35 Оценки на экзамене

Задача. Алиса получила на экзамене оценку a, Боб — оценку b. Оценки выставляются по 10-балльной шкале: $a, b \in \{1, 2, \ldots, 10\}$. Алиса и Боб хотят сравнить свои оценки, не раскрывая их друг другу. В распоряжении Алисы и Боба есть 10 шкафов с замками и по 2 ключа от каждого замка. Помогите Алису и Бобу организовать следующие сравнения: 1) $a = b$? 2) $a \geq b$?

Решение. Организация сравнения $a \geq b$ известна как задача о миллионерах, сравнения $a = b$ — как задача о социалистических миллионерах.

Задача о социалистических миллионерах может быть решена следующим образом:

1. Алиса и Боб извлекают из шкафов все содержимое, закрывают шкафы и приклеивают к ним листки с номерами от 1 до 10. Листки можно сорвать, но нельзя переклеить со шкафа на шкаф. Алиса и Боб расписываются на листках, поэтому на шкафы нельзя наклеить новые листки с другой нумерацией.

2. Алиса оставляет ключ от шкафа с номером a, а остальные ключи разрушает на глазах Боба. Ключи выглядят одинаково, и поэтому Боб не знает, ключ от какого шкафа остался у Алисы.

3. Боб кладет в шкаф с номером b тетрадный листок. Алиса находится в соседней комнате и не может наблюдать за действиями Боба.

4. Алиса срывает со шкафов листки с номерами, меняет шкафы местами. Боб находится в соседней комнате и не может наблюдать за действиями Алисы.

5. Алиса в присутствии Боба пробует открыть своим ключом каждый из шкафов. Если в открывшемся шкафу есть листок Боба, то $a = b$, если нет — то $a \neq b$.

6. Боб в присутствии Алисы открывает все остальные шкафы. Алиса и Боб убеждаются, что ровно один шкаф непустой. В противном случае одна из сторон смошенничала, и результаты сравнения на шаге 5 аннулируются.

Задача о миллионерах может быть решена почти также. На шаге 3 Боб кладет тетрадные листки в шкафы с номерами от 1 до $b - 1$. Если в открывшемся на шаге 5 шкафу есть листок Боба, то $a < b$, если нет — то $a \geq b$. На шаге 6 Боб открывает шкафы в отсутствии Алисы. Боб проверяет, что в шкафах имеется в точности $b - 1$ его листков.

При решении задач мы сделали несколько неявных допущений: все шкафы одинаковы, ключи легко разрушить, подписи Алисы и Боба трудно подделать, Алиса способна переставить шкафы местами, Алиса и Боб не могут наблюдать за действиями друг друга и т.д. В совокупности эти ограничения довольно обременительны и «физические» решения задач оказываются достаточно громоздкими.

«Цифровые» решения дается специальными криптографическими протоколами (см. `http://en.wikipedia.org/wiki/Millionaire%27s_Problem`, `http://en.wikipedia.org/wiki/Socialist_millionaire`). □