КАК БУСЕНЬКА ДЕЛИЛА СЕКРЕТ

Константин Кохась

Дверца, ведущая в погреб, открылась и на пороге появилась мышь Огрыза.

– Всё по плану, – кивнув собравшимся, сказала Огрыза, – он заказал доставку и сборку на 11 утра.

– Ну Кузька, теперь вся надежда на тебя, – сказала Бусенька. – Устанавливать сейф Злобнопотам будет у себя в подвале. Твоя задача – узнать название модели сейфа. Оно может быть написано на задней стенке сейфа, в инструкции пользователя, на чеке, но скорее всего, – просто на коробке. Проберись туда и запомни последние 4 символа.

– Я добуду их во что бы то ни стало! – пафосно сказал Кузька и отправился на задание.

Прошло не более получаса, и Кузька радостно доложил:

– Модель сейфа – 19ДЗ!

– Что ещё за ДЗ? – проворчала Огрыза.

– Серьёзная модель, – объяснил дятел Спятел, – цельнометаллическая конструкция из легированной стали, защита от высверливания, антикувалдное покрытие, новейший электронный кодовый замок, который к тому же очень прост в обращении – ключом к сейфу является число от 1 до 8.

– От 1 до 8? Да мы подберём код за 4 секунды! – сказала Огрыза.

– Не советую, – возразил дятел Спятел. – Сокращение ДЗ означает «динамитный замок» – он взрывается, если ввести неверный код. Поэтому прежде чем открывать сейф, стоит заранее узнать правильный код. А правильный код хозяин сейфа устанавливает по своему усмотрению.

– Всего-то, – сказала Бусенька, – тогда за дело! Навеем Злобнопотаму правильное усмотрение!

* * *

Огрыза, Кузька, Горгулий и Ушася удобно расположились на диване. Дятел Спятел взмахнул дирижёрской палочкой, поклонился зрителям и торжественно отдёрнул занавеску. Бусенька осторожно

выглянула в окно. Убедившись, что Злобнопотам удобно устроился на коврике под дверью и приготовился подслушивать, она громко спросила:

– Так какие у тебя проблемы с секретной комбинацией?

– Видишь ли, – тоже громко ответил дятел Спятел, – в жизни всякое бывает. Я хочу, чтобы в экстренном случае мои друзья – Огрыза, Ушася, Кузька – имели бы возможность открыть мой сейф.

– Ну так скажи им код от замка.

– Но я не хочу из своего сейфа делать проходной двор! – воскликнул дятел Спятел и, отвернувшись от зрителей, трагически произнёс в окно. – Мне не нужно, чтобы в моём сейфе мог рыться кто угодно и когда угодно!! Конечно, я должен сообщить каждому какой-то секрет про кодовую комбинацию, но я не хочу, чтобы они знали сам код. Я хочу, если можно так выразиться, поделить мой секретный код на 3 секретные части, то есть сообщить моим друзьям три таких секрета, чтобы они смогли открыть сейф, только если соберутся все втроём, а вдвоём или поодиночке у них ничего не получилось бы.

– Скажи им какие-нибудь числа, которые в сумме дают код. По отдельности эти числа не имеют никакого отношения к коду. Пока все владельцы частей секрета не соберутся вместе, они не узнают сумму, и значит, не смогут открыть замок.

– Замечательная идея! Но постой… я же забыл про тебя и Горгулия! Впрочем… толпиться впятером возле сейфа – слишком тесно. Как ты думаешь – почти прокричал дятел Спятел, – нельзя ли поделить мой секрет на пять частей так, чтобы любые трое (или больше) из вас смогли открыть сейф, объединив свои секретные данные, а любые двое – не могли?

– Сложная задача, – голосом опытного лектора сказала Бусенька, – но, кажется, я знаю, что нужно делать! Для примера давай я объясню тебе ещё один способ поделить секрет на троих. Заведём табличку, в которой Огрызе, Ушасе и Кузьке выделим по отдельному столбцу. Напишем в каждый столбец число 2, потом в первый и второй столбец впишем 3, во второй и третий – 5, в первый и третий – 7. Теперь каждому

дадим произведение чисел, записанных в его столбце. Тогда Огрыза получит число 42, Ушася получит 30, а Кузька – 70. Это и есть части секрета. Ты поговоришь с каждым своим другом наедине и в знак высокого доверия сообщишь ему секретное число.

А потом, собрав всех вместе, ты скажешь, что ключ к сейфу – это наибольший общий делитель всех чисел, которые ты им сообщил.

ОГРЫЗА	УШАСЯ	КУЗЬКА
2	2	2
3	3	
	5	5
7		7
42	30	70

– Нет-нет, – перебил дятел Спятел, – это очень важный момент, нужно добавить пафоса. Я приглашу их всех к себе и торжественно объявлю: дорогие друзья, ключ к сейфу – это наибольший общий делитель всех чисел, которые я кон-фи-ден-ци-ально сообщил каждому из вас!

– Да, это будет сильная сцена, – согласилась Бусенька. – Но вернёмся к нашему примеру, здесь НОД(42, 30, 70) = 2. Мы-то этот ответ знаем заранее, потому что именно число 2 мы записали в каждый столбец таблицы. Ты ведь можешь сам задавать код сейфового замка?

– Могу! Я могу поставить такой код, какой захочу!

– Вот и прекрасно. Ты задаёшь секретный код «2» и сообщаешь части секрета друзьям. В отличие от тебя твои друзья смогут узнать код, только если встретятся все втроём. Если же встретятся только двое и подсчитают НОД своих чисел, у них получатся совершенно другие ответы: у Кузьки и Огрызы НОД(42, 70) = 14, у Ушаси и Огрызы НОД(42, 30) = 6, а у Ушаси и Кузьки НОД(30, 70) = 10.

– Потрясающе! А зачем мы перемножили числа? Всё равно наши друзья начнут раскладывать числа на множители. Давай сразу дадим им список множителей!

– Во-первых, чтобы искать НОД, раскладывать на множители не обязательно. А во-вторых, ты учти:

они ведь собираются грохнуть твой сейф. Пусть хотя бы немного поработают!

– Да, пожалуй, мой сейф – это не коробочка с мусором, пусть поработают! Но вот что ещё меня беспокоит: когда собираются двое, наибольший общий делитель их чисел обязательно делится на НОД всех трёх чисел, то есть на мой секрет! Если Кузька и Огрыза вычислят, что их НОД равен 14, то они догадаются, что число 14 слишком велико для значения секрета, и начнут перебирать его делители, а их очень мало – 1, 2 и 7. Всего три варианта! Они почти угадали мой секретный код!

– Тогда давай усложним эту схему. Возьмём числа покрупней, а кодом будет не сам НОД, а, например, его остаток при делении на 9. Теперь соображения с величиной числа не сработают.

Кроме того, если вписать в табличку большее количество чисел, то НОД будет иметь много делителей, и перебирать их будет бесполезно.

– Большие числа... А вдруг они ошибутся, пока всё это вычисляют?

– У сейфа динамитный замок! Не ошибутся!

– А ты не забыла, что мне нужно разделить секрет не на три, а на пять частей? Не представляю себе, как это всё можно реализовать и при этом не запутаться! – пожаловался дятел Спятел раскрытому окну.

– Да запросто! Вот смотри: выпишем большой список простых чисел. Есть у тебя листок бумаги?

Да, спасибо, вот выписываю, ну, допустим..., не обязательно же брать все простые числа подряд: 19, 37, 73, 109, 127, 163, 181, 199, 307, 379, 433, 487, 523, 541, 577, 631, 757, 811, 883, 937, 991.

Ага, получилось 21 число. Хватит, пожалуй. У нас есть пятеро друзей, между которыми мы делим секрет. Заведём таблицу с 5 столбцами. Выберем одно из чисел и запишем его в каждом столбце – это число (точнее, его остаток) задаёт код сейфа. Дальше рассмотрим всевозможные пары друзей – (первый, второй), (первый, третий), ..., (четвёртый, пятый) – всего получится 10 пар. И дальше раскладываем оставшиеся 20 чисел по этим парам – два числа в первый и второй столбец, ещё два числа – в первый и третий и т.д.

Когда таблица заполнена, перемножим числа в каждом столбце – это и будут части секрета. Вот и всё!

1	2	3	4	5
937	937	937	937	937
127	127			
883	883			
631		631		
757		757		
...	...	...	...	...
			109	109
			433	433

– Постой-постой, дай-ка я проверю, – сказал дятел Спятел и, взяв бумажку с числами, подошёл к окну. – Допустим, Огрыза и Горгулий вычисляют свой НОД. Секретное число у каждого из них содержит много простых множителей. Среди этих множителей есть общий множитель a, который мы дали всем, а также два простых числа b и c, которые мы дали только им двоим. Получается, что их НОД равен abc. И они знают, что мой секрет – это какой-то делитель этого НОДа, то есть какое-то из чисел 1, a, b, c, ab, bc, ac, abc. Восемь возможностей! Прекрасно! Им ни за что не угадать нужный вариант!

– А если встретятся трое, их секреты будут иметь ровно один общий простой делитель – то число, которое мы дали всем друзьям. Значит, втроём они уже смогут узнать код!

– Ещё нужно будет поделить его с остатком на 9, – добавил дятел Спятел, – ой-ой, сквозняк! держи! хватай, улетает!! – И с этими воплями дятел Спятел, для убедительности опрокинув стул, аккуратно отпустил за окно листок бумаги со списком простых чисел. Листок, покачиваясь и переворачиваясь, стал не спеша опускаться вниз. Раздавшийся снизу хруст веток и тяжёлые быстрые удаляющиеся шаги подтвердили, что письмо нашло своего получателя.

Когда шум и шорохи утихли, сидевшие на диване и до сих пор не проронившие ни звука Огрыза, Кузька, Горгулий и Ушася дружно зааплодировали.

– Ну хорошо, теперь мы знаем код от его сейфа, – сказал Кузька, – а зачем он нам?

Художник Инга Коржнева