Неоднозначные данные, или Доказательство без разглашения

Материалы к научно-популярной лекции А.В.Шаповалова

Анонс

При общении онлайн нам все время приходится сообщать свои секретные данные, например, пароли. А вдруг их кто-то перехватит? Цена может быть очень большой: если злоумышленник или нечестный банковский служащий получит доступ к нашему счету, мы можем всех сбережений лишиться! Но, оказывается, клиент может доказать, что он - это он, не дав возможности другому скопировать это доказательство и затем выдать себя за него. И это можно показать на примерах задач, понятных даже семикласснику.

План

Предъявление пропуска в реальности и в сети. Проблема копирования (отпечаток пальца, сетчатка глаза).
В сети можно скопировать всё. Суммы велики, просто на честность служащего полагаться недостаточно.
Головоломка с пересылкой по почте и двумя замками.
Как доказать, что информацию невозможно узнать? Неразличимые примеры.
Задача о кубе с бриллиантами.
Задача о точке внутри квадрата.
Идеальный шифр.
Бросание на пальцах.
Сложение по модулю и задача о колпаках.
Раздача карт по телефону.
Надо уметь доказать онлайн что ты – тот, за кого себя выдаёшь. При этом, если даже злоумышленник скопировал бы все переданные тобой данные, он не смог бы этим воспользоваться, выдавая себя за тебя.
Взвешивания без разглашения.
Круглая пещера.
Дополнительные знания помогают обмениваться информацией.
7 карт, одну спрятали.

Листок с задачами

«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?

Задача 1. Вы хотите послать другу ценный предмет. У вас есть коробка, которая больше, чем сам предмет. У вас есть несколько навесных замков с ключами. У коробки есть кольцо (петли), которое больше чем было бы достаточно для замка. Но у вашего друга нет ключей ни от одного вашего замка. Что же делать?
Замечание: Вы не можете послать ключ в незапертой коробке, так как его могут скопировать.

Задача 2. У Кащея есть куб, в каждой вершине которого вставлено по алмазу. Известны веса этих алмазов: 1 карат, 2 карата, ..., 8 карат. Кащей предлагает Ивану Царевичу такую игру: он сообщает Ивану сумму весов алмазов на каждом ребре. Если после этого Иван правильно назовет, куда какой по весу алмаз вставлен, то получит этот куб вместе с алмазами, а если хотя бы в одном месте ошибется, то распрощается с головой. Стоит ли Ивану соглашаться играть?

Задача 3. На плоскости расположен квадрат, и невидимыми чернилами нанесена точка P. Человек в специальных очках видит точку. Если провести прямую, то он отвечает на вопрос, по какую сторону от неё лежит P (если P лежит на прямой, то он говорит, что P лежит на прямой). Нужно определить, лежит ли точка P внутри квадрата. Можно ли это наверняка узнать
а) за два вопроса?
б) за три вопроса?

Задача 4. Двое преподавателей хотят выбрать наугад один из 10 столиков в ресторане. Как им быстро бросить жребий, чтобы шансы каждого столика были одинаковы, и вклад каждого в жребий был одинаково решающим?

Задача 5. Король выстроил 7 мудрецов колонну для испытания, и надел каждому на голову колпак. На каждом из колпаков – цифра от 0 до 9 (цифры могут повторяться). Каждый видит только цифры только на колпаках всех впереди стоящих. Далее мудрецы по порядку от заднего к переднему называют вслух по цифре. Тот, кто верно назовет свое число – спасется, остальных с позором уволят. Мудрецы заранее знали условия испытания и могли договориться, как действовать. Какое наибольшее число из них смогут спастись?

Задача 6. Трое игроков А, Б и В хотят сыграть в карты по телефонуДля этого им надо научиться передавать друг другу карты так, чтобы не разглашать лишней информации. Можно считать, что карты пронумерованы цифрами от 0 до 9.
а) Как А и Б могут наугад выбрать карту и сообщить её В, самим не узнав этой карты?
б) Как В может передать известную ему карту А или Б, не узнав, кому именно она досталась, и не сообщая другому, что это за карта?

Задача 7. 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 0 или 1. Адвокат хочет показать, что монета ровно 1. Докажите, что без разглашения этого не удастся.

Задача 8. Из колоды вынули 7 карту, показали всем, перетасовали, и раздали двум игрокам по 3 карты, а оставшуюся карту спрятали. Игроки могут по очереди сообщать вслух открытым текстом любую информацию о своих картах. Могут ли они сообщить друг другу свои карты так, чтобы при этом зритель со стороны не смог вычислить местонахождение ни одной из семи карт?

Сириус, популярная лекция, 20 сентября 2016 г, http://www.ashap.info/Uroki/Sirius/1609/index.html