

## Доказательства без разглашения

«А это вам знать пока рано», – сказала Баба-Яга своим 33 ученикам и скомандовала: «Закройте глаза!». Правый глаз закрыли все мальчики и треть девочек. Левый глаз закрыли все девочки и треть мальчиков. Сколько учеников всё-таки увидели то, что знать пока рано?

**Ты доказываешь банку онлайн, что имеешь право снимать свои деньги. А хакер, скопировав доказательство, не может это доказать! Как так?**

### Не говори лишнего

При обмене информацией важно не предоставить возможности узнать больше, чем положено.

1. Суду предъявлен набор из 100 одинаковых с виду монет. Суд знает, что все настоящие монеты весят одинаково, фальшивые – тоже одинаково, но легче настоящих. Адвокат знает, какие монеты на самом деле фальшивые. Задача адвоката: показать суду, сколько есть фальшивых монет, не разгласив ни про какую монету, фальшивая она или настоящая. (Адвокат должен делать взвешивания на чашечных весах без гирь. Число взвешиваний не ограничено. Запрещены взвешивания и группы взвешиваний, из которых логически выводится, что конкретная монета фальшивая или настоящая.)

а) Суд уже установил, что фальшивых монет 3 или 4. Как адвокату показать, что их ровно 4?

б) Суд уже установил, что фальшивых монет 1 или 2. Может ли адвокат показать, что их ровно 1?

2. В игре «Дипломат» игрокам раздали по 5 карт. В свою очередь хода игрок А может задать любому другому игроку Д любой вопрос типа «Да/Нет» о картах Д. Если Д ответит «Да», игрок А задает следующий вопрос, и т.д. пока не получит ответ «Нет» (тогда очередь хода переходит к след. игроку). Как игроку А успеть за свою очередь сделать известными все карты Д?

3. Из колоды вынули 13 пиковых карт, показали всем, перетасовали, и раздали Грише и Леше по 6 карт, а оставшуюся карту спрятали. Игроки могут по очереди сообщать вслух открытым текстом любую информацию о своих картах. Могут ли сообщить друг другу свои карты так, чтобы при этом посторонний наблюдатель не смог вычислить местонахождение ни одной из карт?

### Зачётные задачи

4. Из колоды вынули 7 карт, показали всем, перетасовали, и раздали Грише и Леше по 3 карты, а оставшуюся карту отдали Коле. Игроки могут по очереди сообщать вслух открытым текстом любую информацию о своих картах. Могут ли сообщить друг другу свои карты так, чтобы при этом Коля не смог вычислить местонахождение ни одной из карт (кроме той, что у него)?

5. В условиях задачи 1

а) Всего 29 монет. Суд уже установил, что фальшивых 1 или 2. Как адвокату показать, что их ровно 2?

б) Всего 80 монет. Суд уже установил, что фальшивых монет 2 или 3. Как адвокату показать, что их ровно 3?