Библиотека вундеркинда — научные сказки

Роман Душкин

Математика и криптография

Тайны шифров и логическое мышление

+ книга-подсказка для родителей

Библиотека вундеркинда. Научные сказки

Роман Душкин

Математика и криптография. Тайны шифров и логическое мышление

«Издательство АСТ»
2017

УДК 82-93
ББК 84-44(2Рос=Рус)

Душкин Р. В.

Математика и криптография. Тайны шифров и логическое мышление / Р. В. Душкин — «Издательство АСТ», 2017 — (Библиотека вундеркинда. Научные сказки)

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)

ISBN 978-5-17-096808-4

Содержание

Роман Душкин
Математика и криптография: тайны шифров и логическое мышление

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 тому 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 поль-

зуешься 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 полученным 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.

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».

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 взломают 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, βε↓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 используются 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.

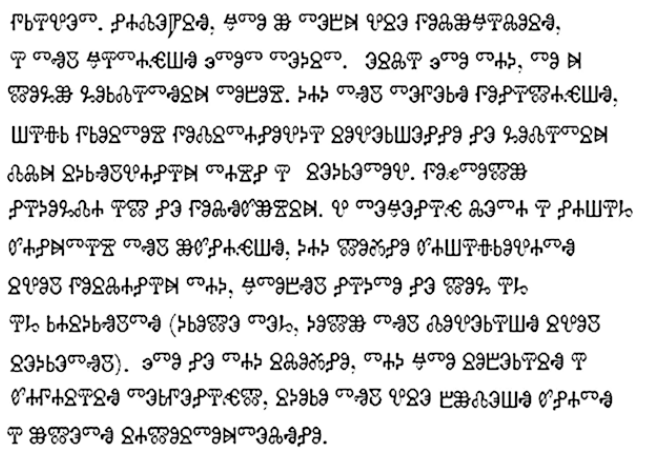
2. *Подбор и проверка сочетаний*. Иногда можно успешно подобрать слова, если они заведомо используются в зашифрованном тексте. Например, если ты знаешь, что шпион передаёт в свой штаб информацию о новом виде вооружения, то наверняка в тексте найдётся название этого вооружения. «Внимание, штаб! Атакующая 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 возможность и желание заниматься. Как только ты устанешь, надо отложить это занятие и заняться чем-нибудь другим. Так за несколько подходов ты сможешь довести дело до конца.

4. После того как частоты всех символов посчитаны, надо нарисовать ещё одну такую же таблицу. Однако теперь записывай в нее символы по убыванию частоты. В первой строке

должен находиться самый часто встречаемый символ и его количество в тексте. Во второй строке – следующий по частоте и т. д. Ты уже понимаешь, к чему мы ведём?

5. Теперь организуй рабочий цикл. В шифрограмме ты видишь символ, который встречается чаще всего. А в русском языке чаще всего встречается буква «О». Можно выдвинуть *гипотезу*, то есть сделать предположение, что этот символ и есть буква «О». После этого впиши букву «О» в тот самый размеченный лист, с помощью которого мы считали буквы в сообщении – в те клетки, которые соответствуют самому часто встречающемуся символу.

6. Теперь посмотри на частично разгаданный текст. В нём могут встретиться слова, о значении которых можно догадаться. Например, если есть слово из двух букв, стоящее после запятой, и вторая буква в этом слове – «О», то наверняка это слово «НО». А уж если оно встречается несколько раз, и всегда после запятой, то это точно слово «НО». Значит, теперь у нас есть вторая буква – «Н». Но если таких предположений сделать нельзя, то надо вернуться к шагу 5 и предположить значение следующего неразгаданного и наиболее часто встречающегося символа.

7. К таблице, которую мы заполняли на шаге 4, необходимо пририсовать ещё один столбец. В него мы будем записывать расшифровки символов.

Так, повторяя шаги 5 и 6, ты сможешь расшифровать весь текст. Однако иногда предположения относительно соответствия символов могут оказаться неверными. Это часто происходит, когда разгаданных символов ещё не так много, чтобы уже можно было видеть целые слова, а частоты разгадываемых символов примерно одинаковы. Тогда надо делать шаг назад в рассуждениях и выносить иное предположение. Также возможно, что в шифрограмме намеренно снижены или повышены частоты некоторых букв, и это может ввести в заблуждение. Но грамотный криптоаналитик в конце концов расшифрует и такой текст.

Давай попробуем разгадать по этому алгоритму ту шифрограмму, которая приведена несколькими страницами раньше. А после этого ты сможешь самостоятельно сделать то же самое с любой другой шифрограммой, текст в которой зашифрован этим способом, но, возможно, при помощи других значков.

Итак, в шифрограмме 419 букв (если твой результат отличается на пару букв, это не страшно, поскольку такая неточность не повлияет на результаты. А вот если ты ошибёшься на десяток букв, то тут уже придётся пересчитывать).

Теперь начнём считать частоты символов. В результате должна получиться примерно такая таблица:

ƒ	11
ь	17

Ф	30
ψ	12
Э	34
ѳ	44

Надеюсь, что ты заполнишь все остальные строки самостоятельно.

После того как таблица будет построена, строчки необходимо отсортировать по убыванию количества символов. Если это сделать, то в результате получится что-то вроде этого:

ϑ	45
ϭ	44
϶	34
Ψ	30
ϗ	27
ϟ	25

Как видно, здесь частота первых двух символов отличается только на единицу. Это очень неприятная ситуация, поскольку придётся делать гипотезы и проверять их. Впрочем, криптоаналитик при дешифровке всегда строит гипотезы и пытается их проверить. Так что давай сейчас построим одну гипотезу. Поскольку самой частой буквой в русском языке является «О», то предположим, что значок из первой строки отсортированной таблицы – это и есть буква «О». Что получится, если в соответствии с догадкой подставить эту букву в наш текст? Вот:

_____. _____, __O _ ____ ___ _O_____O__, _ __ _____ __O_ _____. ____ __O ___, _O _ _O_ _ _O_____ _O_O_. ___ __ _____ _O_____, ____ __O__O_ _O_____O___ _O_____O __ _O____ _ ___ _____ ____ _ _____O_. _O__O__ ___O___ __ __ _O_____. _ _____ ____ _ _____ _____ _ __ _____, ___ _O__O _____O____ __O_ _O_____ ___, __O__ ____O __ _O_ __ _____ (__O__ ___, _O__ __ _O_____ __O_ _____). __O __ ___ __O__O, ___ __O _O_____ _ _____ _____, __O_O __ ___ _____ _____ _ _____ ___O__O_____O.

Не очень-то понятно. Тем не менее это уже что-то.

Что делать дальше? Теперь попробуем подставить следующую по частоте букву. Для русского языка это буква «Е», так что подставим её вместо символа, занимающего вторую строчку в отсортированной таблице. Вот что получится после этого:

_____E. _____, _EO _ E___ ___ _O_____O__, _ E_ __E____ _EOE E___E. ____ _EO E__, EO _ _O__ _O___E___ EO_O_. ___ E_ E_____ _O_____, ____ __O_EO_ _O__E__O___ _O_____O __ _O__E__ ___ _____ E___ _ _____EO_. _O_EO__ ___O___ __ __ _O_____. _ E_____ __E_ _ ___ __ ____E__ E_ _____, ___ _O__O _____O__E_ __O_ _O_____ E__, _EO__ ___EO __ _O_ __ _____ _E_ (__O__ E__, _O__ E_ _O_____ __O_ _____E_). _EO __ E__ __O__O, E__ _EO _O_____ _ ____ ____ E_____, __O_O E_ ___ _____ ___E_ _ ___E_ ___O_EO_E____O.

Сразу видно, что тут что-то не то. Во-первых, можно обратить внимание на слово «ЕО» в первой строке (шестнадцатое слово). Такого слова нет в русском языке. Во-вторых, в тек-

сте неоднократно встречается не до конца разгаданное слово «_ЕО», причём на первом месте стоит один и тот же символ (это слово встречается четыре раза). Какие слова из трёх букв, подходящие под эту форму, есть в русском языке? Посмотрим: ГЕО (довольно редкое болгарское имя), ЛЕО (фамилия или имя из английского языка), НЕО (это из «Матрицы») и РЕО (город во Франции). Как видно, обычного русского слова нет ни одного, и можно предположить, что мы неверно расшифровали первые буквы. Впрочем, уже несуществующее слово «ЕО» позволяет отбросить гипотезу насчёт буквы «Е».

Теперь ты понимаешь, что «короткие» слова на первом этапе могут принести очень большую пользу. Именно на короткие слова надо обращать внимание, когда ты только приступаешь к расшифровке секретного сообщения. Давай пойдём дальше. Таким же образом можно отвергнуть гипотезы о том, что этот второй символ – буква «А» (третья по частоте) или буква «И» (четвёртая). Да, слова «АО» (сокращение от «автономный округ») и «ИО» (спутник Юпитера или имя нимфы из греческой мифологии) в русском языке есть, но они редкие и вряд ли окажутся в этом тексте.

Идём дальше. Следующая по частоте буква – это «Н». Тут, казалось бы, всё нормально, поскольку слово «НО» в русском языке есть, и оно как раз часто стоит после запятой. И буквосочетание «_НО» может означать часто встречающееся слово «ОНО» (но не в нашем случае, ты же понимаешь почему?). Попробуем сформулировать гипотезу и заменить символ буквой:

_____Н. _______, _НО _ Н___ ___ _О_____О__, _ Н_ __Н____ _НОН Н___Н. ____ _НО Н__, НО _ _О__ _О___Н___ НО_О_. ___ Н_ Н_____ _О_______, ____ __О_НО_ _О__Н__О___ _О_____ __О __ _О__Н__ ___ _________ Н___ _ _____НО_. _О_НО__ ___О___ __ __ _О_______. _ Н_____ _ _Н_ _ _____ ____Н__ Н_ _______, ___ _О__О ______О__Н_ __О_ _О_____ Н__, _НО__ ___НО __ _О_ __ ______Н_ (__О__ Н__, _О__ Н_ _О_____ __О_ _____Н_). _НО __ Н__ __О__О, Н__ _НО _О_____ _ ________ Н________, __О_О Н_ ___ ______ ___Н_ _ ___Н_ ___О_НО_Н____О.

Час от часу не легче. Но тут легко можно заметить одиннадцатое слово «_НОН», причём первой буквой у него стоит та же, что и в слове «_НО». В русском языке есть слово «ОНОН» (река в Сибири), но оно не подходит, поскольку букву «О» мы уже отгадали. То есть гипотеза о букве «Н» – некорректная. Попробуем следующую букву, и если она не подойдёт, то придется поставить под сомнение самую первую гипотезу о букве «О». Следующая по частоте буква – это буква «Т». Подставим:

_____Т. _______, _ТО _ Т___ ___ _О_____О__, _ Т_ __Т____ _ТОТ Т___Т. ____ _ТО Т__, ТО _ _О__ _О___Т___ ТО_О_. ___ Т_ Т_____ _О_______, ____ __О_ТО_ _О__Т__О___ _О_______О __ _О__Т__ ___ _________ Т___ _ _____ТО_. _О_ТО__ ___О___ __ __ _О_______. _ Т______ __Т_ _ ___ __ ____Т__ Т_ _______, ___ _О__О ______О__Т_ __О_ _О_____ Т__, _ТО__ ___ТО __ _О_ __ _____ _Т_ (__О__ Т__, _О__ Т_ _О_____ __О_ _____Т_). _ТО __ Т__ __О__О, Т__ _ТО _О_____ _ ____ ____ Т________, __О_О Т_ ___ ______ ___Т_ _ ___Т_ ___О_ТО_Т____О.

Вновь обратим внимание на слова «_ТО» и «_ТОТ», у которых первая буква одинаковая. Тут вариант один: первая буква – это «Э». Попробуем подставить:

_____Т. _______, _ТО _ Т___ ___ _О_____О__, _ Т_ __Т____ ЭТОТ Т___Т. ____ ЭТО Т__, ТО _ _О__ _О___Т___ ТО_О_. ___ Т_ Т_____ _О_______, ____ __О_ТО_ _О__Т__О___ _О_______О __ _О__Т__ ___ _________ Т___ _ _____ТО_. _ОЭТО__ ___О___ __ __ _О_______. _ Т______ __Т_ _ ___ __ ____Т__ Т_ _______, ___ _О__О ______О__Т_ __О_ _О_____ Т__, _ТО__ ___ТО __ _О_ __ _____

_Т_ (__О__ Т__, _О__ Т_ _О_____ __О_ _____Т_). ЭТО __ Т__ __О__О, Т__ _ТО _О_____ _ ____ ____ Т_____, __О_О Т_ ___ _____ ___Т_ _ ___Т_ ___О_ТО_Т____О.

Пока всё нормально. Никаких противоречий на первый взгляд нет. Более того: в тексте встречается последовательность «_ОЭТО__». В этом слове из семи букв открыты четыре, так что можно попробовать догадаться, какое это слово. Поиск по словарю даёт только одно слово: «ПОЭТОМУ». Более того, перед «ПОЭТОМУ» часто пишется запятая, как и в этом случае. Получается, что мы сейчас смогли выдвинуть вполне правдоподобную гипотезу относительно ещё трёх скрытых символов. Пора составить новую таблицу и заполнить её:

ə	45	О
ơ	44	Т
	. . .	
ꝏ	11	М
ꝑ	11	П
	. . .	
ꝸ	9	У
	. . .	
ɜ	4	Э

Подставим-ка все известные на текущий момент символы в шифрограмму. Вот что получится:

П____Т. _____, _ТО У Т___ ___ ПО_У___О__, _ Т_ __Т____ ЭТОТ Т___Т. ____ ЭТО Т__, ТО _ МО_У _О___Т___ ТО_О_. ___ Т_ Т_П___ ПО__М____, ____ П_О_ТО_ ПО__Т__О___ _О___ ____О __ _О__Т__ ___ _____ Т___ _ _____ТО_. ПОЭТОМУ ___О___ _М __ ПО___У___. _ Т___ ___ __Т_ _ _____ ____Т__ Т_ У_____, ___ МО__О _____О__Т_ __О_ ПО_____ Т__, _ТО__ ___ТО __ МО_ __ _____Т_ (__ОМ_ Т__, _ОМУ Т_ _О_____ __О_ _____Т_). ЭТО __ Т__ __О__О, Т__ _ТО _О_____ _ __П_____ Т__П____М, __О_О Т_ ___ _У____ ___Т_ _ УМ_Т_ __МО_ТО_Т____О.

Сразу бросается в глаза первое слово. Ты ещё не догадываешься, что это за слово такое? Тогда подумай, какое слово из шести букв обычно ставят в начале письма, причём начинается оно на «П», а заканчивается на «Т»: «П____Т». Ну, конечно же, это слово «ПРИВЕТ». Ура, у нас есть ещё четыре буквы. Давай внесём их в таблицу расшифровок:

Конец ознакомительного фрагмента.