Роман Душкин

МАТЕМАТИКА И КРИПТОГРАФИЯ:
тайны шифров и логическое мышление

Издательство АСТ
Москва

УДК 82-93
ББК 84-44(2Рос=Рус)
Д86

Душкин, Роман.

Д86 Математика и криптография : тайны шифров и логическое мышление / Роман Душкин. – Москва : Издательство «АСТ», 2017. – 288 с.

ISBN 978-5-17-096808-4.

Хочешь научиться хранить свои тайны, создавать зашифрованные послания и удивлять одноклассников познаниями в криптографии – науке о создании, использовании и взломе шифров? В этой книге тебя ждёт знакомство с тайными знаниями и умениями, которые доступны только избранным – шпионам, секретным агентам, учёным. Вместе мы научимся кодировать сообщения, используя разные методы шифровки, разгадывать уже существующие тайные послания, делать шифровальные машины и даже создавать свои оригинальные шифры и загадки!

У тебя есть уникальная возможность познакомиться с реальным миром тайных агентов и спецслужб, ведь все методы шифрования, описанные в книге, используются до сих пор! А вдруг ты сможешь создать свой уникальный метод шифровки?

УДК 82-93
ББК 84-44(2Рос=Рус)

Для среднего школьного возраста

12+

Научно-популярное издание

Душкин Роман
МАТЕМАТИКА И КРИПТОГРАФИЯ
тайны шифров и логическое мышление

Ответственный редактор *А. Амелькина*
Корректор *Е. Сербина*
Технический редактор *Т. Тимошина*
Компьютерная верстка *Л. Быковой*

Подписано в печать 16.02.2017. Формат 84×108/32. Усл. печ. л. 15,12.
Тираж экз. Заказ №

ООО «Издательство АСТ»
129085 г. Москва, Звездный бульвар, д. 21, строение 3, комната 5
Наш электронный адрес: www.ast.ru
E-mail: astpub@aha.ru

ISBN 978-5-17-096808-4.

Введение

Приветствую тебя, уважаемый читатель!

В этой книге я хотел бы посвятить тебя в некоторые тайные знания и умения, обычно доступные только избранным — шпионам и тайным агентам, пиратам и первооткрывателям дальних стран и, конечно же, учёным. Мы научимся писать зашифрованные послания и расшифровывать тайные записи (то есть разгадывать чужие секреты). Мы узнаем немало нового о том, как секретные умения развивались со временем и к какому состоянию криптография пришла сейчас. Ведь криптография — наука о создании, использовании и взломе шифров — одна из интереснейших и самых таинственных наук.

Мы пройдём с тобой по страницам книги, и ты узнаешь, как можно закодировать сообщение так, чтобы его практически никто не смог прочесть (а если кто и захотел бы, то на расшифровку ему бы потребовалось столько времени, сколько лет всей Вселенной). Также ты узнаешь, как разгадывать чужие сообщения и узнавать содержание тайных посланий. Конечно, расшифровать можно не любой код, но уверяю, что большинство шифров, которыми пользуются простые люди, например твои одноклассники, расшифровываются практически сразу же (если одноклассники ещё не прочитали эту книгу).

Чтобы с пониманием читать эту книгу и успешно применять методы, которые в ней

описаны, желательно, что называется, дружить с математикой — иначе тебе будет непросто понимать описание некоторых способов шифрования и их расшифровки. Ещё лучше, если у тебя есть навыки программирования: тогда многие методы шифрования и расшифровки можно сразу же запрограммировать на компьютере, а не делать всё это вручную. Впрочем, книга написана так, чтобы можно было обойтись и без использования компьютера и языков программирования.

Если на летних каникулах ты прочтёшь эту книгу и выполнишь задания из неё, у тебя, мой уважаемый читатель, останутся не только знания и умения, но и множество интересных и полезных вещиц, вроде таблиц частотности символов и специальных матриц для кодирования перемешиванием. Всё это станет твоим криптографическим багажом, который ты должен беречь как зеницу ока и даже держать его существование в тайне. Ведь один из методов **криптоанализа** (так по-научному называется расшифровка — в противоположность криптографии) — немудрёный шпионаж и кража инструментов для шифрования, паролей и кодов. Целые государства рушились из-за этого, многие войны были проиграны из-за незадачливых шифровальщиков, которые не уделяли должного внимания тайне своей переписки.

Если у тебя есть брат или сестра примерно одного с тобой возраста, то вы можете читать эту книгу вместе и сообща решать загадки, которые вы найдёте на её страницах. Вряд ли вам стоит соревноваться друг с другом. К то-

му же вы сразу же сможете использовать описанные методы для передачи тайных посланий. Но не забудьте, что в этом деле очень важна секретность. Можно привлекать к этой игре и друзей. Единственное, от чего я хочу предостеречь, так это от попыток заниматься криптографией с теми, кому еще не исполнилось десять лет. Они просто могут не понять игры, и она будет им неинтересна.

В Интернете есть различные дополнительные материалы к этой книге, так что ты сможешь найти описания новых методов шифрования, программы для создания паролей и ключей и другие полезные штуки для занятия криптографией. Впрочем, прочитав эту книгу, ты поймёшь, что пользоваться чужими наработками можно только с очень большой осторожностью. В закрытых программах или методах могут оказаться так называемые «прослушки» (или «ловушки», или, как говорят программисты, «закладки»), включённые туда разработчиком. Другими словами, разработчик оставляет для себя возможность разгадать твои секреты, а у тебя при этом нет возможности понять, как работает закрытая программа. Ну а если ты пользуешься чужими ключами для шифровки своих тайн, то не удивляйся, если они в конце концов перестанут быть тайнами.

Давай же сделаем первый шаг в мир загадок и шифров.

Неделя 1

ПРОСТОЙ ШИФР ПОДСТАНОВКИ

Ну что ж, начать, пожалуй, нужно с самого простого. Давай разберёмся, что такое шифр.

Шифрование — это метод сокрытия и раскрытия смысла посланий. Сейчас ты читаешь этот текст и понимаешь его смысл. А если бы я не хотел, чтобы любой человек мог понять то, что здесь написано, я бы использовал шифр — например, так: «14 16 13 16 05 06 24 25 20 16 17 16 17 18 16 02 16 03 01 13». Никто кроме меня и тех, кого я посвящу в метод шифровки этого сообщения, не сможет его расшифровать. Другими словами, шифр (или шифровка, или зашифрованное сообщение) — это открытый текст, смысл которого скрыт.

Что значит «*открытый текст*»? Это такой текст, про который понятно, что он есть. Он доступен не только отправителю (автору) и получателю, но

и любому другому человеку. Обычно сообщения — как шифрованные, так и нет, — являются открытыми. К примеру, текст этой книги — открытый. Но есть и закрытые тексты, то есть такие, о существовании которых доподлинно знают только отправитель и получатель. Остальные люди могут разве что догадываться о его существовании. О закрытых сообщениях мы поговорим чуть позже.

А что же значит «*скрытый смысл*»? Это значит, что даже если сам текст открыт, понять его могут только отправитель и получатель. Остальные могут попытаться его понять, а при должной сноровке и знаниях раскрыть скрытый смысл, расшифровав послание. А вот обычный, нешифрованный текст имеет открытый смысл — он понятен всем, кто владеет языком, на котором текст написан, и обладает достаточным уровнем знаний для понимания.

Итак, представь себе способ шифрования, когда каждая буква текста заменяется каким-либо символом или числом. Самый простой способ заключается в использовании вместо букв

их порядковых номеров. В русском алфавите 33 буквы, так что будут понадобятся числа от 1 до 33. Например, вот так можно зашифровать слово «ШИФР»: 26 10 22 18.

Само собой, это совсем негодный способ шифрования. Боюсь, такой шифр взломает даже тот, кто не читал эту книгу. По крайней мере, большинству людей первым делом придёт в голову попробовать этот способ расшифровки.

Буквы можно заменять и другими буквами. Например, можно воспользоваться правилом «+3»: чтобы зашифровать букву, необходимо взять её номер в алфавите, прибавить к нему «3», а затем использовать букву с по-

Гай Юлий Цезарь

Древнеримский государственный и политический деятель, полководец, писатель. Для передачи секретных сообщений из штаба в войска впервые использовал простой шифр подстановки, сегодня известный как «шифр Цезаря».

лученным порядковым номером. Чтобы зашифровать буквы из конца алфавита, нужно вернуться в начало алфавита, как бы замкнув круг. Это правило позволит зашифровать слово «ШИФР» так: ЫЛЧУ.

Это так называемый «*шифр Цезаря*». Именно в таком виде Юлий Цезарь использовал его для секретной переписки со своими командирами легионов. Да, в те далёкие времена этот шифр обеспечивал секретность. Но теперь и он не очень хорошо сохраняет тайну, поскольку те, кто хоть немного знает о криптоанализе, мгновенно взламывают его (скоро и ты будешь таким человеком).

Наконец, буквы можно заменять на какие-нибудь экзотические значки; их даже можно выдумать самостоятельно. Здесь открывается широкий простор для фантазии. Например, то же слово «ШИФР» в этом случае можно написать бесконечным количеством способов: **ΨΥΞΘ**, **β£↓Ↄ** и т. д. Придумать можно всё что угодно. Однако и в этом случае ни вид символов, ни их сложность не являются защитой — такой шифр можно взломать

так же легко, как и в предыдущем варианте.

Честно говоря, я бы вообще не называл *это* шифрованием. С точки зрения математика и программиста это просто смена кодировки. Мы просто используем другие обозначения для тех же самых букв. Это ни на что не влияет с точки зрения защиты сообщения. Подумай хорошенько: если букву «А» всегда заменять одним и тем же другим символом, букву «Б» — каким-то другим символом и так далее, то это отпугнёт только совсем неподготовленных людей, да и то — после первого испуга каждый сможет разобраться, в чём тут дело.

Другими словами, можно вывести такое правило:

Если заменить буквы на какие-либо иные символы, то секретность сообщения не изменится.

Давай посмотрим, как можно взломать такой шифр. Для этого есть несколько методов:

1. *Частотный анализ* символов. Что обозначает этот термин? Одни и те же буквы, какими бы значками они ни обозначались, всегда используют-

ся в одном и том же языке с одинаковой частотой. Сейчас ты читаешь этот текст (на русском языке); можно подсчитать количество разных букв, использованных в нем, а потом поделить эти количества на общее число букв. Получатся так называемые *частоты* букв. Так вот эти частоты практически всегда одинаковы для любых текстов, особенно больших.

2. *Подбор и проверка сочетаний*. Иногда можно успешно подобрать слова, если они заведомо используются в зашифрованном тексте. Например, если ты знаешь, что шпион передаёт в свой штаб информацию о новом виде вооружения, то наверняка в тексте найдётся название этого вооружения. «Внимание, штаб! Атакующая сторона намерена использовать рогатки». Если вы с друзьями и впрямь намерены использовать рогатки, то резонно предположить, что где-то в тексте есть это слово.

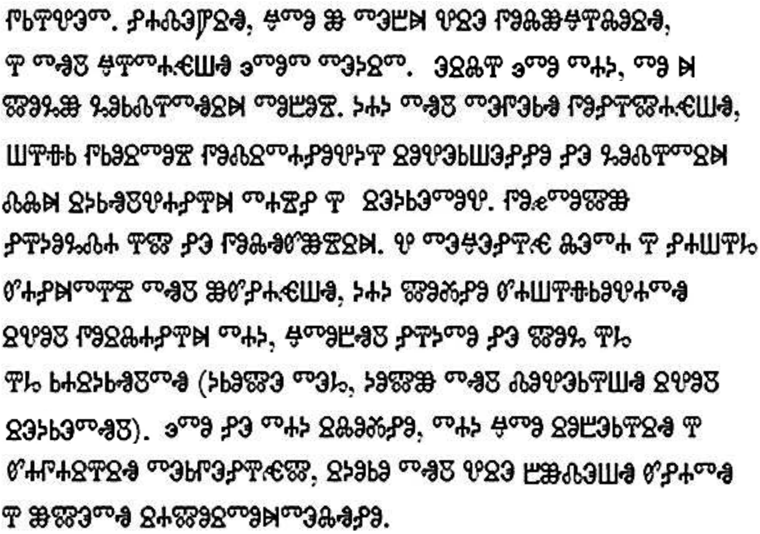
3. *Наращивание объёма сообщений*. Если шпион передаёт небольшие сообщения, то к ним сложно применить методы частотного анализа, а подбор

сочетаний становится иногда делом бессмысленным. В этом случае надо набраться терпения и подождать новых сообщений, которые увеличат объём шифрованного текста. Тогда и можно будет применить оба предыдущих метода.

Эти три метода, используемые вместе или по отдельности, позволяют взломать практически любое сообщение, скрытое *шифром простой подстановки* (именно так называется этот способ шифрования). Но теперь ты можешь понять, как избежать быстрого взлома шифровки. Нужно сделать использование этих трёх методов невозможным. Во-первых, применять такие методы шифрования, которые изменяют частоту символов. Во-вторых, использовать так называемые коды — когда уязвимые для взлома понятия обозначаются специальными словами, кодами. В-третьих, настоящий шпион никогда не использует один и тот же шифр два раза. Никогда!

Об этих методах шифрования мы поговорим позднее. А теперь предлагаю заняться взломом.

Вот, например, тебе пришло письмо, в котором есть такой текст:



Первый взгляд на этот текст заставляет отбросить «это» и заявить, что разгадать его смысл невозможно. Но так ли это? Давай попробуем разобраться.

Выше я уже говорил, что замена символов, которыми обозначаются буквы, не влияет на частоты букв. Именно этим мы сейчас и воспользуемся. Для начала я приведу таблицу, про которую в первую очередь вспоминает всякий уважающий себя криптоаналитик. Вот она:

Буква	Частота %	Буква	Частота %
О	11,08	**Ы**	1,96
Е, Ё	8,41	**Ь**	1,92
А	7,92	**З**	1,75
И	6,83	**Г**	1,74
Н	6,72	**Б**	1,71
Т	6,18	**Ч**	1,47
С	5,33	**Й**	1,12
Л	5,00	**Ж**	1,05
Р	4,45	**Х**	0,89
В	4,33	**Ш**	0,81
К	3,36	**Ю**	0,61
М	3,26	**Э**	0,38
Д	3,05	**Щ**	0,37
П	2,81	**Ц**	0,36
У	2,80	**Ф**	0,19
Я	2,13	**Ъ**	0,02

О чём эта таблица? В ней указаны частоты встречаемости букв в русском языке в обычных текстах. Как видишь, буква «О» встречается чаще всего. Можно сказать, что каждая десятая буква в тексте на русском языке, — это буква «О». Второе место занимает буква «Е» (вместе с «Ё»). Далее, соответственно, идут буквы «А», «И» и т. д. Самая редкая буква в русском языке — «Ъ».

Теперь я приведу примерный *алгоритм*, то есть последовательность шагов для расшифровки сообщения. Вот он:

1. Сначала надо точно подсчитать количество букв в сообщении. Для этого можно взять чистый лист бумаги в клетку и для каждого символа шифрограммы откладывать одну незаполненную клеточку. Клеточки, соответствующие пробелам, надо подчёркивать. После того как всё сообщение будет переведено в клеточки, надо просто посчитать пустые клетки без подчёркиваний.

2. Дальше следует построить таблицу. В ней должно быть два столбца и столько строк, сколько разных символов используется в шифрограмме. В первый столбец надо вписать все использованные символы.

3. Затем необходимо подсчитать количество каждого из отдельных символов и записать результаты во второй столбец. Это самая занудная часть алгоритма, но сделать это необходимо. Может быть, это займёт у тебя очень много времени, поэтому приступай к подсчетам, только когда у тебя есть