Джордж и Анни отправляются в космос, чтобы спасти Землю

Космос, компьютеры и многое другое!

ДЖОРДЖ И КОД, КОТОРЫЙ НЕ ВЗЛОМАТЬ

ЛЮСИ И СТИВЕН ХОКИНГ

Джордж

Стивен Хокинг

Джордж и код, который не взломать

«Розовый жираф»
2014

УДК 821.111-93
ББК 84(4Вел)-44

Хокинг С. У.

Джордж и код, который не взломать / С. У. Хокинг — «Розовый жираф», 2014 — (Джордж)

ISBN 978-5-4370-0107-3

«Джордж и код, который не взломать» – четвертая книга о приключениях Джорджа в космосе, написанная астрофизиком, гениальным пропагандистом науки Стивеном Хокингом и его дочерью, научным журналистом Люси Хокинг. Эта космическая эпопея стала сверхпопулярной среди детей от 7 до 12 лет по всему миру не только благодаря головокружительному и остроумному сюжету, сколько из-за того, как там излагается научная информация. Основные понятия и законы физики и самые последние новости из области космических исследований, точные, понятные формулировки и вдохновляющие статьи ученых, которые прямо сейчас – в обсерваториях или в ЦЕРНе – занимаются актуальными исследованиями. И все это написано понятным и интересным младшему школьнику языком.В четвертой книге Джордж и Анника снова должны совершить невероятные подвиги. На летних каникулах они мечтают о новых путешествиях в космос. А тем временем на Земле разворачиваются совершенно невероятные события: банкоматы плюются деньгами, товары раздаются бесплатно, полки магазинов пустеют, начинаются грабежи, разбои, хаос. Теле- и радиовещание прерываются странными сообщениями… Что происходит? Неужели неведомый сверхмощный компьютер взломал все остальные компьютеры планеты?! Чтобы спасти мир, Джордж и Анни отправляются на встречу с космическими роботами-злодеями.

УДК 821.111-93
ББК 84(4Вел)-44

ISBN 978-5-4370-0107-3

© Хокинг С. У., 2014
© Розовый жираф, 2014

Содержание

Стивен Хокинг, Люси Хокинг
Джордж и код, который не взломать

Lucy & Stephen Hawking
GEORGE AND THE UNBREAKABLE CODE

Переводчик и редактор благодарят П. Е. Гольдина и С. А. Канищева за консультирование по разнообразным научным вопросам: от происхождения жизни миллиарды лет назад до квантового компьютера, который ещё не создан.

© Л. Хокинг, текст, 2014 / Text copyright © Lucy Hawking 2014
© Е. Канищева, перевод на русский язык, 2015
© ООО «Издательство «Розовый жираф», издание на русском языке, 2015
© Издательство «Рэндом хаус», иллюстрации Г. Парсонса, 2014
1-е издание на английском языке, 2014

* * *

Всем, кому доводилось смотреть в ночное небо с любопытством и изумлением

Новейшие научные теории!

В сюжет этой книги вплетены интереснейшие научные очерки, которые помогут тебе наглядно представить, о чём идёт речь. Все они написаны известными учёными:

Мой робот, твои роботы
Профессор Питер Макоуэн,
Лондонский университет Квин Мери

История жизни
Профессор Майкл Рейсс,
Институт образования, Лондонский университет

Квантовые компьютеры
Доктор Реймонд Лафламм,
директор Института квантовых вычислений Университета Ватерлоо

Строительные блоки жизни
Доктор Тоби Бленч,
химик-исследователь

3D-печать
Доктор Тим Престидж,
компания Totempole Consulting

Жизнь во Вселенной
Профессор Стивен Хокинг,
директор Института теоретической космологии Кембриджского университета

Мы благодарим за дополнительные материалы доктора Стюарта Ранкина из Центра высокопроизводительных вычислений при Кембриджском университете.

Глава первая

На какой-нибудь другой планете дом на дереве мог бы стать идеальным местом для наблюдения за звёздами. Например, на планете, где нет никаких родителей. Этот домик между ветвями большой яблони, растущей во дворе, располагался как раз на нужной высоте, в нужном месте и под нужным углом для того, чтобы человек вроде Джорджа мог всю ночь разглядывать звёзды. Но вот у мамы и папы были совсем другие идеалы, в число которых входили домашние задания, помощь по хозяйству, сон в кровати под одеялом, ужин в кругу семьи и «общение» с младшими сестрёнками-близняшками. Ни одно из этих занятий не вызывало у Джорджа ни малейшего интереса.

Джордж хотел сфотографировать Сатурн. Сделать хотя бы одну-единственную крошечную фотографию любимой планеты – огромного замёрзшего газового гиганта с прекрасными кольцами из льда и пыли. Но в это время года, когда солнце садится так поздно, Сатурн появляется на ночном небе почти в полночь. А поскольку Джорджу положено укладываться в постель гораздо раньше, нет никакой надежды, что родители разрешат ему так долго торчать на дереве.

Болтая ногами на краю дощатой платформы, Джордж вздохнул и попытался подсчитать, сколько часов и дней осталось до того, как он наконец вырастет и станет свободным человеком…

– Свистать всех наверх! – прервал его раздумья знакомый голос, и на платформу запрыгнула тоненькая фигурка в мешковатых камуфляжных шортах, толстовке с капюшоном и бейсболке.

– Анни! – обрадовался Джордж.

Анни была его лучшим другом с тех самых пор, как она со своими папой и мамой пару лет назад переехала в Фоксбридж. Анни с Джорджем жили в соседних домах, но дружили они

не только поэтому. Просто Джорджу нравилась Анни: она была очень умная, с ней всегда было весело и интересно, и ещё она ничего не боялась и вообще была супер. Ни одно приключение не обходилось без Анни, ни одна теория у неё не оставалась непроверенной, ни одна гипотеза неоспоренной.

– Чем занимаешься? – спросила Анни.

– Ничем, – вздохнул Джордж. – Просто жду.

– Ждёшь чего?

– Да хоть чего-нибудь. – Голос у него был несчастный.

– Вот и я, – сказала Анни. – Вдруг Вселенная вообще про нас забыла, после того как нам запретили бывать в космосе?

Джордж снова вздохнул.

– Как ты думаешь, – спросил он, – а мы когда-нибудь ещё там побываем?

– Когда-нибудь – да, но не прямо сейчас, – сказала Анни. – А может, всё самое здоровское уже кончилось? Может, теперь, когда нам по одиннадцать, придётся всё время быть серьёзными и заниматься всякими скучными делами?

Джордж встал. Доски под ногами слегка покачнулись. Джордж был почти уверен, что домик у него прочный и закреплён надёжно, так что вероятность того, что они с Анни рухнут на землю, он считал крайне низкой. Он строил его сам – точнее, вместе с папой Терренсом – из материалов, раздобытых на местной свалке. Когда они сооружали платформу, нога у папы провалилась в дырку – доска оказалась трухлявой. По счастью, папа не провалился весь целиком, но Джордж еле-еле выдернул его наверх. А внизу, на земле, близняшки Юнона и Гера покатывались со смеху.

Однако в этой мини-аварии имелся и плюс: мама и папа решили, что дом на дереве – место небезопасное, и категорически запретили дочкам взбираться туда по верёвочной лестнице – к великой радости Джорджа. Это означало, что дом на дереве стал его королевством, его собственной территорией, где можно было укрыться от хаоса. Родители велели ему всегда сворачивать лестницу, чтобы малышки не могли добраться до обожаемого брата. Так что обожаемый брат, понятное дело, тщательно следил, чтобы лестница никогда не оставалась спущенной. А это означало, что…

– Эй! – До него вдруг дошло, что Анни не могла появиться ниоткуда. Не по воздуху же она прилетела! – Ты как сюда забралась?

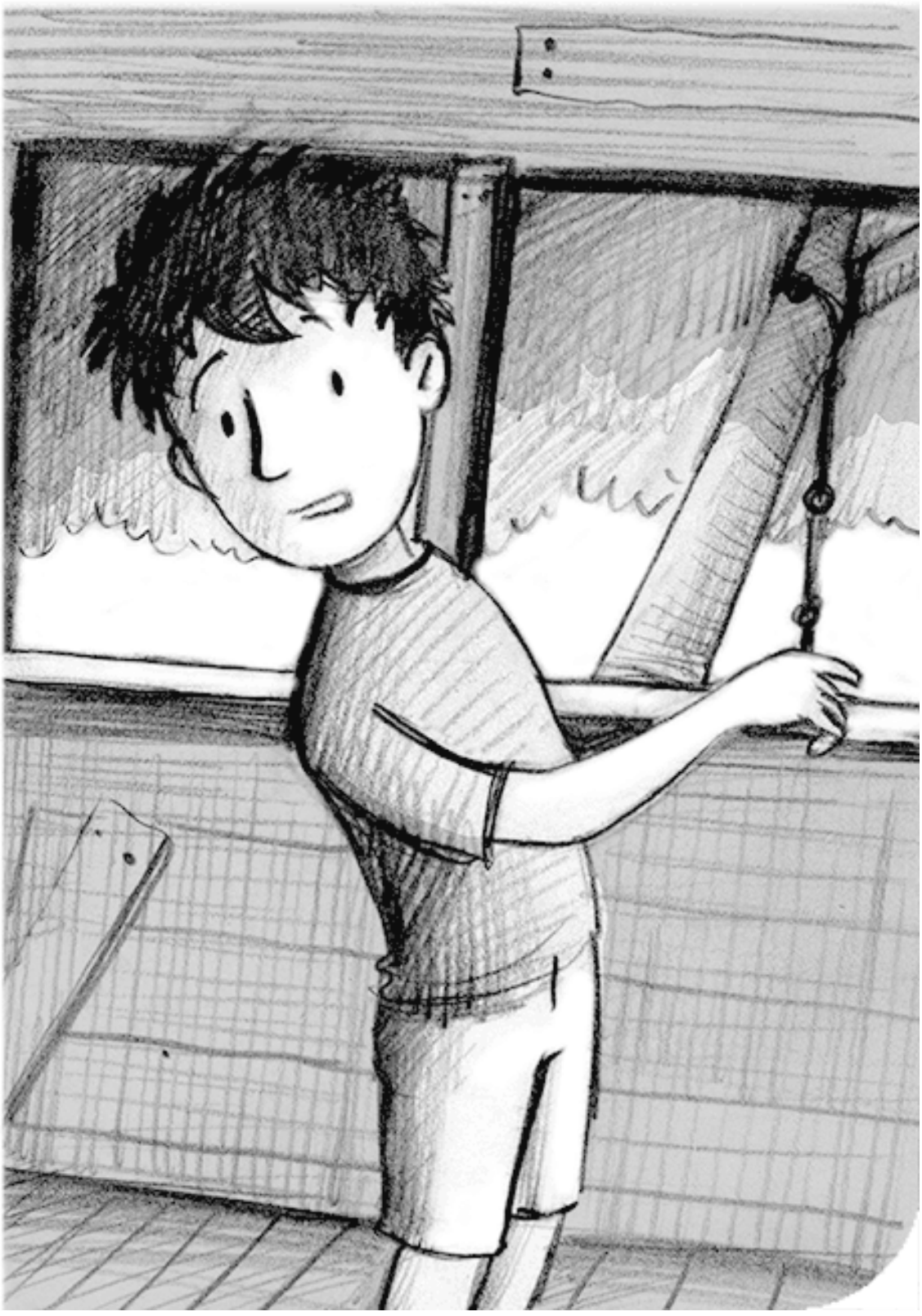
Анни ухмыльнулась.

– Когда я была ещё младенцем, – драматическим тоном начала она, – меня укусил паук. С тех самых пор я наделена магическими способностями, но осознала их лишь недавно…

– Твоя работа? – Джордж указал пальцем на толстый сук, на котором была затянута петля – видимо, верёвку набросили, как лассо.

– Ну, моя, – призналась Анни уже нормальным голосом. – Просто хотела проверить, получится или нет.

– Крикнула бы мне, я бы тебе лестницу спустил, – сказал Джордж.



– В прошлый раз, когда я тебя об этом попросила, ты заставил меня угадывать тыщу мильонов паролей, – пожаловалась Анни. – И всё равно мне потом пришлось отдать тебе половинку «Кит-Ката»!

– Это был не «Кит-Кат», – напомнил ей Джордж. – Это был тот «шоколад», – он изобразил в воздухе кавычки, – который ты пыталась создать в лабораторных условиях. Ты завернула его в обёртку от «Кит-Ката», чтобы проверить, почувствую я разницу или нет.

– Если можно у мыши на спине вырастить ухо, то почему я не могу вырастить «Кит-Кат»? Создать самовоспроизводящиеся молекулы шоколада, которые будут бесконечно себя дублировать!

Анни была подающим надежды химиком-экспериментатором. В качестве лаборатории она нередко использовала кухню, чем доводила свою маму Сьюзен до белого каления. Открыв холодильник, чтобы достать, к примеру, яблочный сок, Сьюзен то и дело натыкалась на что-нибудь вроде растущего кристаллического белка.

– К твоему сведению, – заявил Джордж, – на вкус твой «Кит-Кат» был как палец ноги динозавра.

– Ничего подобного! Мой авторский шоколад был безупречен. Я вообще не понимаю, о чём ты. И кстати, где это ты успел попробовать палец ноги динозавра?

– Коготь, – уточнил Джордж. – Коготь пальца ноги динозавра. Окаменевшего триллион лет назад. Жуткая гадость.

– Обхохочешься, – саркастически парировала Анни. – Не знала, что ты такой дурмэ.

– Дурмэ? Интересно, и что же это такое? – с вызовом спросил Джордж.

– Дурмэ, – сквозь смех проговорила Анни, – это когда, как дурак, наешься чего попало, а потом ни бэ ни мэ! – На последних словах она так развеселилась, что от хохота вывалилась из кресла-мешка.

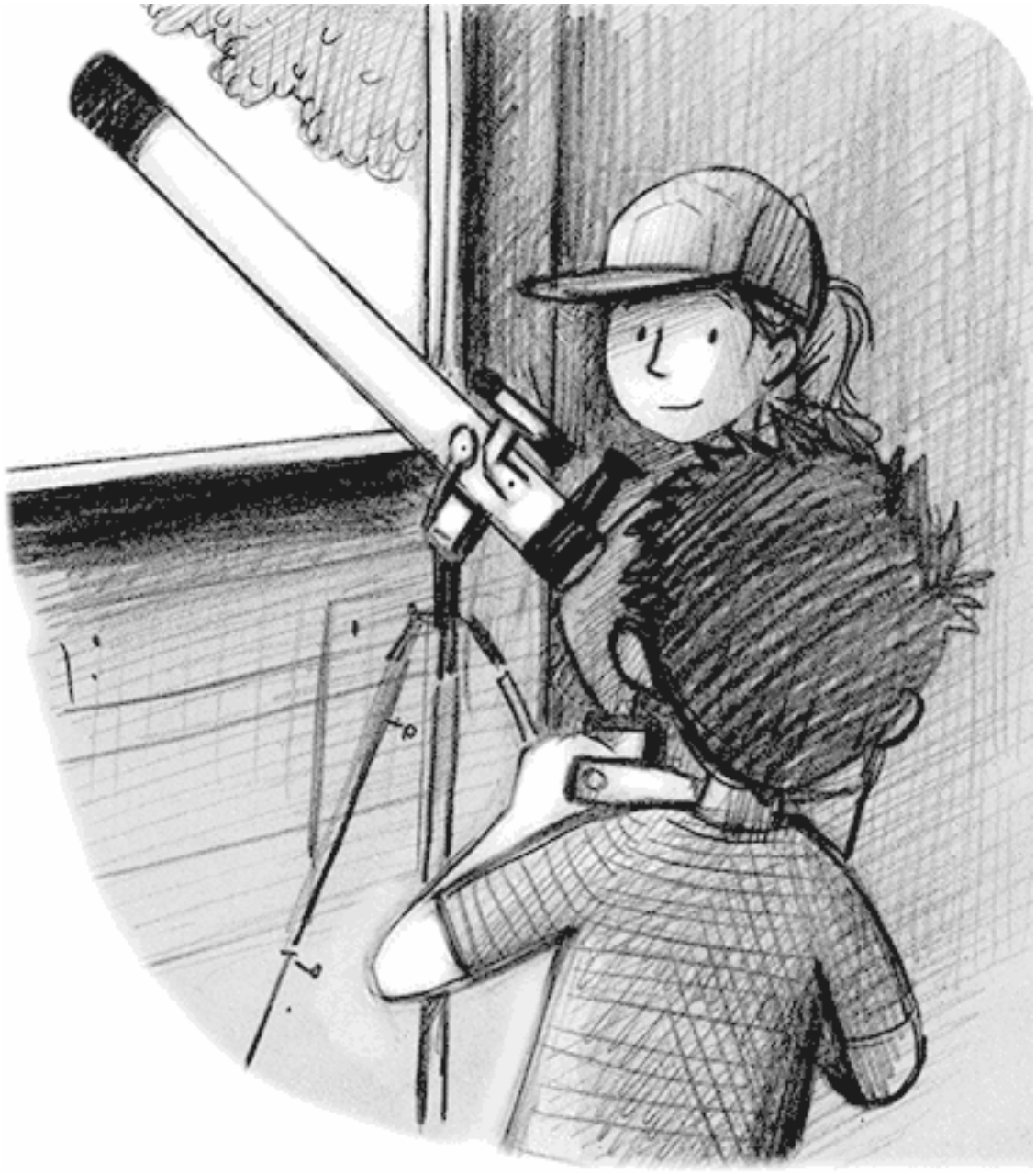
– Сама ты дурочка, – добродушно сказал Джордж.

– Ага, дурочка, с ай-кью сто пятьдесят два. – Анни поднялась и расправила плечи. Неделей раньше она прошла тест на ай-кью – коэффициент интеллекта – и теперь старательно следила за тем, чтобы никто не забывал о полученном ею результате.

Тут она заметила приборы, расставленные и разложенные в ряд.

– А что это у тебя?

– Готовлюсь к наблюдениям. – Джордж кивнул на технику, которую он спас от сестрёнок и из соображений безопасности держал теперь в доме на дереве. Здесь был шестидесятимиллиметровый телескоп – белый, с двумя чёрными кольцами с двух концов – и камера, которую он собирался приладить к телескопу, чтобы фотографировать объекты своих наблюдений. Телескоп ему подарила бабушка Мейбл, а камера, как ни удивительно, была родом всё с той же свалки. – Хочу, как стемнеет, сфоткать Сатурн. Если родители не запретят. Они иногда такие зануды. А это, между прочим, моё задание на каникулы.



– Круто! – Анни прищурилась и заглянула в видоискатель, но тут же воскликнула: – Фу! Тут какая-то липкая гадость!

– Что?! – вскрикнул Джордж и бросился к телескопу.

Действительно, видоискатель был облеплен чем-то клейким и розовым.

– Ну всё, с меня хватит! – Джордж решительно шагнул к верёвочной лестнице. Через несколько секунд он уже мчался к дому.

– Куда ты? – закричала вслед Анни. – Это же ерунда, подумаешь! Мы запросто всё ототрём!

Но Джордж даже не обернулся. С пылающим от гнева лицом он распахнул дверь и ворвался в кухню, где папа пытался накормить Юнону и Геру полдником.

– …ложечку за па-а-пу, – приговаривал Теренс, поднося эту самую ложечку ко рту Геры. Та с готовностью открыла рот, позволила забросить туда зеленоватое пюре и тут же фонтаном выплюнула его обратно, прямо в папу. Результат привёл её в восторг: она залилась смехом и радостно забарабанила ложкой по своему столику, отчего громоздившиеся на нём объедки и огрызки запрыгали, как мячики. Юнона, которая во всём брала пример с сестры, тоже принялась колотить ложкой по столу и вдобавок издавать губами противные булькающие звуки.

Теренс повернулся к Джорджу. На лице его было написано страдание вперемешку с умилением. Зелёная слизь стекала с бороды на домотканую рубаху.

Джордж набрал в грудь побольше воздуха и открыл рот, чтобы разразиться гневной тирадой о малявках, не имеющих ни малейшего уважения к чужой собственности, но тут в дверь просочилась Анни.

– Привет, мистер Гри! – пропела она. – Привет, красотульки!

Красотульки ещё неистовее застучали ложками и забулькали, радуясь новому поводу отвлечься от еды.

– Я зашла спросить: можно Джорджу пойти ко мне поиграть? – прощебетала Анни и щекотнула Геру под липким подбородком, отчего та обмякла и захихикала.

– А мой телескоп? – сердито спросил Джордж за спиной у Анни.

– Мы. С ним. Разберёмся, – одними губами прошептала она через плечо и тут же заворковала над близнецами: – Какое всё-таки это счастье – младшие сёстры! Вот бы у меня были такие чудесные, милые сестрёнки! Я одна-одинёшенька на всём белом свете… – И она изобразила на лице невыносимую грусть.

– Хм! – Джордж был бы счастлив поменяться с Анни – жить в её доме, битком набитом достижениями современной науки и высоких технологий, с её папой-учёным и мамой-музыкантом.

Ни тебе младших сестёр, ни органических овощей, ни бедлама – не считая, конечно, Аннинных химических опытов в кухне-лаборатории.

– Э-эм-м… ладно, дети, идите, – сказал Теренс. – Но только ненадолго, Джордж! Не забывай, что у тебя ещё много дел по дому. – Папа постарался произнести это внушительным голосом, чтобы показать, что у него всё под контролем.

– Ура! – воскликнула Анни, подталкивая Джорджа к выходу.

Джордж знал: если уж Анни раскомандовалась, то лучше отдаться на волю этого бурного потока. Так что он послушно направился к выходу: пойти в гости к Анни – это всегда прекрасно. Всяко лучше, чем болтаться дома в скверном настроении.

– Пока, мистер Гри и малышки! – на бегу прокричала Анни. – Всем приятного вечера!

– И не забудь про диаграмму успехов, Джордж! – крикнул им вслед Теренс. Он имел в виду диаграмму, в которой Джорджу было велено отмечать сделанные домашние дела. – У тебя ещё три сектора не заполнены!

Но Джордж уже скрылся из виду, увлекаемый Анни в восхитительные пределы Дома по Соседству, который виделся Джорджу воплощением всего самого современного, прогрессивного, научно-технического, электронного и просто потрясающего.

Глава вторая

К дому Анни они пробирались через дыру в заборе. Эту дыру между двумя садами проделал в своё время кабанчик по имени Фредди – ещё один подарок Джорджу от неугомонной бабушки Мейбл. В тот день, следуя за копытцами свободолюбивого Фредди, Джордж и познакомился с Анни, её папой Эриком, мегаучёным и супергением, а также с их компьютером по имени Космос, самым умным и мощным в мире, умеющим рисовать портал, через который можно попасть в любую нужную тебе точку известной Вселенной (если, конечно, ты в скафандре). С тех пор Джордж успел попутешествовать по Солнечной системе на комете, побродить по Марсу, вступить в поединок со злодеем-учёным в одной из дальних звёздных систем… Короче говоря, знакомство с соседями изменило его жизнь бесповоротно.

– Слушай, – сказала Анни на бегу, – не обижай сестричек!

– Ты это о чём? – Джордж и думать забыл о сёстрах. – Я их не обижал!

– Это только потому, что я помешала, – обличающе ткнула в него пальцем Анни. – А так ты как раз собирался сказать им что-то ужасное.

– Потому что я на них рассердился! Чего они мои вещи трогают? И лазят в мой дом на дереве!

– Ты просто не понимаешь, как тебе повезло, что у тебя есть сёстры, – сказала Анни. – У меня вот нет никого и ничего.

– Это у тебя-то ничего нет? – взорвался Джордж. – Да у тебя всё есть! У тебя есть Космос, у тебя есть практически собственная лаборатория, у тебя игровая приставка, у тебя смартфон, у тебя ноутбук, айпод, айпад, ай-всё-на-свете, у тебя радиоуправляемая собака, и скутер с мотором, и…

– Это всё не то! Настоящий брат или сестра – это совсем другое.

– Если бы у тебя на самом деле был брат… или сестра… а лучше двое… спорим, ты бы об этом пожалела!

Друзья вбежали в кухню, и Анни с ликующим криком подскочила к гигантскому холодильнику.

У Беллисов даже холодильник был не как у всех – он скорее походил на лабораторный шкаф: массивный, стальной, с множеством выдвижных ящиков и отсеков, позволяющих изолировать разные вещества друг от друга. Профессиональное оборудование, так же похожее на обычный холодильник, как бумажный самолётик – на космический корабль. Это была одна из причин, по которым Джорджа так тянуло в этот дом: здесь было полно неожиданных устройств и научных диковинок, которые Эрик купил, или отыскал, или получил в подарок в ходе многолетних занятий наукой. Джордж с завистью смотрел на холодильник, излучавший странное голубое сияние. У него-то в доме даже компьютер наверняка обладает меньшей вычислительной мощностью, чем вот этот холодильник…

Удручённо размышляя об этом, Джордж не сразу осознал, что из гостиной доносятся голоса.

– Анни! Джордж! – Папа Анни, Эрик, показался в дверях кухни. Его лицо сияло улыбкой, глаза за толстыми стёклами очков блестели, узел галстука был ослаблен, манжеты расстёгнуты. В руках у Эрика были два хрустальных бокала.

– Пришёл наполнить, – объяснил он, ставя бокалы на стол.

Он взял в руки пыльную старую бутылку, с громким «чпок» выдернул пробку и плеснул в бокалы тёмно-янтарную жидкость.

– Зайдите, поздоровайтесь с моей гостьей! – Эрик снова широко улыбнулся, отчего в уголках его глаз появились морщинки. – У неё есть кое-что такое, что может вас заинтересовать.

Джордж и Анни вмиг забыли о своём споре и проследовали за Эриком в гостиную, уставленную от пола до потолка рядами книг. Это была прекрасная комната, полная разнообразных прелюбопытнейших предметов, таких как Эриков древний медный телескоп. Научно-технический прогресс, правивший бал в остальных частях дома, здесь не так бросался в глаза: гостиная была не то что крутой или футуристической, а скорее просто уютной. На продавленном диване, оставшемся у Эрика ещё со студенческих лет, сидела очень старая, просто-таки древняя дама.

– Берил, – обратился к даме Эрик, вручая ей бокал хереса, – позвольте представить вам Анни и Джорджа. Анни, Джордж, это Берил Уайльд.

Берил благосклонно приняла напиток и сразу отпила глоток.

– Очень приятно! – сказала она и приветственно помахала рукой.

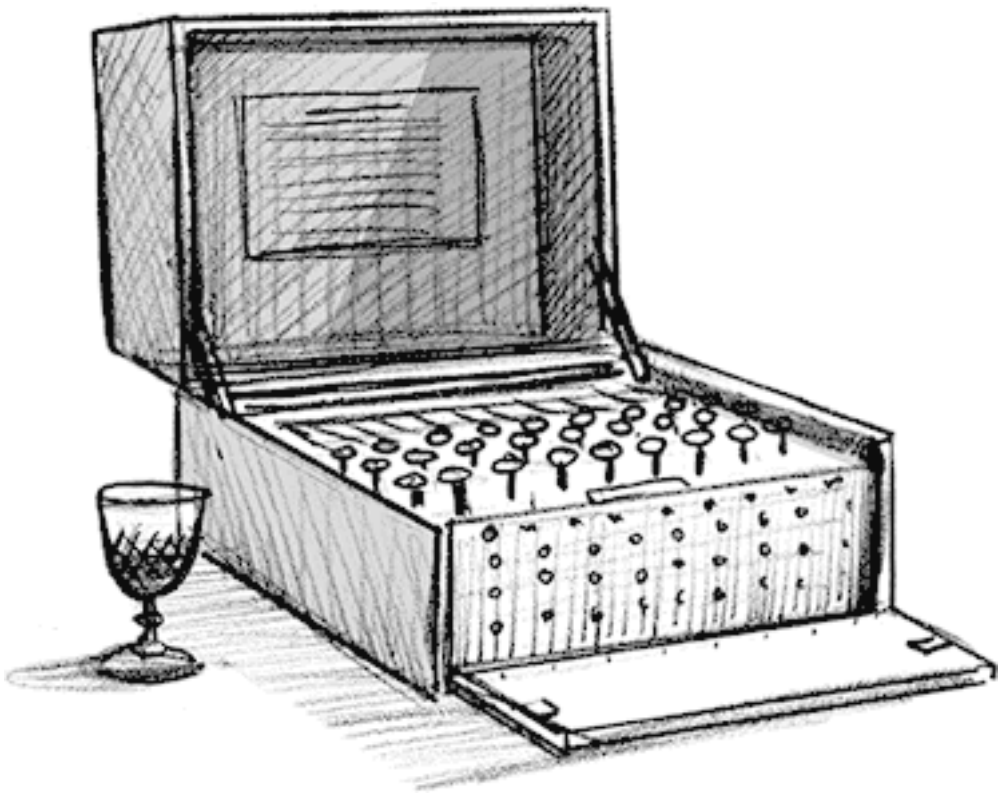
– Берил – один из величайших математиков нашего времени, – произнёс Эрик очень торжественно.

Берил расхохоталась.

– Ах, ну что за нелепость, право!

– Но это действительно так! – возразил Эрик. – Если бы не математический гений Берил, погибло бы гораздо больше миллионов людей.

– Каких людей? – спросил Джордж.



Анни достала смартфон и принялась искать в Википедии статью про Берил Уайльд.

– Как правильно пишется ваша фамилия? – спросила она.

– Вся информация обо мне защищена законом о государственной тайне, – сказала Берил, догадавшись, для чего Анни её фамилия. Её выцветшие бледно-голубые глаза проницательно блеснули. – До сих пор, по прошествии стольких лет. Так что в интернете меня не найти.

Эрик указал на загадочный предмет на кофейном столике напротив дивана, больше всего напоминавший старомодную пишущую машинку.

– Это, – произнёс он выразительно, – не что иное, как «Энигма», шифровальная машина, которую во времена Второй мировой войны применяли для кодирования сообщений. Даже перехватив такое сообщение, разведчики не могли его прочитать. А Берил была в числе немногих математиков, сумевших расшифровать код «Энигмы». Благодаря чему война закончилась скорее, чем могла бы, и погибло гораздо меньше людей.

Системы счисления

Десятичная

Система, которой мы обычно пользуемся при счёте – *десятичная* система, – имеет основание 10, по числу цифр от 0 до 9.

Мы считаем от 1 до 9 и переходим к следующему разряду – десяткам. Например:

36 = 3 × 10 плюс 6 × 1;

48 = 4 × 10 плюс 8 × 1;

148 = 1 × 100 плюс 4 × 10 плюс 8 × 1

и так далее.

Двоичная

В первых компьютерах применялась *двоичная* система счисления. Она названа так потому, что её основание – число 2: это значит, что в ней есть только две цифры – 0 и 1.

10 = 1 × 2 плюс 0 × 1 – то есть число 2 в десятичной системе;

11 = 1 × 2 плюс 1 × 1 – то есть число 3;

111 = 1 × 4 плюс 1 × 2 плюс 1 × 1 – то есть число 7.

В микросхемах первых компьютеров было всего два положения: «выключено» и «включено»; поэтому двоичный код – код, основанный на двоичной системе, – хорошо подходил для вычислений: ноль в ней соответствовал положению «выключено», а единица – «включено».

Шестнадцатеричная

Современные компьютеры намного сложнее, и код часто пишут в шестнадцатеричной системе счисления с основанием 16. Счет идёт от 0 до 9, а дальше 10 обозначается буквой A, 11 – буквой B и так далее до буквы F (то есть до 15).

Следовательно, C обозначает 12 из десятичной системы.

10 – так в *шестнадцатеричной* системе записывается число 16;

11 – это 17;

1F – это 31 (то есть 1 x 16 плюс F × 1 (15));

20 – это 32 (2 × 16);

F7 – это 247 (F × 16 (15 × 16 = 240) плюс 7 × 1);

100 – это 256.

Взлом кода

Взломом обычно называют расшифровку сообщений, когда у расшифровщика нет доступа к секретному ключу, которым пользовался отправитель. Другое название этого процесса – *криптоанализ*.

В докомпьютерную эру

До появления цифровых компьютеров шифровальщики работали с буквами или же с цифрами, заменявшими буквы. Например, можно было заменить каждую букву в сообщении другой буквой. В простом коде буква А заменялась на Д, Б заменялась на Е и так далее. Или же расположение букв в алфавите изменялось определённым образом.

При расшифровке такого сообщения имело смысл подсчитать, сколько раз та или иная буква появляется в зашифрованном тексте (это называется *частотный анализ*), а затем угадать какие-то из замен. Например, мы знаем, что буква «о» встречается в очень многих словах, так что если в зашифрованном тексте часто попадается буква «ч», то можно предположить, что она заменяет букву «о». А учитывая, что в сообщении всегда присутствует смысл, одной верной догадки может оказаться достаточно, чтобы правильно определить остальные замены.

В более сложных шифрах для каждой буквы сообщения могут применяться комбинации букв алфавита, и возможности для шифрования очень широки: так, если в алфавите 33 буквы, то для шифрования первой

буквы комбинации могут составляться из 33 букв, для второй – из 32 букв, для третьей – из 31 и так далее.

Современная дешифрация сообщений

Современные методы применимы не только к буквам, но и к битам (единицам и нолям). При зашифровке и дешифровке используется секретный ключ, который представляет собой длинную последовательность битов (единиц и нолей).

256-битный ключ считается в наши дни вполне достаточным для того, чтобы помешать взломщику кода, сидящему за суперкомпьютером, найти ключ «лобовым методом» – полным перебором возможных вариантов.

ВЗЛОМ КОДА (+ 1 БУКВА) ГИМПН ЛПЕБ
ДЖОРДЖ (+ 3 БУКВЫ) ЖЙСУЖЙ
АННИ (– 1 БУКВА) ЯММЗ

– Вот это да! – воскликнула Анни, отрывая взгляд от телефона. – Значит, вы могли читать тайные послания, а те, кто их писал, понятия не имели, что вы в курсе их планов? Это как если бы кто-то сейчас прочитал все мои мейлы… Хотя, конечно, я ни с кем не воюю, – добавила она. – Разве что с Карлой Кусзанос, которая надо мной издевалась, когда я неправильно написала что-то на доске…

– Именно, – кивнула Берил. – Мы перехватывали их послания, расшифровывали и таким образом узнавали их планы. И это давало нам огромное преимущество.

– Круто! – восхитилась Анни. – Уважуха, Берил! – И она снова принялась печатать на телефоне.

– Это что, настоящая «Энигма»? – Джордж пожирал машину глазами. В доме Беллисов появилось очередное умопомрачительное устройство! Он в миллионный раз пожалел, что родился у своих мамы с папой, а не у Беллисов.

– Да, – сказала Берил, улыбаясь ему. – И я дарю её Эрику.

Энигма

Военные тайны

Во время Второй мировой (1939–1945) воюющие страны для шифрования важных сообщений использовали машины. В Германии это была машина «Энигма», в Британии – «Тайпекс».

Оператор «Энигмы» печатал послание на клавиатуре, расположенной в передней части машины, а машина выдавала зашифрованный текст, указывая на каждую закодированную букву вспыхиванием маленькой электрической лампочки. Зашифрованное сообщение записывали от руки, переводили в азбуку Морзе и затем передавали по радио.

Три ротора

У «Энигмы» было три ротора – три колеса, начинённые сложными электросхемами. Роторы можно было вынимать из машины и вращать таким образом, чтобы каждый из трёх можно было поставить в любую из 26 возможных позиций (26 – число букв английского алфавита). Таким образом, имелось шесть (3 × 2 × 1) способов взаимного расположения роторов и 26 × 26 × 26 позиций для каждой буквы. Чтобы ещё усложнить эту

систему, можно было подключить к передней панели до десяти коротких проводков, и каждый из способов подключения создавал полностью новую систему из 26 × 26 × 26 шифров для сообщения. У получателя сообщения была своя «Энигма», настроенная точно таким же способом, и он вводил в неё зашифрованное сообщение. Записывая, какие лампочки загорались, можно было прочесть исходный текст. Каждый оператор «Энигмы» ежедневно узнавал, куда и в какое положение нужно поставить какой ротор и какие провода подключать к передней панели.

Взлом «Энигмы»

Шифровальная система была основана на секретной информации, известной отправителю и получателю. В случае «Энигмы» это были ежедневные инструкции по настройке и использованию машины, и задача заключалась в том, чтобы надёжно передать их большому числу людей. Ошибка любого из них привела бы к утечке важной информации. Инструкции в печатном виде тоже были уязвимы – их могли похитить или захватить в бою. Благодаря нескольким ошибкам немцев, достижениям математики и творческому мышлению, взломщики кода – сначала в Польше, а позже в Блетчли-Парке в Англии – сумели распознать настройки машин «Энигма» и получили возможность расшифровывать немецкие сообщения. Важнейшим элементом этого метода была особая машина, которую сконструировал гений математики Алан Тьюринг; эту машину называли «бомбой Тьюринга». В Блетчли-Парке также был разработан «Колосс» – первая программируемая вычислительная машина на электронных лампах; с помощью «Колосса» взломали код другой немецкой шифровальной машины, которая называлась «Лоренц».

Универсальная машина тьюринга

Воображаемое устройство

В 1936 году «компьютером», то есть «вычислителем», называли не машину, а человека, который что-то вычисляет. Машина Тьюринга, придуманная гениальным математиком Аланом Тьюрингом, – воображаемое устройство, способное воспроизводить всё, что делает в хо де расчётов человек-компьютер. То есть машина Тьюринга – не реальный прибор, а математическое устройство, позволяющее понять, что такое вычисление и чего можно достичь путем вычислений. В реальности такой машины быть не может: например, у неё должны быть и бесконечная «память», и неограниченное время работы, а ни то, ни другое невозможно.

Цепочка нулей

Действие, выполняемое машиной, описывается конечным списком зашифрованных инструкций. Представим себе очень длинную ленту, на которой написана очень длинная цепочка нулей (такая же длинная, как сама лента). Эта лента, которая тянется бесконечно в обоих направлениях (предположим, что она бесконечно длинная), – «память» вычислительной машины. Между нулями вкраплено конечное число единиц – они представляют введённые в машину «данные». На ленте установлено

управляющее устройство (процессор). Процессор может читать ровно один символ, проходящий через него в данный момент, и может либо ничего с ним не делать, либо заменить на 0 или 1.

Процессор также включает в себя часовой механизм, который ритмично тикает, и с каждым тиканьем процессор читает символ, который видит в данный момент. Затем он может сделать одно из двух – в зависимости от того, что он прочёл, и от своего текущего состояния. Он может:

• изменить прочитанный символ на 0 или 1; сдвинуться по ленте на одну позицию влево или вправо; возможно, перейти в другое состояние; ждать следующего тиканья;

• сделать всё то же, после чего остановиться (отключиться).

Что именно сделает процессор, зависит от правил («программы»), которые мы зададим, и от того, что он прочтёт на ленте. Предположим, что машина начинает работу в состоянии 0, с длинной цепочкой нулей на ленте, и где-то справа несколько нулей заменены единицами – эти единицы образуют в двоичной системе число, которое мы даём машине в качестве входных данных.

Тогда правило для начала работы выглядит так: *если в состоянии 0 мы читаем 0 – перейти в состояние 0, написать 0 и перейти вправо.*

Это означает, что если вначале машина видит 0 (находясь в состоянии 0), она остаётся в состоянии 0, не изменяет запись 0 на ленте и переходит на шаг вправо. Если следующий знак – опять 0, повторяется то же самое: машина остаётся в состоянии 0, не делает отметок на ленте и передвигается ещё на шаг вправо.

Всё это повторяется с каждым тиканьем часов, пока наконец машина не достигнет первой единицы на ленте. Теперь требуется правило, объясняющее, что делать, когда процессор читает 1 в состоянии 0. Простейшим правилом будет: *оставаться в состоянии 0, записать 1, перейти на шаг вправо и остановиться*. Теперь слева от машины будет записана единица, и это будет результат вычисления.

Этот алгоритм можно описать как «*печатать 1, если входные данные корректны*», где «корректны» означает «содержат по меньшей мере одну единицу». Если бы на момент начала работы справа от управляющего устройства не было ни одной единицы, она бы никогда не остановилась, а продолжала бы движение в вечном и бесплодном поиске единицы. Такое может произойти и с настоящим компьютером: программа может «зациклиться», и в конце концов компьютер сломается.

К сожалению, такая возможность – неотъемлемое свойство и машины Тьюринга, и реальных компьютеров. Однако этого легко избежать, если изначально указать, что среди «корректных» входных данных должна быть по меньшей мере одна единица, так, чтобы первое правило не могло применяться до бесконечности.

Тьюринг также математически показал, что даже машина Тьюринга не может решить все задачи! Иными словами, некоторые задачи в математике не решаются с помощью вычислительной техники – то есть математиков пока нельзя заменить машинами.

Любое возможное вычисление

> Если есть достаточно времени и есть возможность записать на ленте ввода нужное число единиц, то выполнимо любое механическое действие с целыми числами, какое только можно придумать. Для этого требуется дать машине Тьюринга входное число справа от машины, запустить часы, дождаться остановки – и прочесть ответ слева от машины. К таким действиям относится любой арифметический расчёт, какой может произвести человек с помощью ручки и бумаги. Алан Тьюринг предложил такое определение вычислимого: вычислимо то, что может вычислить машина Тьюринга. Удивительно, но спустя примерно 80 лет это определение по-прежнему считается верным: все известные компьютеры могут выполнять вычисления только в пределах возможностей машины Тьюринга.

Эрик ахнул. Она явно не предупредила его о своих намерениях.

– Нет, вы не можете… – начал он.

– Очень даже могу, – твёрдо сказала Берил. – Я дарю её вашему математическому факультету. Вы, с вашими работами по квантовым компьютерам, – самый подходящий человек для такого подарка. Так что лучшее место для неё и придумать трудно.

– Что такое квантовый компьютер? – насторожился Джордж. Для него это была новость. Он давно обратил внимание на то, что Эрик в последнее время стал очень скрытен. На вопросы о том, над чем он сейчас работает, выдающийся учёный отвечал туманно и уклончиво.

Однако сегодня Эрик оказался существенно говорливее, чем обычно.

– Это очередной прорыв, – ответил он Джорджу. – Уже произошла *цифровая* революция в мире информации, а теперь мы стоим на пороге *квантовой* революции. Если мы сумеем создать квантовый компьютер – и не только создать, но и управлять им, что в данный момент кажется чрезвычайно сложным, – то сможем делать многое из того, что при нынешнем уровне компьютерных технологий выглядит совершенно непредставимым.

– Например? – спросил Джордж.

– С помощью квантового компьютера можно взломать любой код – на Земле не существует системы ограничения доступа, которая могла бы его остановить! – сказал Эрик, сияя. – И тогда мы сможем делать просто невероятные вещи в области обработки данных, в медицине, физике, машиностроении, математике. Это будет очередной гигантский прорыв в науке.

– Но при чём тут «Энигма»? – спросил Джордж.

– При том, – ответила Берил, – что «Энигма» – предшественница множества поразительных технологий. И важно, что «Энигма» на самом деле существует и доказала свою действенность. А квантовый компьютер на данный момент ещё не действует, поскольку не существует.

– Да! – Эрик рассмеялся. – Моя нынешняя работа по большей части состоит в исправлении ошибок в квантовых вычислениях…

– Кстати, – Берил указала на Эрика, – перед вами единственный, наверное, человек на Земле, способный управлять квантовым компьютером – если бы, конечно, такой компьютер существовал.

Эрик расплылся в довольной улыбке.

– Выявлять ошибки в квантовых вычислениях, – сказал он, – по сути означает убедиться в том, что, получив функционирующий квантовый компьютер, мы будем способны держать его под контролем. Пока что это выглядит маловероятным! С «Энигмой» такой проблемы не было.

Что такое компьютерный код?

Код как тайнопись

Люди с давних времён научились кодировать – шифровать – сообщения так, чтобы тем, кто не знает шифра, эти сообщения казались абракадаброй. Это позволяло посылать союзникам тайные послания, которые не сможет прочесть враг.

В наши дни всякий, кто что-то покупает в интернете – например, музыку, книги или подарок, – тоже вынужден зашифровывать номер своей банковской карты, чтобы никто не украл его деньги. Современные компьютеры не только обеспечивают шифрование сообщений, но и дают возможность убедиться, что сообщение не подделано и что отправитель – не подставное лицо.

Шифрование в компьютере происходит очень быстро, ведь шифруются *биты*, а не буквы; а вот взломать такой шифр, если нет секретного ключа, чрезвычайно трудно. Однако взломщиков это не останавливает, они придумывают всё новые и новые методы, и вполне возможно, что рано или поздно все существующие шифры будут взломаны. Что ж, тогда придётся изобретать новые!

Языки программирования

С точки зрения математики кодирование – это превращение одного набора символов в другой по определённым правилам.

Если правильно «закодировать» (ещё говорят – «запрограммировать») команды и данные в виде ноликов и единичек, то компьютер их поймёт. Как именно это сделать? По специальным правилам, которые у каждого процессора свои. Получившиеся нолики и единички, которые «понимает» процессор, называются *машинным кодом*. Каждый набор правил – это особый *алгоритм*. Запасшись терпением, программу из ноликов и единичек можно составить самому и записать ручкой в тетради. Но у компьютера это получится гораздо быстрее.

Люди пишут программы на легко читаемых языках программирования, таких как C или FORTRAN; оба эти языка состоят из обычных английских слов, так что нет нужды возиться с ноликами и единичками. Существует много разных языков программирования, на которых мы можем «говорить» с ком пью те ром. Под «компьютерным кодом» мы обычно подразумеваем программу, написанную на одном из таких языков.

Компиляторы – это специальные программы, которые преобразуют программы на высокоуровневых языках программирования в понятный процессору машинный код. Машинный код обычно записывают в шестнадцатеричной системе счисления.

Взломать компьютерный код – значит добиться сбоя в программе или сделать нечто совершенно непредвиденное. Так, злоумышленники в интернете из хулиганских или преступных побуждений пытаются получить несанкционированный доступ к компьютеру жертвы (например, чтобы завладеть данными кредитной карты и украсть с неё деньги).

Алгоритмы

Алгоритм – это пошаговый процесс с чёткими правилами, объясняющими, как на каждом шагу преобразовать один набор символов в другой. Например, мы учимся умножать или делить в столбик по шагам –

эти шаги и есть *алгоритм* умножения или деления в столбик. Для любого примера на умножение или деление больших чисел алгоритм работает одинаково: на каждом шагу промежуточный результат записывается на новой строчке до тех пор, пока не будет получен ответ.

Алгоритмы существуют давно. Например, Евклид описал алгоритм нахождения наибольшего общего делителя двух целых чисел примерно за 300 лет до нашей эры (хотя сам алгоритм, возможно, ещё старше).

Слово «алгоритм» происходит от имени персидского математика IX века Аль-Хорезми, который, в частности, описал алгоритмы арифметики, а также внёс большой вклад в развитие алгебры.

В XX веке математики пытались дать точное определение алгоритма на языке математики, но все их попытки оказались эквивалентны уже знакомому нам определению: «То, что может машина Тьюринга». Ни один компьютер пока не способен на большее.

Любая компьютерная программа сводится к алгоритму, который меняет значения битов в памяти компьютера на каждом цикле процессора.

– А мы смогли бы пользоваться «Энигмой», мы с Анни? Смогли бы посылать друг другу шифровки? – спросил Джордж.

– «Энигма» не умеет *посылать* сообщения. – Берил допила свой херес. – Она их зашифрует и расшифрует, но вам понадобится ещё и средство передачи. Раньше было принято передавать шифрованные сообщения по радио с помощью азбуки Морзе. Но в наши дни имеются технологии, которые позволяют делать и то и другое: ежесекундно зашифровывать миллиарды сообщений и рассылать их по всей планете по проводам или с помощью радиоволн; это делают компьютеры. А потом уже другие компьютеры расшифровывают эти сообщения. Любое электронное письмо, любой поисковый запрос, любой текст в командной строке – это зашифрованное сообщение. Некоторые шифры, правда, предназначены для того, чтобы их понимали все, а то в интернете сам чёрт сломал бы ногу. Но всё же, покупая в интернет-магазине, например, носки, вы наверняка захотите, чтобы как минимум номер вашей кредитной карты был зашифрован, иначе кто-то может подглядеть его и украсть ваши денежки. Представьте себе, сколько в мире компьютеров, от которых зависят важнейшие области человеческой жизни – возьмём хотя бы электричество, транспорт, оборону. Во всех этих компьютерах используется шифрование, чтобы какие-нибудь злоумышленники не сумели помешать их работе. Тот, кто взломает этот шифр, сможет шантажировать весь мир, навязывая ему свои условия.

– Не подсказывайте им, – деланно строгим голосом сказал Эрик. – Не хватало ещё, чтобы эти двое пробурились в какую-нибудь сверхсекретную правительственную программу и поставили на уши все спецслужбы.

– О, это было бы восхитительно! – воскликнула Берил. – Надеюсь, они так и сделают!

Джордж многозначительно глянул на Анни: эта Берил, кажется, может много о чём порассказать.

– Да уж, Берил, хороший пример вы подаёте детям, – проворчал Эрик, но голос у него при этом был не сердитый, скорее, наоборот, весёлый. – Ну-ка, уматывайте отсюда оба, пока Берил не записала вас в отряд юных секретных агентов.

– Ну па-аап, – заныла Анни. Ей как раз стало до того интересно, что она даже телефон отложила. – Я же и хочу быть секретным агентом!

И работать в разведке! Это моя главная, самая заветная мечта и цель! Можно мы останемся? Ну па-аап!

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.