиады), а k+1. Это сделано для того, чтобы один и тот же сигнал брелка не мог быть использован дважды. Запишем теперь по пунктам действия злоумышленника.

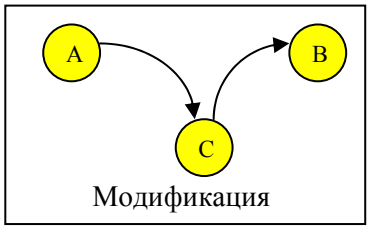
1) Пусть сейчас замок открыт. Владелец хочет запереть машину и уйти. Пусть СБ=k и СЗ=m, где k не меньше m. Владелец нажимает кнопку брелка. Злоумышленник запоминает посланный сигнал k и ставит помеху. В результате СБ=k+1 и по-прежнему СЗ=m, т.е. замок не закрылся.
2) Заметив, что машина не заперта, владелец повторно нажимает кнопку брелка. Злоумышленник снова запоминает сигнал k+1 брелка и опять ставит помеху. Значит СБ=k+2, а замок так и остается открытым, т.е. СЗ=m.
3) Выполнив действия пункта 2, злоумышленник немедленно посылает замку ранее запомненный сигнал k. Замок закрывается, и при этом СЗ=k+1. Владелец уходит, полагая, что машину запер он сам.
4) Злоумышленник посылает замку ранее запомненный сигнал k+1, и замок открывается.

К сожалению, многие участники решали задачу, исходя из слишком упрощенной модели реальной ситуации, отводя владельцу роль эдакого простачка, который, запирая машину, то ли не может, то ли забывает проверить сработал замок или нет: предлагалось выбрать момент, когда владелец попробует запереть автомобиль, поставить помеху, не дав тем самым замку сработать, а затем подождать пока владелец уйдет.

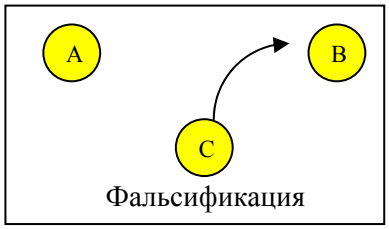
Задача №5
Коды аутентификации

При передаче информации по незащищенному (общедоступному) каналу связи возникает задача защиты от активных атак со стороны злоумышленника. Под активными

атаками понимают попытки фальсификации (имитации) и модификации (подмены) сообщения.



Модификация



Фальсификация

Цель активных атак — дезинформация получателя. Не вдаваясь в детали, сообщим, что сегодня имеется техническая возможность проведения подобных атак.

Для противодействия активным атакам используются так называемые *коды аутентификации* (кратко — A*-коды*). Они дают возможность получателю сообщения проверить его подлинность (или аутентичность). Проверка использует некий секрет, известный лишь отправителю и получателю сообщения, точно так же, как при обеспечении секретности используется секретный ключ шифрования. В общем виде код аутентификации представляет собой совокупность (S,E,M) трех конечных множеств, где S — множество *состояний источника*, E — множество *правил кодирования*, M — множество *сообщений*. Каждый элемент $e \in E$ представляет собой отображение $e: S \to M$. Правила кодирования "кодируют" состояния источника $s \in S$ в сообщения $m \in M$. Таким образом, сообщения передают информацию о наблюдаемом отправителем состоянии источника. Таковыми могут быть, например, результаты подбрасывания монеты при проведении жребия по телефону или обычные текстовые сообщения. Отображение $e \in E$ должно быть "обратимым", чтобы по данным m и e можно было однозначно восстановить s. Формально это требование записывается с помощью отображения f_e: $M \to S \cup \{0\}$, где 0 — число ноль (не принадлежащее S), и

$$f_e(m) = \begin{cases} s, \ \textit{если} \ e(s) = m, \\ 0, \ \textit{если такого} \ s \ \textit{не существует.} \end{cases}$$

Так вот в определении A-кода требуется, чтобы выполнялось равенство $f_e(e(s)) = s$, для любых $s \in S$ и $e \in E$.

Как стороны A и B используют A-код для аутентификации передаваемой информации? Прежде всего, они сообща выбирают (втайне от злоумышленника) правило кодирования $e \in E$. Пусть A желает передать состояние источника $s \in S$. Тогда он вычисляет $m = e(s)$ и посылает m к получателю B по каналу связи. Получив m, B использует то же правило кодирования e для вычисления $f_e(m)$. Если $f_e(m) \neq 0$, то m принимается как аутентичное. В противном случае — нет. На практике используются лишь такие A-коды, для которых вычисление $f_e(m)$ производится так же просто, как и $e(s)$.

При анализе надежности защиты от активных атак с помощью A-кодов предполагается, что злоумышленник знает об A-коде все, кроме секретного правила кодирования (ключа). Он (злоумышленник) проводит атаки на основе анализа свойств A-кода. При этом его действия являются наиболее целесообразными с точки зрения достижения успеха атаки. Приведем пример.

Рассмотрим A-код, для которого $S=\{H,T\}$ (сокращение от head — герб, tail — решётка), $E=\{e_1,e_2,e_3\}$, $M=\{m_1,m_2,m_3\}$. Действие правил кодирования запишем в виде таблицы (матрицы кодирования):

	m_1	m_2	m_3
e_1	H	T	0
e_2	T	0	H
e_3	0	T	H

В этой таблице указано, например, что состояние источника H кодируется с помощью правила e_1 в сообщение m_1, и т.д.

Пусть состояние источника выбирается случайно (как при подбрасывании монеты). При этом одно из двух состояний появляется чаще другого (как при использовании несимметричной монеты). Пусть p — "доля" состояния H. Тогда $(1-p)$ — "доля" состояния T. Например, если при бросании монеты она в среднем в двух случаях из трех выпадает гербом, то $p=2/3$. С целью уменьшения шансов на успех злоумышленника, A и B выбирают правило кодирования случайно. Пусть при этом $p(e_i)=x_i$ — "доля" e_i, $i=\overline{1,3}$. Числа x_i лежат в интервале $(0,1)$ и их сумма равна 1. Пусть $P(E)=(x_1,x_2,x_3)$. Эта тройка чисел называется *стратегией защиты*. Эта стратегия выбирается стороной защиты с таким расчетом, чтобы минимизировать "шансы" злоумышленника на успех.

Не вдаваясь в детали, укажем, что для данного A-кода при выбранной стратегии $P(E)$ эти шансы злоумышленника характеризуются величиной

$$L(\bar{x})=\max\{px_1;(1-p)x_2\}+\max\{(1-p)x_1;(1-p)x_3\}+\max\{px_2+px_3\}.$$

Сторона защиты выбирает *оптимальную стратегию* $P^{(0)}(E)$ так, чтобы минимизировать $L(\bar{x})$. Таким образом, возникает задача вычисления $\min\limits_{\bar{x}\in\Delta} L(\bar{x})$, где

$$\Delta=\{(x_1,x_2,x_3): 0<x_i<1,\ x_1+x_2+x_3=1\}.$$

Этот минимум можно вычислить, разбивая область Δ на подмножества Δ_j, $j=\overline{1,8}$, в которых раскрывается каждый максимум в выражении $L(\bar{x})$. Например, в случае, когда

$$\begin{cases} x_1p\ge x_2(1-p), \\ x_1\le x_2, \\ x_2\ge x_3, \end{cases}$$

$L(\bar{x})$ имеет вид $L(\bar{x})=p(x_1+x_2)+(1-p)x_3$. Как раз эта задача была предложена на олимпиаде. Решается она, например, следующим образом.

Заметим, прежде всего, что из условий следует неравенство $p\ge 1/2$. В самом деле,

$$x_1p\ge x_2(1-p)\ge x_1(1-p),$$

откуда $p\ge 1-p$ или $2p\ge 1$.

Выразив x_3 из условия $x_1+x_2+x_3=1$, получим следующее выражение:

$$L(\bar{x})=(x_1+x_2)(2p-1)+1-p.$$

Легко видеть, что минимальное значение это выражение принимает при максимально большом значении x_3. Остается найти достижимую верхнюю границу для значения x_3.

Из цепочки неравенств $x_3\le x_2\le\dfrac{p}{1-p}x_1$ получаем:

$$1 = x_1 + x_2 + x_3 \geq \frac{1-p}{p} x_3 + x_3 + x_3,$$

откуда следует, что $x_3 \leq \frac{p}{p+1}$. Ясно, что равенство $x_3 = \frac{p}{p+1}$ достигается лишь в случае, когда в указанной цепочке неравенств выполняются равенства, т.е. если $x_3 = x_2 = \frac{p}{1-p} x_1$. Мы нашли максимальное значение x_3. Отсюда получаем, что

$$\min L(\bar{x}) = \left(\frac{1-p}{p+1} + \frac{p}{p+1} \right) p + \frac{p}{p+1}(1-p) = \frac{p(2-p)}{p+1}.$$