Михаил Масленников

# Занимательная криптография. Часть 1

Михаил Масленников

# Занимательная криптография. Часть 1

«Автор»
2026

**Масленников М. Е.**

Занимательная криптография. Часть 1 / М. Е. Масленников — «Автор», 2026

Я решил попробовать изложить некоторые современные понятия криптографии на простом и понятном языке неискушенному читателю, популяризировать криптографию. Криптография – это один из разделов математики, поэтому при ее популяризации не обойтись без математических выкладок с математическими понятиями и формулами, которые могут быть непонятны рядовому читателю. Я, как мог, постарался объяснить их на простом житейском языке, частенько прибегая к различным выдумкам и фантазиям. Надеюсь, что получилась занимательная криптография, которая может быть полезной широкому кругу читателей.

© Масленников М. Е., 2026
© Автор, 2026

# Содержание

# Михаил Масленников
# Занимательная криптография. Часть 1

## Предисловие

В детстве я очень любил читать книгу Я. И. Перельмана «Занимательная физика». В предисловии к одному из изданий этой книги сказано: «Составитель старался, насколько мог, придавать изложению внешне интересную форму, сообщать привлекательность предмету». Мне, будучи тогда еще школьником средней школы, очень нравилась манера изложения и разъяснения автором сложных физических понятий и эффектов, вопреки довольно скучному стилю типового учебника по физике. Недаром Яков Исидорович Перельман остался в памяти у многих поколений людей как замечательный популяризатор естественных наук, в частности физики и математики.

Слово «криптография», как я надеюсь, слышали многие. Это наука о тайнописи, известная еще с доисторических времен Цезаря и древней Спарты.

Классическая криптография – это наука о тайнописи, о том, как сохранить в тайне какое-то секретное сообщение от посторонних глаз. Для этого еще в глубокой древности придумали много разных способов, заменяя в секретном сообщении понятный текст на непонятный набор символов в зависимости от некоторого секретного ключа, известного только тем, с кем ведется секретная переписка. Отправитель и получатель должны иметь один и тот же секретный ключ – это классическая криптография, традиционная симметричная схема.

Пока вопросов нет, вроде все ясно даже простому человеку, далекому от криптографии. Но различные симметричные схемы шифрования были хороши только до определенного момента времени, до тех пор, пока не появились компьютеры и Интернет. Дело в том, что при появлении Интернета и компьютерных сетей резко возросла потребность в шифровании передаваемой по ним информации.

Потребность в шифровании резко возросла, следовательно, резко возросла и потребность в ключах, на которых осуществляется шифрование. И вот тут традиционные симметричные схемы оказались неудобными из-за того, что ключи для зашифрования и расшифрования должны быть одинаковыми у отправителя и получателя. Как этого добиться?

Первое, что приходит в голову – заготавливать комплекты секретных ключей заранее и выдавать их каким-то секретным способом абонентам, ведущим между собой секретную переписку. Сотни лет именно так и поступали, из-за чего симметричная криптография становилась все более тяжеловесной и неудобной для широкого практического применения.

Криптографы стали думать и гадать, как упростить процедуру шифрования, чтобы сделать ее доступной в обычных, повседневных случаях, не связываясь с тяжеловесной симметричной ключевой системой.

В середине 70-х годов XX века американцы совершили революцию в криптографии – предложили новые и весьма нетривиальные подходы к шифрованию сообщений, ввели такое понятие, как электронно-цифровая подпись, или сокращенно ЭЦП. В обиходе криптографов появилось такое понятие, как асимметричная криптография. С появлением и внедрением в повседневную жизнь компьютерных сетей и Интернета роль криптографии стала стремительно расти. Без нее сейчас немыслимы банковские расчеты в режиме OnLine, работа различных серверов, содержащих конфиденциальную информацию, защищенный обмен конфиденциальными сообщениями и многое, многое другое. Потребность в использовании криптографии

стремительно растет, а осведомленность потребителей в современных криптографических методах защиты информации часто остается на прежнем уровне, когда все, что касалось криптографии, было строжайше засекречено.

Я решил попробовать изложить некоторые современные понятия криптографии на простом и понятном языке неискушенному читателю, популяризировать криптографию. Криптография – это один из разделов математики, поэтому при ее популяризации не обойтись без математических выкладок с математическими понятиями и формулами, которые могут быть непонятны рядовому читателю. Я, как мог, постарался объяснить их на простом житейском языке, частенько прибегая к различным выдумкам и фантазиям. Надеюсь, что получилась занимательная криптография, которая может быть полезной широкому кругу читателей.

# Сказка про числа, которые не хотели делиться

В действительном множестве, рациональном подмножестве жили-были натуральные числа. То есть числа 1, 2, 3, 4, 5 и т.д. Их еще иногда «числами в натуре» называли. Основным занятием натуральных чисел было умножаться-делиться в соответствии с операциями умножения и деления. Про умножение – все понятно, любое число могло умножаться с любым другим числом без проблем, а вот с делением все обстояло куда как сложнее. Не со всяким другим числом могло делиться натуральное число, бывало заартачится: не хочу с ним делиться, хоть обнуляйте меня совсем! Столько споров и дискуссий вызывала эта операция деления натуральных чисел, что в конце концов она-то и стала главной в этой сказке.

Понятно, что все делились с числом 1, это число было вроде как Царь-Батюшка во всем множестве натуральных чисел (МНЧ). Но деление с этим числом было совсем безобидное, в результате такого деления каким было число до деления, таким и оставалось после него, вроде как лозунг «Коммунизм победит» в советское время – количество мяса в магазинах от него не изменялось. Поэтому все натуральные числа периодически исполняли этот религиозный обряд – деление на 1 – без каких-либо последствий для себя, просто как символ верности МНЧ и проводимой им политике арифметических операций.

У числа 1, как и у любого нормального Царя, была своя Администрация, где утверждали важнейшие арифметические Законы МНЧ: кто, с кем и как будет делиться. А в штате Администрации были молоденькие запятые, которые целыми днями отпечатывали эти законы на пишущих машинках, ибо компьютеров в те далекие времена в МНЧ еще не знали.

Ну а о другом важном числе – 0 – нельзя со 100% уверенностью сказать, что оно жило в МНЧ. У него был специальный особняк, который все другие числа называли Конторой числа 0, или просто Конторой. Все числа из МНЧ побаивались числа 0, а причина – простая. Само число 0 могло делиться на кого угодно, после чего результат навсегда попадал в Контору, а вот если кто-то сам пытался делиться на 0, то его без лишних эмоций превращали в лагерную пыль. То есть число 0 жило по своим арифметическим законам, отличным от законов МНЧ, и ожидать от него можно было всего, чего угодно.

Число 2 было хитрым. Оно разделило ровно пополам всех обитателей МНЧ на тех, кто с ним делился, и тех, кто это делать категорически отказывался. Первых число 2 называло честными и даже создало из них специальную партию: Партию Честных Чисел. Мы ее, для краткости и по привычке, всюду в этой сказке будем звать просто партией. В партии, как и положено, было создано Политбюро из наиболее известных честных чисел: 2,4,6 и 8. Параграф 1 Устава партии гласил, что в ней могут состоять любые числа, признающие Устав и Программу партии и оканчивающиеся на одного из членов Политбюро. Устав приняли под бурные и продолжительные аплодисменты, но когда число 2 принесло его на согласование в Контору, там параграф 1 дополнили: и 0. Так его и утвердил Царь. А Программа партии была простая: наша цель – бесконечность. Эту программу Царь признал светлым будущим всех прогрессивных чисел из МНЧ.

В партии сразу же появились карьеристы, которые стремились поделиться с числом 2 не один, а целых два раза. Они попытались было, по примеру старших товарищей, создать партию честных – пречестных чисел, но Царь сказал, что и одной партии вполне достаточно, две народ просто не прокормит. Так что название «честное-пречестное число» осталось на уровне анекдотов и народного фольклора.

Число 2, как партийный вождь, было очень идейным. «Удвоение ВВП», «Две нормы за смену» – такие лозунги постоянно появлялись на улицах МНЧ. Оно также очень скрупулезно

следило за чистотой партийных рядов, не разрешая одному члену партии делиться на другого. Иногда за такие проступки могли и партбилет отобрать.

А вот за числом 3 закрепилась – как бы это поделикатнее сказать – отличная от числа 2 репутация. Алкогольная. Как соберутся в weekend числа отметить какое-нибудь событие, так обязательно разобьются на группы по три числа в каждой. Часто болела головушка у числа 3, допилось оно в результате до чертиков и стало мистическим символом МНЧ: три богатыря, три белых коня, пятилетку – в три года. Тяжело было числам из МНЧ строить свое светлое будущее – бесконечность, вот и почитателей у числа 3 было достаточно. Вместо красных носов у чисел ходило такое правило: число является алкоголиком, если сумма его цифр – алкоголик. Так и утвердил это правило Царь.

Еще пару слов про число 5. Оно было в Президиуме всех праздничных собраний и юбилейных дат, все в наградах и орденах аж до самого своего нижнего кончика, поэтому и звали число 5 нашим дежурным юбиляром. Безобидное число, партий своих создавать не пыталось, а на выборах всегда выдвигалось от единого и нерушимого блока честных и беспартийных. Делились на него те, у кого на конце было 5. Или 0, справедливо дополнили меня в Конторе.

Кстати, о Конторе. Там собирали разные сплетни из жизни МНЧ и вот какую историю я узнал от местных аборигенов.

В гости к жителям МНЧ часто заезжали другие, ненатуральные числа. И вот как-то раз приехал важный гость – заморское число $\pi$, ему как раз на днях исполнилось ровно 100 лет – два честных-пречестных юбиляра-разюбиляра. Естественно, по такому случаю число $\pi$ устроило праздничный банкет, на который пригласило число 100 и другие числа: 1, 2, 4, 5, 10, 20, 25, 50, но только не 3. Число $\pi$ терпеть не могло этого алкоголика, с которым его вечно путали. Ну, понятное дело, дым коромыслом, праздник в разгаре, гости начали разбиваться на группы по 3 числа. А число $\pi$ никак не хочет принимать участие в группе из 3-х чисел, и, прихватив число 100, нашло себе компаньона – какого-то генерала с денщиком. Получилась как бы группа не на троих, а, с учетом денщика, на 3,14. Число $\pi$ было жутко довольно, и, как потом писало число 100 в донесении числу 0, рассказывало неприличные истории про число 3. В частности, американский алгоритм шифрования 3DES – Triple DES – обзывало «Триппер DES».

Генерал хохотал весь вечер, к концу совсем расслабился, пил с $\pi$ и с 100 на брудершафт, потом его повели к очаровательным запятым из ведомства числа 1 – в общем, жизнь удалась. Наутро, не желая оставаться в долгу, генерал заявил, что никогда не забудет этого банкета и в память о нем назовет какое-нибудь оружие.

Так в армии появился пистолет.

Но были в МНЧ и диссиденты: числа, не вступившие в партию, и вообще, не желавшие ни с кем делиться, кроме Царя. В народе их называли еще простыми числами. Строго говоря, и всеми уважаемые числа 2, 3 и 5 тоже были простыми диссидентами, но благодаря куче поклонников – других чисел из МНЧ, которые с ними делились, – Царь считал их «своими» диссидентами и никаких репрессий к ним не применял. А вот числу 13 не повезло. Оно жило рядом с честным-пречестным числом 12 и постоянно пыталось отучить его от алкоголизма. Как бы не так! Число 12 написало кляузу в Контору, после чего отдел Пропаганды Царя-Батюшки объявил число 13 причиной всех бед и несчастий в МНЧ и обозвал его «чертовой дюжиной».

Так и жили тысячу лет в МНЧ, умножались и делились, стремясь достигнуть светлой цели, записанной в Программе правящей партии – бесконечности, но никак не могли этого сделать. А когда провозглашается что-то заведомо недостижимое, то в конце концов народ начинает выражать свое недовольство: умножаемся, делимся, а все без толку, бесконечности так и нет. Решив стравить пар народного недовольства, партийные вожди однажды провозгласили

перестройку: «Давайте делиться с остатком!». Мол побесятся натуральные числа, наиграются, и все вернется к прежним умножению и делению, когда никаких тебе остатков, все – общее.

А народ в МНЧ был такой, что палец ему в рот не клади – руку по локоть откусят. Раз провозгласила правящая партия деление с остатком, то все сразу смекнули, что остаток-то – штука неплохая. Главное, чтобы он в 0 не обратился, как было в прежней, доперестроечной жизни. И вот ведь что еще негодяи придумали – конечные группы. До того всем числам на всех политзанятиях только и внушали: наша цель – бесконечность, а тут – упала дисциплина, перестали слушать партийных пропагандистов, а на улицах стали появляться антиправительственные листовки: наша цель – конечная группа. Сам такую листовку раз видел на площади прямо около Конторы. Прихватил ее с собой, вот она.

Наша цель – конечная группа!

Всем! Всем! Всем!

Натуральные числа! Не слушайте пропагандистов из партии честных чисел – никакие они не честные! Врут они нам, что наша цель – бесконечность, не достигнуть ее ни через 100, ни через 1000 лет, сколько бы мы ни умножались и делились. Наша цель – конечная группа!

Вам забивают голову этой мистической бесконечностью, а мы расскажем вам, как быстро создать реальную конечную группу.

***Выбирайте себе*** *модуль* ***, умножайтесь и делитесь на него с остатком! Частное выбрасывайте, а остатки образуют конечную группу.***

Нет бесконечности!!!

Контора сперва хотела принять радикальное решение: показать всем этим вольнолюбцам настоящую бесконечность, обратив их в лагерную пыль. Но хитрое число 2 надоумило Контору не делать глупостей – не 37 год на дворе, надо действовать тоньше и с выгодой для себя. Надо просто подсунуть горлопанам подходящий модуль. Например, честного-пречестного алкоголика – число 12.

Идет как-то на нетвердых ногах число 3, а навстречу ему прямо сияет честное-пречестное число 8.

– Давай вступим в конечную группу по модулю 12.

– Давай!

Вступили. Перемножились. Раньше такое сколько раз вытворяли и в Контору за это никто не попадал. А тут как только привели результат по модулю 12, глазом не успели моргнуть, как он уже в Конторе.

Ну что, сынки, помогло вам ваше деление с остатком?

Возмутились числа: что такое, в конечной группе могут быть делители нуля! Не делители, а осведомители – поправили их в Конторе.

Приуныли натуральные числа. Неужели опять – все по-старому, наша цель – бесконечность? А нельзя ли как-то получить конечную группу без конторских осведомителей?

День думали, два, а на третий вспомнили о простых числах, тех, которые ни с кем не делятся. Взяли, к примеру, соседа числа 12 – бедное и затравленное число 13. И, о чудо! Кто с кем в его конечной группе ни умножался по модулю 13, а результат в Контору так и не попал! Не верите? Проверьте сами.

И стали в МНЧ очень популярны числа, которые не хотели ни с кем делиться. Как только выберут такое число модулем, так в его конечной группе законность и порядок, все арифметические операции выполняются четко и правильно, без всяких чуровых и делителей-осведомитлей числа 0. Старик Евклид придумал способ, как не только умножаться, но и делиться в такой конечной группе, причем как умножаться, так и делиться стали абсолютно все, от мала

до велика, кто на кого захочет. Кроме, естественно, числа 0, которому в этой группе места уже не было.

Контора была в ярости. Это кто ж теперь в модулях ходит? Без 0 в конце, беспартийные, непьющие, без юбилейных медалей! По-обычному ни с кем не делятся – простые! Да таких простых – раз два – и обчелся! А как же светлое будущее – бесконечность? С кем его строить-то будем, если все простые скоро закончатся?

Не закончатся – ответил Конторе старик Евклид в своих «Началах».

На всякий случай в Конторе решили поставить все конечные группы на учет под буквой Z, от слова zero – агентурной клички числа 0: Z/2 – группа по модулю 2, Z/3 – группа по модулю 3 и так далее. А натуральные числа, для конспирации, чтобы не употреблять раздражающее Контору выражение «делиться в конечной группе» заменили его на благородное «решать сравнение первой степени по модулю».

Группа Z/2 была совсем неинтересной и состояла из одного Царя-Батюшки – числа 1.

Группа Z/3 состояла из Царя и партийного Вождя – числа 2. Забавные превращения там получались. Партийный вождь, перемножившись сам с собой, превращался в Царя. Ну это еще можно понять, такие превращения бывали не только у натуральных чисел. А вот Царь-то, Царь – хорош гусь! Поделившись на партийного Вождя, сам становился партийным Вождем! Такие чудеса происходили только в этой VIP-группе, в других группах и народу было поболее, и умножение-деление повеселее.

Вскоре из конечных групп стали создавать нечто вроде ночных клубов для отдыха трудящихся чисел: «Семеро козлят», «Футбольная команда», «Чертова дюжина», «17 мгновений весны» и прочая, прочая, прочая.

Натуральные числа были рады их появлению. Особенно рад был Царь-Батюшка. Сидит, бывало, в своем дворце целыми днями один-одинешенек, и поделиться-то не с кем, ни на кого он не делился. А тут, в конечной группе – делись с кем хочешь, хоть до утра. И число 2 меньше стало внимания уделять своей партии – надоели, зануды. Пойдут, бывало, Царь вместе с партийным Вождем в weekend в какие-нибудь «Мгновения» душу отвести, наделиться всласть на всю трудовую неделю вперед, а там уже и число 3 (меньше пить стало!) и 5 (без медалек!) и 12, подружившееся с 13, все веселые, друг с другом делятся. Да и вообще, все сразу же перевернулось с ног на голову, какие тут партии и партбилеты! Без особых проблем число 2 согласилось на переименование своей партии в множество, а тут еще запятая из Администрации Царя, перепечатывая Указ о деполитизации в МНЧ и думая о чем-то своем, девичьем, пропустила одну букву, и вместо Ума, Чести и Совести нашей эпохи – Партии Честных Чисел – получилось самое обыкновенное множество четных чисел.

Но все это было несерьезно, развлекалочки какие-то. Серьезные дела начались в МНЧ с появлением там персональных компьютеров. Первым по достоинству оценило их появление число 2. Оно ведь было не только хитрым, но и умным числом. Вместо прикрытой за ненадобностью Партии Честных Чисел число 2 создало очень нужную для компьютеров двоичную систему счисления и теперь каждое число из МНЧ имело свое двоичное представление на компьютере. В МНЧ появились и такие немыслимые раньше слова, как информационные технологии, информационная безопасность, электронно-цифровая подпись, RSA. А вот RSA как раз и стал таким алгоритмом, в котором без простых чисел обойтись никак невозможно. Только простые числа p и q для RSA нужны большие – ведь они же секретный ключ! Думало – думало об этом число 2 и решило, что длина простого числа в RSA, как правило, должна быть 512 или 1024 бит. Пол-литра и литр – по-своему расшифровало эти значения число 3.

И брошен был клич: все на поиски больших простых чисел, пол-литровых и литровых, ибо без них не будет в МНЧ ни Internet Banking, ни электронной коммерции, ни современной цивилизации, а будем только вечно к бесконечности стремиться. А простые числа – скромные,

тихо сидят себе по своим конечным группам, никаких явных признаков у них нет. Как их отыскать в многотриллионном множестве натуральных чисел?

Задачу эту поручили Конторе. Ну а Контора – что с нее взять – выполнила это поручение так, как умела.

Переписали в Конторе все простые числа до 256 и поехали по отдаленным уголкам необъятного множества натуральных чисел. Случайно заезжают в какую-нибудь глухомань и хватают там первого попавшегося пол-литрового аборигена.

– Говори, падла, с кем делишься?

– Что Вы, что Вы, гражданин начальник, ни с кем не делюсь.

– Врешь, гад!

– Клянусь: век бесконечности не видать!

И начинают его делить на все припасенные простые числа, да еще при каждом делении запятую к заду норовят присоединить. Отвалилась запятая – врет, делится. Но даже если выдержал мужичок все эти пытки, то Контора на этом не успокаивается.

– Говори, паскуда, сколько у тебя свидетелей простоты?

И вот только после того, как найдет такое число m достаточное ($\log_2(m)$) число свидетелей своей простоты, сажают его в машину и везут в столицу: RSA-ключом будет. Всю эту садистскую процедуру прозвали в МНЧ тестом Миллера-Рабина.

Вылавливают таким образом пару пол-литровых мужичков – числа p и q, и готов секретный ключ. Перемножают их, получают литровый открытый ключ – n, который затем одевают в нарядный сертификат.

И, надо признаться, даже несмотря на эту садистскую процедуру, чисел, желающих вырваться из деревенской глуши в столицу в качестве RSA-ключей было предостаточно. А о том, чтобы всех их просто пересчитать, не говоря уже об опробовании, не могло быть и речи. Слишком много. Поэтому алгоритм RSA для пол-литровых и литровых простых чисел был признан стойким.

# 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.