

КАК БУСЕЦЬКА СБРАСЫВАЛА ПАРОЛЬ

– Этот сейф вле-е-етел мне в копеечку, – жаловался коллега Спрудль Горгулию и дятлу Спятлу. – Продавец целый час расхваливал неубива-а-емость этого сейфа и его сверхнадёжность – «но-а-а-вейшие технологии защиты», «современнейшие материалы», «прогрессивнейшая система хранения пароля» – бульк!

– Боюсь, мы не сможем ничем вам помочь. Сейфы – не наш профиль, – бесстрастно сообщил Горгулий. – Мы специализируемся на услугах только математического характера!

– Вот у меня-а-а и возникло с этим сейфом, бульк,... математическое затруднение. Я забыл пароль!

– Какой пароль? – спросил дятел Спятел.

– Ну какой-какой. Обычный. Кодовую комбина-а-ацию. Многочлен, с помощью которого открывается дверца.

– Многочлен? Для открывания дверцы? – Горгулий с удивлением посмотрел на коллегу Спрудля. – Мне кажется, кто-то из нас спятил!

– Это все «на-а-адёжнейшие методы», – пояснил коллега Спрудль. – В качестве кодовой комбинации сейфа используется секретный многочлен девятой степени. Коэффициенты многочлена – 10 произвольных натуральных чисел – это, можно сказать, бульк! и есть пароль.

– Десять чисел? – воскликнул Горгулий. – Как можно запомнить 10 чисел?

– Иногда можно, причём без особых проблем, – возразил дятел Спятел. – Например, 10 единиц запомнить не очень трудно.

– Мне пришла в голову комбина-а-ация 1, 2, 3, ..., 9, 10, – похвастался коллега Спрудль. – Но инструкция к сейфу запрещает использование «столь примитивных па-а-аролей». Пришлось придумывать пароль посложнее. А теперь оказалось, что я его забыл! Помню, что я рассма-а-атривал разные последовательности, например такую

1, 1, 2, 3, 5, 8, 13, 21, 34, 55,

или такую, бульк,

1, 9, 36, 84, 126, 126, 84, 36, 9, 1,



или даже та-а-а-ую¹

1, 11, 21, 1211, 111221, 312211, 13112221,
111321321...

Но потом я случайно наткнулся на совершенно потряса-а-а-ющую последовательность коэффициентов, только вот теперь не могу вспомнить, какую именно. А другим способом этот сейф никак не открыть – он «а-а-абсолютно невзламываемый»!

– Неужели «прогрессивная система хранения пароля» не предполагает, что хозяин может забыть такой сложный пароль?

– Не «прогрессивная», а «прогресси-и-ивнейшая». Предполагает. «В случае если вы забыли пароль, предусмотрена операция „сброс пароля”».

– Вот и славненько, – жизнерадостно улыбнулся Горгулий, аккуратно сложив в стопку папки, лежавшие на столе. – Сбросьте пароль, и всё будет хорошо. А мы сегодня уже закрываемся.

Но коллега Спрудль, кажется, не понял намёка.

– Для сброса паро-о-о-ля, – пояснил он, – используется пульт управления сейфом. Вот, видите, он выглядит как обычный калькуля-а-атор, только экран побольше, бульк. Да-а-а это, собственно, и есть калькулятор, но с одной дополнительной кнопкой – Pass. В обычном режиме работы пульта при нажатии на эту кнопку ни-и-ичего не происходит.

– Главное – не навредить, – философски похвалил дятел Спятел.

– А в режиме сброса паро-о-о-ля, – продолжил коллега Спрудль, – эта кнопка «позволяет вычислить значение секретного многочлена F в любой точке», то есть если набрать на экра-а-ане число x и нажать Pass, бульк, экран покажет значение $F(x)$.

– Каждое найденное значение даёт уравнение на коэффициенты, – сказал Горгулий, – например, если $F(t) = s$, мы получаем уравнение

$$a_1 t^9 + a_2 t^8 + \dots + a_9 t + a_{10} = s.$$

Накопите побольше уравнений и, решив полученную систему, найдите коэффициенты a_1, a_2, \dots, a_{10} . Не стоило ради такой ерунды обращаться к нам за помощью!

¹ Попробуйте её продолжить, распознайте остальные последовательности.





– Да, именно так и написано в инструкции, – согласился коллега Спрудль, по-прежнему игнорируя намёки. – «Конечно, такой способ восстановления пароооля очень громоздок, но чего же вы хотели, бульк, забывание пароля – это возмутительная бе-е-е-зответственность!» Проблема в том, что они разреша-а-ают вычислить всего лишь 10 значений, бульк! После этого кнопка **Pass** отключается.

– Вам ровно 10 значений и потребуется, – подтвердил Горгулий, – получится система из 10 уравнений с 10 неизвестными.

– Но я не могу найти 10 значе-е-ений! – воскликнул коллега Спрудль. – Я ради эксперимента вычислил несколько значений до того, как обратил внима-а-ание на запрет. И естественно, ни одного из них не запомнил, бульк. А тепе-е-ерь кнопка **Pass** позволит сделать всего лишь три-четыре вычисления.

– Свяжитесь с сервис-центром производителя сейфа! – строго сказал Горгулий.

– Они сказали, что единственный способ, который может помочь в этой ситуа-а-ации, – это обратиться в вашу фирму!

Горгулий скорчил гримасу и посмотрел на коллегу Спрудля.

– Ну что ж, – вздохнул Горгулий, – давайте составим договор на оказание интеллектуальной услуги...

* * *

– Какой интересный калькулятор, – сказала Бусенька, разглядывая пульт от сейфа. – Сколько тут разных функций!

– Халтурщики, – возразил дятел Спятел, имея в виду производителей сейфа. – Вместо того чтобы разработать собственный оригинальный пульт, они взяли инженерный калькулятор и слегка его переделали.

– Почему при включении пульта на экране появляется число 1?

– Они называют это «энергосберегающим реше-е-ением!» – пояснил дятел Спятел. – Реклама, короче. Обычно включаешь калькулятор, и на экране появляется 0. А у этих – не 0, а 1. Якобы для изображения единицы меньше расходуется заряд, чем для нуля.

– А что делает кнопка **Num**?

– Как я понял, – объяснил Горгулий, – калькулятор умеет показывать числа в разных системах счисления. Поменять систему счисления можно кнопкой **Num**. Набираешь 8, нажимаешь **Num** – и теперь все вычисления будут в восьмеричной системе счисления. Набираешь 38, нажимаешь **Num** – и вычисления будут в тридцативосьмеричной системе счисления.

Бусенька тут же нажала **3**, **8**, **Num**. На экране появилась запись **10**.

– Да, ты прав, – сказала Бусенька, – число 38 в 38-ричной системе счисления как раз и записывается как **10**. А вот и кнопка с кружочком, чтобы рисовать экзотические цифры. Ну-ка проверим.

И Бусенька нажала **1**, **2**, **○**. На экране появилось число **12**, которое в 38-ричной системе счисления является однозначным числом. Как и положено однозначному числу, оно записывается с помощью одной 38-ричной цифры – цифры «12». Бусенька нажала кнопку **x²** и на экране появился результат: **330**.

– Ух ты, работает! – воскликнул Горгулий. – Число **330** в 38-ричной системе счисления – это $3 \cdot 38 + 30 = 144$, то есть как раз 12 в квадрате!

– Неплохо, – похвалила Бусенька. – Думаю, с помощью этой кнопки мы сумеем разделаться с нашим клиентом особенно зрелищно.

* * *

Когда на следующий день коллега Спрудль явился в назначенное время, его уже ждали дядел Спятел, Бусенька и Горгулий.

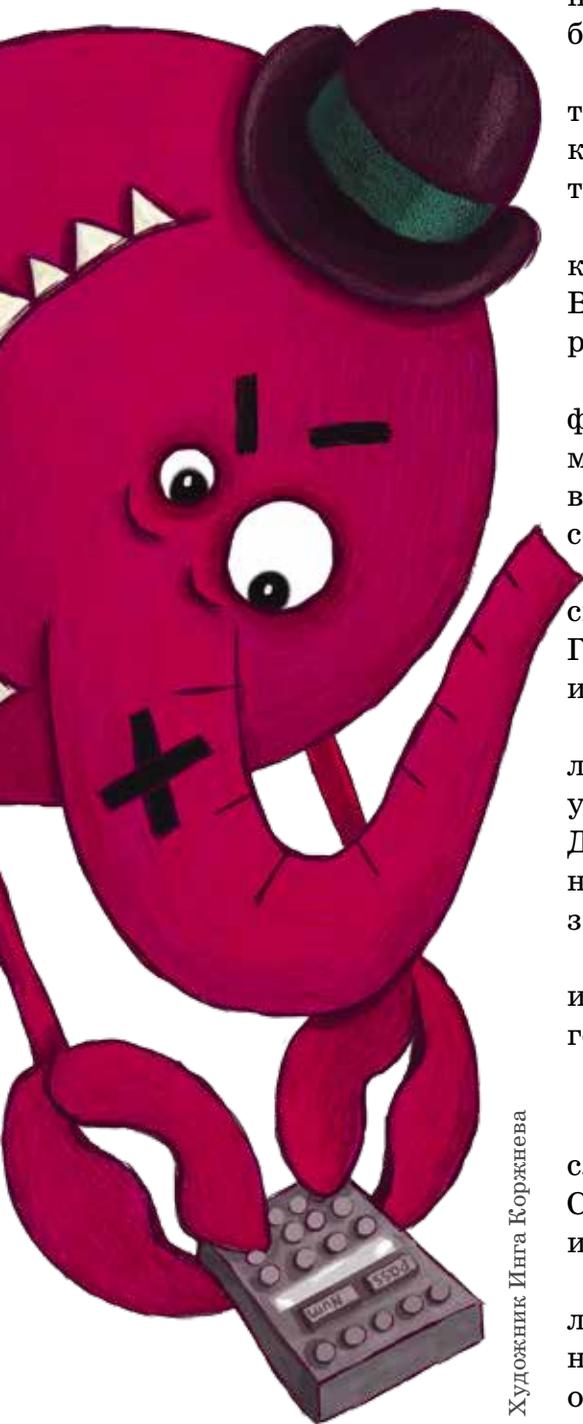
– Послушайте заключение нашего эксперта, – сразу взялся за дело Горгулий, кивнув в сторону Бусеньки.

– Традиционный способ восстановления пароля, – сообщила Бусенька, – требует решения системы, состоящей из 10 линейных уравнений с 10 неизвестными.

– Да-да, именно так и устро-о-оен мой сейф, – подтвердил коллега Спрудль.

– Самый популярный способ решения линейных систем – метод Гаусса. В нашем случае он потребовал бы нескольких тысяч операций, – продолжила Бусенька. – Ваш пульт, конечно, обладает некоторыми вычислительными возможностями, но тут не обойтись без настоящего компьютера. Ситуация, однако,





Художник Инга Корженева

отягощается тем, что мы даже не можем получить эту систему целиком! Поэтому нам пришлось изобрести совершенно новый метод восстановления пароля.

– Предлагаю назвать его «методом Бусеньки – Гаусса», – прокомментировал Горгулий. – Для восстановления пароля этим методом компьютер не понадобится, достаточно иметь пульт от сейфа.

– Да, вычислительная эффективность нового метода потрясает воображение, – гордо сказала Бусенька. – Вместо выполнения многих тысяч операций, потребуется лишь трижды нажать кнопку на пульте!

– Да что вы, всего-о-о три раза? – удивлённо воскликнул коллега Спрудль и тут же взревел: – Что-о-о?! Вы выписали мне этот дикий счёт за вычисление, которое реализуется нажатием трёх кнопок?! Бульк?!

– Я же лично отговаривал вас обращаться в нашу фирму! – воскликнул Горгулий. – Вы проявили чрезвычайную настойчивость, если не сказать назойливость, и заказали услугу, за которую не взялся даже сервис-центр производителя!

– Но вы поступили очень мудро, найдя настоящих специалистов, – дипломатично сказал дятел Спятел. – Главное – не навредить! Мы же хорошо знаем, что происходит, когда вы сами начинаете жать на кнопки.

– Короче, уплыли ваши денежки, – подытожила Бусенька. – Сядьте поудобнее и просто получайте удовольствие, наблюдая за работой профессионала. Должна вам честно сказать, что потребуется ещё одно нажатие – мне придётся сначала включить пульт. Но зато кнопку `Pass` я нажму всего два раза.

Она положила перед коллегой Спрудлем пульт и включила его в режиме сброса пароля. На экране загорелась единица. Бусенька нажала `Pass`, `Num`, `Pass`:

④ ③ ③ ⑥ ④ ⑤ ④ ⑥ ⑥ ⑥.

– Это она, моя совершенно потряса-а-ающая последовательность! – восхищённо произнёс коллега Спрудль. – Надо же, восстанови-и-и-или и даже без использования компьютера!

– Можем и с компьютером, – радостно откликнулась Бусенька. – Тогда хватит всего одного нажатия на кнопку `Pass`. Только компьютер должен считать с о-о-очень большой точностью!

См. пояснения в ответах