

18+

ЗОДИАК ПО СЛЕДАМ ЗЛА



АНДРЕЙ ЗАЛЕВСКИЙ

Андрей Залевский

Зодиак. По следам зла

<https://litres.ru/74139452>

SelfPub; 2026

Аннотация

Сан-Франциско скован животным страхом. Неуловимый серийный убийца не просто отнимает жизни — он превращает смерть в жестокое шоу. Он отправляет в газеты зашифрованные манифесты и фрагменты окровавленной одежды. Он обещает расстрелять школьный автобус, заставляя миллионный мегаполис цепенеть от ужаса. Он называет себя Зодиак.

«Зодиак. По следам зла» — захватывающий документальный триллер о величайшем нераскрытом преступлении в истории США.

Как один психопат с синим фломастером взял в заложники целую нацию? Почему криминалистика 1960-х оказалась бессильна, а нелепая ошибка патрульных подарила монстру бессмертие?

Опираясь на рассекреченные архивы ФБР, книга проводит читателя по следам маньяка от первых выстрелов во тьме до декабря 2020 года, когда суперкомпьютер наконец взломал его самый сложный шифр.

Код разгадан. Но раскрыта ли тайна? Шагните в туман, где до сих пор скрывается идеальный убийца.

Содержание

ВНИМАНИЮ ЧИТАТЕЛЯ / ПРАВОВОЙ	4
ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ	
(DISCLAIMER)	
ПРЕДИСЛОВИЕ ОТ АВТОРА	8
Глава 1. Белый шум	12
Глава 2: Сдвиг матрицы	24
Глава 3:	34
Конец ознакомительного фрагмента.	35

Зодиак. По следам зла

ВНИМАНИЮ ЧИТАТЕЛЯ / ПРАВОВОЙ ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ (DISCLAIMER)



Данная книга создана в жанре документального триллера (narrative non-fiction) и основана на реальных событиях, материалах уголовных дел, рассекреченных отчетах полиции и ФБР, официальных протоколах допросов, свидетельствах

очевидцев и публикациях в СМИ, касающихся серии нераскрытых преступлений, совершенных в Калифорнии в 1960–1970-х годах человеком под псевдонимом «Зодиак».

**При чтении и дальнейшем
использовании данного материала
просим учитывать следующее:**

1. Художественная реконструкция

С целью создания связного, целостного и психологически достоверного повествования, некоторые диалоги, внутренние монологи героев, эмоциональные реакции и мелкие детали обстановки были реконструированы автором. Эти элементы беллетризации строго опираются на фактологический фундамент следствия и не искажают задокументированного хода событий, однако не должны восприниматься как дословная стенограмма (за исключением прямых цитат из писем преступника и записей диспетчерских служб).

2. Презумпция невиновности

В книге упоминаются реальные исторические лица, проходившие по делу в качестве подозреваемых (включая Артура Ли Аллена, Лоуренса Кейна, Гэри Фрэнсиса Поста и других). Автор и издатель подчеркивают: **ни один из упомянутых подозреваемых никогда не был признан судом виновным** в преступлениях Зодиака. В соответствии с фундаментальным принципом презумпции невиновности, перед

законом эти люди считаются невиновными. Их упоминание в тексте отражает исключительно исторический ход полицейского расследования, следственные гипотезы и теории независимых исследователей того времени, и ни в коей мере не является прямым обвинением или утверждением их вины со стороны автора.

3. Использование торговых марок и брендов

Все торговые марки, названия компаний, учреждений и бренды (такие как часы *Zodiac*, *San Francisco Chronicle*, *Yellow Cab*, *Volkswagen*, *Wing Walkers* и другие), упоминаемые в тексте, являются собственностью их соответствующих владельцев. Они используются в книге по принципу добросовестного использования (*fair use*) исключительно в исторических, документальных и информационных целях для точного воссоздания духа эпохи и деталей уголовного дела. Автор не заявляет о наличии связи, спонсорства или одобрения со стороны владельцев данных товарных знаков.

4. Возрастное ограничение и предупреждение о контенте (Trigger Warning) [18+]

Книга предназначена строго для взрослой аудитории. Текст содержит документальные описания сцен насилия, жестокости, использования огнестрельного и холодного оружия, а также детальный анализ психопатологии серийного убийцы и методов психологического террора. Чтение данного произведения категорически не рекомендуется несовершеннолетним, лицам с нестабильной психикой, беременным

женщинам и людям, остро реагирующим на описания реальных трагедий.

5. Отказ от ответственности

Книга не является учебным, криминалистическим, юридическим или медицинским пособием. Автор и издатель не несут ответственности за любой психологический дискомфорт или эмоциональный ущерб, вызванный прочтением данного материала, а также за любые действия читателей, предпринятые на основе информации из этой книги.

ПРЕДИСЛОВИЕ ОТ АВТОРА



Мы привыкли к уютным детективным историям. Культура воспитала в нас веру в неизбежность правосудия: сыщик собирает улики, находит мотив, срывает маску со злодея, и в финальной главе мир снова возвращается в состояние равновесия. Но реальная жизнь редко пишется по законам классического жанра. Иногда зло не просто остается безнаказанным — оно смеется нам в лицо, оставляет издевательскую записку на кухонном столе и растворяется в утреннем тумане, превращаясь в бессмертный миф.

Эта книга — о самом известном нераскрытом уголовном деле в истории Соединенных Штатов. О человеке, который

выбрал себе имя «Зодиак».

Когда я начинал работу над этим документальным триллером, передо мной стояла сложная задача. О Зодиаке написаны тысячи статей, сняты десятки фильмов и сериалов. Его образ затерт до дыр поп-культурой. Но за этим медийным глянцем часто теряется подлинный, осязаемый, липкий ужас тех дней. Мы забываем, как один человек с помощью синего фломастера, дешевой почтовой бумаги и безграничного высокомерия смог взять в заложники целый мегаполис.

Зодиак не был самым кровавым маньяком в истории. Он не был гениальным стратегом. Но он стал пионером того, что сегодня мы называем «информационным терроризмом». Он понял то, чего не понимали многие до него: чтобы парализовать общество, не обязательно убивать тысячи людей. Достаточно убить нескольких, а затем грамотно продать свой страх прессе. Он превратил полицию в своих бесплатных статистов, а газеты — в рекламные агентства.

Толчком к написанию этой книги стал декабрь 2020 года. В разгар глобальной пандемии, когда мир сидел по домам, международная команда криптографов с помощью суперкомпьютеров совершила невозможное — они взломали шифр Z340, который Зодиак отправил в полицию полвека назад. Пятьдесят один год этот текст оставался немым. Когда программа наконец выдала осмысленные слова, я, как и миллионы людей по всему миру, почувствовал холодок по спине. Голос из прошлого прорвался сквозь время.

Но вместо разгадки мы получили лишь очередную порцию бредового самолюбования.

Именно этот контраст — триумф цифровых технологий XXI века и полная беспомощность перед загадкой из 1969 года — заставил меня обернуться назад. Я захотел исследовать не только личность фантома, но и саму эпоху.

На страницах этой книги мы спустимся в «аналоговый паралич» конца шестидесятых. Это было время, когда не существовало баз ДНК, когда юрисдикции общались медленными телетайпами, а бесценные биологические улики навсегда уничтожались парами йода в попытках найти смазанный отпечаток пальца. Вы увидите, как система, созданная для защиты людей, буксовала и совершала фатальные ошибки, отпуская монстра буквально из собственных рук.

Предупреждение для читателя: здесь не будет выдуманных, счастливых концовок. Я не предложу вам сенсационного разоблачения, указывая пальцем на случайного человека, чтобы красиво закрыть гештальт. Эта история реконструирована на основе реальных полицейских рапортов, рассекреченных файлов ФБР, отчетов криминалистов и воспоминаний выживших.

Я приглашаю вас пройти этот путь вместе со следователями, которые выгорали на работе, пытаясь поймать тень. Вы ощутите ледяной ветер на темной обочине Лейк-Херман-Роуд, почувствуете запах крови и пороха в салоне желтого такси в Пресидио Хайтс и услышите монотонный, лишенный

эмоций голос диспетчера: «*Внимание всем постам...*»

Эта книга — анатомия страха. Изучение того, как хрупка наша безопасность и как легко один невидимый человек может заставить целую нацию смотреть на любой проезжающий мимо школьный автобус с содроганием.

Переверните страницу. Добро пожаловать в Сан-Франциско 1969 года. Туман уже сгущается.

И, как сказал бы он сам: «This is the Zodiac speaking...»

Глава 1. Белый шум



Декабрь 2020 года накрыл планету тяжелым, непроницаемым саваном. Мир, запертый в четырех стенах карантином, погрузился в стерильную, неестественную тишину. Улицы мегаполисов опустели, превратившись в декорации к неснятому фильму-катастрофе. Но в этой глобальной, оглушающей паузе, где время, казалось, утратило свою линейность и стало вязким, как смола, существовало иное измерение. Цифровое подполье, где не было ни пандемии, ни смены дня и ночи. Там царил лишь непрерывный, монотонный гул охлаждающих систем, прогоняющих кубометры воздуха через раскаленные ребра процессоров.

В этом измерении обитал «белый шум» — криптографическая энтропия, абсолютный математический хаос. И именно в этот хаос ежесекундно вглядывались три человека, разбросанные по разным континентам, но связанные одной маниакальной целью, которая давно переросла рамки простого научного интереса.

Они пытались взломать Z340. Шифр, который сводил с ума лучшие умы планеты на протяжении пятьдесят одного года.

Вирджиния, США. Дэвид Оранчак потер воспаленные, покрасневшие глаза. Монитор в полумраке его домашнего кабинета излучал мертвенно-бледный синий свет, выхватывая из темноты стопки распечаток, покрытых геометрическими символами. Спина ныла от многочасового сидения в одной позе, в шее пульсировала тупая боль — верный спутник человека, чье тело стало лишь приложением к вычислительной машине.

Дэвид откинулся на спинку кресла и сделал глоток давно остывшего, горького кофе. На экране перед ним застыла сетка. Двадцать столбцов. Семнадцать строк. Триста сорок символов.

Среди них были обычные буквы алфавита, перевернутые заглавные «Р» и «R», закрашенные наполовину круги, кресты, треугольники и тот самый проклятый круг с перекрестием — личный знак маньяка, называвшего себя Зодиаком.

Оранчак занимался этим кодом четырнадцать лет. Четыр-

надцать лет он спускался в эту кроличью нору, пытаясь нащупать логику там, где, возможно, скрывалось лишь издевательское безумие. Он знал наизусть частотность каждого из 63 уникальных символов. Он помнил, в каких строках концентрируются определенные знаки. Z340 стал для него не просто криптограммой; он превратился в паразита, поселившегося в его нейронных связях.

Физиология этого одержимого состояния была ему хорошо знакома. Сначала приходит азарт — легкий тремор в пальцах, когда программа выдает кажущийся осмысленным фрагмент. В кровь выбрасывается адреналин. Зрачки расширяются, фокус зрения сужается до размеров нескольких пикселей на экране. Кажется, вот оно. Вот сейчас завеса падет. Но затем следует неизбежный удар о стену: алгоритм спотыкается, и «осмысленный» кусок текста растворяется в первобытном хаосе бессмысленных буквосочетаний. Адреналин сменяется кортизолом, оставляя после себя лишь пепельную усталость, сухость во рту и давящее чувство интеллектуального бессилия.

В истории криптографии гомофонический шифр подстановки — это не самая сложная преграда. Идея проста: часто встречающиеся буквы (например, 'Е' или 'Т' в английском языке) заменяются не одним символом, а несколькими разными. Это сглаживает статистику, лишая криптоаналитика его главного оружия — частотного анализа. Когда первый шифр Зодиака (Z408) был опубликован в 1969 году, супруги

Харден — простой школьный учитель и его жена — взломали его за несколько дней за кухонным столом. Они просто угадали слова, которые эгоцентричный убийца должен был использовать. Например, слово «KILL» или «I».

Но Z340 был другим зверем. Он был создан в ноябре 1969 года, после того как убийца понял свои ошибки. И с тех пор этот шифр издевался над всеми.

Дэвид смотрел на экран и вспоминал призраков тех, кто пытался до него. Аналитики ФБР, оснащенные лучшими на тот момент перфокарточными ЭВМ. Криптографы АНБ, привыкшие перехватывать и расшифровывать донесения советских подводных лодок. Военно-морская разведка. Все они обломали зубы об эти 340 знаков. Годы шли, аналоговая криминалистика сменялась цифровой, вычислительные мощности росли в геометрической прогрессии, но код оставался нем.

Он был похож на монолит. Никакие стандартные атаки не работали. Программы перебора, основанные на алгоритмах «восхождения на холм» (hill-climbing), задыхались. Суть алгоритма проста: программа случайным образом назначает символам буквы, затем меняет одну связь и смотрит, стал ли получившийся текст больше похож на английский язык (оценивая частоту пар и троек букв). Если да — изменение сохраняется. Если нет — отвергается. Программа «карабкается» на вершину осмысленности. Но в случае с Z340 все алгоритмы неизбежно застревали на «локальных максимумах»

— вершинах, которые оказывались лишь миражами. Выдаваемый текст выглядел как: «THE T KILL A MAN I...», а дальше шла абсолютная нечитаемая каша. Белый шум.

Дэвид моргнул, прогоняя из-под век жгучую резь. Изоляция 2020 года дала ему то, чего всегда не хватало — непрерывное время. И это время сводило его с ума. Он повернулся к другому монитору, где мигал интерфейс мессенджера. Там, на других концах планеты, в эту же самую секунду, не спали его напарники.

Антверпен, Бельгия. Ярл Ван Эйк сидел в темноте своей тесной комнаты. За окном занимался серый, промозглый бельгийский рассвет. Моросил мелкий, колючий дождь, типичный для декабря. Тело Ярла гудело от тупой, изматывающей боли. Мышцы спины и рук помнили каждую коробку, каждый тяжелый поддон, который он перетащил за свою смену на складе.

Днем он был обычным рабочим. Механическим винтиком в логистической цепи, где его главной задачей было физическое перемещение объектов в пространстве. Но ночью, когда гул складских погрузчиков затихал в его ушах, Ярл Ван Эйк становился кем-то другим. Он становился архитектором самого грозного криптоаналитического оружия в мире.

Его детище, программа *AZDecrypt*, была шедевром математической логики и программирования. Пока другие исследователи пытались использовать готовые инструменты, Ярл написал свой собственный код с нуля. Он оптимизиро-

вал его до такой степени, что алгоритм мог обрабатывать миллионы ключей в секунду, выжимая из обычного процессора максимум его возможностей. AZDecrypt был холодным, безжалостным скальпелем, созданным для вскрытия гомофонических шифров.

Ярл смотрел на бегущие по черному экрану командной строки зеленые цифры. Температура процессора его компьютера держалась на отметке 85 градусов. Вентиляторы ревели, пытаясь отвести тепло от перегруженного кремниевого сердца машины. В комнате стоял запах разогретой пластмассы и озона.

Сотни тысяч итераций в секунду. Программа вгрызалась в Z340, пыталась подобрать ключи, оценивала биграммы, триграммы, тетраграммы. И раз за разом выдавала отрицательный результат.

Интеллектуальное напряжение Ярла было сродни медитации. Он не позволял себе эмоций. Никакого страха перед личностью убийцы, никакого отвращения к его деяниям. Для Ван Эйка Зодиак не был человеком из плоти и крови, который терроризировал Калифорнию полвека назад. Он не был монстром, убивающим студентов на темных аллеях. Для бельгийского программиста Зодиак был просто неисправностью. Ошибкой в матрице. Сложной, упрямой, но поддающейся логическому разбору задачей.

Однако сейчас логика давала сбой. Ярл потер виски. AZDecrypt достигла предела своей эффективности в рамках

стандартного подхода. Программа идеально решала классические шифры подстановки. Тот факт, что она не могла расколоть Z340, означал только одно, и эта мысль ледяным сквозняком пробиралась сквозь усталость: *шифр был устроен иначе*. Это была не просто замена букв. Символы были перемешаны. Переставлены. Разорваны на части.

И чтобы найти правильный порядок их чтения, требовались мощности, превосходящие возможности даже его оптимизированного кода. Требовалась грубая, титаническая сила суперкомпьютеров и совершенно иной математический подход.

Ярл переключил окно и набрал короткое сообщение Дэвиду и Сэму: *«Линейное чтение мертво. Мы бьемся головой в бетон»*.

Мельбурн, Австралия. Для Сэма Блейка декабрь означал начало удушающего лета. Пандемия заперла австралийцев в жестком локдауне. Улицы Мельбурна плавились от жары и пустоты. Сэм, математик с академическим бэкграундом, сидел в своей гостиной, окруженный графиками и формулами. В отличие от Дэвида, который был архивариусом и исследователем дела, и Ярла, который был гениальным кодером, Сэм видел мир сквозь призму чистой математики. Топология, комбинаторика, теория вероятностей.

Сэм смотрел на матрицу Z340, распечатанную на огромном листе ватмана. Он не пытался угадать слова. Он рассматривал сетку как физический объект, подверженный дефор-

мации.

Он понимал, почему ФБР и АНБ потерпели неудачу в 70-х. Они исходили из предпосылки, что Зодиак, будучи самоучкой, не мог создать ничего сложнее прямолинейной подстановки, возможно, с парой уловок. Они искали смысл, читая текст слева направо и сверху вниз. Строка за строкой. Как обычную книгу.

Но что, если автор Z340, опьяненный безнаказанностью и собственным мнимым величием, решил усложнить игру? Что, если он сначала зашифровал сообщение, а затем разрезал его на куски и перетасовал, как колоду карт?

Подобная техника называется транспозицией. И если она применена вместе с гомофонической подстановкой, количество возможных вариантов прочтения текста устремляется в бесконечность.

Сэм сделал глубокий вдох, чувствуя, как спертый, горячий воздух наполняет легкие. Чтобы проверить гипотезу транспозиции, ему нужно было прогнать сетку через тысячи различных геометрических искажений, а затем каждое из них скормить программе Ярла AZDecrypt. Это требовало колоссальных ресурсов.

К счастью, у Сэма был доступ к суперкомпьютеру Мельбурнского университета — Spartan.

В течение последних нескольких недель Блейк запускал на Spartan скрипты, которые генерировали миллионы возможных вариантов прочтения Z340. Он заставлял машину

читать текст змейкой. По спирали. Снизу вверх. Справа налево. Через один символ. Через два. Он создавал математические модели, которые скручивали двухмерную плоскость шифра в трехмерные цилиндры и торы, пытаясь найти тот самый алгоритм, по которому убийца записал свой текст перед тем, как разбить его на блоки.

Всего Сэм сгенерировал 650 000 (шестьсот пятьдесят тысяч) уникальных вариантов перестановок. И каждый из этих вариантов отправлялся Ярлу, чья программа прогоняла их через мясорубку статистического анализа.

Результат? Тот самый сводящий с ума белый шум.

Сэм чувствовал, как начинает сдавать. Анатомия интеллектуального отчаяния работает безотказно: мозг, не получая вознаграждения в виде дофамина от решения задачи, начинает саботировать работу. Внимание рассеивается. Строки сливаются в единое серое пятно. Символы начинают танцевать перед глазами, стоит только моргнуть. Это был предел. Человеческий разум не предназначен для того, чтобы так долго вглядываться в Бездну бессмыслицы без потери рассудка.

На экране всплыло сообщение от Ярла: *«Линейное чтение мертво. Мы бьемся головой в бетон».*

Сэм горько усмехнулся. Он знал это. Спартан пережевывал полмиллиона линейных и геометрических комбинаций и выплюнул их обратно.

Блейк встал из-за стола и подошел к ватману на стене. Он

провел пальцем по первому символу в левом верхнем углу — букве «Н». Затем его взгляд скользнул по строке.

«Мы бьемся головой в бетон, потому что считаем, что этот бетон сплошной», — прошептал Сэм в тишину душной комнаты.

Он закрыл глаза, пытаясь абстрагироваться от усталости. Физиология страха перед неудачей сжала желудок. Полвека поражений. Десятки разрушенных карьер. Сотни фальшивых расшифровок от сумасшедших, утверждавших, что код содержит имена президентов, инопланетян или рецепты бомб. И вот теперь они — трое энтузиастов, застрявших в изоляции в своих домах, — подошли к краю той же самой пропасти.

Сэм снова открыл глаза и посмотрел на матрицу. Двадцать на семнадцать.

А что, если Зодиак вообще не думал категориями сложных криптографических машин? Что, если его метод был до примитивности физическим и визуальным? Что, если он не перемешивал символы случайным образом, а использовал конкретный, механический сдвиг при записи?

В криптографии существует понятие «децимации» — выбора каждого N -го символа из последовательности. Сэм посмотрел на первую строку. А затем его взгляд упал на вторую строку, но не под первой буквой, а сместившись вправо.

По диагонали.

Сердце математика дрогнуло, пропуская удар. Это было

не озарение, это был жест отчаяния, шаг в сторону от классических догм.

Он быстро вернулся к компьютеру, его пальцы запорхали по клавиатуре с новой, лихорадочной энергией. Гул вентиляторов ноутбука казался теперь не раздражающим шумом, а боевым барабаном.

Он открыл общий чат с Дэвидом и Ярлом.

«Дэвид. Ярл. Вы здесь?» — напечатал Сэм. Ответы пришли мгновенно. Никто из них не спал.

«Слушайте меня внимательно», — пальцы Сэма выбивали дробь по клавишам. — *«Мы испробовали сотни тысяч перестановок. Спирали, змейки, колонки. Все это было слишком математически правильно. Слишком академично. Мы пытались найти сложную логику там, где работала злая, утилитарная хитрость».*

Он прикрепил к сообщению изображение матрицы Z340.

«Давайте перестанем читать по горизонтали или вертикали. Давайте разобьем архитектуру самого пространства. Я хочу, чтобы мы применили ход конем. Как в шахматах».

«Что ты имеешь в виду?» — пришел ответ от Дэвида из заснеженной Вирджинии.

«Сдвиг матрицы», — напечатал Блейк, чувствуя, как по спине пробегает холодный пот напряжения. — *«Мы берем первый символ в верхнем левом углу. Затем спускаемся на одну строку вниз и сдвигаемся на два шага вправо. И берем*

следующий символ. Читаем по диагонали, пропуская ячейки. Один вниз, два вправо. Один вниз, два вправо. Мы разрезаем эту чертову сетку по косой. Мы заставим алгоритм Ярла прочитать код так, как никто до нас не пытался».

В чате повисла пауза. Тяжелая, цифровая тишина, пересекающая океаны и континенты. В этой паузе заключались пятьдесят лет неразгаданной тайны.

Затем на экране Сэма Блейка загорелось сообщение от Ярла Ван Эйка:

«Пишу скрипт. Запускаем».

Глава 2: Сдвиг матрицы



Глухая тишина цифрового пространства не имеет физического воплощения, но для тех, кто проводит в ней годы, она обретает плотность, вес и даже текстуру. Это была текстура ожидания. В Мельбурне, Антверпене и Вирджинии три человека одновременно смотрели на экраны, где разворачивалась невидимая битва между абсолютным хаосом и математическим порядком.

Криптография по своей сути — это наука о разрушении паттернов. Любой язык имеет свою внутреннюю архитектуру, свой неизменный ритм. В английском языке буква «Е» встречается с неотвратимой регулярностью — примерно в

12–13 процентах случаев. Буквы «Т», «А», «О» следуют за ней плотной группой. Редкие «Z» или «Q» появляются лишь эпизодически. Этот статистический закон — ахиллесова пята любого простого шифра подстановки. Если убийца заменяет букву «Е» на символ треугольника, криптоаналитику достаточно посчитать, какой символ встречается чаще всего, чтобы обрушить всю конструкцию.

Зодиак знал это. Когда в 1969 году школьный учитель Дональд Харден с женой Бетти за выходные вскрыли его первый шифр Z408, используя банальный частотный анализ, эгоманьяка получило болезненный удар. Он понял, что недооценил противника. Поэтому, создавая Z340, он решил применить гомофоническую подстановку.

Суть этого метода изящна в своей параноидальной хитрости. Чтобы скрыть частотность буквы «Е», создатель шифра назначает ей не один символ, а, скажем, семь разных. Букве «А» — пять символов. Букве «Т» — шесть. В результате гистограмма текста становится плоской. Редкие и частые буквы сливаются в единую серую массу. Статистика слепнет. Треугольник, крест и заштрихованный круг могут означать одну и ту же букву, а могут — совершенно разные.

Но для программы Ярла Ван Эйка, знаменитого алгоритма AZdecrypt, гомофонический шифр не был непреодолимой преградой. Программа была натренирована выявлять связи более высокого порядка. Она искала не отдельные буквы, а биграммы (сочетания из двух букв, вроде «ТН», «НЕ»,

«IN») и триграммы («THE», «AND», «ING»). AZdecrypt использовал метод, известный в информатике как «алгоритм восхождения на холм» (hill-climbing).

Представьте себе слепого альпиниста, которого высадили в неизвестной гористой местности. Его задача — найти самую высокую вершину. Он делает случайный шаг. Если нога чувствует подъем, он делает следующий шаг в том же направлении. Если чувствует спуск — возвращается назад и пробует другую сторону.

Внутри AZdecrypt происходило то же самое. Программа брала зашифрованный текст Z340 и назначала символам случайные буквы. Получался абсолютно нечитаемый мусор. Затем программа оценивала этот мусор по системе баллов: чем больше случайных совпадений с типичными английскими биграммами и триграммами, тем выше балл. После этого алгоритм менял значение всего одного символа. Если балл (высота холма) рос, изменение сохранялось. Если падал — отвергалось. Программа карабкалась вверх, делая миллионы таких шагов в секунду.

Однако в случае с Z340 алгоритм раз за разом застревал на так называемых «локальных максимумах» — небольших холмиках, откуда любой шаг вел только вниз, хотя настоящая вершина скрывалась где-то в тумане. Причина была проста: Зодиак не просто заменил буквы, он сломал саму геометрию текста.

Сэм Блейк смотрел на строчки кода, которые он только

что отправил Ван Эйку. В них была заложена гипотеза транспозиции — сдвига матрицы.— Мы исходили из того, что он писал как нормальный человек. Слева направо, сверху вниз, — голос Блейка в аудиоконференции звучал хрипло от усталости.— Но он хотел запутать нас. Он применил децимацию.

Матрица Z340 представляла собой сетку: 20 столбцов и 17 строк. Сэм предложил прочитать ее по диагонали. Правило было математически четким: начать с левого верхнего угла, прочитать символ, затем спуститься на одну строку вниз и сдвинуться на два столбца вправо. «Один вниз, два вправо» — как ход коня на шахматной доске, только растянутый.

Но что происходит, когда алгоритм доходит до правого края матрицы? Блейк применил концепцию тороидальной топологии. Представьте, что лист бумаги свернули в цилиндр: достигнув правого края, вы просто продолжаете движение с левого края той же строки. А если свернуть этот цилиндр в кольцо, соединив верх и низ, получится тор (форма пончика). Пространство становится замкнутым и бесконечным. Алгоритм, сдвигаясь «один вниз, два вправо», будет непрерывно наматывать круги по этой невидимой геометрической фигуре, пока не соберет все 340 символов в новую, вытянутую в одну линию последовательность.

Ярл Ван Эйк получил скрипт Сэма. В его тесной бельгийской комнате, освещенной лишь агрессивным свечением монитора, раздался щелчок мыши. AZdecrypt принял новую строку — последовательность, собранную по диагонально-

му правилу Блейка из миллионов возможных перестановок, сгенерированных суперкомпьютером Spartan.

Дэвид Оранчак в Вирджинии затаил дыхание. На его экране транслировался рабочий стол Ярла.

Запустился процесс. Индикатор на экране, показывающий «оценку текста» (n-gram score), задрожал. Обычно этот показатель болтался в районе нескольких сотен баллов — верный признак бессмысленного набора букв.

Внезапно цифры прыгнули. Алгоритм восхождения на холм нашел крутой подъем. Оценка взлетела. Восемьсот. Тысяча. Тысяча двести.

Ярл подался вперед, почти касаясь носом монитора. AZdecrypt начал выбрасывать на экран фрагменты текста, которые больше не выглядели как случайный мусор.

В первой строке, среди каши из символов, отчетливо проступило слово «НОРЕ» (НАДЕЮСЬ). Чуть дальше, после цепочки бессмыслицы, выскочило «TRYING» (ПЫТАЕТЕСЬ). Затем появилось зловещее «CATCH ME» (ПОЙМАТЬ МЕНЯ).

— Боже мой, — прошептал Оранчак. Волосы на его затылке встали дыбом. Пятьдесят один год этот текст хранил молчание, и сейчас он заговорил.

Но радость длилась всего несколько секунд. Алгоритм рванул вверх, но внезапно ударился о невидимый потолок. Оценка замерла на отметке, которая была высока для случайности, но недостаточна для полного, осмысленного тек-

ста. После слова «САТСН МЕ» программа снова начала выдавать чистую, беспросветную энтропию. Белый шум вернулся, поглотив английскую речь. Машина забуксовала.

— Что произошло? — голос Блейка дрогнул. — Почему он остановился? — Локальный максимум, — сухо ответил Ярл, хотя его пальцы, летающие по клавиатуре, выдавали крайнюю степень напряжения. — Программа подобрала идеальные ключи для первых слов, но дальше эти же ключи выдают бред. Логика рушится.

Оранчак открыл матрицу на своем экране. Он впился взглядом в оригинальную сетку из 340 символов. Если гипотеза Сэма «один вниз, два вправо» работала в начале, но переставала работать потом, значит, проблема была не в алгоритме. Проблема была в самом шифре.

Дэвид абстрагировался от светящегося экрана. Он попытался перенестись мыслями туда, в ноябрь 1969 года.

Сан-Франциско. Напряжение в городе звенит, как натянутая струна. Полиция сбилась с ног, патрулируя улицы и сопровождая школьные автобусы. А где-то в дешевой съемной комнате или грязном подвале за столом сидит человек. Он чувствует себя всемогущим богом, дергающим за ниточки целый штат. Перед ним лежит лист миллиметровки, карандаш и линейка. Он создает свой шедевр. Он чертит матрицу 20 на 17.

Затем он берет свой черновик с посланием, которое хочет зашифровать. И начинает кропотливо, вручную, переносить

буквы в сетку, следуя своему хитроумному правилу «один вниз, два вправо». Он отсчитывает ячейки. Вниз. Раз, два, вправо. Пишет символ. Вниз. Раз, два, вправо. Пишет символ.

Это скучная, монотонная работа. Требуемая предельной концентрации.

А психопат с линейкой — всего лишь человек. Человек, который может устать. Которого может отвлечь шум за окном, лай собаки или собственные параноидальные мысли.

Дэвид водил курсором по строкам, повторяя путь убийцы. Первая строка, вторая, третья... Идеально. Восьмая строка. Девятая...

Стоп.

В девятой строке паттерн, по которому строились английские слова в программе Ярла, ломался с хрустом. Оранчак приблизил изображение.

В 1969 году, дойдя до девятой строки матрицы, Зодиак совершил банальную, глупую, непростительную для «гения» ошибку. Переносил символ по правилу диагонали, он промахнулся. Возможно, его линейка соскользнула на одну клетку. Возможно, он обсчитался. Но он поставил знак не в ту ячейку. И, не заметив этого (или заметив, но поленившись переписывать весь лист заново), он продолжил шифровать дальше, отталкиваясь уже от этой ошибочной позиции.

В линейном тексте это была бы просто опечатка, пропущенная буква. Но в криптографии транспозиции, где по-

зиция каждого символа математически связана со всеми остальными через алгоритм, сдвиг на одну ячейку вызвал катастрофическую цепную реакцию. Вся архитектура шифра, начиная с девятой строки, сместилась. Фаза была сбита. Безупречный алгоритм AZdecrypt пытался натянуть правильную геометрию на искривленный человеческой небрежностью каркас — и терпел крах.

— Парни, — голос Дэвида прорезал тишину с хирургической резкостью. — Проблема не в машине. Проблема в нем. Он облажался.

Он быстро вывел на общий экран свои расчеты. — Смотрите. Паттерн работает только для первых 170 символов. Это ровно половина матрицы. Если мы разделим шифр на части...

Блейк мгновенно уловил математическую суть. — Он разбил матрицу. Он не шифровал ее как единый блок 20 на 17. Он разделил ее по горизонтали!

Они начали лихорадочно препарировать матрицу. Оранчак провел воображаемые линии, разрезая блок. Вырисовывалась новая структура: верхний блок из 9 строк. Средний блок из 9 строк. И нижний огрызок из 2 строк.

— В первом блоке, в 9-й строке, он сбился с шага. Сместил координаты, — Дэвид быстро набирал текст. — Нам нужно вручную исправить его ошибку. Нам нужно очистить код от человеческого фактора.

Это была скрупулезная, почти нейрохирургическая рабо-

та. Программистам предстояло сделать то, что не мог сделать ни один суперкомпьютер мира: понять логику ошибки психопата и компенсировать ее. Они выделили символ, который Зодиак поставил мимо нужной клетки, и аккуратно «подвинули» всю последующую последовательность обратно в правильную математическую фазу. Они выровняли матрицу, исправив кривой почерк безумца.

Сформировав новую, скорректированную строку, Оранчак переслал ее Ярлу. В Антверпене шел проливной дождь, капли барабанили по стеклу, сливаясь с гулом охлаждающих кулеров.

— Строка получена, — сухо констатировал Ван Эйк. В его голосе не было эмоций, но Дэвид знал: бельгиец сейчас напряжен, как оголенный провод. — Заряжаю в AZdecrypt. Перезапуск.

На экране снова появилось черное окно командной строки. Алгоритм восхождения на холм получил новые стартовые координаты. Он снова оказался у подножия горы, но на этот раз местность перед ним была свободна от непроходимых разломов, оставленных дрогнувшей рукой убийцы.

Начался процесс мутации ключей. Программа подставила случайные значения. Оценка: 300 баллов. Она изменила букву «Е». Оценка: 500 баллов. Изменила «Т». Оценка: 900 баллов. Шаг за шагом алгоритм карабкался вверх. Он больше не спотыкался на 9-й строке. Локальный максимум был пройден на огромной вычислительной скорости.

Оценка: 1500. Оценка: 2200.

Дэвид почувствовал, как сердце гулко бьется о ребра, отдаваясь в ушах пульсирующим ритмом. По спине потек холодный пот. Сэм в Мельбурне застыл, не смея даже моргнуть.

Оценка текста пробила отметку в 3000 баллов. Это был статистический водораздел. Точка невозврата. За этой отметкой случайности не существовало. За этой отметкой начиналась чистая, математически подтвержденная правда.

Зеленые символы на черном фоне дрогнули, перестраиваясь. Геометрические фигуры, кресты, полукружья и треугольники, которые издевались над следователями ФБР, криптографами АНБ и армией любителей полвека, начали схлопываться, уступая место английскому алфавиту. Белый шум матрицы рассеивался, как утренний туман под палящим солнцем.

Программа приняла исправление. Бессмысленные обрывки слились в монолитный блок текста.

На экране Дэвида, буква за буквой, из цифровой бездны начало проступать послание из 1969 года.

«I HOPE YOU ARE...» (Я НАДЕЮСЬ ВЫ...)

Дэвид вцепился пальцами в подлокотники кресла. Алгоритм завершал последние корректировки, расставляя на места редкие буквы. Строки заполнялись смыслом, обнажая холодный, надменный разум человека, который пятьдесят лет ждал, чтобы с ними заговорить.

Глава 3:

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.