Криптоанархия: что общего между феней и математическими алгоритмами и как американские военные породили даркнет-рынки

Серое Фиолетовое

15 февраля 2018

Оглавление

Бродячие торговцы дореволюционной России — офени — имели собственный язык с русской грамматикой, но с весьма своеобразной лексикой: она включала в себя диалектизмы, а также тюркские, финно-угорские, греческие заимствования. Говорящих друг с другом офеней носители русского языка понять не могли. Так, девушка по-офенски звалась «карючок», деньги — «биряне», купцов же именовали «алафитами». Согласно некоторым теориям, арго офеней — «феня» — послужило одним из источников для более позднего воровского жаргона.

Такая ситуация отнюдь не уникальна для России: мещерский был секретным языком болгарских строителей, баргунс — криминалитета и мелких странствующих торговцев Нидерландов, а ротвельш играл аналогичную роль на юго-западе Германии и в Швейцарии.

Ученые XVI и XVII столетий использовали иной способ шифрования своих сообщений: для сохранения приоритетного права на собственные открытия они записывали их в виде анаграмм — сочетаний букв, которые при должной перестановке и расстановке пробелов дадут фразу, свидетельствующую о научном достижении и подтверждающую авторство.

Так, в 1610 году Галилео Галилей зашифровал сообщение об открытии им колец Сатурна в виде анаграммы smaismrmilmepoetaleumibunenugttauiras.

Иоганн Кеплер неправильно расшифровал ее — и решил, что речь идет о спутниках Марса. Их существование следовало из вычислений немецкого астронома, но увидеть Фобос и Деймос в телескоп оказалось возможным лишь через два с половиной столетия — в 1877 году.

Однако использование и развитие настоящих систем шифрования и сложных способов сокрытия информации оставалось в основном делом государств: военных, дипломатов, разведок.

Массовое же их применение и создание независимых систем коммуникации стало возможным лишь к концу XX века с распространением электронных средств связи и шифрования с открытым ключом. Последнее основано на генерации двух криптографических «ключей»: один из них можно передавать публично, с его помощью кодируют сообщения, а другой — закрытый, известен только ограниченному кругу лиц и применяется для расшифровки.

Передача открытых ключей без задействования секретных каналов связи сделала возможным массовое использование криптографии в появляющихся телекоммуникационных сетях.

Первые алгоритмы шифрования такого типа были открыты британскими военными криптографами в начале 1970-х годов (об этом стало известно лишь в конце 1990-х), а гражданскими — в середине того же десятилетия. Речь идет об алгоритме обмена ключами Диффи — Хеллмана, созданном американцами Уитфилдом Диффи, Мартином Хеллманом и Ральфом Меркле, а также знаменитом алгоритме RSA, авторами которого стали сотрудники MIT Рон Ривест, Ади Шамир и Леонард Адлеман.

Оба они основаны на вычислениях с простыми (то есть не имеющими делителей) числами, или задачах дискретного логарифмирования и разложения числа на простые множители. Впоследствии список пополнился множеством других алгоритмов подобного рода и их вариаций.

С появлением концепции квантового компьютера, который позволил бы значительно ускорить операции с простыми числами, возникли и новые области науки: постквантовая и квантовая криптография.

Первая исследует алгоритмы, устойчивые к вычислениям на таких чудо-машинах, вторая — специфические методы шифрования, связанные с использованием квантовой информации.

Однако эти вопросы, занимающие теоретиков шифрования, так и остались бы специфической областью прикладной математики, если бы не быстрое развитие интернет-технологий. К середине 1980-х криптомир стал реальностью, и в 1985 году в американском журнале «Сообщения Ассоциации вычислительной техники» появилась статья Дэвида Чома «Безопасность без идентификации: системы верификации, которые делают Большого Брата устаревшим».

В статье обсуждались вероятные конфигурации электронных подписей, анонимных систем онлайн-платежей и заключения контрактов — ранних предшественников нынешних криптовалют и блокчейн-технологии.

В этой работе Чом говорит об анонимной коммуникации с использованием криптографии с открытым ключом. Подобные идеи он развивал с начала 1980-х и в итоге воплотил в исторически первой системе анонимных онлайн-платежей DigiCash, функционировавшей в середине 1990-х, при содействии американского Mark Twain Bank и ряда крупных банков различных европейских стран.

В августе 1988 года криптоанархия получила и свое идеологическое оформление. Американский инженер, технический писатель и радикальный интеллектуал Тим Мэй распространил на конференции Crypto’88, проходившей в калифорнийском городе Санта-Барбаре, свой «Манифест криптоанархиста». Широкой аудитории текст стал доступен в 1992 году.

В манифесте Мэй пишет:

> **«Призрак бродит по современному миру, призрак криптоанархии.**
>
> Компьютерные технологии стоят на пороге того, чтобы дать возможность отдельным людям и группам общаться и взаимодействовать абсолютно анонимно. Два человека смогут обмениваться сообщениями, заниматься бизнесом, заключать электронные контракты, не имея возможности установить Подлинные Имена, личности друг друга. Взаимодействие в Сети невозможно будет отследить из-за многократных изменений маршрутов зашифрованных пакетов и предупреждающих от несанкционированного

вмешательства блоков, которые наделяют криптографические протоколы практически идеальной защитой. <…>

Государство, очевидно, боясь социальной дезинтеграции, попытается замедлить или приостановить распространение таких технологий, ссылаясь на соображения национальной безопасности, использование этих технологий наркоторговцами и неплательщиками налогов. Любое из этих соображений будет обоснованным: криптоанархия позволит свободно торговать национальными секретами, а также незаконными препаратами и краденым. Анонимный компьютеризированный рынок сделает возможным даже создание отвратительного рынка заказных убийств и вымогательств. Криминальные элементы и иностранцы станут активными пользователями CryptoNet'а. Но это не остановит криптоанархию.

Точно так же, как технология книгопечатания изменила социальный строй и уменьшила могущество средневековых гильдий, криптографические методы принципиально изменят корпорации и роль государства в экономических транзакциях. <…>

Действуйте, ибо вам нечего терять, кроме этих изгородей из колючей проволоки!»

К началу 90-х анонимными ремейлерами — средствами пересылки писем без известного отправителя — пользовались десятки тысяч людей.

В 1991 году выходит созданная Филом Циммерманом программа PGP (Pretty Good Privacy), используемая для защищенной переписки. В 1993 году против ее автора было возбуждено уголовное дело (ничем впоследствии не окончившееся): тогдашние американские законы рассматривали криптографию как форму военной технологии, и экспорт подобной «продукции» был запрещен. В ответ на это Циммерман вместе с издательством Массачусетского технологического института издал код PGP в виде книги: любой желающий мог ее отсканировать, распознать текст и скомпилировать софт. Распространение же программного кода, в том числе и за пределами Америки, охранялось защищающей свободу слова Первой поправкой к Конституции США.

Читайте также

Первый гелиоцентрист: *Аристарх Самосский против всех*
Астрономки, поэтессы, жрицы. *Женщины и точное знание в Древней Месопотамии*

На протяжении всех 1990-х новообъявившиеся криптоанархисты судились с американскими спецслужбами, обвинявшими их в обнародовании документов по истории шифрования. Они пытались основать черный рынок информации BlackNet со своей собственной валютой CryptoCredits, биржу-казино, принимающую ставки на скорую смерть тех или иных политических деятелей, а в начале 2000-х — хостинг-компанию с серверами на территории «Княжества Силандия» (это была «объявившая

о своей независимости» заброшенная морская оборонная платформа времен Второй мировой войны, расположенная у берегов Великобритании). Но в отличие от широко распространившейся PGP и ее аналогов, более радикальные социальные проекты криптоанархистов особого успеха не имели.

Однако первая по-настоящему масштабная война за независимость киберпространства состоялась не на землях гражданской криптографии. Ее полем боя стало право на свободное копирование информации. Все началось в середине 1999 года: 1 июня американцы Шон Фэннинг и Син Паркер (18 и 20 лет соответственно) запустили первый файлообменный пиринговый сервис Napster. Передача информации в нем происходила не «вертикально» — с сервера на компьютер пользователя, а «горизонтально» — между самими юзерами. А в октябре того же года 15-летний житель небольшого норвежского городка Харстад Йон Йохансен выпустил DeCSS — программу, позволявшую дешифровать содержимое коммерческих DVD. Впервые появилась возможность читать такие диски в свободной операционной системе Linux.

Ответные действия крупных корпораций не заставили себя ждать.

После удовлетворения судебных исков группы Metallica, рэп-исполнителя Dr. Dre, а затем и коллективного иска компаний — членов Американской ассоциации звукозаписи Napster к середине 2001 года был вынужден прекратить свою деятельность.

В 2002–2003 годах шел и уголовный процесс против Йона Йохансена, который вел норвежский центр по борьбе с экономическими преступлениями по инициативе американских организаций, осуществляющих контроль над копированием DVD, и киноассоциации.

Йохансен был полностью оправдан, однако проекты с механикой свободного файлообмена оказались под угрозой, и ситуация в этой сфере стала сложнее. Завязанные на те или иные компании и инициативы сервисы, такие как Gnutella, eDonkey, KaZaA, не выдерживали судебных исков и либо исчезали, либо в существенной степени маргинализировались.

Их место занял созданный Брэмом Коэном в 2001 году протокол BitTorrent. Борьба же государств и корпораций против использования этой технологии породила первое широкое политическое движение за сетевую автономию.

Самой известной из многочисленных историй, связанных с торрентами, стала та, что произошла в Швеции: в 2003 году боровшееся против копирайта НКО «Пиратское бюро» создало торрент-трекер «Пиратская бухта» (The Pirate Bay), ставший символом сопротивления копирайту.

В отличие от многих других торрент-трекеров, легко закрывавшихся властями после обысков и конфискации оборудования, The Pirate Bay пережил множество подобных акций (включая эпизоды с тюремным заключением его основателей: Петера Сунде, Готтфрида Свартхольма и Фредрика Нея). В ответ на глобальную кампанию

против проекта возникло международное политическое движение — интернационал пиратских партий. Организация выступает за изменение отношения к авторскому праву, расширение механизмов прямой демократии, а также — один из центральных пунктов программы борьбы за свободный интернет — против государственной и корпоративной слежки за гражданами.

На сегодняшний день пиратские партии представлены в парламентах Исландии и Чехии, в Европарламенте, а также на региональном или местном уровне во многих европейских странах.

Несмотря на свое массовое распространение, торренты имеют принципиальную проблему: они совершенно неанонимны. В таких странах, как США и Германия, где давление корпораций оказалось значительно сильнее напора граждан и власти выбрали политику индивидуального преследования пользователей за распространение защищенных копирайтом материалов, число ежегодно подвергаемых угрозам штрафа людей оказывается весьма велико.

Множество немецких юридических фирм практикует слежку за пользователями торрентов и рассылку писем с требованиями оплатить «штраф» без судебного разбирательства. Тем не менее до реального суда доходит лишь небольшая часть дел: компании готовы довольствоваться доходами, получаемыми от тех, кто раскошелится при первой угрозе.

Однако массовое развитие коммерческих стриминговых сервисов наряду с постоянными полицейскими операциями против владельцев крупных трекеров привело к тому, что пиринговые ресурсы сейчас занимают куда более маргинальную нишу, чем десятилетие назад. Если в 2004 году их доля в общем интернет-трафике составляла около 60 %, то на сегодняшний день этот показатель равен лишь 6 %.

Появление пиринговых сервисов файлообмена, предоставляемых крупными компаниями, и нарастающая коммерциализация поделенного между ними интернета далеко не единственное явление, с которым столкнулись пользователи в начале 2000-х. Ответом на все меньшую сетевую анонимность и все большее внимание государств к происходящему в сети стало возникновение «даркнета» — функционирующих поверх обычных протоколов программ, создающих «параллельный интернет», где слежка за пользователями оказывается крайне затруднена.

Это не только ставшая знаменитой (и на самом деле наименее безопасная из всех) сеть, порожденная проектом Tor, но и более медленные и сложные в использовании i2p и Freenet.

Tor используется как для сохранения анонимности интернет-пользователя, так и для доступа к ресурсам самой сети, но изначально он не был активистским проектом. В нем применяется технология «луковой маршрутизации» — перенаправления шифрованных данных через постоянно меняющуюся цепочку промежуточных компьютеров. Она была создана в середине 1990-х американскими военными исследователями (как и 30 годами ранее — технологии, которые легли в основу интернета

как такового). С 2004 года финансированием и развитием проекта сперва занимался некоммерческий Фонд электронных рубежей, а затем — специально созданная организация Tor Project. Последняя существует за счет средств, выделяемых правительствами США и европейских стран, а также различными компаниями. Одной из основных декларируемых целей Tor остается доступ к информации для людей, проживающих в авторитарных государствах.

Более активистским по своей природе было происхождение других сетей даркнета. Например, в основе работы Freenet, созданной в 1999 году студентом Эдинбургского университета Яном Кларком, лежит не просто случайное перенаправление шифрованных данных, но и случайное их хранение.

Разрозненные фрагменты закодированной информации расфасованы по компьютерам пользователей сети, при этом где именно хранится каждый из них, узнать невозможно.

Следующей по времени — и до сих пор продолжающейся — революцией в области децентрализованного и анонимного общения стало создание криптовалют и блокчейнов — распределенных зашифрованных баз данных. Теоретические основы технологии были заложены еще в 1990 году, когда два сотрудника исследовательской компании Bellcore представили доклад «Как сделать метку времени создания на электронном документе» на криптографической конференции в Санта-Барбаре. Однако до практического воплощения этих идей оставалось еще почти два десятилетия.

31 октября 2008 года неизвестный, называвший себя именем Сатоши Накамото, опубликовал в одной из криптографических рассылок статью «Биткойн: пиринговая система электронной валюты». 9 января 2009 года было выпущено и соответствующее программное обеспечение — в мире появилась первая криптовалюта.

Основой технологии стала база данных, содержащая в зашифрованном виде историю всех транзакций, когда-либо произведенных с биткойнами. Это позволило решить проблему «двойной траты» — двойного расходования одной и той же единицы цифровой валюты, которая долго являлась главным препятствием на пути к полной децентрализации электронных денег. Раньше для того, чтобы определить, «потрачены» ли виртуальные накопления, необходимо было иметь центральный сервер, например банковский, с данными которого можно было бы сравнить состояние кошелька на компьютере пользователя. Это означало, что у любой электронной валюты есть некий «главный управляющий» и он может так или иначе манипулировать ситуацией. Биткойн же основан на базе данных, постоянно обновляющейся при помощи пиринговой сети. Ее копии хранятся на бесчисленном множестве компьютеров по всему миру. Через нее осуществляется проверка возможности каждой новой транзакции, и в случае, если она совершена, база незамедлительно пополняется. Так происходит сравнение состояний счетов. Данные представляют собой цепь блоков с информацией о транзакциях, в каждом из которых имеется ссылка на предыдущий и последующий. Получается «цепь блоков» — блокчейн.

Объем этой базы постоянно растет и по состоянию на январь 2018 года составлял около 150 гигабайт.

В середине 2010 года Сатоши Накамото вышел из проекта BitCoin и передал его сформировавшемуся сообществу: споры о том, кто же скрывался за этим псевдонимом, не утихают до сего дня.

После появления в анонимном интернете анонимной же децентрализованной валюты возникли новые возможности для международной анонимной торговли. Первыми, кто ими воспользовался, стали создатели даркнет-рынка «Шелковый путь» анархо-индивидуалист Росс Уильям Ульбрихт, а также люди, скрывавшиеся под псевдонимами Вэраети Джонс и Смедли Чарджер. Около 70 % предложений здесь составляли запрещенные психоактивные вещества, известные нам как наркотики.

«Шелковый путь» был открыт в феврале 2011-го, и уже в октябре 2013-го ФБР смогло заблокировать сайт и арестовать Росса Ульбрихта, обвинявшегося в отмывании денег, торговле наркотиками и взломе компьютеров. Кроме того, его подозревали в шести попытках заказа убийства, но впоследствии эти обвинения были сняты. Создателя торговой площадки приговорили к пожизненному заключению без права на освобождение (теперь для его выхода на свободу необходимо решение президента США).

«Шелковый путь» стал далеко не первым рынком подобного рода. Еще в начале 1970-х годов в интернете (называвшемся тогда ARPANET) была заключена коммерческая сделка: студенты Стэнфордского университета покупали у «коллег» из Массачусетского технологического института марихуану. А скрытый внутри сети Tor «Фермерский рынок» (в рамках которого принималась, однако, не криптовалюта, но обычные переводы внутри разных платежных систем) открылся на год раньше «Шелкового пути».

Масштаб проекта оказался впечатляющим, а его популярность только растет: в результате постоянных рейдов и закрытий даркнет-рынков они отнюдь не прекратили свое существование, но, напротив, сделались постоянным объектом публичного дискурса.

В последние годы технологии криптовалют (количество которых уже достигает нескольких сотен!) стремительно развиваются: они расширились до теоретически сконструированных в середине 1990-х Ником Сабо автоматически функционирующих «умных контрактов», новых моделей децентрализованных анонимных социальных сетей и «интернет-наций» с добровольным членством.

Запланированный выход Telegram на рынок криптовалют и блокчейнов также воодушевляет многих пропагандистов анонимного и свободного будущего, претворяющих в жизнь положения из манифестов криптоанархистов 1980-х. Однако растущий контроль государств и вертикально организованных корпораций над криптомиром может свидетельствовать о другом. Грядет интеграция новых технологий в строящийся мировой порядок с его беспрецедентной «прозрачностью», сводящейся к всеобщей слежке и многообразным зависимостям людей от услуг крупных компаний и государства, затягивающих их в свои системы нормализации, регулирования, управления.

Произойдет ли криптографическая революция? Или же новые технологии будут отчасти ассимилированы обладающими политической и экономической властью институтами, а отчасти оттеснены в маргинализированную «свободную зону», требующую специальных технических навыков для использования ее ресурсов? Покажет только будущее. Одно можно сказать точно: пока существуют системы подавления, будет существовать и сопротивление государственной, рыночной и социальной власти, одним из инструментов которого является шифрование — сокрытие информации от ненужных взглядов.

Библиотека Анархизма
Антикопирайт и инфоанархизм

Серое Фиолетовое
Криптоанархия: что общего между феней и математическими алгоритмами и как американские военные породили даркнет-рынки
15 февраля 2018

web.archive.org
С древних времен люди пытались скрыть информацию от внешнего мира. Это обеспечивало их автономию и свободу. Так возникали разнообразные «секретные наречия» — будь то известные лишь посвященным ритуальные языки, шифры магов и алхимиков или же многочисленные «арго исключенных» — речь мелких торговцев, воров, бездомных, квиров, непонятная (или не вполне понятная) обывателю.

ru.anarchistlibraries.net