

ИВАН ЕФИШОВ

# ТАИНСТВЕННЫЕ СТРАНИЦЫ



ЗАНИМАТЕЛЬНАЯ КРИПТОГРАФИЯ



Иван Ефишов

# Таинственные страницы

Занимательная криптография

Москва

Издательство «Манн, Иванов и Фербер»

2016

УДК 003.26  
ББК 32.973-18.2  
Е91

*В издании использованы иллюстрации с нортала Shutterstock*

**Ефишов, Иван Иванович**

**Е91** Таинственные страницы. Занимательная криптография / Иван Ефишов. — М. : Манн, Иванов и Фербер, 2016. — 240 с.

ISBN 978-5-00100-130-0

В истории любой науки (и не только науки) есть загадки, закодированные послания, скрытая от посторонних информация. В этой книге собрано множество захватывающих историй дешифровки, причем читатель с небольшой помощью автора, специалиста в области компьютерной безопасности, разгадает секретные сообщения сам, и для этого ему не потребуются знания сложных разделов математических наук.

УДК 003.26  
ББК 32.973-18.2

*Все права защищены.  
Никакая часть данной книги не может быть  
воспроизведена в какой бы то ни было форме  
без письменного разрешения владельцев авторских прав.  
Правовую поддержку издательства обеспечивает  
юридическая фирма «Вегас-Лекс»*

**VEGAS LEX**

ISBN 978-5-00100-130-0

© Ефишов И. И., 2016  
© Оформление. ООО «Манн, Иванов и Фербер»,  
2016

# Содержание

<i>Предисловие</i> .....	9
Этюд I. O tempora! O mores! .....	13
Этюд II. Большой труд Аристотеля .....	16
Этюд III. Индийская словесная система нумерации .....	19
Этюд IV. Числа Фибоначчи .....	22
Этюд V. Суеверный писец .....	30
Этюд VI. Шифр Бэкона .....	32
Этюд VII. Нет повести печальнее на свете .....	43
Этюд VIII. Невезенье шевалье Луи де Рогана .....	51
Этюд IX. Любовный шпион .....	55
Этюд X. Гарна мама .....	58
Этюд XI. 510 .....	63
Этюд XII. Логогриф Эйлера .....	73
Этюд XIII. Музыкальная подпись .....	98
Этюд XIV. Трацом .....	101
Этюд XV. Дневник юного принца .....	109

Этюд XVI. Египетские иероглифы .....	114
Этюд XVII. Горе уму .....	127
Этюд XVIII. И дум высокое стремление .....	138
Этюд XIX. Князь-анархист .....	147
Этюд XX. Соня и Лев .....	155
Этюд XXI. Слепопись .....	159
Этюд XXII. Шерлок Холмс .....	167
Этюд XXIII. Английский детектив .....	183
Этюд XXIV. Christie for Christmas .....	190
Этюд XXV. Игры Клода Шеннона .....	195
Этюд XXVI. Дешифровка линейного письма Б .....	200
Этюд XXVII. О пользе знания языков .....	207
Этюд XXVIII. Аэропорт .....	214
Этюд XXIX. Лепет .....	217
Этюд XXX. Криптографическая смесь .....	221
<i>Послесловие</i> .....	228
<i>Благодарности</i> .....	230
<i>Литература</i> .....	231

*Посвящается  
веселой девчушке-кудряшке Соне*





Делу время и потехе час.  
Царь Алексей Михайлович

# Предисловие

Эта книга составлена из криптографических этюдов, основой для которых послужили игры, проводимые автором в студенческой аудитории. Главная цель этих игр — в занимательной форме как на историческом, так и на литературном материале, сначала на перемене, а потом и в ходе занятия познакомить студентов с простыми шифрами.

Студенты-криптографы обычно изучают сложные разделы высшей алгебры и других математических наук, содержание которых не предполагает развлечения: сплошные формулы и абстракции; никакой романтики и тайных шифров. Здесь же подобраны такие загадки из истории шифрования, решение которых студенты осиливают в игровой форме за пять-десять минут. Игры всегда динамичны; студенты, разгадывая очередной ребус или криптограмму, кооперируются друг с другом, обсуждают задачу с преподавателем. Решение данных этюдов не требует большого багажа знаний ни по математике, ни по криптографии (в книге

приведена всего одна математическая формула). Материал доступен каждому, кто захочет немного больше узнать о шифрах и криптограммах.

Криптография косвенно присутствует уже в детских играх. Вспомните себя: у вас, наверное, тоже был свой, тайный от взрослых язык, который вы использовали в играх.

Вот, к примеру, стихотворение, написанное на одном из многочисленных тайных детских языков, так называемой поросячьей латыни:

Триси мусудресеца в осодносом тасазусу  
Пусустисилисись посо мосорюсю в grosозусу,  
Бусудь посопросочнесеесе  
Стасарысый тасаз,  
Длисиннесеесе бысыл бысы  
Мосой расасскасаз.

При быстром разговоре на такой ученой «латыни» окружающие часто не различают слов и не понимают, о чем идет речь. Таким образом, шифр сделал свое дело: содержание разговора скрыто от посторонних. Но сколько удовольствия игра доставляет юным собеседникам!

Принцип сокрытия тайны в этом языке безыскусен: после каждого гласного звука добавляется еще один слог: с первым звуком «с» и вторым — тем же гласным, какой был в предыдущем слог. Теперь осталось только дешифровать приведенное выше детское стихотворение из сборника «Сказки матушки Гусыни»:

Три мудреца в одном тазу  
Пустились по морю в грозу,  
Будь попрочнее  
Старый таз,  
Длиннее был бы  
Мой рассказ\*.

Героиня одного из этюдов Агата Кристи вспоминала в автобиографии, что именно через игру отец привил ей любовь к «числовым головоломкам и вообще всему, что связано с числами». Папа будущей писательницы несколько лет был судьей на играх в крикет в ее родном городке. Агата с шестилетнего возраста помогала ему в подсчетах: сколько было пропущено калиток, сколько пробежек сделала каждая команда... Для нее это было лучшей тренировкой в счете. Впоследствии она напишет: «Я продолжала заниматься арифметикой с папой. <...> Я находила все это совершенно захватывающим. Я бы стала <...> математиком и спокойно и счастливо дожила бы до самой смерти» [28].

Герою другого этюда, Вольфгангу Амадею Моцарту, было и того меньше — четыре года, «когда отец, как бы затевая веселую игру, начал разучивать с ним на клавире некоторые менуэты и другие пьесы. За короткий срок он смог играть их с совершеннейшей чистотой и в строжайшем ритме. Вскоре в нем пробудилось стремление к самостоятельному творчеству. Пяти лет Вольфганг сочинял маленькие

---

\* Пер. С. Я. Маршака. Здесь и далее прим. авт.

пьесы, которые проигрывал своему отцу с просьбой записать их на бумаге» [1]. Друг семьи Моцартов Иоганн Андреас Шахтнер вспоминал о маленьком гении: «Он всегда настолько целиком отдавался тому, чему его заставляли учиться, что забывал обо всем остальном, даже о музыке; например, когда он учился считать, то стол, стулья, стены, даже пол были покрыты цифрами, написанными мелом» [1]. Как видим, и изучение цифр для юного Моцарта стало захватывающей игрой. Мало похоже на строгий урок все это «пачканье» стен и пола мелом!

Уделите и вы этой книге час-другой, поиграйте в криптографию.

Когда я был ребенком, мой отец тоже играл со мной «в арифметику» по дороге в детский сад и обратно, за что папе большое спасибо. Он в быстром темпе называл одно и то же небольшое число много раз подряд, указывая, вычесть его или прибавить к сумме, а потом спрашивал, каков результат. Позже отец мне признался, что незаметно для меня загибал пальцы при сложении и разгибал их при вычитании, чтобы самому не ошибиться при конечном подсчете. Я проделывал то же самое, но в уме. Зная, сколько осталось «пальцев» в итоге, мне удавалось быстро складывать заданное число нужное количество раз. Это было подчас нелегко, но надо же обыграть папу! Отец всегда удивлялся, как мне удавалось не сбиться со счета и почти мгновенно назвать правильный ответ. Свою «тайну» я не выдавал: так было гораздо интереснее играть.

# O tempora! O mores!

Древнейшим зашифрованным сообщением, дошедшим до нас, признана надпись, вырезанная на гробнице знатного человека по имени Хнумхотеп, князя Хебену, носившего также титул «начальник Востока», примерно в 1900 году до н. э. в древнеегипетском городе Менат-Хуфу на берегу Нила [25]. Примененная писцом система «тайнописи» основывалась на изменении начертания отдельных (не всех) иероглифов. Поэтому вырезанная в камне надпись не была тайнописью в полном понимании этого слова и не является полноценным шифром. Писец всего лишь попытался придать ей больше важности. По египетским верованиям, тот, кто читал надписи на гробнице, способствовал вечной загробной жизни усопшего. Фактически это была головоломка, требующая большего времени, нежели чтение просто текста, заставляющая задуматься и вызывающая у прохожего желание разгадать скрытый смысл.

Но постепенно многие записи начинают преследовать и другую, важную для криптографии цель — секретность.

В некоторых случаях секретность была нужна для усиления колдовской силы поминальных текстов.

А в наше время люди начали, например, зашифровывать свое имя на автомобильных номерах. Особенно широкое распространение мода на «личные» номера получила в Европе и США [24]. Хоть какое-то развлечение в пробках! Стоишь и от нечего делать разгадываешь номер-ребус впереди идущей машины: как зовут владельца, кто он по профессии. Но почему же не написать свое имя просто, без всяких загадок?

Так как уникальный номер, например с именем «Игорь», может быть только один, то всем остальным Игорям приходится действовать подобно упомянутому выше древнеегипетскому писцу: изменять начертания отдельных (или всех) букв.

Попробуем разгадать некоторые такие номера. Они не выдуманы и принадлежат реальным людям.

ALE551A. Здесь все ясно: 5 очень похожа по начертанию на букву S, то есть зашифровано было имя Alessia (Алеся).

A8RAM. На какую букву похожа 8? Очевидно, что на две буквы O! Если серьезнее, то на латинскую B. Ответ — Abram (Абрам).

Внимательнее посмотрим на следующий европейский номер ART 157E. Что 5 — это S, мы уже знаем, а 1 (единица), может быть, латинское L? Получили ART LS7E. Что-то не так. Тогда I? Ответ становится очевиден: ARTIS7E — это artiste. Владелец машины решил указать, что он человек творческой профессии.

А вот еще один профессиональный номер — D34 LER. Здесь чуть сложнее: 3 — это зеркальное отражение чуть измененной графически буквы E. А на что похожа в английском языке цифра 4? Посмотрим еще раз на номер: DE4 LER — и ответ ясно виден. Дилер.

Еще один замысловатый номер — 64ME. Маленькая подсказка: зашифровано то, что мы с вами сейчас делаем! Это game (игра).

А вот любитель напитка богов, нектара — NEC74R.

И последний, самый сложный номер — P14 NER. Многие наверняка предположили, что это пионер. Но, увы, по-английски это слово пишется через O и с двумя буквами E — pioneer. А может, владелец намекает, что его автомобиль P14 NER (planer) летит как самолет или планер? Но самолет по-английски airplane, планер — glider (ох уж эти ложные друзья переводчика!). Или автомобилист подчеркивал, что он чертежник (англ. planner), решив, однако, не писать дважды букву N? В англо-русском словаре находим, что planer — строгальщик, рубанщик; уст. рубанок, фуганок. То есть владелец данного автомобиля, как и артист или дилер, указал свою рабочую профессию рубанщика.

## Этюд II

# Большой труд Аристотеля

В IV веке до н. э. древнегреческий философ и ученый Аристотель писал, что это «<...> [большой] труд, потому что неясно, к чему что относится <...>» [4].

Что же за великий труд подразумевал философ в данной сентенции?

Попробуйте найти ключ и дешифровать следующий текст [37]:

угривтиненетихвглинесмолавеливдубенет

Возможно, вам поможет следующая аналогия. Одним из самых ранних известных примеров использования греческого алфавита является дипилонская надпись, записанная на древнегреческом керамическом сосуде, датированном приблизительно 740 годом до н. э. Оригинальный ее текст:

HOΣYNYOPXEΣTONΠANTONATAΛOTATA  
ΠAIZEITOTODEKAMIN



Буквальный перевод: «Кто ныне из всех танцоров наиболее изящно (резво) танцует, тому это...» Предполагается, что эта ваза служила призом в некоем танцевальном конкурсе.

Облегчим вышеприведенную задачу:

угривтине нетихвглине смолавели вдубенет.

Мы, подобно дешифровщикам дипилонской надписи, всего лишь «разорвали» исходный текст и, таким образом, частично дискретно декодировали исходную фразу.

Теперь дешифруем текст окончательно. Внеся в него все знаки препинания и пробелы (это и есть ключ к решению данной задачи), получим:

угри в тине, нет их в глине;  
смола в ели, в дубе — нет.

В заключение осталось только привести первоначальную цитату Аристотеля в более подробном виде: «Вообще написанное должно быть удобочитаемо и удобопонимаемо, а это одно и то же. Этими свойствами не обладает речь со многими союзами, а также речь, в которой трудно расставить знаки препинания, как, например, в творениях Гераклита — [большой] труд, потому что неясно, к чему что относится, к последующему или к предыдущему, как, например, в начале своей книги он говорит: “Относительно разума требуемого всегда люди являются непонятливыми”. Здесь неясно, к чему нужно присоединить знаком [запятой] слово “всегда”».

За два столетия до Аристотеля, во времена Гераклита, греки писали без всяких знаков препинания и пробелов между словами, как в дигиплонской надписи, поэтому «дешифровка» таких текстов и была большим трудом.

На основании вышеприведенного фрагмента из «Риторики» Аристотеля традиционно определяют время появления знаков препинания. К началу I века до н. э. древние греки применяли всего лишь три знака препинания — точку, располагавшуюся внизу, в середине или вверху строки. Первая из них соответствовала нынешней точке, другая — запятой, третья — двоеточию.

### Этюд III

# Индийская словесная система нумерации

Как известно, Индия была единственной страной, где широкое распространение получила словесная система нумерации [13]. Цифры и числа в подобной системе заменяются различными словами. Чтобы хорошо разбираться в словесных числах, необходимо знать индийскую литературу, религию, музыку. Каждому числу соответствовало несколько слов со своими многочисленными синонимами. Так, например, только слово «земля», которому соответствует единица, в санскрите имело одиннадцать синонимов. Всего же для обозначения единицы использовалось тридцать девять слов.

Были и правила для облегчения запоминания. Так, единица обозначалась словами, находящимися в единственном числе; для двойки использовались парные слова, применяемые для обозначения парных предметов или понятий. Для некоторых чисел, например девяти и одиннадцати, использовались имена богов, и т. д.

Ниже приведены три хронограммы (словесные цепочки, обозначающие число), применяемые для записи

одного и того же числа в индийской словесной системе нумерации:

- 1) небо-земля-глаза-время;
- 2) пустой-брахман-близнецы-миры;
- 3) отверстие-луна-губы-Шива.

Попробуйте догадаться, что это за число.

Зачем же была необходима такая сложная система записи чисел? К сожалению, в те времена информация, записанная на высушенных пальмовых листьях, страдала от влажного индийского климата и со временем бесследно пропадала. Рукописи также часто сгорали либо при случайном пожаре, либо в огне войны. Содержащиеся в них знания по математике, астрономии исчезали навсегда.

Наряду с рукописями существовала богатая устная традиция передачи знаний. Длинный ряд чисел, различные формулы память человека удерживает плохо. Выучить множество правил с содержащимися в них числами значительно легче в стихотворном виде: здесь-то и пригодилось образное обозначение чисел. Поэтому дошедшие до нас древние индийские научные трактаты изложены в стихотворной форме, краткой до чрезвычайности: только основные правила, важнейшие факты, которые ученые запомнили наизусть.

Как было замечено выше, для единицы используется слово «земля». Слова «брахман» и «луна» также обозначают единицу: на небе мы видим только одну Луну, да и Земля

тоже только одна. Что касается слова «брахман», в индийской философии им обозначается «душа мира», первооснова всех вещей.

Единица в Древней Индии могла обозначаться также словами «начало», «тело», «предок», «Вишну», «Брахма».

«Глаза», «близнецы» и «губы» суть парные слова, и согласно правилам они используются для обозначения двойки.

Какому же числу или цифре соответствуют слова «время», «миры» и «Шива»? Те, кто знаком с индуизмом, могут вспомнить, что у Шивы на лбу имеется третий глаз. Тогда становятся понятными аналогии и со временем (у индусов, как и у нас, время делится на прошлое, настоящее, будущее) и с мирами (подземный, наш и небесный).

Таким образом, загаданное число имеет вид \*123. Что же находится в первой позиции? Небо, пустой, отверстие. «Пустой» — можно предположить, что это слово подходит, как никакое иное, для обозначения нуля; вспомним, что и латинское *nullus* означает «никакой». «Отверстие» тоже подходит для обозначения нуля. Небеса также пусты, незримы, как воздух.

Итак, возможный ответ — 0123 или 123. Но зачем записывать 123 так сложно, с нулем впереди? Тем более что нуль появился позднее других цифр; вряд ли после его появления могла сложиться традиция записывать его перед «старыми» цифрами, да и не нужен он там! Правильный ответ в данном случае — 3210: числа в хронограммах, как правило, записывали справа налево.

## Этюд IV

# Числа Фибоначчи

Американский писатель Дэн Браун (р. 1964) в своем «Коде да Винчи» использовал для декодирования информации числа Фибоначчи. Кратко напомним канву событий, связанных с этими загадочными числами.

В здании Лувра обнаружен труп куратора музея Жака Соньера. Убитый обнажен и лежит в позе, воспроизводящей знаменитый рисунок Леонардо да Винчи «Витрувианский человек». На теле — зашифрованная кровавая надпись: Соньер в последние минуты жизни «использовал собственную кровь в качестве чернил или краски, а собственный обнаженный живот — как полотно». Надпись была следующей:

13-3-2-21-1-1-8-5

На вид идола родич!

О мина зла!

Что за мина зла? Да еще родич какого-то идола... Что касается чисел — если их расположить по возрастанию (1, 1, 2, 3, 5, 8, 13, 21), то мы получим первые восемь чисел бес-

конечного ряда Фибоначчи. Впрочем, передадим теперь слово главному герою романа, профессору Гарвардского университета Роберту Лэнгдону: «Искаженный ряд Фибоначчи — это ключ. Числа являются намеком на то, как следует расшифровывать остальную часть послания. Соньер специально нарушил последовательность, намекая на то, что такой же подход можно применить и к тексту».

Таким образом, Жак Соньер оставил намек, что написанное им — криптограмма! То есть, переставив буквы в послании, мы получим другой смысл записки. Первая строка записки с искажениями (ведь ряд Фибоначчи тоже искажен) дает «Лиодардо да Винчи!», вторая декодируется как «Мона Лиза!». Смысл записки теперь более или менее ясен: она оставлена куратором Лувра, где и хранится знаменитая картина:

«Леонардо да Винчи! Мона Лиза!»

Указание на знаменитую картину позволило найти золотой ключ к сейфу швейцарского депозитарного банка. Кроме того, числа Фибоначчи оказались также и кодом доступа к этому сейфу.

Но почему Жак Соньер выбрал для кода доступа именно числа Фибоначчи? Вот как это объясняет сам Дэн Браун на страницах романа: «Если превратить последовательность Фибоначчи в простой набор из десяти цифр, она становится практически неузнаваемой. Запомнить легко, а на первый взгляд цифры кажутся выбранными наугад. Гениальный,

потрясающий цифровой код, который Соньер никогда бы не забыл».

Рассмотрим историю этого «гениального, потрясающего цифрового кода». Откуда взялись эти цифры?

Совпадение! Их открыл тоже Леонардо, и тоже итальянец, но, увы, не знаменитый да Винчи, а некий купец Леонардо Фибоначчи (1170–1250). В своем первом математическом труде «Книга Абаки» (Liber Abaci, 1202 год) он рассмотрел задачу о размножении кроликов. В результате появились замечательные числа, позже названные именем Фибоначчи:

$$f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, \dots, f_{12} = 144, \dots$$

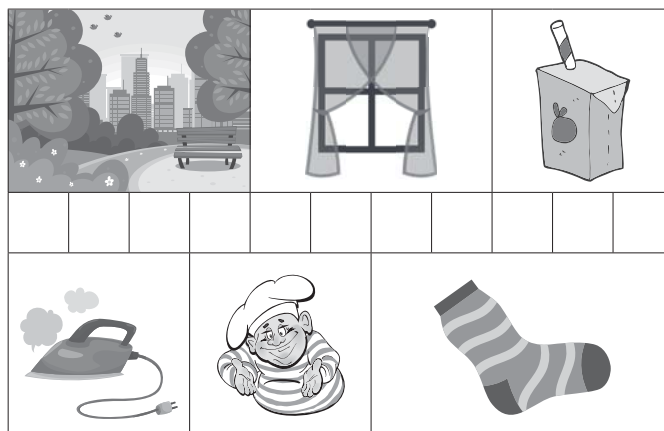
Первые два числа в этой последовательности заданы и равны единице, то есть  $f_1 = 1, f_2 = 1$ , а каждое последующее число равно сумме двух предыдущих чисел. Например,  $f_6 = f_5 + f_4$  (или  $8 = 5 + 3$ ). Счет можно продолжить. Так, например, двенадцатое число Фибоначчи равно  $f_{12} = 144$ .

Числами Фибоначчи можно описать как корзинку подсолнуха, так и расположение спиральных рукавов Галактики.

Отметим, что в своем труде Леонардо Фибоначчи, который по делам торговли не раз оказывался в арабском Алжире, рассмотрел впервые в европейской математике арабскую систему счисления. Привычная нам десятичная позиционная система, которую все мы изучаем в школе, в свое время стала крупнейшим прорывом в математике. Не будь ее, нам пришлось бы до сих пор пользоваться римской нотацией, столь неудобной при вычислениях.



Плавнo перейдем к другой задаче по кодированию и передаче информации, где также возникают вездесущие числа Фибоначчи. Но предварим ее небольшим двойным линейным кроссвордом.



По верхнему ряду рисунков кроссворд разгадывается следующим образом: «парк, окно, сок», по нижнему ряду — «пар, кок, носок».

Как видим, сообщение «паркоknосок» можно прочесть двумя способами. В данном случае информацию, состоящую из одиннадцати букв, вы легко дешифровали, используя подсказки-картинки. Но у криптоаналитика подсказок, как правило, нет.

Рассмотрим аналогичную задачу [11], связанную с передачей информации, также состоящей из одиннадцати символов, но не сопровождающейся дополнительными подсказками.

Вот ее условие. Некоторый алфавит состоит из шести букв, которые для передачи по телеграфу кодируются одним или двумя знаками следующим образом:

•, —, ••, — —, • —, — •.

При передаче некоего слова не сделали промежутков, отделяющих букву от буквы, так что получилась сплошная цепочка точек и тире, состоящая из одиннадцати знаков.

Сколькими способами можно прочесть переданное слово?

Сделаем задачу более наглядной. Предположим, что вам передали следующее слово:

•• — — • — — — • — •

Попробуйте для начала разобраться с этим частным случаем.

Задача полностью аналогична той, которую вы разгадывали в линейном кроссворде. Но там вы отделяли друг от друга слова, а здесь придется отделить закодированные буквы в слове. Известно, что при передаче телеграмм или радиogramм применяется азбука Морзе, в которой, например, буква А всегда кодируется двумя знаками • —, тогда как буква Е — это одна точка •, а буква Т — просто тире —. Таким образом, получив сообщение из двух знаков • — (в котором преднамеренно пропущен пробел), вы можете его декодировать либо как букву А, либо как две буквы ЕТ.

Теперь попробуйте применить подобный подход для слова из одиннадцати знаков. Не забудьте, что наш этюд называется «Числа Фибоначчи»!

Попробуйте сделать это самостоятельно, потратьте на задачу час, два, три... Столько, сколько вам понадобится. Но не забегайте вперед, чтобы просто прочитав ответ. Задача не так сложна: при ее решении вам не придется воспользоваться ни одной математической формулой!

Подсказка: ответ задачи — двенадцатое число Фибоначчи.

Решим эту задачу подробно — шаг за шагом. Итак, слово длиной в одиннадцать знаков уже задано. Предположим, что сначала нам дана последовательность из 1 знака, затем из 2, 3, ..., 11 знаков. Каждый знак, как вы помните, — это либо точка, либо тире.

Первый шаг. Вначале имеем слово длиной в один знак: \*, где \* обозначает либо точку, либо тире.

Очевидно, слово у нас прочитается единственным образом. Когда конкретное сообщение из одного знака у вас перед глазами, то вы увидите либо • либо —.

Второй шаг. Теперь задано слово длиной уже в два знака: \*\*.

(\*)(\*), (\*\*) — два способа декодирования. Других комбинаций попросту нет. Здесь круглыми скобками выделены отдельные буквы (однозначные либо двузначные) в полученном нами слове.

Третий шаг. Имеем слово длиной в три знака: \*\*\*.

(\*)(\*)(\*), (\*)(\*\*), (\*\*)(\*) — уже три способа декодирования (будем располагать последовательность из букв в лексико-

графическом\* порядке их длины). Как мы помним, буквы из трех знаков (\*\*\*) по условию нашей задачи не существует.

Четвертый шаг. Имеем слово длиной в четыре знака: \*\*\*\*.

(\*)(\*)(\*)(\*), (\*)(\*)(\*\*), (\*)(\*\*)(\*), (\*\*)(\*)(\*), (\*\*)(\*\*) — вот так сюрприз! У нас теперь не четыре, как можно было бы ожидать, а целых пять способов декодирования.

Пятый шаг. Имеем слово длиной в пять знаков: \*\*\*\*\*.

(\*)(\*)(\*)(\*)(\*), (\*)(\*)(\*)(\*\*), (\*)(\*)(\*\*)(\*), (\*)(\*\*)(\*)(\*), (\*\*)(\*)(\*)(\*), (\*)(\*\*)(\*\*), (\*\*)(\*)(\*\*), (\*\*)(\*\*)(\*) — восемь вариантов декодирования.

Можно продолжать в том же духе. Но попытаемся угадать закономерность, возникающую в ходе решения задачи.

Выпишем количество способов декодирования, полученных на каждом нашем шаге.

Первый шаг — 1 способ.

Второй шаг — 2 способа.

Третий шаг — 3 способа.

Четвертый шаг — 5 способов.

Пятый шаг — 8 способов.

И т. д...

---

\* То есть вначале будем стараться выписывать слова, которые начинаются с букв, имеющих наименьшую длину, то есть состоящих из одного знака (\*); а слова, содержащие буквы из двойных знаков (\*\*), будем стараться выписывать после первых. Иначе говоря, слово (\*)(\*)(\*\*) будем писать перед словом (\*)(\*\*)(\*), так как одиночных знаков слева у первого слова больше, чем у второго.

Теперь хорошо видно, что справа у нас стоят числа Фибоначчи:

$$f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, \dots$$

Так как при решении задачи на первом шаге мы получили второе число Фибоначчи  $f_2 = 1$ , на втором шаге — третье число  $f_3 = 2$ , то, следовательно, правильным ответом будет двенадцатое число Фибоначчи  $f_{12} = 144$ , так как полученное слово состоит из одиннадцати знаков.

Какая элегантная и красивая задача! И вполне по силам любому. Надеюсь, вы получили море удовольствия при ее самостоятельном решении и не подглядывали в ответ.

## Этюд V

# Суеверный писец

Широко использовалась тайнопись и на Руси. Переписчики древних текстов (как правило, монахи) обычно в конце рукописи зашифровывали свое имя. «Употребление тайнописи вызывается здесь традицией «смирения», ради которого пишущий, хотя и желает оставить по себе память, находит нескромным назвать себя открыто» [49]. Возможно, такая скрытность была вызвана боязнью дурного глаза [38].

В начале рукописи, найденной в Вологде и относящейся к 1643 году, писец сделал следующую приписку, в которой зашифровал свое имя:

ррррр ааааа аааа о іііііііііі ъ .

Этот вид тайнописи назывался «мудрая литорея» и основывался на замене буквы соответствующим ей числом в кириллической системе счисления.

Дело в том, что вплоть до начала XVIII века на Руси достаточно было поставить знак «титло» (¨) над буквой, чтобы превратить ее в число. Например, первая буква кириллицы

«аз» (А) превращалась в единицу (Ѧ), третья\* буква «веди» (В) — в два (Ѣ) и т. д. С одиннадцатой буквы «и», числовое значение которой равнялось десяти (Ї), начинался отсчет десятков. Сотни обозначались с буквы «рцы» (Ѳ) и т. д.

Затем полученная с помощью литореи числовая последовательность преобразовывалась посредством простых арифметических действий.

По сути, литорея — шифр простой замены, который не составляет труда дешифровать.

Попробуем угадать имя суеверного (или скромного) писца. Десять «и» в конце имени при сложении дадут сто, что соответствует букве «рцы» (Ѳ). Таким образом, получили окончание имени «оръ». А что с первой буквой имени? Имеем пять букв «рцы», то есть пять раз по сто, или пятьсот. Переберем последовательно буквы кириллицы: «рцы» — 100, «слово» (Ї) — 200, «твердо» (Ћ) — 300, «ук» (Ѧ) — 400, «ферт» (Ѳ) — 500. Следовательно, первая буква в имени «Ф». Здесь нетрудно уже и догадаться, что писца звали Федор.

---

\* Некоторым буквам, например второй «буки» и седьмой «живете», не повезло: в кириллице они числового значения не имели.

## Этюд VI

# Шифр Бэкона

В своем труде «О достоинстве и преумножении наук»\* [10], написанном на латыни, английский философ, историк и политик Фрэнсис Бэкон (1561–1626) размышляет в числе прочего об искусстве шифрования: «Существует довольно много видов шифра: простые шифры; шифры, смешанные со знаками, ничего не обозначающими; шифры, изображающие по две буквы в одном знаке; шифры круговые; шифры с ключом; шифры словесные и т. д. Шифры должны обладать тремя достоинствами: они должны быть удобными, не требующими многих усилий для их написания; они должны быть надежны и ни в коем случае не быть доступны дешифровке; и, наконец, если это возможно, они не должны вызывать подозрения. Ведь если письма попадут в руки тех, кто обладает властью над тем, кто пишет это письмо, или над тем, кому оно адресовано, то, несмотря на надежность шифра и невозможность его прочесть, может начаться расследование соответствующего дела, если

---

\* De Dignitate et Augmentis Scientiarum, 1623 год.



только шифр не будет таким, что не вызовет никакого подозрения или же ничего не даст при его исследовании».

Обратим особое внимание на третье условие: шифры «не должны вызывать подозрения». Это редкое требование к шифрам; Бэкон думает также и о сокрытии факта самого существования секретного сообщения. Ведь бессмысленный текст типа «ffff uuu gg e» в перехваченном письме дает основания заподозрить, что здесь применен некий шифр. А теперь попробуйте понять, что не так со следующей фразой, первоначально написанной на латыни [10], к которой как раз и применен шифр, не вызывающий подозрения:

Manere te volo donec venero  
(Я хочу, чтобы ты оставался на месте,  
пока я не приду).

Вы заметили что-нибудь необычное в шрифте этой фразы? Нет? А ведь при ее наборе использовалось два похожих, но тем не менее различных шрифта! К тому же фраза самая обычная. Шифры «не должны вызывать подозрения». Это принцип стеганографии\*: даже перехватив послание, вы ничего странного в нем не заметите, даже не будете подозревать, что здесь что-то не так.

Другое дело, если бы факт существования шифра не скрывался так тщательно, тогда вышеприведенная фраза была бы более наглядной:

---

\* Термин происходит от двух греческих слов: *στεγανός* — скрытый и *υράφω* — пишу; буквально «тайнопись».

MaNeRE te VOlo DOnc Venero.

Как видим, все дело в двух различных шрифтах. Вот что пишет по этому поводу сам Бэкон: «Нужно иметь два алфавита\*: один — состоящий из обычных букв, другой — из букв, не имеющих никакого значения, и отправить одно в другом сразу два письма: одно — содержащее секретные сведения, другое — имеющее достаточно правдоподобное для пишущего содержание, которое, однако, не должно навлечь на него никакой опасности».

Заметим, что выделенное большими жирными буквами слово **NREVODOV** не имеет никакого смысла, зашифровано совсем другое сообщение! **NREVODOV** всего лишь состоит «из букв, не имеющих никакого значения».

Теперь, когда шифр стал явным, может быть, вы сможете дешифровать его? Для облегчения задачи приведем аналогичным образом зашифрованную фразу на русском языке:

Я хочУ, чтОбЫ ты оСтАВалСя на месте,  
пока я не приду.

Как видим, здесь выделенных букв **УОЫСТВС** даже меньше, чем в оригинальном варианте. Да и стоят они на других местах...

Еще одна подсказка: количество букв в дешифруемом слове как в латинском, так и русском варианте текста совпадает и равно четырем. В латинском тексте в четырех словах

---

\* Под алфавитом в данном контексте Бэкон имеет в виду шрифт.

есть выделенные буквы, а в русском — только в трех. Так что общего в двух приведенных примерах?

Попробуем разбить фразы на составные части следующим способом:

MaNeR || E te VO || lo DOn || ec Ven || [ero].  
(Я хочУ, || чтОбы || ты оСТ || аВалС || [я на месте,  
пока я не приду]).

Лишь теперь, после разбиения фразы на пятерки букв, мы видим, что дешифруемое слово состоит ровно из четырех букв. Места расположения выделенных букв в пятерках не совпадают, так как русское слово не является калькой с латинского и пишется иначе. В квадратные скобки заключен лишний текст, который не использовался при шифровании; при дешифровке он легко будет отброшен как ненужный.

Этот шифр Бэкон изобрел «еще в ранней юности», в семнадцать лет. В шестьдесят он писал: «Даже сейчас, как нам кажется, это изобретение не потеряло своего значения и не заслуживает забвения. Ибо оно представляет собой высшую ступень совершенства шифра, давая возможность выражать всё через всё (omnia per omnia). Единственным условием при этом оказывается то, что внутреннее письмо должно быть в пять раз меньше внешнего; никаких других условий или ограничений не существует».

Вы уже догадались, в чем дело, или пора в качестве очередной подсказки дать ответ?

Итак, секретное послание, состоящее из одного слова, — это *fuge* (лат. «беги»).

Как же это слово возникло из фразы, по какому алгоритму? Рассмотрим все по порядку:

**MaNeR** соответствует при дешифровке *f*;

**EteVO** — *u*;

**loDOn** — *g*;

**ecVen** — *e*;

**ero** — ничему не соответствует, так как в этом остатке фразы слишком мало букв.

Улавливаете закономерность? Вспомним, что мы используем два шрифта для данного шифра. Заменяем все обычные буквы фразы на цифру 0, а **ВЫДЕЛЕННЫЕ** — на 1. Получаем, что

$$f = 00101, u = 10011, g = 00110, e = 00100,$$

или в русскоязычном варианте:

$$б = 00001, е = 00101, г = 00011, и = 01001.$$

Если первой букве классического латинского алфавита\* А поставить в двоичной системе счисления (в которой всего две цифры: 0 и 1!) в соответствие число 0 (или, используя пять символов, 00000), то второй латинской

---

\* Напомним, что Ф. Бэкон писал *De Dignitate et Augmentis Scientiarum* на языке науки того времени — латыни.

букве В (в русском языке Б) будет соответствовать 00001, третьей букве С (В) — 00010, четвертой букве D (Г) — 00011, пятой букве E (Д) — 00100, шестой букве F (Е) — 00101, седьмой букве G (Ё) — 00110, ... , десятой букве K (И) — 01001, ... , двадцатой букве V\* (Т) — 10011.

У математиков бытует шутка, что на свете существует 10 типов людей: те, кто понимает двоичную систему счисления, и те, кто не понимает\*\*. Надеюсь, что в предыдущем абзаце вы прекрасно разобрались.

Заметим, что внешнее письмо может быть написано на одном языке, а внутреннее — на другом. Так, если вышеприведенную фразу на латыни записать как:

ManeRe tE vOlo dONeC veNero,

то, зная, что тайное послание записано на русском языке, в результате дешифровки получаем «беги».

Конечно, Бэкон ничего не знал о двоичной системе счисления, которая была полностью разработана в европейской математике в трудах Г. В. Лейбница\*\*\* несколько позже.

---

\* Непосредственно в классическом латинском языке буква V использовалась также в качестве современной буквы U. В поздней латыни эти две буквы разделились для большего удобства. Поэтому букве U, как и букве V в шифре Бэкона соответствует одно и то же число 10011

\*\* Соль шутки в том, что цифра 2 в двоичной системе записывается как 10.

\*\*\* Готфрид Вильгельм Лейбниц (Gottfried Wilhelm von Leibniz, 1646–1716) — великий немецкий философ, математик, дипломат и изобретатель.

Он просто заметил, что на каждую букву достаточно пяти символов (где каждый символ — это либо буква *a*, либо *b* или, как у нас в этюде, равнозначные им цифровые символы 0 и 1), чтобы полностью заменить весь латинский алфавит различными сочетаниями этих знаков: «Перестановки из двух букв\* по пяти дадут нам тридцать два различных сочетания, что более чем достаточно для замещения двадцати четырех букв, из которых состоит наш алфавит».

Последовательность из символов 0 и 1 (или, если угодно, из «двух букв» *a* и *b*, как в сочинении Бэкона) является двоичной последовательностью, без которой теперь немыслима работа ни одного компьютера. Бэкон словно предчувствовал большое будущее такого способа передачи информации: «...это изобретение приводит нас к чрезвычайно важным выводам. Ведь из него вытекает способ, благодаря которому с помощью любых объектов, доступных зрению или слуху, мы можем выражать и передавать на любое расстояние наши мысли, если только эти объекты способны выражать хотя бы два различия. Такими средствами могут быть: звук колоколов или рога, пламя, звуки пушечных выстрелов и т. п.». Со временем человечество усовершенствует способы передачи информации: телеграф, радио, интернет... А на тот момент хватало и звона колокола.

---

\* Выше в этюде вместо «двух букв» использованы две цифры 0 и 1, как и в современной двоичной системе.

В своем труде лорд Бэкон пишет и о том, что «...учение о дешифровке <...> это, конечно, очень трудное дело, требующее в то же время большой изобретательности; это искусство (точно так же как и искусство шифра) используется в секретных государственных делах. Но если проявить достаточно ловкости и предосторожности, то можно было бы сделать это искусство бесполезным, хотя, судя по нынешнему положению дел, оно приносит немалую пользу».

Заметим, что шифр Бэкона не уникален: примерно в то же время в Париже этот метод включил в свою книгу (вышедшую в 1586 году) французский дипломат Виженер. Бэкон опубликовал свое описание позже, но заявил дату создания шифра более раннюю, чем Виженер.

На следующей странице приведен в качестве примера шифровки отрывок из первого письма древнеримского политика и философа, блестящего оратора Марка Туллия Цицерона проконсулу Публию Корнелию Лентулу Спинтеру. (В своей работе Бэкон дает текст письма, для удобства чтения, на более поздней латыни, в которой буквы V и U уже разделились; но в тексте все равно кое-где вместо U написано V. Например, во втором предложении явно написано *vt quoniam tu* вместо *ut quoniam tu*.)

Письмо является внешним текстом, в котором спрятан другой, внутренний. Применяя полученные знания, попытайтесь его дешифровать. Руководствуйтесь тем, что буквы алфавита одного шрифта объединяют какие-нибудь общие черты: наличие или отсутствие засечек, ширина, общая округлость букв и т. п.

Ego omni officio, ac potius pietate erga te, ceteris satisfacio omnibus. Mihi ipse nunquam satisfacio. Tanta est enim magnitudo tuorum erga me meritorum, ut quoniam tu, nisi perfectam re, de me non conquiesci; ego, quia non idem in tua causa efficio, vitam mihi esse acerbam patem. In causa haec sunt: Ammonius Regis Legatus aperte pecuniam nos oppugnat. Res agitur per eosdem creditores, per quos, cum tu aderas, agebatur. Regis causa, si qui sunt, qui velint, qui pauci sunt, omnes ad Pompeium rem deferri volunt. Senatus Religionis calumniam, non religionem, sed malevolentiam, et illius Regiae largitionis invidiam comprobant. &c.

Отрывок из письма Цицерона с внутренним скрытым посланием воинов Спарты, зашифрованным методом Ф. Бэкона



В рассмотренном выше примере различие между шрифтами было явно выделенным. Естественно, будучи одним из высших сановников королевства, лорд-канцлер Англии, барон Веруламский и виконт Сент-Олбанский разработал для своего метода шифрования такие шрифты, чтобы при чтении текста разнородность букв не бросалась в глаза. Но — Praemonitus praemunitus («Предупрежден — значит вооружен») — вы, несомненно, заметите тонкие различия.

Для проверки приведем этот же текст с явным выделением шрифтов и исправлением опечаток исходного латинского текста письма:

EGO Omni Officio, ac potius pietate erga te, ceteris  
satisfacio omnibus: mihi ipse nunquam satisfacio. Tantum  
est enim magnitudo tuorum, erga me meritorium, ut  
quoniam tu, nisi perfectus es, de me non conquiesci: ego,  
quia non idem in tua causa officio, vitam mihi esse  
acerbum putem. In causa haec sunt: ammonius regis  
legatus aperte pecunia nos oppugnat. Res agitur per  
eosdem creditores, per quos, cum tu aderas, agebatur.  
Regis causa, si qui sunt, qui velint, qui pauci sunt, omnes  
ad pompeium rem deferri volunt. Senatus religionis  
calumniam, non religionem, sed malevolentiam, et illius  
regiae largitionis invidia, comprobatur, etc.

Теперь вам осталось дешифровать спрятанный текст и сверить его с ответом, приведенным в следующем абзаце.

Скрытое, внутреннее письмо — это письмо спартанцев, посланное ими некогда на скитале\*: *Perditae res: Mindarus cecidit: milites esuriunt: neque hinc nos extricare, neque hic diutius manere possumus.* («Все погибло. Миндар убит. Воины голодают. Мы не можем ни уйти отсюда, ни оставаться здесь дольше».)

Подсчитайте: сколько ошибок вы допустили на первом этапе дешифровки? Сколько букв оказалось не на своем месте? Насколько вы были внимательны?

Типографское искусство в те времена «по современным меркам стояло на столь низком уровне, что при разглядывании в сильную лупу двух отпечатков одной и той же литеры на одной и той же странице всегда можно было обнаружить небольшие различия. Свинцовые литеры были несовершенны, набор нередко повреждался, типографская краска высыхала неравномерно на грубой увлажненной бумаге, к тому же наборщики часто путали два шрифта на одной и той же странице» [16]. Неудивительно, что с подобным качеством типографского текста вы допустили при дешифровке письма какое-то количество ошибок. Не позавидуешь дешифровщикам той поры!

---

\* Скитала (от греч. σκυτάλη — жезл), известный также и как шифр Древней Спарты, представляет собой прибор, используемый для осуществления шифрования; состоит из цилиндра (железа) и узкой полоски пергамента, обматывавшейся вокруг него по спирали, на которой писалось сообщение вдоль длины цилиндра. Когда полоска снималась с цилиндра, текст превращался в беспорядочный набор букв.

## Этюд VII

# Нет повести печальнее на свете

В XIX веке, почти два столетия спустя после смерти Уильяма Шекспира (1564–1616), англичане начали сомневаться в авторстве созданных им произведений (и продолжают сомневаться до сих пор). Антистратфордианцы\* выискивали любое малейшее обстоятельство, свидетельствующее против авторства Шекспира. Так, в лагерь своих сторонников они зачислили и писателя Чарльза Диккенса, который считается величайшим творцом характера в английской художественной литературе после Шекспира: «Это большое утешение, как мне думается, что так мало известно о поэте. Жизнь Шекспира — это какая-то прекрасная тайна, и я каждый день трепещу, что она окажется открытой»\*\* [58].

---

\* Шекспир родился и умер в городе Стратфорд-он-Эйвон (Stratford-on-Avon), поэтому тех, кто сомневается в его авторстве, называют антистратфордианцами.

\*\* В оригинале: It is a great comfort, to my way of thinking, that so little is known concerning the poet. The life of Shakespeare is a fine mystery and I tremble every day lest something turn up.

В особенности же противники драматурга любили цитировать последнее предложение из вышеуказанной цитаты. При этом игнорировались другие его слова по поводу авторства Шекспира, например: «Начавшаяся с тех пор спекуляция его великим именем потерпела крах, и я теперь искренне желал бы, чтобы это славное имя оставили в покое» [20]. Диккенс даже иронизирует, что братство противников «сомнительной личности, именуемой Шекспиром», надо «снабдить <...> таким шрифтом, что ни одна душа на свете не сможет в нем разобраться» [21] и их пасквили, таким образом, никто не сможет прочесть.

Обратим особое внимание на слова о шрифте, в котором «ни одна душа на свете не сможет <...> разобраться». Это прямой намек на героя нашего предыдущего этюда Фрэнсиса Бэкона, которому нередко приписывали авторство пьес Шекспира. Не будем сейчас касаться всех причин, по которым англичане отказывают в авторстве Шекспиру, но одна из них — сомнение в том, что простой «малограмотный» актер из провинции мог так тонко знать высший свет, обладать таким обширным словарным запасом, немислимым для человека его круга. Поэтому-то выбор и пал на одного из образованнейших людей того времени — философа, политика, аристократа Бэкона, который к тому же изобрел шифр, использующий малозначительные отличия двух шрифтов.

Один из самых сильных доводов бэконистов в пользу авторства лорда-канцлера — место из шекспировской

«Бури» (The Tempest; акт I, сцена 2), в котором героиня пьесы Миранда произносит слова:

You have often  
Begun to tell me what I am, but stopp'd  
And left me to a bootless inquisition,  
Concluding 'Stay: not yet'\*

Выделенные буквы **BACon**, по мнению сторонников Бэкона, — это тайная подпись настоящего автора пьесы, который использовал псевдоним, чтобы защитить себя от позорного клейма литератора — занятия, недостойного вельможи. Кроме того, Бэкон якобы старался избежать преследований со стороны властей за пропаганду республиканской формы правления. Однако, как думается, Бэкон смог бы лучше зашифровать свою подпись в акrostихе, например первую строчку начал бы с буквы F, первой литеры своего имени. Но, на взгляд автора, гораздо интереснее контекст «акrostиха»: «Вы часто собирались мне открыть, // Кто мы; и прерывали свой рассказ // Словами: “Нет, постой, еще не время...”» Не правда ли?

Барон Веруламский и виконт Сент-Олбанский Фрэнсис Бэкон завещал похоронить себя в церкви Святого Михаила в Сент-Олбансе. Шекспир был захоронен в церкви Святой Троицы родного города Стратфорда. На надгробиях обоих есть эпитафии.

---

\* «Вы часто собирались мне открыть, // Кто мы; и прерывали свой рассказ // Словами: “Нет, постой, еще не время...”» (пер. М. Донского).

У Бэкона эпитафия, написанная на латыни, в переводе гласит:

Некогда так сидел Фрэнсис Бэкон, барон  
Веруламский, виконт Сент-Олбанский,  
Известный более славными титулами —  
«Светоч Науки» и «Закон Красноречия».  
После того как постиг Мудрость Природы  
И секреты Гражданской Жизни,  
Он исполнил предназначение Природы  
В год Господа нашего 1626 в возрасте 66 лет.  
Да возвратится все к первоначальным элементам!

Его секретарь и друг Фома Меотис поставил Бэкону памятник из белого мрамора: сидящий в кресле философ погружен в размышления. Внизу эпитафии можно прочесть подпись: «В память такого великого человека воздвиг этот монумент Фома Меотис, исполняя долг того, кто пережил, проникнутый восторгом к пережитому».

На более скромном надгробии Шекспира стихотворная эпитафия написана на английском языке.

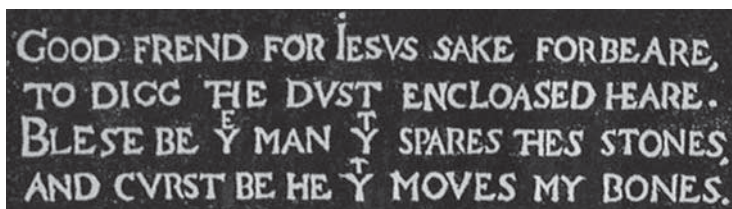
На современном английском она звучит так:

Good friend, for Jesus' sake forbear,  
To dig the dust enclosed here.  
Blessed be the man that spares these stones,  
And cursed be he that moves my bones\*.

---

\* Друг, ради Господа, не рой // Останков, взятых сей землей; // Нетронувший блажен в веках, // И проклят — тронувший мой прах.  
(Пер. А. Величанского.)

Приглядимся к оригиналу внимательнее (см. фото надгробия ниже). Обратите внимание на орфографию, принятую во времена Шекспира.



Лигатура\* **Y** обозначала тогда the, а **T** — thy, которое позднее трансформировалось в that. Также, присмотревшись, можно заметить менее очевидные лигатуры в словах the, heare, thes во второй и третьей строках.

В 1887 году некий Хью Блэк (Hugh Black) счел, что в этой надписи есть два вида шрифта, как в шифре Бэкона. Приняв буквы одного за 0, а другого — за 1, и посчитав некоторые лигатуры за одну букву, он применил к полученной последовательности цифр шифр Бэкона и получил следующий текст:

saehrbayeerprftaxarawar [25].

После чего Блэк графически разделил его следующим образом:

saehr  
baye || ep  
rfta || xa  
rawar.

---

\* Лигатура — графическое соединение двух и более букв.

Далее он немного перегруппировал буквы и получил текст, разделенный уже на две части:

saehrepха || bayerftarawar.

Как видим, результатом стали две анаграммы, решение которых — Shaxpeare и Fra Ba wrt ear ay. Первая часть, очевидно, означает «Шекспир», а вторая была истолкована верным бэконянцем как Francis Bacon wrote Shakespeare's plays («Фрэнсис Бэкон написал шекспировские пьесы»).

Ну что ж, пришла очередь задания. После знакомства с таким длинным вводным объяснением почувствуйте себя сторонником бэconiанцев и найдите написанные другим шрифтом буквы на надгробии Уильяма Шекспира. Затем самостоятельно проделайте те же действия, что и Блэк: примените шифр Бэкона и дешифруйте эпитафию.

Удалось ли вам рассмотреть второй, едва отличимый от первого шрифт? Если, конечно, он вообще присутствует в эпитафии... Не знаю, каким чудесным образом Хью Блэку удалось разглядеть его, но согласно предложенной им дешифровке эти два шрифта должны быть расположены следующим образом:

Good Frend for Iesvs **SAKE** forbearе,  
To digg ThE Dust EncloAsed (**HE**)**ARE**.  
Blese be ThE Man (**THY**) spares ThEs Stones,  
And cvrst be **He** (**THY**) moves my Bones.



Второй шрифт выделен жирными прописными буквами, в скобки взяты те лигатуры, которые он посчитал за одну букву этого другого шрифта. Осталось только вместо светлых строчных букв подставить 0, а вместо прописных жирных — 1, и получим зашифрованный, тайный текст (разобьем его сразу для удобства на пятерки цифр):

10001-00000-00100-00111-10000-00001-  
00000-10110-00100-00100-01110-  
10000-00101-10010-00000-10101-00000-  
10000-00000-10100-00000-10000.

Теперь переведем двоичные числа в привычные для нас десятичные (как это сделать, рассказано в предыдущем этюде) и заменим каждое полученное число на соответствующую ему букву, чей порядковый номер в алфавите совпадает с самим десятичным числом. Так, семнадцатой букве латинского алфавита *s* (если считать, что букве *a* соответствует 0, как у Бэкона) в двоичной системе будет соответствовать число 10001. В итоге этих несложных манипуляций и получается скрытый текст *saehrbayeerprftaxarawar*. Осталось только догадаться, что это за анаграммы, и с некоторыми натяжками «правильно» их дешифровать.

Убедил ли вас в достоверности своих выводов Хью Блэк или все же не окончательно? Дадим слово специалистам-криптографам супругам Фридманам — Уильяму Фредерику, начальнику дешифровальной службы войск связи США с момента ее основания в 1929 году, и Элизабет, сотруднице

той же службы: «Для обыкновенного человека, — писали они в своей книге “Исследование шекспировских шифров”, — этого текста было бы вполне достаточно, чтобы доказать, что никакой шифр здесь не используется. Бэкониянец же отличается от обыкновенного человека, и разница между ними заключается, по нашему мнению, в степени упорства и изобретательности» [25].

## Этюд VIII

# Невезенье шевалье Луи де Рогана

Шевалье Луи де Роган (1635–1674), который занимал высокую придворную должность главного ловчего Франции, своим разгульным образом жизни навлек на себя немилость «короля-солнца» Людовика XIV и примкнул к заговору, целью которого была сдача голландцам за деньги французской крепости Кийбёф [43]. Заговор провалился, и де Роган попал в Бастилию. Его судьба всецело зависела от другого заговорщика, Труомона, который лежал при смерти в той же тюрьме. Если он во всем сознается, то шевалье признают виновным в измене и казнят. Не слишком веря в стойкость друга, де Роган несколько дней мучился неизвестностью в своей камере.

Незадолго до судебного разбирательства шевалье передали узел с одеждой, в котором он обнаружил зашифрованную записку, прикрепленную к рукаву рубашки:

mg eulhxclgu ghj yxuj lm ct ulgc alj.

Всю ночь де Роган пытался расшифровать сообщение, но наступил рассвет, а шифр ему так и не поддался. Быстро

сломавшись во время жестокого допроса, Луи де Роган во всем признался, и его приговорили к казни.

Ему удалось бы спасти свою жизнь благодаря высокому положению и слезам его матери, герцогини Анны де Сен-Мор, сумей он за ночь разгадать этот элементарный шифр. В записке по-французски сообщалось:

Le prisonnier est mort; il n'a rien dit  
(«Узник умер; он ничего не сказал»).

Шевалье Луи де Роган окончил свои дни на эшафоте. Как и подобало дворянину, он принял смерть от меча.

Попытаемся восстановить алгоритм шифра, иными словами найти его ключ. Нам уже известен начальный текст зашифрованной записки на французском языке и ее настоящий смысл, поэтому, чтобы немного усложнить задачу, дешифруем аналог тайного послания на английском языке:

PVQ RDOWYFQD OW XQSX  
VQ WSOX FYPVOFC.

Данный шифр является моноалфавитным шифром простой замены с использованием английского алфавита, то есть каждому символу открытого текста ставится в соответствие какой-либо иной символ этого же алфавита. В случае с шевалье де Роганом (так как мы знаем открытый текст и криптограмму) таблица соответствий для записки, написанной на французском языке, выглядит так:

Открытый алфавит	l	e	p	r	i	s	o	n	t	m	a	d
Шифр-алфавит	M	G	E	U	L	H	X	C	J	Y	T	A

Данная простая замена введена случайным образом, то есть не прослеживается какой-либо закономерности в том, какие символы были поставлены в соответствие буквам алфавита. В этом случае единственным способом дешифровки текста является частотный анализ, то есть поиск и анализ наиболее часто используемых букв либо буквосочетаний в исследуемом тексте по известным статистическим характеристикам.

Заданный на английском языке шифр-текст PVQ RDOWYFQD OW XQSX VQ WSOX FYPVOFC по условию зашифрован этим же методом, и у него своя таблица соответствий.

Подсчитаем буквы, их ровно тридцать. По одному разу встречаются буквы C и R, два раза — D, P, S и Y, три раза — F, V, W и X, четыре раза — O и Q. Наиболее часто встречающиеся буквы в английском — *e* и *t*. Предположим, что  $Q = e$ , и тогда первое слово из трех букв примет вид PVe. Возможно, что это артикль *the*, тогда  $P = t$ ,  $V = h$ ; тем более что в английском языке буква *h* часто стоит перед буквой *e*, а в пятом слове VQ (*he*) как раз такая комбинация.

Подставив эти три буквы в исходный текст, получим:

*the* RDOWYFeD OW XeSX *he* WSOX FY*th*OFC.

На третье место (согласно правилам построения предложений в английском языке) напрашивается служебный глагол, состоящий из двух букв OW. Буква O — одна

из наиболее частотных; *a*, *o* и *i* — это также самые распространенные английские буквы, которые мы еще не использовали. Можно предположить, что *O* = *i*, и сам глагол — *is*. Таким образом, *W* = *s*, и тогда:

*the RDisYFeD is XeSX he sSiX FYthiFC.*

Внимательно посмотрев на текст, сделаем предположение, что после местоимения *he* (он) находится глагол *said* (сказать). Получаем, что *S* = *a*, *X* = *d*, и фраза мгновенно становится более осмысленной:

*the RDisYFeD is dead he said FYthiFC.*

Результатом окончательной дешифровки, очевидно, будет фраза:

the prisoner is dead he said nothing  
(«Узник умер; он ничего не сказал»).

Шевалье Луи де Роган вполне мог бы прочесть записку и спасти свою голову, если бы знал правила частотного анализа.

## Этюд IX

# Любовный шпион

Девчонка гадает у быстрой реки,  
Ромашки лучистые губит.  
И, словно снежинки, летят лепестки:  
Любит? Не любит? Любит!

Ты правду всю знаешь, цветок полевой,  
Иль это придумали люди?  
За все отвечаешь своей головой:  
Любит? Не любит? Любит!

(В. Рождественский)

Язык цветов (флюорографика) пришел к нам с утонченного Востока, где он использовался для выражения чувств в тех случаях, когда о них нельзя было сказать открыто. Так, красный мак означал удовольствие; бледно-желтый нарцисс — кротость и смирение, а также безответную любовь; белая лилия была символом невинности и чистоты.

Сами по себе цветы не скрывали текст послания. Любой посвященный в этот тайный язык мог его прочесть. Но букеты

цветов также могли использоваться при скрытой передаче иного рода информации путем сохранения в тайне самого факта передачи. В годы Второй мировой войны цензура США, стремясь перекрыть максимальное число стеганографических каналов связи, категорически запретила отправку по почте целого ряда сообщений. Так, невинная телеграмма, направленная в обычный магазин цветов: «Вручите в субботу моей жене три белые орхидеи» — была настолько удобной для передачи и сокрытия секретной информации, что цензура была вынуждена запретить указывать в подобных телеграммах названия цветов и день вручения [25].

Знала о возможности использования цветов в стеганографии и королева детектива Агата Кристи. В рассказе «Цветы смерти»<sup>\*</sup> мы можем прочесть: «Миссис Бентри протянула руку и взяла проспект. Открыв его, она не без удовольствия прочла вслух: *“Ульрих Шпат. Чистая линия. Удивительно красивый цветок на длинном прочном стебле. Замечательно украшает сад и хорошо срезается. Брайан Джексон. Похожий на хризантему цветок краснокирпичного цвета. Енох Перри. Блестящий красный, очень декоративный. Йорк — знаменитый долго цветущий оранжево-красный тюльпан”*. “Из начальных букв названий этих цветов складывается слово “убей”», — пояснила мисс Марпл».

Лепестки цветков издревле служили также и для гадания. На Руси с давних пор гадали на ромашке — любит,

---

<sup>\*</sup> Пер. В. Постникова, А. Шарова.



не любит... В Древней Греции на любовь гадали с помощью цветка, который так и называли — «любовный шпион». Девушки обрывали его лепестки, положив их на образованный согнутыми большим и указательным пальцами левой руки круг, ударяли по нему ладонью и по силе хлопка определяли, как сильно влюблен в них молодой человек [45].

Ниже приведена таблица, в которой указано современное название цветка и старинное, которое использовалось различными народами в далеком прошлом. Но внимание: слова во втором столбце перемешаны! Проверьте свою интуицию, разгадайте «код» цветка, расставив все по своим местам. Разоблачите любовного шпиона!

Водяная лилия	Любовный шпион
Мак	Одолень-трава
Пион	Романова трава
Ромашка	Целебник

Проверяем ответы.

На Руси «любовную гадалку» ромашку ранее именовали романовой травой, а в старинном рукописном травнике кувшинка (водяная лилия) называется одолень-травой, с помощью которой можно было одолеть любую нечисть.

Название прекрасному пиону дал древнегреческий бог целителей Пеан, его название означает «врачующий, целебный».

Ну а «любовным шпионом» в Древней Греции был красный мак.

Этюд X

## Гарна мама

Если в слове или фразе при перестановке букв получается другое слово или даже фраза, мы имеем дело с анаграммой. Попробуйте проделать это с названием данного этюда («гарна мама» на украинском языке означает хорошая или красивая мама). Ответ лежит на поверхности: из «гарна мама» получается «анаграмма»!

Анаграммы с XVII века начали широко применяться учеными мужами. Для того чтобы застолбить свое авторство, ученые кратко формулировали суть открытия, в полученном тексте переставляли буквы и посылали письмо с получившейся анаграммой коллегам. Иногда такие анаграммы публиковались учеными в приложениях к изданиям их текущих трудов. После тщательной проверки своего открытия они позже спокойно публиковали полученный результат с дешифровкой соответствующих анаграмм.

Так, нидерландский физик, математик, астроном и изобретатель Кристиан Гюйгенс (1629–1695), усовершенствовав

телескоп, увидел в него нечто такое, что поспешил зафиксировать в виде анаграммы на латыни:

a a a a a a c c c c c d e e e e e g  
h i i i i i i l l l l m m n n n n n n n n n  
o o o o p p q r r s t t t t t u u u u u.

Как видим, ученый не стал придумывать осмысленную анаграмму, а удовлетворился перечислением букв в алфавитном порядке. Это надежный «замок». Всего в анаграмме 62 буквы. Полное количество вариантов дешифровки равно примерно  $10^{60}$ , что больше числа атомов на Земле, которое оценивается в  $10^{50}$  единиц.

Через три года, убедившись в правильности своих предположений, Гюйгенс разъяснил смысл анаграммы: *Annulo cintigar tenui, plano, nusquam cohaerente, ad eclipticam inclinato*. В переводе: «Окружен кольцом тонким, плоским, нигде не подвешенным, наклонным к эклиптике». Таким образом Гюйгенс зашифровал открытие им колец у Сатурна. И не зря! Ведь еще за полвека до этого итальянский ученый Галилео Галилей тоже видел странные придатки у планеты, но так и не понял, в чем дело.

Современник Гюйгенса, английский физик и математик Роберт Гук (1635–1708) оставил после себя целый список открытых им законов в виде анаграмм, причем некоторые из них не дешифрованы до сих пор.

Анаграммы во все времена активно использовали поэты и писатели: кто-то скрывался таким образом

от преследований, кому-то было удобно объединять таким образом некоторые произведения в циклы, кто-то просто играл с читателями.

Например, под псевдонимом Харитон Макентин писал русский поэт Антиох Кантемир. Строго говоря, анаграмма не вполне точная (в псевдониме есть лишняя «н»), но в литературной среде это нередкое допущение.

А что связывает этих людей?

- Самуель Грейфн-Зон фом Гиршфельд (Samuel Greifn-Son vom Hirschfeld),
- Израель Фромшмит фон Гугенфельс (Israel Fromschmit von Hugenfels),
- Герман Шлейфхейм фон Зульсфорт (German Schleifheim von Sulsfort).

Присмотритесь внимательно к именам. Для верности выпишите их буквы по алфавиту.

Слишком много совпадений? Да это просто один и тот же человек.

Это немецкий писатель Кристоффель фон Гриммельсгаузен (Christoffel von Grimmeishausen, 1622–1676). Для каждого своего романа, которых было более десятка, он выдумывал новый псевдоним-анаграмму для себя или для главного персонажа; а в одном на титульном листе просто выписал, подобно Гюйгенсу, в порядке алфавита все буквы своего имени: догадайтесь сами, кто автор!

Приведем анаграмму посложнее, на латыни. В ней говорится об одном знаменитом ученом муже из Англии:

Ieova sanctus unus\*.

Здесь путь решения более витиеватый: две латинские буквы *и* (в английском языке название буквы произносится как «ю») в угадываемой фамилии сливаются в одну букву английского алфавита *w* («дабл ю», или «двойное ю»), которая отсутствовала в латинском алфавите.

Итак, кто же этот англичанин?

«Едва научившись читать и писать, Исаак Ньютон понял, что анаграмма его имени указывает на богоизбранность: в самом деле, никто не может отрицать, что *Isaacus Newtonus* дает *Ieova sanctus unus*» [12]. Известно также, что факт своего рождения в день Рождества Ньютон, создатель классической физики, считал особым знаком судьбы. «Ведь он, подобно Спасителю, появился на свет в Рождество» [3].

До эпохи Просвещения анаграммам вообще придавалось сакральное значение, в них искали знаки судьбы и предсказания, а сейчас это просто способ приятного времяпрепровождения, тренировка ума.

Попробуем разгадать пару анаграмм попроще [7].

Первая анаграмма — всего тринадцать букв.

Макар не ел гель.

---

\* Переводится как «святой и единый Иегова».

Подсказка: здесь говорится о первой женщине на посту канцлера в истории Германии. Натюрлих, речь идет об Ангеле Меркель.

Вторая анаграмма:

Даме слон не пара.

Действительно, есть дамы с камелиями, дамы с собачками, но со слоном?!

Даю наводку: кто у вас ассоциируется со «Спасателями Малибу»? Правильно — Памела Андерсон.

## Этюд XI

# 510

Quid juvat immensas librorum condere moles  
Queis tua Pyramidas provocat arcta domus?  
Omnia quid legisse juvat tibi si legis uni?  
Et paucis viva es bibliotheca domi?  
Incipe jam tandem diffundere flumina mentis,  
Incipe doctrinae spargere grandis opes;  
Quod si forte minus te publica vota movebunt,  
At Domini tangat gloria certa tui\*.

Поэзия и математика — как они связаны друг с другом? Русский математик Софья Ковалевская, с детства сочинявшая стихи, считала: математика — «это наука, требующая наиболее фантазии, и один из первых математиков нашего

---

\* Как разместиться смогли мириады томов этих книг // В доме твоём? Пирамиды размером поменьше их ведь? // Что помогает тебе фолианты прочесть эти, друг? // В библиотеке твоей сколь же долго ютятся они? // Прямо сейчас ты попробуй потоки сознания нести // Людям, начни же ученья великого свет излучать; // Граждане вряд ли оценят сей труд и заплатят тебе, // Господа нашего слава коснется, возможно, тебя. *Пер. с лат. автора.*

столетия говорит: совершенно верно, что нельзя быть математиком, не будучи поэтом в душе. Только, разумеется, чтобы понять верность этого определения, надо отказаться от старого предрассудка, что поэт должен что-то сочинять несуществующее, что фантазия и вымысел — это одно и то же. Мне кажется, что поэт должен только видеть, чего не видят другие, видеть глубже других. И это же должен видеть математик»\*.

Но вышеприведенное восьмистишие принадлежит перу другого знаменитого математика. Попробуйте догадаться, кому принадлежат строки эпиграфа к данному этюду. Дадим вам в помощь три подсказки, три интересных факта, характеризующих многогранность личности этого человека.

- Он первым обосновал необходимость измерять температуру тела у больных.
- Его интересовала просветительская деятельность китайского императора\*\*, который высоко ценил европейскую науку и был знаком с трудами Евклида. В результате ученый узнал о древнем китайском счислении. Рассказы на эту тему навели его на мысль изобрести новую арифметику, в которой достаточно двух цифр — 0 и 1.
- О русских он говорил, что они «крещенные медведи». Тем не менее в 1712 году царь Петр I присвоил ему звание тайного советника с жалованьем 1000 рейхсталеров.

---

\* Ковалевская С. В. Из письма Шабельской [33]. Математик, не названный Ковалевской, по-видимому, Карл Вейерштрасс.

\*\* Имеется в виду император Канси из династии Цинь (род. 1654, правил 1661–1722).



В ответ ученый присылал Петру I всякого рода преобразовательные «проекты», в том числе разработанный во всех деталях план русской Академии наук. Высказывается также мнение, что Петр пригласил ученого в Россию в том числе «и для создания российской криптографической службы по европейскому образцу» [22].

Итак, вышеприведенные поэтические строки принадлежат Готфриду Вильгельму Лейбницу (1646–1716) — великому немецкому философу, математику, дипломату, талантливому механику и изобретателю.

Сам ученый считал себя крупным поэтом — «по тогдашним понятиям истинный поэт мог писать только на латыни или по-гречески» [52]. В эпиграфе к этюду приведен отрывок из элегии, адресованной другу Лейбница, знаменитому флорентийскому библиотекарю и ученому Антонио Мальябеки.

Можно привести еще много интересных пестрых фактов о Лейбнице, но вернемся к криптографии.

Когда вы совершаете операции с использованием банковской карточки, то, наверное, и не подозреваете, что безопасность ваших действий обеспечивают некоторые разделы высшей математики, например теория чисел. Введенный вами номер кредитки при оплате покупки в интернете шифруется с использованием расчетов по модулям простых чисел. Впрочем, в большинстве обыденных случаев вам достаточно знать свой PIN-код или пароль доступа в интернет-банк для подтверждения своей личности. При проверке

своей электронной почты вы также используете пароль, таким образом защищая свою информацию от несанкционированного доступа.

Именно надежностью паролей был обеспокоен Лейбниц. Немного поговорим собственно о создании паролей.

Если вы придумаете простой, легко запоминающийся пароль (например, football или хоккей), опытный мошенник легко его взломает. Любые осмысленные слова в пароле легко высеиваются специальной программой, хотя это и зависит, в частности, от того, включил ли хакер русский или, к примеру, цезский (один из языков Дагестана) в словарь используемой программы.

С другой стороны, если вы придумаете сложный и длинный пароль, то, вполне возможно, вскоре сами его забудете.

Наши предки в дописьменную эпоху запоминали огромный объем нужной им информации в стихотворной или песенной форме. Как известно, стихи (или песни) нередко были единственным средством учета времени при первобытных производственных процессах — неважно, варке ли бронзового сплава или изготовлении лечебного зелья.

«Необразованные» предки легко могли запомнить намного больший объем информации, чем пароль из шести букв или цифр. В том числе и неосмысленные — кодовые, часто труднопроизносимые слова (используемые в магии) вроде «абракадабра». Напомним, что в PIN-коде всего четыре цифры из-за того, что современные образованные люди в массе своей не способны без применения мнемотехник

запомнить большее количество цифр. Изобретатель банкомата шотландец Джон Шепард-Баррон (1925–2010) сначала предполагал ввести шестизначный цифровой PIN-код, но его супруга запоминала всего четыре цифры. Пришлось этим и ограничиться.

Размышляя над проблемой пароля, Готфрид Вильгельм Лейбниц предложил удобную систему перевода цифровых кодов в благозвучные слова и наоборот. Он предложил сопоставлять цифрам некоторые согласные. Например, те, с которых начинается название самой цифры (выделим для наглядности первые буквы в названии цифры).

1	Р		В	8
2	Д		Д	2
3	Т	3	З	3
4	Ч		Н	0
5	П		П	5
6	Ш		Р	1
7	С		С	7
8	В		Т	3
9	Щ		Ч	4
0	Н		Ш	6
			Щ	9

Согласно вышеприведенному рисунку, 1 — **р**аз, 2 — **д**ва, 3 — **т**ри (и/или «3»), 4 — **ч**етыре, 5 — **п**ять, 6 — **ш**есть, 7 — **с**емь, 8 — **в**осемь, 9 — **д**евять («перевернутая» шестерка), пусть будет «Ш», 0 — **н**оль.

После чего берем любую стихотворную строку, выбираем из нее согласные буквы, оставляем те из них, которые можно заменить цифрами, и получаем число — ваш новый пароль.

Что ж! Попробуем так и сделать, а заодно и сыграем. Возьмем строку Александра Сергеевича Пушкина. Надеюсь, все еще со школьной скамьи помнят некоторые его стихотворения! Можно было, конечно, взять стихотворения самого Лейбница, но они, к сожалению, малоизвестны.

Наш первый цифровой пароль:

5 0 4 2 0 0 8 0

Строчки поэта посвящены Анне Петровне Керн, урожденной Полторацкой. Все уже догадались, несомненно. Но все же дадим вторую подсказку, чтобы вы проверили собственное чутье.

5 0 4 2 0 М Г 0 8 0 Ъ

Здесь пароль расширен дополнительными клеточками, в которые вписаны все другие согласные разгадываемой строчки и добавлен мягкий знак.



Вверху выписана уже вся строка: восстановлены пробелы между словами, цифры заменены на соответствующие им буквы, \* обозначает гласный звук.

Все верно! «Я помню чудное мгновенье...» — правильный ответ. Теперь, если оставить в этой строчке только согласные, а затем, используя рисунок с предыдущего разворота, заменить согласные на цифры, то, последовательно выписывая их, получим наш код-пароль 50420080.

Усложним задание. Рассмотрим следующий цифровой пароль:



Стихотворение посвящено Софье Федоровне Паниной, урожденной Пушкиной. Софья Федоровна была дальней родственницей поэта, первой женщиной, к которой А. С. Пушкин официально посватался в октябре 1826 года, но получил отказ.

Во второй подсказке снова добавим к паролю все другие согласные и мягкий знак, согласно их расположению в строке поэта:



И наконец, пришел черед последней подсказки, восстановлены пробелы между словами, цифры заменены на соответствующие им буквы, \* обозначает гласный звук.

П	Р	*	К	Р	*	С	Н	*	*		Б	*	Т	ь
	Н	*	В	*	З	М	*	Ж	Н	*	...			

Вот эта строчка, написанная рукой влюбленного поэта:  
«Прекраснее быть невозможно...»

«И мысли в голове волнуются в отваге... и пальцы просят-  
ся к перу, перо к бумаге...» Надеюсь, что и вы испытываете это  
состояние при решении наших поэтических головоломок!  
Напоследок попробуем поработать с еще одним паролем:

3	1	2	0	8	7	5	0	3	8	1	0	5	3	8
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Эти строки посвящены Калипсо Полихрони, которая  
была музой двух великих поэтов. Джордж Гордон Байрон  
посвятил ей стихотворение «Песнь Лейкалы». Говорили, что  
он познакомился с пятнадцатилетней Калипсо, путешествуя  
по Востоку. В 1821 году юная гречанка вместе с матерью бе-  
жала после начала константинопольских погромов из Тур-  
ции в Кишинев, где встретила с Пушкиным.

Традиционная вторая подсказка:

3	1	Ж	2	0	8	7	5	Л	М	0	3	ь	8	Б
1	Ж	0	5	3	8									

И для проверки ваших гипотез приведем третью подсказку:

Т	*		Р	*	Ж	Д	*	Н	*		В	*	С	П
Л	*	М	*	Н	*	Т	Ь		В	*	*	Б	Р	*
Ж	*	Н	*	*		П	*	*	Т	*	В	...		

Я уверен, что вы не подглядываете в ответ, все честно сами сделали. Приведение мною ответа, по сути, является простой формальностью. «Ты рождена воспламенять // Воображение поэтов...» Обратите внимание, что Пушкин написал слово «поэтов» во множественном числе, помня о Байроне.

В заключение заметим, что криптография умеет хранить свои секреты долго. Только недавно стало известно [60, 61], что Готфрид Вильгельм Лейбниц летом 1688 года изложил свои мысли о построении *Machina Deciphratoria* императору Священной Римской империи Леопольду I. Механическая машина для шифрования и дешифрования была предназначена для «переписки со многими министрами одновременно и использовала целое множество практически неразрешимых шифров». На ней можно было работать, подобно «игре на музыкальном инструменте, например клавикорде, так что текст появляется благодаря касанию клавиш и его нужно только перенести на бумагу». За девять лет до этого он предлагал свой проект и герцогу Ганновера.

Но ни тот ни другой венценосец не проявили интереса к новинке, полагая, что их старые добрые ручные шифры достаточно надежны.

Хотя до Лейбница были известны устройства, облегчающие процесс шифрования (например, диск Альберти), именно машина немецкого ученого стала первой шифровальной машиной в полном смысле слова. Пройдет почти 250 лет, прежде чем появится достойный ее потомок — немецкая портативная шифровальная машина «Энигма».

Осталось только пояснить, почему этюд называется 510. Все просто: дешифрованное его название по приведенному здесь алгоритму — «Пароль Лейбница».



## Этюд XII

# Логогриф Эйлера

Российский ученый швейцарского происхождения Леонард Эйлер (1707–1783) в самом конце своего довольно длинного письма коллеге и другу Христиану Гольдбаху (1690–1764) от 4 июля 1744 года пишет\*: «Некоторое время назад я разработал следующий логогриф, в котором все буквы значимы и сам текст написан на латинском языке:

pxqjfwlnjdvynftiddkqxhleebfpxdfgtlbccfbkfodxokfnglqxnf  
shejmlckzxhrfwjgfhxvzjnbgyxcdgixkoxjmlncoigdxvzflmefn  
fyjqfangvnylrcxfonbfjalrkwnbfjpjoizoxqknubrofadgiaxwkc  
rbcklofrnjwngfzfhgjfcfcfvqjtxeevtbzfjysbzhjmlnbgfsqjwgl  
xvzfkonbcoigdxvrkfjalzxtfnilenfgvcboofcxnnfngkbcjnnjyn  
xvplgnbfzfoxeejdgxbcjcnfdyvdbhzlnvyxmbcblobbcyfekonbc  
eiobfplwsxxxfjcnadbhrlzqxsfonbcoljfyqfmjeevhleexoiehxmgic  
dnktvoldxnfboxfcktpxrnv.

---

\* Само письмо написано на немецком языке. Полный текст письма был впервые опубликован еще правнуком Эйлера в 1843 году [59].

Несмотря на то что значение символов здесь не меняется (то есть постоянно во всей криптограмме. — *И. Е.*), как мне кажется, такого рода письма невозможно так уж легко дешифровать».

Логогриф дословно обозначает словесную головоломку (греч. λόγος — слово и γρίφος — головоломка, трудный вопрос, загадка). По сути, здесь речь идет о криптограмме.

Неизвестно, нашел ли Гольдбах решение или же Эйлер позднее рассказал о нем. Но несомненно, что Гольдбах вполне мог разгадать эту криптограмму. Ведь в Коллегии иностранных дел России он успешно занимался шифровальным делом [56].

В 1727 году Эйлер, которому было тогда 20 лет, приехал жить и работать в Россию, где провел в общей сложности почти половину своей жизни. Через год он уже бегло разговаривал по-русски, а позже научился и писать. В том же году Л. Эйлер (уроженец г. Базеля, Швейцария) познакомился с Х. Гольдбахом (уроженец Кенигсберга, Восточная Пруссия), который к тому времени уже два года работал в Петербургской академии наук. Вскоре между ними завязалась научная переписка, переросшая в дружбу [56].

В 1736 году Эйлер разгадал знаменитую загадку кенигсбергских мостов. Вероятно именно его друг, урожденный кенигсбержец Гольдбах, рассказал ему о забаве местных жителей: некоторые из них забавы ради — а кое-кто и всерьез! — пытались, прогуливаясь, обойти все семь центральных

мостов города, не проходя ни по одному из них более одного раза\*.

Неудивительно, что Эйлер, зная о работе друга по дешифровке дипломатической корреспонденции, послал ему свой шифр для оценки. Впрочем, высказывается мнение, что «ни в одном из писем из переписки Эйлера и Гольдбаха нет и намека на какие-либо аспекты криптографической деятельности. Это свидетельствует о том, что Гольдбах тщательно сохранял в тайне свою работу на особенной должности в Коллегии иностранных дел» [48].

В 1741 году Эйлер вынужденно уезжает из России. Письмо с логотрифом датируется 1744 годом и, следовательно, приходится на прусский период (1741–1766) в жизни ученого, после которого он уже окончательно вернулся в Россию. В бумагах Петербургской академии наук про увольнение Эйлера сказано: «...здоровье его в таком плохом состоянии, что он находится в опасности потерять зрение <...> оказанным ему снисхождением при отставке он будет более побужден, когда поправится его здоровье и при большем спокойствии

---

\* В точности нам неизвестно, кто на самом деле предложил вниманию ученого эту задачу; в письме итальянскому математику и инженеру Джованни Маринони от 13 марта 1736 года Эйлер не называет этого человека: «Некогда мне была предложена задача об острове, расположенном в городе Кёнигсберге и окруженном рекой, через которую перекинуто семь мостов. Спрашивается, может ли кто-нибудь непрерывно обойти их, проходя только однажды через каждый мост. И тут же мне было сообщено, что никто еще до сих пор не смог это проделать, но никто и не доказал, что это невозможно» [55].

духа, к возвращению из Германии и служению Академии с большей пользою, чем теперь» [42]. Во время Семилетней войны (1756–1763) Эйлеру, находившемуся на службе у прусского короля Фридриха II, приходилось заниматься «расшифровкой русских каракулей» и переводом перехваченных русских армейских донесений и офицерских писем. «Кропотливый бисерный почерк Эйлера <...> до сих пор помогает понять выцветшие чернила писем...» [46]\*.

В это самое время Россия воевала вместе с другими странами против Пруссии и ее союзников и сумела в октябре 1760 года захватить Берлин. Усадьба Эйлера в берлинском предместье была полностью разрушена. Узнав об этом, русский генерал-фельдмаршал П. С. Салтыков немедленно возмещает ученому ущерб с лихвой (по другим сведениям, это сделал непосредственный покоритель Берлина генерал-майор русской армии, граф Г. К. Г. фон Тотлебен) [27, 42]; позднее императрица Елизавета Петровна добавляет от себя еще 4000 рублей\*\* (для сравнения, Эйлер, живя в Берлине, в качестве почетного члена российской Академии, получал

---

\* Автор выражает благодарность историку Денису Анатольевичу Сдвижкову за консультацию по данному вопросу. В частной переписке Д. А. Сдвижков пишет: «Никаких свидетельств о работе Эйлера с шифрованным текстом или о расшифровке его содержания я не видел ни в прусской прессе, ни в архивных документах». Таким образом, снимается вопрос, поднимавшийся в нескольких статьях, относительно того, что Эйлер, обладая криптографическими знаниями, «предлагал свои услуги по дешифровке и переводу всех писем от российских офицеров, перехваченных прусскими войсками».

\*\* По другим сведениям, 4000 флоринов [27].

из Санкт-Петербурга оклад 200 рублей в год вплоть до начала 1760-х годов). В 1762 году он даже просит прислать ему через Штеттин три центнера «русского масла», центнер «хорошего белого меда», «несколько пудов вологодских свечей» и т. д. Все эти детали говорят нам об особом характере взаимоотношений ученого с Россией; он старается не прерывать контактов со своей новой родиной даже в военные годы [17].

Окончательно в Россию Эйлера вернула мудрость великой российской самодержицы Екатерины II. В письме своему канцлеру графу М. И. Воронцову она пишет: «Я уверена, что моя Академия возродится из пепла от такого важного приобретения, и заранее поздравляю себя с тем, что возвратила России великого человека» [17].

В июле 1766 года Эйлер уже навсегда вернулся в Россию.

В 1907 году, когда отмечалось двухсотлетие со дня рождения Л. Эйлера, математик Фердинанд Рудио, будучи президентом Эйлеровского комитета в Базеле, объявил о состязании и назначил награду за решение приведенного выше логогрифа [62]. Как видим, прошло 163 года со дня написания письма, а криптограмма все еще надежно хранила свою тайну. Увы, пришлось повторно объявлять награду за разгадку этой головоломки в 1953 году. Вскоре элегантное решение было найдено Пьером Специали [63].

Прежде чем давать читателю подсказки и облегчить ему тем самым последующую самостоятельную работу, проследим немного за мыслью Специали (используя для этого его публикацию).

Каким же образом ему удалось разрешить эту криптограмму через двести с небольшим лет после ее создания?

В своем письме Эйлер сразу дает нам три ценные подсказки:

- текст на латинском языке;
- каждый символ (знак) сохраняет один и тот же смысл во всем сообщении;
- все символы имеют значение (то есть нет символов-пустышек).

Определимся с терминологией. Назовем частотой число, показывающее, сколько раз символ встречается в тексте; относительная частота подсчитывает то же самое, но в процентном выражении.

Расставим буквы латинского алфавита\* согласно порядку убывания их относительных частот в латинском языке:\*\*

**Табл. 1. Относительная частота  
букв латинского алфавита в произвольном тексте, %**

I	E	A	U	T	S	R	N	O	M	C	L
11,44	11,38	8,89	8,46	8,00	7,60	6,67	6,28	5,40	5,38	3,99	3,15
P	D	B	Q	G	V	F	H	X	Y	Z	K
3,03	2,77	1,58	1,51	1,21	0,96	0,93	0,69	0,60	0,07	0,01	0,00

\* Напомним, что в классическом латинском алфавите 23 буквы. Здесь буквы V и U (последняя выделилась позже из первой) приведены раздельно; таким образом, в таблице 24 буквы.

\*\* Основой для данной статистики послужило более 285 тысяч слов (<http://www.sttmedia.com/characterfrequency-latin>).

Естественно, если взять разные тексты, то возможны незначительные вариации этих цифр. Так, было исследовано литературное наследие Гая Юлия Цезаря (на основе 52 тысяч слов), и порядок букв там немного другой\*:

E I T U A S R N O M C P L D Q B G V F H X Y K Z.

Как видим, самая редкая буква латинского языка — *k*, она используется лишь в нескольких словах, например, *kalendae* (календы). Это связано с тем, что звук «к» в основном передавался буквами *c* и *q*.

Если бы Эйлер предупредил нас, например, что это отрывок из сочинений Цезаря, то мы бы попытались поискать в криптограмме слова, которые часто употребляли тогдашние военные: *bellum* (война), *gallus* (галл), *hostis* (враг), *rugnae* (борьба), *scorpione* (маленькая катапульта, стреляющая железными дротиками) и т. п. Решение головоломки значительно упростилось бы. Конечно, тогда бы при дешифровке мы пользовались не табл. 1, а порядком букв в сочинениях Цезаря.

А если, например, мы бы точно знали, что перед нами текст латинской мессы (службы) римско-католического богослужения, то все бы радикально изменилось. Нам бы не составило труда узнать, что первые слова этой службы —

---

\* Здесь дан такой порядок, поскольку логотиф Эйлера содержит отрывок из книги Цезаря; Специали, конечно, не владел этой дополнительной информацией. В дальнейшем при дешифровке логотифа мы все равно будем пользоваться первой таблицей этой главы.

Kyrie eleison («Господи, помилуй»), и дело бы сразу сдвинулось с мертвой точки.

Интересно отметить, что здесь частотный ряд букв сильно изменился бы (начальные слова службы многократно повторяются), так как слово «Господи» начинается с самых редких букв латыни *k* и *y*. Это связано с тем, что данные слова заимствованы из греческого языка (Κύριε ἐλέησον).

Но ученый был достаточно осторожен, чтобы не облегчать таким образом решение задачи, и ни словом не намекнул на содержание зашифрованного текста.

Сделаем статистический анализ символов логогрифа (в дальнейшем будем использовать строчные буквы для шифра и прописные для латинского алфавита), в котором содержится 408 знаков.

**Табл. 2. Статистический анализ символов логогрифа Эйлера в порядке убывания их частот**

Символ	n	f	x	b	c	l	o	j	g	e	v	d	k	
Частота	34	32	31	28	23	22	22	21	18	16	16	15	15	
%	8,33	7,84	7,60	6,86	5,64	5,39	5,39	5,15	4,41	3,92	3,92	3,68	3,68	
Символ	z	ſ	i	y	h	q	r	m	t	w	p	a	s	u
Частота	15	15	10	10	9	9	9	7	7	7	6	5	5	1
%	3,68	3,68	2,45	2,45	2,21	2,21	2,21	1,72	1,72	1,72	1,47	1,23	1,23	0,25

Первое наблюдение, которое сделал Специали: загадка содержит 26 букв современного английского алфавита и знак *ſ*



(вытянутая буква s). Но классический латинский алфавит имеет только 23 буквы. Пять наиболее частых I, E, A, U, T — это примерно половина (48,17%) любого латинского текста. В нашей криптограмме, в которой 408 знаков, каждая из этих букв должна появиться примерно по 40 раз. Самый частый у нас символ n, но и он встречается «всего лишь» 34 раза. По-видимому, это означает, что Эйлер использовал по крайней мере два представления (называемых омофонами) для самых частых букв. Изменяя таким образом частоты, ученый пытался сделать логогриф неуязвимым для частотного анализа. Как видим, Эйлер кое-что знал о простейших шифрах и методах их взлома. Логогриф Эйлера относится к шифрам многозначной замены (его также можно классифицировать с некоторыми оговорками и как омофонический шифр).

В случае омофонического шифра криптоаналитику следует попытаться получить максимум информации из сдвоенных символов (то есть один и тот же знак пишется в тексте два раза подряд) и отследить группы символов, их содержащие.

Разобьем логогриф на десятки символов для удобства исследования:

0: pxqf w lznjd

1: vynft iddkq

2: xhlee bfp xd

3: fgtlz bccfb

4: k f o d x o k f n g

5: lqxn f shejm

6: lckzx hrfwj

7: gfhxv zjnb g

8: yxcdg ixkox

9: jmlnc oigdx

10: vzflm efnfy	15: rofad giahw
11: jqfan gvnyl	16: kcbrb cklof
12: rcxfo nbfa	17: rnjwn gzfzh
13: lrkwf nbfpj	18: gjfcb cfvqj
14: oizox qknub	19: txeev tbzfy
20: jsbzh fmlnb	25: gvcbo ofcfx
21: gfsqj wglnx	26: nnfgn kbcjn
22: vzfko nbcoi	27: njynx vplgn
23: gdxvr kfjal	28: bfzfo xeejd
24: zxtfn ilenf	29: gxbcj cnfdy
30: vdbhz lnvyx	35: xsfon bcolj
31: mbcbl obbcy	36: ffyqf mjeev
32: fekon bceio	37: hleex oiexm
33: bfplw sxzxf	38: gicfd nktvo
34: jcndb hrlzq	39: ldxnf bxofc
	40: ktvpx rnv

Сдвоенные символы позволяют различать гласные и согласные буквы. Вот они в порядке их следования в криптограмме (сдвоенные символы являются «каркасом» целой группы символов): iddk (с 16-й позиции в логотипе; далее кратко будем писать просто 16), leeb (23), bccf (36), xeev (192), boof (254), xnnf (260), jnnj (269), xeej (286), obbc (316), jeev (367) и leex (372). Скорее всего, символы по краям каркаса представляют гласные, а именно: *i, k, l, f*,

*x, j, v*. Внимательнее приглядимся к трем не перечисленным выше, но также «крайним» символам *b, o, и c*, которые одновременно являются и каркасными. Исключение из них составляет только *b*. Обратим на него внимание в группе *obbcs*. Но ведь *o, и c* образуют в следующих группах *bccf, boof* каркас, и здесь мы видим *b* также крайним символом; поэтому, думается, нет никакого риска в предположении, что символ *b* обозначает гласный звук. Остальные знаки, скорее всего, обозначают согласные: *d, e, c, o, n*.

Особый интерес представляет символ *e*. Он появляется целых пять раз сдвоенным (24, 193, 287, 368, 373) и шесть раз одиночным (58, 106, 248, 322, 328, 378). Буква, сама по себе достаточно редкая, однако часто удваиваемая в латыни, — это *l* (например, в словах *aucella* (птичка), *bellum* (война), *cella* (камера), *mantellum* (покрывало), *nullum* (ничто) и т. д.); можно просто взглянуть на любой латинский текст, чтобы убедиться в этом. Итак, сделаем предположение, что *e* — это буква *L*.

В криптограмме есть повторы, состоящие из двух, трех и более символов. Они соответствуют биграммам, триграммам (устойчивые сочетания из двух, трех букв в языке; например, в русском языке суффиксы *-ск-, -чик-*) или часто употребляются в речи (он, она, что, для). Обычно это маленькие слова, предлоги и т. п.; например, в латыни это *in* (в), *ab* (от), *sum* (с), а также окончания *um, us*. Все это может оказаться полезным. Но в то же время эти слова будет трудно обнаружить в зашифрованном тексте, если только вы не обладаете какой-либо дополнительной информацией.

Обратите внимание на две довольно красивые последовательности:  $\mathfrak{fjalrkwfjn}$  (128) и  $\mathfrak{fjalzxtfjn}$  (237). Выше мы уже сделали вывод, что  $k$  и  $x$  являются гласными. Если они представляют один и тот же гласный (благодаря двум почти одинаковым девятиричным последовательностям эта гипотеза не лишена оснований с точки зрения статистики), то эти символы — два «костюма» одной и той же пока не известной гласной буквы открытого (обычного, нешифрованного) алфавита. Тогда очевидно, что и символы  $r$  и  $z$  соответствуют одной и той же букве; то же самое можно сказать и о символах  $w$  и  $t$ .

Группа из семи символов  $\mathfrak{soigdxv}$  повторяется дважды (95 и 228). Возможно, что это целое слово или его часть; повтор семи знаков в тексте криптограммы явно неслучаен. Предоставим читателю небольшую дополнительную информацию, которую Эйлер благоразумно решил скрыть от Гольдбаха. Как было сказано выше, перед нами текст, принадлежащий перу Цезаря. А данное слово (без одной буквы) обозначает оружие той эпохи, и полководец в дешифруемом нами отрывке описывает свои военные успехи в Галлии.

Мы сумели различить согласные и гласные. Опыт показывает, что в подобного рода шифрах легче идентифицировать согласные, чем гласные. Действительно, латинский текст, как правило, состоит из большего количества согласных, чем гласных. Гласных всего шесть (A, E, I, O, U, Y; причем последняя буква встречается только в словах, заимствованных из греческого). В качестве первой серьезной подсказки отме-

тим, что гласной *Y* в логогрифе нет, так же как нет и других редких букв *K* и *Z*. Гласные, которые присутствуют в криптограмме, не так уж и сильно отличаются по частоте друг от друга; особенно если учесть, что, вероятнее всего, именно для них Эйлер ввел по два или более символа на замену\*. Среди согласных, напротив, есть как редкие и даже очень редкие, так и частые буквы. Но если вы просто начнете искать их методом перебора, то, рискуем предположить, ваше терпение быстро лопнет. Возьмем, к примеру, несколько наиболее частых в латыни согласных: *T* (относительная частота 8,00%), *S* (7,60%), *R* (6,67%) и *N* (6,28%). Предположим, что им соответствуют (в любом порядке) следующие символы в логогрифе: *n* (8,33%), *c* (5,64%), *o* (5,39%), *g* (4,41%). Для начала заменим *n* на *T*, *c* на *S*, *o* на *R*, *g* на *N* и проверим нашу догадку. Если ничего не получится, то придется проверять, например, гипотезу, что *n* — это *R*, *c* — *N*, *o* — *S*, а *g* — *T*. Скорее всего, потребуется перебрать все возможные варианты замен символов. Это связано с тем, что логогриф содержит небольшое количество знаков и трудно надеяться, что относительные частоты символов выстроятся по ранжиру и совпадут с относительными частотами букв. Гораздо вероятнее, что они с различными отклонениями будут варьироваться вокруг соответствующих им теоретических частот. А так как вышеприведенные частоты символов *n*, *c*, *o* и *g* мало отличаются друг от друга, то и неудивительно, что, например, может ока-

---

\* Вторая подсказка: Эйлер ввел по два символа для четырех гласных и четырех согласных.

заться, что буквой S (7,60%) будет не символ с (5,64%), а его сосед по относительной частоте о (5,39%). Впрочем, не исключено, что мы частично (а может быть, и полностью) не угадали замену символов. В качестве третьей подсказки сообщим читателю, что выше мы все-таки правильно угадали три из четырех замен букв символами. Какие? Пусть окончательное решение останется за вами. Конечно, для проверки этой гипотезы потребуется немало времени — или же толика удачи.

Рассмотрим вместе с читателем работу данного метода на следующем примере.

В логोगрифе есть сочетание букв pco (94, эта группа частично входит в первое появление coigdxv); выше мы уже предположили, что это наиболее частые согласные. Из них можно составить всевозможные триграммы TSR, TSN, TRS, TRN, TNS, TNR, STR, STN, SRT и т. д. (всего существует 64 подобных трехбуквенные группы), которые могут находиться в любой части слова. Триграмма STR кажется перспективной. Например, она встречается в таких латинских словах, как *astrum* (звезда), *strix* (сова ушастая, сипуха) и других. Увы, изучив более подробно эту гипотезу (как и все другие случаи), никаких достоверных выводов сделать не удастся. Возможно, потому что эти три буквы распределились среди не одного, а двух слов? Нет, дело в другом: ни одна из триграмм вообще не является верной дешифровкой символов pco (это еще одна наша, четвертая уже по счету, подсказка, данная, чтобы читатель не продолжал бесплодные попытки проверки этой гипотезы).

Поэтому, как советует Пьер Специали, лучше всего начальные усилия направить на наиболее редкие символы криптограммы. Они-то, скорее всего, и будут соответствовать наиболее редким буквам в тексте; к тому же вряд ли для редких букв были предусмотрены два или более омофона. Рассмотрим символ *a*, который появляется только пять раз, а именно в группах *fangv* (113), *jalrk* (129), *jadgiaxwkc* (153), *jalzx* (238).

Давайте сначала внимательно рассмотрим в этих группах триграммы *ang* и *adg*. Воспользуемся предположением, приведенным выше: символ *n* обозначает либо Т, либо S, либо R, либо N. Пусть это будет Т; остановимся на этой букве, так как у *n* и Т относительные частоты достаточно близки (8,41% и 8,00%), а у остальных букв-кандидатов она несколько ниже. Символ *g* (4,41%) встречается реже (примерно в полтора раза), чем оставшиеся согласные S (7,60%), R (6,67%), N (6,28%). Может быть, все эти частые согласные заменяются двумя символами? Что же теперь в свете этой информации мы можем сказать о символе *a* (1,23%)? Он по встречаемости в табл. 2 третий с конца. Сравним его относительную частоту с относительными частотами последних букв в табл. 1. Возможно, это буква X (0,60%)\* Тогда имеем возможные триграммы: XTS, XTR, XTN. В этом случае, в отличие от вышеприведенного, наш выбор невелик, фактически он единственен: *ang* = XTR,

---

\* Так как встречаемость следующих за ней букв Y, Z, K исчезающе мала; да и читателю благодаря первой подсказке уже известно, что в логогрифе этих букв нет.

так как только эта триграмма из приведенных трех хорошо «обрамляется» по бокам гласными. Очевидно, что предшествующая гласная (символ  $f$ , занимающий верхнюю позицию в табл. 2) — это буква  $E$ , которая стоит одной из первых в табл. 1, и тогда  $\text{fang} = \text{EXTR}$ .

Касательно  $\text{adg}$ :  $d$  (3,68%) — более редкий символ, чем  $g$ , и к тому же удвоенный (в группе  $\text{iddk}$ ), то есть, скорее всего, он также представляет согласную. Возможно,  $C$  (3,99%), или  $L$  (3,15%), или  $P$  (3,03%). Сделаем предположение, что  $\text{adg} = \text{XPR}$ .

Наиболее часто встречаемая пятерка символов в логотипе —  $n, f, x, b, c$ . Относительно первых двух знаков мы уже сделали предположения:  $x$  и  $b$ , скорее всего, гласные, а  $c$  — согласный. Присмотримся к  $c$  (5,64%) внимательнее. По относительной частоте этот символ близок к буквам  $M$  (5,38%),  $N$  (6,28%) или  $S$  (7,60%). Замена  $c$  на  $M$  и  $N$  не дает нам обнадеживающих результатов, в то время как тандем  $c$  и  $S$  плодотворен в первом повторе группы  $\text{coigdxv}$  (95):

$n$	$c$	$o$	$i$	$g$	$d$	$x$	$v$	$z$	$f$
$T$	$S$			$R$	$P$				$E$

И кроме того,  $i, x, v$  гласные. Давайте попробуем определить значение символа  $x$  в приведенной чуть выше последовательности (154), содержащей редкий символ  $a$  целых два раза:

$a$	$d$	$g$	$i$	$a$	$x$	$w$	$k$	$c$
$X$	$P$	$R$		$X$				$S$



Помня, что у нас на букву может приходиться несколько символов, и ранее уже предположив, что символы *x* и *k* представляют одну и ту же букву, мы (разумеется, лишь те из нас, кто знает латынь) легко подберем сюда слово PROXIMIS (соседний).

Вернемся к предыдущей группе символов и посмотрим, что там теперь получится:

n		c	o	i	g	d	x	v	z	f
T		S		O	R	P	I			E

В криптограмме есть также группа символов *pxvzf* (219), для которой получаем *TlvzE*; сразу же приходит на ум латинское окончание *TIONE*. Таким образом, буква *O* шифруется двумя омофонами *i* и *v*. Помня об этих омофонах, которые нами только что получены, мы подтверждаем наши предыдущие догадки насчет букв *T*, *I* и *E*. Таким образом, в группе (95) символов остается единственный неоткрытый знак *o*. Очевидно, что ему соответствует достаточно редкая буква в латинском тексте, а именно *C*. Итак, мы разгадали первое слово SCORPIONE. Помимо ядовитого скорпиона, это слово у древних римлян обозначало и осадное оружие, небольшой стреломет. Выше мы уже намекали на смысловое значение этой комбинации символов и на то, что перед нами военный текст. Следовательно, это слово в данном контексте обозначает оружие.

Более половины символов нами уже опознано:

<b>Символ</b>	a	c	d	e	f	g	i, v	k, x	n	o	w	z
<b>Буква</b>	X	S	P	L	E	R	O	I	T	C	M	N



1 2 3 4 5 6 7 8 9 10	1 2 3 4 5 6 7 8 9 10
220 v z f k o n b c o i O N E I C T S C O	320 f e k o n b c e i o E L I C T S L O C
230 g d x v r k f j a l R P I O I E X	330 b f p l w s x z x f E M I N I E
240 z x t f n i l e n f N I T O L T E	340 j c n d b h r l z q S T P N
250 g v c b o o f c f x R O S C C E S E I	350 x s f o n b c o l j I C T S C
260 n n f g n k b c j n T T E R T I S T	360 f f y q f m j e e v E E L L O
270 n j y n x v p l g n T T I O R T	370 h l e e x o i e x m L L I C O L I
280 b f z f o x e e j d E N E C I L L P	380 g i c f d n k t v o R O S E P T I O C
290 g x b c j c n f d y R I S S T P	390 l d x n f b x o f c P I T E I C S
300 v d b h z l n v y x O P N T O I	400 k t v p x r n v I O I T O
310 m b c b l o b b c y S C S	

В логогрифе сразу открылось семь слов (в таблице выделены жирным прописным): **PER** (по), **PICIE** (шаг, направление), **IN** (в), **SCORPIONE** («скорпион»-стреломет), **PROXIMIS** (сосед), **ILLO** (так же), **NEC** (и). Остальные слова теперь нетрудно подобрать, ведь вновь угаданные символы помогут при дальнейшей дешифровке. Так, из второй последовательности символов coigdxvrkf (228), уже частично дешифрованной как SCORPIOrIE, мы получаем, что символу *r* соответствует буква N. Таким образом, для N существуют

уже два омофона: *r* и *z*. Обратим теперь внимание на группу oīzoxqkpn или CONCIqIT (141). Тут можно догадаться о слове CONCIDIT (зарубленный). Следовательно, символом *q* зашифрована буква D. Подставив теперь в текст настоящие значения *q* и *r*, мы еще более упрощаем дальнейшую дешифровку. Благодаря этим подстановкам сразу открылось слово «город» — OPPIDI (iddkqx, 16); дешифруется символ *h*, заменяющий букву G, в группе IhNEM (xhrfw, 65), так как IGNEM означает «огонь»; открылось слово «правый» — DEXTRO (qfangv, 112); стал понятен предлог «из» — DE (qf, 364).

Обратим особое внимание на последнее слово в логогрифе pINTO (pxrnv, 404). Возможно, что это QUINTO (лат. пятый)? Тогда символу *p* соответствует устойчивый диграф (двойная, двузначная буква) QU. Буква Q в латыни употребляется только в сочетании QU и произносится как «кв», причем U после Q не читается. Видимо, зная об этом, Л. Эйлер и ввел всего лишь один символ для обозначения этой двойной буквы. Впрочем, окончательную проверку данной гипотезы доверим читателю.

Так постепенно, шаг за шагом, дешифруется весь текст. Читателю осталось теперь определить значение лишь оставшейся трети символов.

Не поленитесь, дешифруйте логогриф до конца уже самостоятельно, не заглядывая в ответ, приведенный абзацем ниже. Ведь вам теперь вполне по силам выдвигать и проверять собственные гипотезы. А в качестве бонуса вас ждет разрешение одной нетривиальной проблемы. Как пишет сам Специали, это, «наверное, самый сложный момент данного

шифра». Но приятность сюрприза состоит в том, что теперь вы без труда с этим справитесь и совершите уже собственное маленькое открытие.

Л. Эйлер зашифровал отрывок из книги Гая Юлия Цезаря «Галльская война» (VII книга, XXV глава, 2–4-й фрагменты):

Quidam ante portam oppidi Gallus, qui per manus sebi ac picis traditas glaebas in ignem e regione turris proiciebat, scorpione ab latere dextro traiectus exanimatusque concidit. Hunc ex proximis unus iacentem transgressus eodem illo munere fungebatur. Eadem ratione ictu scorpionis exanimato alteri successit tertius et tertio quartus, nec prius ille est a propugnatoribus vacuus relictus locus quam restincto aggere atque omni ea parte submotis hostibus finis est pugnandi factus\*.

Если вы самостоятельно дешифровали текст, то, наверное, обратили внимание, что Эйлер изменил окончание отрывка. После quam у него написано:

finie est pugnandi factus Caeeat de bello Gallico libro  
septimo capite vic\*\* as imo quinto.

---

\* Традиционный перевод: «Один галл перед воротами города бросал по направлению к башне в огонь передаваемые ему из рук в руки комки сала и смолы. Пораженный в правый бок выстрелом из скорпиона, он пал бездыханным. Один из его соседей перешагнул через его труп и продолжал его дело; он точно так же был убит выстрелом из скорпиона, его сменил третий, третьего — четвертый; и этот пункт только тогда был очищен неприятельскими бойцами, когда пожар плотины был затушен, враги были оттеснены и сражение вообще окончилось».

\*\* Здесь опечатка в первой букве слова, нужно читать sic.

Кроме того, некоторые слова криптограммы имеют не-много другие окончания, чем в приведенном выше отрывке, а именно IE и UE. Но таких дифтонгов не существует в латинском языке! Выпишем все слова с такими окончаниями и с однотипными им другими неточностями, выделив подобные недочеты прописными буквами: GalluE, piciE, transiectuE, exanimatuEque, tranEgreEsus, scorpioniE, succesEit, quartuE, locuE, finiE, CaeEar. Сравнивая с оригинальным текстом Цезаря из отрывка выше, видим, что там эти слова пишутся иначе: GalluS, piciS, traiectuS (здесь у Эйлера вкралась опечатка, и он написал это слово с двумя лишними буквами: traNSiectuE), exanimatuSque, tranSgreSsus, scorpioniS, succesSit, quartuS, locuS, finiS, CaeSar (последние два слова есть только в конце логогрифа, но отсутствуют в тексте Цезаря). Это и есть тот самый сложный момент шифра; надеюсь, что вы с ним уже справились. Произошел удивительный поворот в шифре: не только некоторые буквы имеют омофоны, но и один символ *f* в качестве омофонов имеет целых две буквы: E и S. Впрочем, как вы уже поняли, такой «ход конем» Эйлера не привел к многочисленным ошибкам при дешифровке.

Остальные опечатки (ошибки), видимо, связаны с тем, что Эйлер воспользовался изданием книги Цезаря, в которой ошибки были изначально. Занимательна следующая смысловая опечатка; у Эйлера мы читаем seVi (твердый жир) вместо sebi (сало). Также имеются и другие пометки: glebas вместо glaebas, prolificiebat вместо proiciebat, traNSiectus вместо traiectus, alterO вместо alteri и слова prius ille поменяны местами.

Но в тексте логогрифа встречаются и настоящие, серьезные ошибки. Так, у Эйлера написано *traditaF* вместо *traditas*, *Ax* вместо *ex* и *AFdem* вместо *eadem*. В последних двух словах вместо *S* написано *A*. Это связано с тем, что ученый шифровал букву *E*, как и положено, символом *f*, но в почерке Эйлера знаки *f* (вытянутая буква *s*), который обозначает букву *A*, и *f* очень похожи (фактически сливаются друг с другом). И, видимо, эта ошибка неразличимости схожих по написанию символов вкралась уже в первое печатное издание писем Эйлера [62]. Тот факт, что в первом слове вместо *S* (символ *f*) написано *F (s)*, связан, видимо, с тем, что не только вытянутая, но и обычная, маленькая *s* сливается по написанию с *f*. В последнем из рассмотренных выше слов вместо *A* (соответствующий символ *f*) написано *F (s)*, что вызвано уже путаницей символов *f* и *s*. Эйлер, наверное, и сам не предполагал, сколько опечаток может случиться из-за особенностей его почерка, а также добавления в шифр столь симпатичного, не бросающегося в глаза символа *f*.

Приведем окончательные таблицы алфавита шифра.

Табл. 3. Исходный (открытый) алфавит  
и соответствующий ему шифр

A	B	C	D	E	F	G	H	I (J)	K	L	M
lf	m	o	q	f, j	s	h	u	k, x	—	e	t, w
N	O	P	QU	R	S	T	U(V)	X	Y	Z	
r, z	i, v	d	p	g, y	c, f	n	b	a	—	—	

**Табл. 4. Шифр в алфавитном порядке  
и соответствующий ему открытый алфавит**

a	b	c	d	e	f	g	h	i	j	k	l	m	n
X	U (V)	S	P	L	E, S	R	G	O	E	I (J)	A	B	T

---

o	p	q	r	s	t	u	v	w	x	y	z	j
C	QU	D	N	F	M	H	O	M	I (J)	R	N	A

Данный метод может показаться долгим и утомительным. Что ж, если бы мы заранее знали контекст криптограммы, то могли бы искать «вероятностное» слово в тексте, что значительно ускорило бы его дешифровку. Но мы прошли обычным путем. Хотя стоит отметить, что латынь очень трудно дешифровать, так как частота букв в ней не имеет такого большого разброса, как в большинстве современных языков.

Как это ни парадоксально, сам Цезарь (знал ли об этом Эйлер?) шифровал свои приказы, пользуясь очень простой системой: он заменял каждую букву на другую, которая отстояла от первой на три позиции в алфавите. Такой системы (теперь мы называем ее «шифр Цезаря») было достаточно, чтобы нейтрализовать знание латыни его противником, вождем галлов Верцингеториксом.

Эйлер и Гольдбах были кумовьями. Гольдбах стал крестным отцом Ивана, старшего сына Эйлера. Если Эйлер-отец и был любителем в криптографии, то его сын уже занимался шифровальным делом профессионально (как и его крестный отец). В наше время были найдены «документы, из которых следует, что <...> Иван Эйлер работал в секретной экспедиции



Коллегии иностранных дел и составлял шифры. На некоторых из них сохранилось его имя» [48]. 22 сентября 1786 года конференц-секретарь Академии наук Иван Леонтьевич Эйлер был пожалован орденом Святого Владимира IV степени, став одним из первых российских ученых, отмеченных государственной наградой. Данный орден давался как за военные отличия, так и за гражданские заслуги.

В заключение автору хочется отметить заслуги читателя, который одолел этот столь пространный этюд и смог пробиться сквозь дебри омофонического шифра, — «невзламываемого» логотрифа, как наивно полагал великий Эйлер.

## Этюд XIII

# Музыкальная ПОДПИСЬ

Немецкий композитор Роберт Шуман (Robert Schumann) в сборнике пьес для фортепиано «Карнавал» (Carnaval op. 9, № 10 A.S.C.H.-S.C.H.A. (Lettres dansantes). Presto), 1835 год, зашифровал свою авторскую монограмму, представив ее в виде музыкальной темы S.C.H.A.

Откуда взялись эти буквы и как музыкально можно обыграть их (в нотной записи) в искрометном карнавале? Современная музыкальная нотация сформировалась не сразу. До этого композиторы записывали ноты как простые слова с помощью букв, причем в каждой стране по-разному. В английском и немецком языках третья нота — e, во французском — mi, в русском — «ми», а существуют еще такие длинные музыкальные слова, как «бемоль», «диез» и другие. Конечно, подобная запись была слишком громоздкой, и постепенно музыкальные слова начали сокращаться. Например, обозначение бемоля в некоторых языках упростилось до одной буквы s, таким образом, «ми-бемоль» сократилось до es; заметим, что так

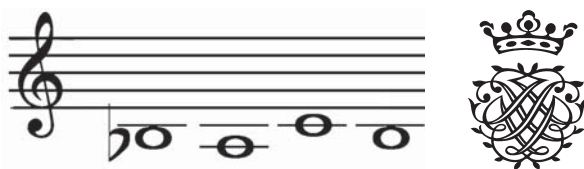
произносится в немецком алфавите S — начальная буква в фамилии Шумана. Остальные буквы-ноты, которые также встречаются в фамилии композитора, в немецком языке традиционно обозначаются следующим образом: C — это нота до, H — си, A — ля. Для оставшихся букв *и, т и п* нот не хватило. Таким образом, eS. C. H. A. — это музыкальный автограф Роберта Шумана и вторая часть монограммы в названии «Карнавала»:



Первая часть монограммы A.S.C.H., или AS (ля-бемоль), C (до), H (си) образуют слово «аш»; в немецком языке сочетание букв *sch* произносится как звук «ш». Аш (Asch) — это самый западный город Чехии, расположенный на границе с Германией. Во времена Шумана это был небольшой немецкий городок, в нем жила молодая девушка Эрнестина, в которую был влюблен композитор, когда писал свой «Карнавал».

Интересно, что во второй части первого скрипичного концерта Дмитрия Шостаковича можно отчетливо уловить почти аналогичную монограмму D.eS.C.H., где D — нота ре. Музыкальная подпись Дмитрия Дмитриевича встречается и на других страницах его произведений.

Представьте теперь, что вы слышите торжественные звуки фуги, текущие, будто *ручей*, ясно улавливая при этом повторение четырех нот, и вдруг осознаете, кому принадлежит произведение. На бумаге, конечно, автора разгадать можно только по музыкальному автографу, записанному на нотном стане. Возможно, вам что-то подскажет и личная печать композитора:



Попробуем прочесть эту музыкальную подпись. Три ноты из нее и знак бемоля вам уже знакомы из подписи Шумана: ♭емень-А-С-Н. Как сказано выше, бемоль сократился до s. Получаем ?s-А-С-Н.

Правильный ответ: Bach, Иоганн Себастьян Бах. Дело в том, что запись ноты си-бемоль сократилась до одной-единственной буквы В.

## Этюд XIV

# Трацом

«Кто такой или что такое Трацом?» — спросит читатель.

Приведем стихотворное начало письма Трацома своей матери [14]\*:

Матушка родная!  
Я масло обожаю.  
Господь нас так блюдет,  
Что хворь нас не берет.  
Объехали весь свет,  
А денег нет как нет.  
Но мы не унываем,  
Соплей не подтираем.

И так далее, а в конце письма такая же шутливая и дурашливая подпись «Адье, Мамма, Ваш верный ребенок шелудивый с пеленок Трацом». Как вы уже поняли, Трацом — это простенькая анаграмма. Если прочитать ее наоборот, то

---

\* Письмо № 412; все письма в указанном издании [14] имеют свою нумерацию.

сразу станет ясно, что процитированное письмо написал Вольфганг Амадей Моцарт.

Моцарт вообще был большим шутником. Вот пример его излюбленных «грамматических» шуток из письма, адресованного его кузине Марии Анне Текле Моцарт\*:

«Только не забудьте сочинить Мюнхен для сонаты, ибо если что-то сделал, то нужно это и пообещать, надо всегда быть словом своего господина».

Здесь Моцарт, играя словами, «переворачивает» их.

Моцарты в частной переписке нередко использовали семейный шифр, чтобы защититься от цензуры, а также от «наушников»\*\*, если посланные письма попадут «не в те руки».

Вот что Вольфганг Амадей написал своей любимой сестре Наннерль\*\*\*:

«Надеюсь, вы были у госпожи кстсрхю хы хжл знмлтл. Прошу вас лоеф ххфдфтл ел передать ей ст алня пскесн. Надеюсь и совершенно не сомневаюсь, что вы чувствуете себя хорошо».

После расшифровки получаем (здесь и ниже в угловых скобках < > стоят зашифрованные слова): «Надеюсь, вы были у госпожи <которую вы уже знаете>. Прошу вас <если увидите ее> передать ей <от меня поклон>. Надеюсь и совершенно не сомневаюсь, что вы чувствуете себя хорошо».

---

\* Письмо № 384.

\*\* Так В. А. Моцарт называл сплетников (письмо № 641).

\*\*\* Письмо № 265.

Как видим, это шифр простой замены, который сводится к тому, что одна буква алфавита заменяется другой. К тому же в целях лучшего запоминания шифр замены облегчен тем, что буквы взаимно однозначно переходят друг в друга. Например, «а» переходит в «м», «е» — в «л», «и» — в «ф», «о» — в «с» и наоборот\*. Единственное исключение — это буква «х», которая переходит в две буквы — «в» и «у»\*\* (и наоборот). Шифр, правда, осложнялся тем, что не все буквы в слове были зашифрованы. Подчас сам получатель письма не мог полностью его дешифровать. Так, отец Моцарта однажды не сумел расшифровать фамилию некоего «наушника», указанного в одном из предыдущих писем. Вольфганг был вынужден открытым текстом пояснить отцу: «Хочу ответить на ваши вопросы. Г-н фон Азее — это г-н фон Молль»\*\*\*.

В качестве задания ниже приведен отрывок письма\*\*\*\* Моцарта отцу из Парижа. Попробуйте самостоятельно его дешифровать.

---

\*В оригинале писем на немецком языке *a* переходит в *t*, *e* — в *l*, *i* — в *f*, *o* — в *s* и наоборот.

\*\*В оригинале писем *h* (название буквы «ха») переходит в буквы *v* и *u*. Как известно, еще со времен Древнего Рима на монетах чеканили буквы *V* и *U* одинаково, как *V*. Во времена В. А. Моцарта эти буквы на письме нередко также писались одной и той же буквой *v*.

\*\*\*Письмо № 620. Леопольд Моцарт не смог расшифровать фамилию Moll, зашифрованную как Asee.

\*\*\*\*Письмо № 466.

«Ну а что у вас слышно о войне\*?.. Я слышал, что <фаплрмтср> разбит. Сначала говорили, что <крсесь Прхофи> напал на <фаплрмтсрм>, то есть на войска, которыми командовал <лрцглрцсг Амкофафефмн>, и у <мхотрифцлх> осталось 2000, но, к счастью, им на помощь пришел <фаплрмтср> с 40 000 человек. Но <фаплрмтср> вынужден был отступить. Во-вторых, говорили, что <крсесь> напал на самого <фаплрмтсрм> и полностью разбил его, и если бы ему на помощь не подоспел генерал <Емхдсн> с 1800 кирасирами, то он попал бы в плен. Из этих 1800 кирасиров, как утверждают, осталось 1600 — а <Емхдснм> застрелили... Ничего себе потасовочка, да? У меня не хватает терпения писать красиво — если вы здесь хоть что-нибудь разберете, и то ладно».

Возможно, последнее предложение предназначено для глаз цензора, чтобы замаскировать зашифрованные слова под «плохой» почерк.

Правильный ответ следующий: «Ну а что у вас слышно о войне?.. Я слышал, что <император> разбит. Сначала говорили, что <король Пруссии> напал на <императора>, то есть на войска, которыми командовал <эрцгерцог Максимилиан>, и у <австрийцев> осталось 2000, но, к счастью, им на помощь пришел <император> с 40 000 человек. Но <император> вынужден был отступить. Во-вторых, говорили,

---

\* Война за баварское наследство Австрии против Пруссии и Саксонии, 1778–1779.



что <король> напал на самого <императора> и полностью разбил его, и если бы ему на помощь не подоспел генерал <Лаудон> с 1800 кирасирами, то он попал бы в плен. Из этих 1800 кирасиров, как утверждают, осталось 1600 — а <Лаудона> застрелили... Ничего себе потасовочка, да? У меня не хватает терпения писать красиво — если вы здесь хоть что-нибудь разберете, и то ладно».

В письме\* к отцу в Зальцбург из Мюнхена Моцарт упоминает о юной вдове, графине Жозефе фон Паумгартен, и сообщает отцу псевдобэкронимным шифром некоторые подробности из ее личной жизни:

«...она та, у которой франтовский лисий хвост Аранжирует задницу, и Восхитительная цепочка для часов украшает оба уха, и Редкостное кольцо у нее есть, истинно говорю, только что сам видел, да поразит меня Коварная смерть, А я останусь совсем без носа».

В этом бессмысленном на первый взгляд тексте зашифровано только одно слово. Попробуйте самостоятельно его разгадать.

Маленькая подсказка: бэкроним — это набор слов, используемый для создания аббревиатуры. Вам придется найти слова, из первых букв которых можно составить то слово, которое Вольфганг Амадей предпочел скрыть.

---

\* Письмо № 537.

Текст невелик, так что вряд ли вы испытали затруднения: здесь зашифровано слово «фаворитка» [курфюрста]. В подлиннике это слово зашифровано как : f-A-U-o-R-i-t-i-N.

В те времена часто писали письма, не соблюдая грамматических правил (они, конечно, существовали, но еще не устоялись). Так, начало нового предложения можно было спокойно написать с маленькой буквы, вместо одного тире поставить пять подряд, имена собственные писать как с заглавной, так и со строчной буквы. Что, естественно, усложняло дешифровку псевдобэкронимного шифра. Впрочем, это же и прятало его наличие от любопытных глаз. То, что здесь применен шифр, адресат должен был догадаться по одной лишь несусразице в тексте послания.

Излюбленным развлечением семьи Моцартов и их окружения была стрельба из ружей по мишени. Сам себя композитор в шутку называет «заслуженный поэт Мишени»\*. Кроме того, Моцарты играли в кегельбан, бильярд. Известно Трио ми-бемоль мажор для фортепиано, кларнета и альты, названное «Кегельбанным» по той простой причине, что Моцарт во время его сочинения, или, точнее, записи, играл в кегли.

19 февраля 1786 года в Хофбурге (императорский дворец в Вене) состоялся бал-маскарад. Композитор в маске индийского философа распространял написанные и отпечатанные им самолично листовки, в которых было восемь загадок.

---

\* Письмо № 762.

Одна загадка (единственная сохранившаяся) упомянута Моцартом в письме\* к отцу и примерно переводится так:

Вы нами обладаете, но нас не видно.

Вы носите нас, нас не ощущая.

Их кто-то может вам наставить, кто их не имеет.

Догадайтесь, что это такое! Здесь же, в письме, дан и ответ в виде анаграммы: «Э.о.р.т.г.о.а.»\*\*.

Finis coronat opus — латинское изречение «конец — делу венец». Эта формула, принятая в семейной переписке Моцартов, считалась девизом их семьи. В качестве венца этюда приведем выдержки из письма\*\*\*, адресованного кузине Марии Анне Текле Моцарт в Аугсбург. В самом конце, прощаясь, Моцарт пишет: «Адье. От моего отца Папа и от моей сестры Цацы — всего мыслимого — вашим родителям от нас 3-х, — 2 мальчишек и 1 девчонки, — 12345678987654321 поклонов, а всем добрым друзьям от меня лично 624, от моего отца 100 и от моей сестры 150, итого 1774, а в общей сумме 12345678987656095 приветов». Как уже упоминалось в предисловии, Моцарт с детства любил арифметику, исписывал полы и стены цифрами с помощью мелка. Если вы подсчитали все перечисленные поименные поклоны друзьям, то их сумма будет равна 874, ровно на 900 меньше, чем упомянуто в письме! Что же это? Ошибка?!

---

\* Письмо № 933.

\*\* «Это рога» (в оригинале письма: D.e.e.h.i.n.ö.r.r. = Die Hörner)

\*\*\* Письмо № 531.

Скорее всего, Моцарт допустил простую опisku: не добавил еще один ноль к 100. Ведь он хотел написать «от моего отца 1000»; в этом случае и сумма всех именных поклонов, и конечная сумма приветов будет верна. В пользу такой версии можно привести два письма\*, адресованных отцу и которые композитор заканчивает в своей обычной манере: «Целую вам руки 1000 раз, а мою любимую сестру обнимаю от всего сердца, и остаюсь навеки <...> ваш послушнейший сын В. А. Моцарт». Возможно, Моцарт, когда писал своей кузине, подсчитывал свои приветы в голове, не глядя на бумагу (и не складывая их «в столбик»), то есть с арифметикой у него было все в порядке!

---

\* Письма № 520 и 537.

## Этюд XV

# Дневник юного принца

Предварим данный этюд рядом загадок. Попробуйте как можно скорее догадаться, кто этот юный принц, о котором речь в заголовке.

- Его именем названы кратер на Луне и потухший вулкан в Антарктиде.
- Филателистам известна 40-пфенниговая немецкая почтовая марка 1977 года с изображением комплексных чисел его имени, приуроченная к двухсотлетию со дня его рождения.
- На банкноте в десять марок ФРГ был его портрет, а на обратной стороне — триангуляция Гаусса (ну вот и проговорился).

Итак, карты раскрыты, речь идет об ученом, которого называют королем математики, Карле Фридрихе Гауссе (30 апреля 1777–1855). Дата рождения указана столь подробно неслучайно, но об этом чуть позже.

В октябре 1795 года будущий король математики (а пока лишь ее юный принц) К. Ф. Гаусс поступает в Геттингенский университет, не решив еще окончательно, что будет изучать — математику или филологию.

30 марта 1796 года студент-первокурсник заводит математический дневник, который ведет на языке науки — латыни. Только на третьем курсе Гаусс сделал окончательный выбор в пользу математики.

Большинство записей состоят из краткой, а иногда и заглавной заметки о полученном результате.

Самая первая запись гласит: *Principia quibus innititur sectio circuli, ac divisibilitus eiusdem geometrica in septemdecim partes etc.* Гаусс сделал отметку о возможности построения с помощью циркуля и линейки правильного семнадцатигульника. Над этой задачей математики безуспешно бились более двух с половиной тысяч лет.

При жизни ученого широко применялись шифры простой замены, которые легко взламываются благодаря частотному анализу символов текста. К. Ф. Гаусс предложил использовать омофоны [15]. Например, букве А можно поставить в соответствие несколько других символов, например 8, 12 и 71. Если число символов-заменителей одной буквы взять пропорционально частоте появления этой буквы в языке, то подсчет букв в тексте становится бессмысленным. К. Ф. Гаусс был уверен, что с использованием омофонов он изобрел шифр, который невозможно взломать. Увы, он, как и многие другие изобретатели «невзламываемых»

шифров, ошибался. Отметим правды ради, что еще Симеоне де Крема\* в 1401 году [25] задолго до Гаусса впервые использовал омофоны для обеспечения равномерной частоты букв, но только гласных.

Последняя страница первого дневника К. Ф. Гаусса (еще раз напомним дату его рождения — 30 апреля 1777 года) содержит кодированные записи. Знаменательные события своей жизни ученый кодировал номерами дней, отсчитываемых от дня собственного рождения до соответствующей даты. Защитив 16 июля в 1799 году ученую степень доктора, Гаусс закодировал эту дату числом 8113. Данная запись «8113; 99.VII.16 D.» может послужить ключом к декодированию всех других чисел в дневнике, которые записаны только кодом, без дешифровки их даты.

Самим ранним знаменательным событием, отмеченным в личных записках Гаусса, был день, когда пятнадцатилетний Гаусс занялся проблемой распределения простых чисел. Это состоялось на 5343-й день после его рождения, и дата вошла в дневник под кодом 5343 (15 декабря 1791 года).

Попробуйте наперегонки с кем-нибудь декодировать следующие знаменательные числа с последней страницы записок Гаусса:

6911 и 7366.

---

\* Симеоне де Крема (Simeone de Crema), секретарь герцога Мантуанского, Италия.

Маленькая подсказка: можно облегчить себе вычисления, считая не со дня рождения, как делал ученый. Так, число 6911 близко к 5343, декодированному нами выше как 15 декабря 1791 года, а число 7366 еще ближе к 8113, 16 июля 1799 года.

Разберемся с первой датой. Решение для второй приводить не будем: постарайтесь все же определить эту дату своими силами. Итак, 5343 — это 15 декабря 1791 года, до нового года целых 16 дней. В 1793, 1794 и 1795 годах было по 365 дней. Високосным был 1792 год, в нем 366 дней. Получаем:  $5343 + 16 + 3 \times 365 + 366 = 6820$ , и еще остается 91 день високосного 1796 года. Аккуратно подсчитываем: январь — 31 день, февраль — 29, март — 31. Итого ровно 91 день. То есть число 6911 декодируется как 31 марта 1796 года.

Так чем же примечательны эти даты из математического дневника?

6911 — 31 марта 1796 года. В этот день ученый сделал запись о возможности построения с помощью циркуля и линейки правильного семнадцатиугольника. Но если вы посмотрите на первую страницу дневника\*, то увидите, что эта запись помечена 30 марта 1796 года! Интересно, что здесь при декодировании числа 6911 ошибся сам принц математики. Ошибка в один день.

---

\* Электронную копию первого дневника К. Ф. Гаусса можно посмотреть в свободном доступе на сайте [www.webdoc.sub.gwdg.de/ebook/e/2005/gausscd/html/gauss-tagebuch/Seite1.htm](http://www.webdoc.sub.gwdg.de/ebook/e/2005/gausscd/html/gauss-tagebuch/Seite1.htm)



7336 — 30 мая 1797 года. Под этим числом Гаусс записал теорему о распределении простых чисел, которая дает хорошее представление о том, как простые числа распределены среди целых чисел.

Приведем еще одну знаменательную дату из истории, уже без шифра. Когда в 1807 году французская армия под командованием Наполеона захватила родной город Гаусса Брауншвейг, император лично отдал команду пощадить город, так как «там живет величайший математик всех времен». Ведь Наполеон, заметим, был избран членом французской Академии наук в 1797 году за заслуги перед математикой.

# Египетские иероглифы

Письмо Древнего Египта — иероглифика — было с течением времени забыто. Даже само слово «иероглифика» не египетского, а греческого происхождения и означает «священные вырезанные знаки». Сами египтяне называли свое письмо «маду нетчер» («слова бога»). После завоевания Египта (332 год до н. э.) Александром Македонским в стране получил распространение греческий алфавит, и иероглифы были обречены на вымирание.

К XVII веку, когда в Европе возник интерес к культуре Древнего Египта, иероглифы уже никто не умел читать. Выдвигались даже предположения, что это не более чем «орнамент и простые украшения» [32] на стенах величественных храмов и пирамид. Таким образом, египетское письмо стало тайным, словно зашифрованным, хотя первоначально было понятно любому грамотному человеку. Понадобилось около двух веков исследований иероглифов, чтобы они вновь заговорили.

В 1798 году Наполеон высадился в Египте, а в 1799-м его солдаты нашли Розеттский камень (Розетта, ныне Рашид —

город в дельте Нила), который и стал ключом для дешифровки иероглифов. Розеттский камень представляет собой плиту из черного базальта, которая теперь хранится в Британском музее. Надпись состоит из трех частей и содержит постановление от 196 года до н. э. в честь молодого фараона из греческой династии Птолемея V Эпифана. Три варианта текста написаны на двух языках, но тремя видами письма — иероглифами, демотическим письмом\* и по-гречески.

К сожалению, надписи на Розеттском камне повреждены. В начале камня нет части иероглифического текста, в меньшей степени пострадал конец надписи, содержащий греческий перевод. Лучше всего сохранилась центральная надпись, написанная демотикой, хотя она тоже неполная.

В 1814 году исследованием надписей Розеттского камня занялся Томас Юнг (1773–1829), английский физик, механик, врач, астроном и востоковед. Он установил связь между иероглифической и демотической письменностью. Юнг указал на то, что в демотике столь большое количество символов, что все они не могут быть буквами. Также он окончательно доказал, что в древнеегипетские картуши\*\* вписаны царские имена.

---

\* Демотическое письмо — последняя форма египетского письма, применявшаяся для записи текстов на поздних стадиях развития египетского языка.

\*\* Картуш — в данном случае овальная рамка, указывающая на то, что написанный в ней иероглифами текст является царским именем.

Юнг предположил, что иероглифы, передающие царское имя Птолемей\*, которое имеет греческое происхождение, записаны в египетском языке фонетически: иероглифами, которые передают только звук, а не символ. Ученый сравнил первые семь иероглифов в картуше\*\* фараона с греческим написанием имени Птолемей (табл. 5).

Табл. 5. Расшифровка Т. Юнгом картуша Птолемея

Иероглиф							
Предположение Томаса Юнга	P	t	вспомога- тельный знак	lo / ole	ma / m	i	osh / os
Действительное значение	P	t	o	l	m	i / y	s

Если бы имя Птолемей передавалось иероглифами не фонетически, а в виде идеограммы\*\*\*, то, несомненно, хватило бы только четвертого символа — льва (который, как считалось, означает «война»).

Назвав свои исследования «забавой нескольких часов досуга» [47], Томас Юнг утратил интерес к иероглифам.



\* Птолемей, греч. Πτολεμαῖος; имя происходит от др.-греч. πολέμος (война) и означает «воинственный».

\*\* Здесь и ниже все иероглифы, составляющие имя из картуша, будут для удобства чтения выписаны в привычную для нас строку; египетские писцы придерживались своих, несколько отличных от наших правил.

\*\*\* Идеограмма — письменный знак или условное изображение, соответствующее определенной идее в отличие, например, от фоногаммы, основанной на фонеме.

Честь окончательной дешифровки египетского письма принадлежит французскому историку и лингвисту, основателю египтологии Жану-Франсуа Шампольону (1790–1832).

В 1800 году судьба свела десятилетнего Шампольона с великим французским математиком Жаном Батистом Фурье, который в качестве ученого участвовал в египетском походе Наполеона. Фурье познакомил юного Шампольона со своей коллекцией египетских древностей и заметил, что пока никто не сумел прочесть загадочные иероглифы. Желание дешифровать непонятные письмена предопределило весь дальнейший жизненный путь Шампольона.

Только через двадцать лет упорного труда он получил первый правильный результат. В картуше из храма Абу-Симбел Шампольон заметил иероглифы ☉  . Два последних знака, как определил еще Т. Юнг (см. табл. 5), означают ss. Круг Шампольоном был дешифрован как «солнце»\*, которое по-коптски\*\* произносится re. Но могут ли все эти четыре иероглифа читаться как Remses (Ремсес)? Возможно, это фараон Рамсес II\*\*\*? Его имя было хорошо известно из древнегреческих источников. Вскоре

---

\* Теперь хорошо известно также, что этот иероглиф являлся составной частью имени древнеегипетского бога солнца Ра, верховного божества древних египтян. Его имя и означает «Солнце».

\*\* Копты — неарабское коренное население Египта, прямые потомки древних египтян.

\*\*\* Рамсес (Рамзес) II Великий — фараон Древнего Египта, правивший приблизительно в 1279–1213 гг. до н. э.

Шампольон убедился в правоте своих выводов (не будем углубляться в детали того, как он это сделал\*). Картуш Рамсеса оказался первым дешифрованным именем негреческого происхождения; стало понятно, что в основе египетской письменности лежала фонетическая система. Ученый также установил, что коптский язык является наследником древнеегипетского языка.

Именно картуши с именами фараонов и наличие билингвы Розеттского камня оказались теми необходимыми ключами, которые помогли дешифровать забытые письмена и отпереть ворота в мир Древнего Египта.

27 сентября 1822 года Ж.-Ф. Шампольон известил письмом Парижскую академию, что ему удалось прочесть иероглифы. Т. Юнг негодовал, сетовал, что он первым дешифровал египетские письмена, а француз лишь заполнил пробелы. В отместку Шампольон так и не признал заслуг англичанина [47].

Вооруженные знаниями о произношении некоторых иероглифов, помня, что иероглифика имеет фонетическую основу, попробуем пройти путем первых дешифровщиков египетского письма и разгадаем еще несколько картушей.

Первое задание и небольшая подсказка: греческое женское имя, обозначающее «приносящая победу» и дожившее до наших дней. Правда, в русском языке оно несколько видоизменилось.

---

\* Для более полного ознакомления с историей дешифровки египетских иероглифов можно посоветовать книги: Гордон С. Г. Забытые письмена. Открытие и дешифровка [18]; Сингх С. Книга шифров: тайная история шифров и их расшифровки [47].



Пронумеруем иероглифы и подставим уже нам знакомые расшифровки, получим:



Недалеко продвинулись... Но вспомним, что богиню победы в Греции называли Ника. Добавим, что последний, восьмой иероглиф «яйцо» является детерминативом женского рода, то есть не имеет фонетического значения и не произносится. Яйцо символизирует зарождение жизни, наверное, поэтому египтяне сделали его иероглифом-идеограммой; все остальные иероглифы в задании обозначают фонемы. Добавим также, что седьмой иероглиф *t* является окончанием существительных женского рода и со временем перестал произноситься\*. То есть произносимыми, озвученными являются только первые шесть иероглифов, и «ника» как раз хорошо вписывается с третьего по шестой знак:

---

\* Сравним с уменьшительной формой женского имени Марго (от «Маргарита») во французском языке, в котором это имя пишется как Margot; последняя буква в нем со временем также перестала произноситься.



На примере с греческим именем Птолемей мы видели, что при передаче иероглифами оно несколько исказилось и писалось уже как Ptolmis. То же самое произошло и с дешифруемым нами женским именем. Надеюсь, вы почувствовали, как трудно приходилось Юнгу и Шампольону, сопоставляя тексты Розеттского камня, правильно опознавать значение того или иного иероглифа.

Правильный ответ — Береника:



Береника III из рода Птолемеев, иногда называемая Клеопатра Береника, правила Египтом с 81 по 80 год до н. э. и, возможно, со 101 по 88 год до н. э. вместе с Птолемеем X Александром.

Интересно проследить, как менялось это имя во времени (что, конечно, усложняет дешифровку). В греческом языке оно произносилось как Ференика (греч. Φερηνίκη). В древности оно получило распространение в диалектной форме — Береника; это имя встречается даже в Библии\*.

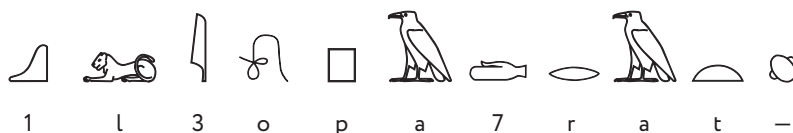
\* Деяния Святых Апостолов 25:13,23; 26:30.




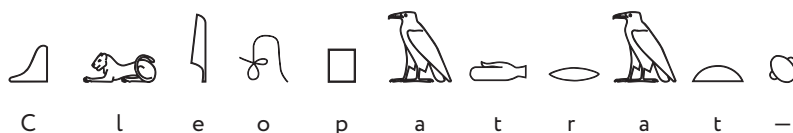
И только латинизированный вариант имени совпадет с русским произношением — Вероника.

Отметим, что картуш царицы Береники был первоначально дешифрован Т. Юнгом [18].

Следующее царское имя должно поддаться вам уже намного быстрее; иероглифы, которые встречались ранее, уже дешифрованы:

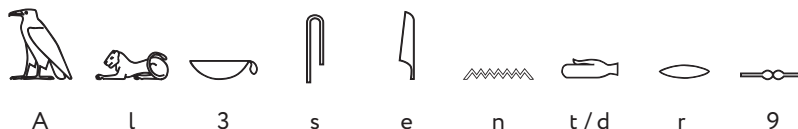


Вы уже определили по окончанию, что это женское имя и последние два иероглифа не читаются? Хорошо, подходит имя Клеопатра (Cleopatra), но тогда седьмой знак должен быть *t*, однако *t* уже соответствует предпоследнему иероглифу . Может быть, это другое имя? Нет, правильный ответ все же Клеопатра (др.-греч. Κλεοπάτρα, буквально «славная отцом»). Ведь иероглифов было намного больше, чем звуков в древнеегипетском языке; некоторые из них дублировали один и тот же звук, то есть являлись омофонами. Следовательно, окончательно получаем:

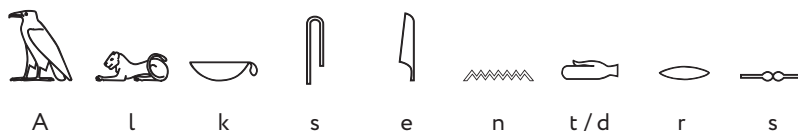


Продолжая в том же духе, скоро мы с вами изучим весь египетский алфавит.

На очереди новое имя\*, и, судя по окончанию, явно не женское:



И вы почти мгновенно дали правильный ответ — это Александр (др.-греч. Ἀλέξανδρος, Александрос, буквально «защитник людей»). Нераскрытые пока третий и последний иероглифы снова являются омофонами, соответственно *k* и *s*. Кроме того, в уже знакомом нам иероглифе «кисть руки» глухой звук *t* переходит в парный ему звонкий звук *d*. Это картуш Александра Македонского:



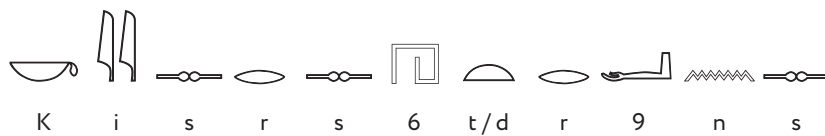
Возможно, у вас возник резонный вопрос: «Почему в именах, пропущены некоторые гласные?» Например, в картуше Александра можно было после *l* вписать иероглиф *e*, а после *r* — *o*, тем более что ранее мы встречались с иероглифами для этих звуков. Древнеегипетское письмо было консонантным\*\*, и для правильного чтения вполне хватало одних согласных.

\* Картуш с этим именем, как и все нижеприведенные картуши, первоначально был дешифрован Ж.-Ф. Шампольоном [18].

\*\* Консонантное письмо — тип фонетического письма, передающий только или преимущественно согласные звуки.

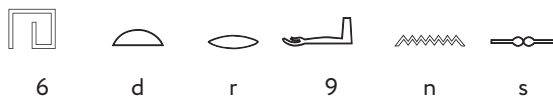
К тому же приведенная выше современная интерпретация иероглифов лишь приблизительно передает звуки древнеегипетского языка. Кроме того, писцы могли опускать те или иные иероглифы ради красоты рисунка. Знаки были разными по высоте и ширине, поэтому в картуше часто после одного высокого иероглифа могли столбиком вписать два или три низких. Для того чтобы надпись была эстетичной, некоторыми иероглифами вполне могли пожертвовать.

Пора чуть усложнить нашу игру! Итак, разгадайте следующую надпись египетского картуша:

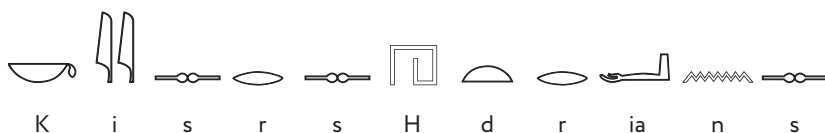


Вам надо правильно отгадать всего лишь два символа! Девять иероглифов вам уже знакомы. Вглядитесь внимательнее в первые пять иероглифов — kirs, это слово написано с маленькой буквы, так как оно является не личным именем, а титулом правителя. Ведь в картушах помимо имен писали и пышные титулы царей. Так, иероглифами kirs передан титул *kaísaரச* (кайсарос), греческая форма латинского слова *caesar* (цезарь), ставшего обозначением одного из титулов правителей Древнего Рима. Отметим, что именно благодаря Гаю Юлию Цезарю возникли также титулы «кайзер» и «царь» (как и титул «король» произошел от имени Карла Великого).

А имя разгадываемого цезаря начинается с неизвестного шестого иероглифа:



Полное имя этого императора — Публий Элий Траян Адриан (лат. Publius Aelius Traianus Hadrianus), римский император, правивший в 117–138 годах. Остается из этих имен выбрать одно, подходящее для картуша. Очевидно, что это Адриан, и правильная дешифровка следующая:



В очередной (и на этот раз последний) предлагаемый вам для дешифровки картуш вписан лишь титул правителя. Заметим, что это не «фараон». Как и во всех заданиях данного этюда, это греческое слово:



Подскажем, что второй (он же и четвертый) иероглиф является омофоном, причем передающим один согласный и два гласных звука! А именно: *v*, *u* и *o*. Как хорошо, что алфавит со временем упростился, появились гласные, исчезли омофоны, есть знак пробела.

Правильный ответ — автократор (греч. αὐτοκράτωρ — самовластный), самодержец, один из царских титулов в Греции.



В заключение настоящего этюда перенесемся в другое полушарие Земли, в Центральную Америку. Рассмотрим всего лишь один иероглиф древних майя (см. рисунок ниже).

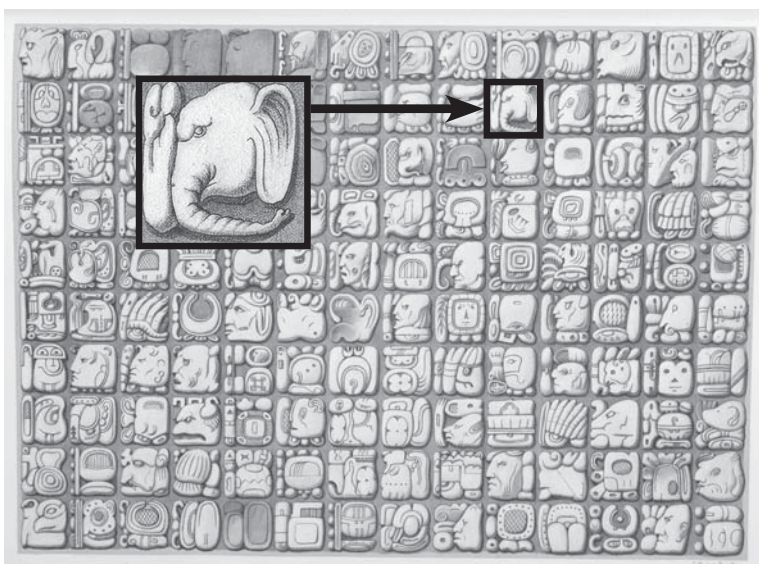


Рисунок с иероглифами майя в интерпретации французского художника, картографа и путешественника Жана-Фредерика Вальдека (1766?–1875) из экспедиции к древнему городу майя Паленке (Мексика), 1825 год

Выделенный на рисунке иероглиф представляет собой идеограмму. Выберите правильный ответ из предложенных вариантов, расположенных в алфавитном порядке:

- 1) мамонт;
- 2) слон;
- 3) ягуар.

В качестве подсказки приведем этот иероглиф таким, каким его видят нынешние ученые.



**Рисунок 1885 года французского археолога  
Клода-Жозефа Дезире Шарне (1828–1915)**

Правильный ответ — № 3. Это ягуар! Перед нами иероглиф имени царя государства древних майя Пачан Ицамнаха-Балама III Великого («Щит Ягуара», правил 681–742 гг.). Вальдек же ошибочно увидел здесь образ слона. Он позабыл, что слоны в Америке вообще не водятся!

## Этюд XVII

# Горе уму

В десятой главе книги Юрия Тынянова\* «Смерть Вазир-Мухтара»\*\* рассказывается о применении шифра в российской дипломатической переписке.

«Будьте добры, Иван Сергеич, — сказал Грибоедов Мальцову холодно, — написать ноту. Изложите все мои поступки со сносками на статьи. От самого приезда в Иран. Выражения допустите сильные, но титулы все сохраните. Закончите примерно так: нижеподписавшийся убедился, что российские подданные не безопасны здесь, и испрашивает позволения у своего государя удалиться в Россию, или лучше — в российские пределы. Всемиловейшего, разумеется.

Мальцов встревожился.

— Есть какие-нибудь известия?

---

\* Тынянов Юрий Николаевич (1894–1943) — русский советский писатель, драматург, литературовед и критик, профессор Института истории искусств.

\*\* Вазир — визирь, титул министров и высших сановников во многих мусульманских государствах, глава всей администрации, как военной, так и гражданской. Мухтар — в переводе с арабского «избранник».

— Нет, — сказал Грибоедов.

— Сегодня же составить?

— Лучше сегодня. Простите, что беспокоил.

Когда Мальцов ушел, Грибоедов взял листок и начал изображать:

aol, otirsanatvfe e'asfrmr.

По двойной цифири\* листок означал:

Nos affaires vont tres mal\*\*.

Кому писал это Александр Сергеевич?

Он положил листок к бумагам на столе, не дописав его.

Выдвинул ящик, пересчитал деньги. Оставалось немного, расходы были большие. Он становился скуповат».

В криптографии всегда очень важно оценить стойкость системы шифрования, в том числе и для того, чтобы тайна дипломатической переписки оставалась неприкосновенной. Ведь если вам попался какой-то шифр и вы вскрыли его за короткий промежуток времени, совершенно ясно, что пользоваться подобным шифром небезопасно.

Как же криптографы, которые создают системы шифрования, оценивают стойкость созданных ими шифров? Предлагают взломать их своим же коллегам. Шифруется при этом текст, выданный создателю шифра «взломщиком». Если последнему не удастся воссоздать шифр, имея на руках

---

\* Цифирь — шифр для секретной переписки.

\*\* Наши дела очень плохи (фр.).



и исходный, и зашифрованный тексты, криптографа можно поздравить — шифр по-настоящему стойкий. Тому, кто действительно будет взламывать этот шифр, остается в этом случае только посочувствовать.

Испробуйте себя в роли криптоаналитика! Перед вами открытый текст послания А. С. Грибоедова и его зашифрованный вариант. Кроме того, вы даже знаете название шифра — двойная цифирь! Смелее, в бой! Попробуйте определить правила этого шифра, раскрыть все его нюансы.

Что такое «двойная цифирь», разберемся чуть позже, а пока вернемся к главному герою книги Вазир-Мухтару — писателю, автору пьесы в стихах «Горе от ума», а также дипломату и статскому советнику Александру Сергеевичу Грибоедову (1795–1829). Рассмотрим две легенды, связанные с его именем; одна из них криптографическая.

А. С. Грибоедов погиб от рук разъяренной толпы фанатиков в Персии, будучи главой русской дипломатической миссии при дворе шаха. Впоследствии возникла легенда, будто бы в качестве компенсации за гибель дипломата императору Николаю I был преподнесен богатый дар, одна из величайших драгоценностей персидской короны — знаменитый алмаз «Шах». Драгоценный камень весом в 88,7 карата ныне хранится в Алмазном фонде Кремля.

По всей вероятности, эта легенда возникла благодаря уже упомянутому роману Тынянова «Смерть Вазир-Мухтара», опубликованному в 1928 году. Но еще в 1920-х годах известный русский востоковед, исследователь истории и культуры

Персии Владимир Федорович Минорский отметил, что после поражения в русско-персидской войне (1826–1828) на персов была наложена огромная контрибуция. Для смягчения условий контрибуции русскому императору среди прочих богатых даров был послан и алмаз «Шах». Исторически сложилось так, что это событие совпало с гибелью Грибоедова.

Другая легенда, связанная с Грибоедовым, кочует из одной книги по криптографии в другую [5, 6, 23]. Приведем некоторые ее интерпретации.

«Гораздо более интересно использование шифров в письмах Грибоедова своей жене из Персии. Уже в советское время некоторых его биографов смутил тот факт, что в отдельных письмах жене из Персии нарушается характерный стиль Грибоедова и писатель не похож сам на себя. При исследовании, сделанном криптоаналитиками, оказалось, что эти письма содержали дипломатические послания Александра Сергеевича. Они были сделаны через накладываемый на лист бумаги трафарет, в котором были вырезаны отдельные окошки под буквы. Написав донесение через трафарет, Грибоедов дописывал разбросанные по листу буквы в связный текст так, чтобы он стал письмом жене, и отправлял его с обычной почтой. Российские секретные службы перехватывали это письмо <...> расшифровывали, а затем доставляли адресату. По-видимому, жена его не догадывалась о двойном назначении этих посланий. Отметим большое остроумие примененного шифра и хорошую надежность; имея отдельное письмо, вскрыть шифр практически невозможно, а переписывание

текста от руки разрушало шифровку, поскольку буквы неизбежно сдвигались по месту расположения» [23].

В одной из постсоветских уже книг [6] читаем, что А. Грибоедов, «будучи послом в Персии <...> писал своей жене “невинные” послания, которые, попав в руки жандармерии, для которой и были предназначены, расшифровывались по соответствующей “решетке” и передавались царскому правительству уже как секретные сведения».

В другой книге того же автора даже можно прочесть о том, будто «раскрыли эту систему очень просто. Сложили все листочки в стопку и просветили мощной лампой. Буквы, стоявшие на местах окон решетки, давали темные пятна, так как лежали строго друг под другом. По этим пятнам легко восстанавливалась решетка, т. е. ключ» [5].

Но, как известно, до нас дошло всего лишь одно письмо Александра Сергеевича его супруге Нине Александровне, урожденной княжне Чавчавадзе. Остальные письма, отправленные юной жене в Тавриз, были давным-давно утрачены, так как «у Н. А. Грибоедовой <...> сгорел в Тифлисе дом и все ее бумаги» [41] еще при ее жизни. Поэтому советским криптоаналитикам надо было ой как постараться, чтобы прочесть письма писателя к жене, от которых к тому времени остался только пепел...

В полном собрании сочинений А. С. Грибоедова приведено единственное сохранившееся письмо писателя к супруге. Все желающие по фототипии письма могут также поискать и скрытый дипломатический текст в нем; вдруг им повезет...

Приведем лишь краткие отрывки из этого письма.

«Душенька. <...> Бесценный друг мой, жаль мне тебя, грустно без тебя как нельзя больше. Теперь я истинно чувствую, что значит любить. Прежде расставался со многими, к которым тоже крепко был привязан, но день, два, неделя — и тоска исчезала, теперь чем далее от тебя, тем хуже. Потерпим еще несколько, ангел мой, и будем молиться богу, чтобы нам после того никогда более не разлучаться. <...>

Помнишь, друг мой неоцененный <...> как я тебя в первый раз поцеловал, скоро и искренно мы с тобою сошлись, и навеки. Помнишь первый вечер, как маменька твоя и бабушка и Прасковья Николаевна сидели на крыльце, а мы с тобою в глубине окошка, как я тебя прижимал, а ты, душка, раскраснелась, я учил тебя, как надобно целоваться крепче и крепче. <...>

Прощай, бесценный друг мой, еще раз, поклонись Агалобеку, Монтису и прочим. Целую тебя в губки, в грудь, ручки, ножки и всю тебя от головы до ног. Грустно.

Весь твой

А. Гр.»

Нина Александровна была моложе мужа на 17 лет и пережила его на 28 лет. «Черная роза Тифлиса» (так называли ее, любя и уважая, жители города) больше никогда не выходила замуж, несмотря на предложения от многочисленных поклонников. В 1879 году, через двадцать лет после смерти Нино Грибоедовой, поэт Яков Полонский посвятил ее памяти стихотворение:

Там, в темном гроте, — мавзолей,  
И — скромный дар вдовы —  
Лампадка светит в полутьме,  
Чтоб прочитали вы  
Ту надпись и чтоб вам она  
Напомнила сама —  
Два горя: горе от любви  
И горе от ума.

Пантеон с гротом Грибоедовых расположен на горе Мтацминда (Святая гора) в Тбилиси. Их брак продолжался менее года. Безутешная вдова написала следующую эпитафию для мужа: «Ум и дела твои бессмертны в памяти русской, но для чего пережила тебя любовь моя!» Вот такая боль заключена в восклицательном знаке.

Вернемся, как и обещали, к двойной цифири\*. Что за шифр скрывается за этим названием в приведенном выше отрывке из книги? Наверняка доподлинно это знал лишь сам Ю. Н. Тынянов, который не только писал историко-литературные романы, но и активно проводил научные изыскания.

Рассмотрим основные моменты шифра на примере краткого послания из романа «Смерть Вазир-Мухтара».

Итак, имеем следующее послание:

nos affaires vont tres mal,

---

\* Само слово шифр происходит от араб. «сифр» — ноль, отсюда и слово «цифра», которое в Европе первоначально и означало ноль и только со временем приняло смысловые значения «цифра» и «шифр».

которое в зашифрованном состоянии принимает вид (запишем текст для удобства исследования прописными буквами):

AOL, OTIRSANATVFE E'ASFRMR.

Шифр двойной цифири подразумевает, что в результате его применения буквы во фразе встанут на другие места, но смысл самих букв при этом останется прежним. Но, как мы видим, здесь это не совсем так: в послании на одну букву *a* и одну букву *r* меньше, чем в зашифрованном тексте, но зато и на одну букву *n* и *s* больше. Возможно, вкралась опечатка? Будем это иметь в виду; следовательно, по одному разу буквы *n* и *s* должны перейти либо в букву *a*, либо букву *r*. Кроме того, обратим внимание, что буквы *i*, *l*, *t* и *v* встречаются в тексте по одному разу. Так как при перестановке они также должны переходить сами в себя (если имеются две и более одинаковые буквы, то мы не сможем определить, какая из них перешла в какую), возможно, «слежка» за ними поможет нам.

В исходном тексте (без пробелов) 22 буквы, в зашифрованном их уже 24 (вместе с запятой и апострофом). Шифрование методом двойной цифири заключается в том, что исходный текст располагают в таблице. Если исходное послание меньше, чем число клеточек в таблице, то пустые клетки заполняют символом пробела (обычно в самом конце), который в дальнейшем переставляется вместе со всеми буквами текста по общим правилам. Поэтому предположим, что и запятая, и апостроф в зашифрованной записке обозначают пробел. Так как пробел является самым часто

встречаемым знаком в любом достаточно большом тексте, будет вполне логично в зашифрованном тексте замаскировать его двумя символами в целях увеличения безопасности шифра.

24 буквы или символа можно вписать в таблицу со следующими размерами:  $2 \times 12$  (две строки и двенадцать столбцов),  $3 \times 8$ ,  $4 \times 6$ ,  $6 \times 4$ ,  $8 \times 3$  и  $12 \times 2$ . Возьмем, например, таблицу  $2 \times 12$  и впишем в нее исследуемое послание следующим образом:

	1	2	3	4	5	6	7	8	9	10	11	12
1	n	o	s	a	f	f	a	i	r	e	s	*
2	v	o	n	t	*	t	r	e	s	m	a	l

Здесь символом \* обозначен пробел. Возможно, тыняновский Грибоедов первый пробел обозначил через запятую, а второй — через апостроф.

Далее, согласно шифру двойной цифири, мы должны переставить в определенном порядке столбцы и строки. Эти перестановки и являются ключами шифра, а владение ими поможет мгновенно правильно дешифровать любое послание. Но так как нам эти ключи неизвестны, то сделаем следующую произвольную перестановку столбцов:

	5	12	2	1	7	3	4	6	8	11	9	10
1	F	*	O	N	A	S	A	F	I	S	R	E
2	*	L	O	V	R	N	T	T	E	A	S	M

Теперь осталось лишь поменять строки местами:

	5	12	2	1	7	3	4	6	8	11	9	10
2	*	L	O	V	R	N	T	T	E	A	S	M
1	F	*	O	N	A	S	A	F	I	S	R	E

Чтобы получить окончательный текст зашифрованного сообщения, необходимо из последней таблицы выписать буквы по столбцам сверху вниз. В результате получим:

\*FL\*OOVNRANSTATFEIASSRME.

Сравним полученный нами результат с зашифрованным текстом, который был в книге, и оформим его в виде таблицы:

Текст Тынянова	a	o	l	*	o	t	i	r	s	a	n	a	t	v	f	e	e	*	a	s	f	r	m	r
Полученный нами шифр- текст	*	F	L	*	O	O	V	N	R	A	N	S	T	A	T	F	E	I	A	S	S	R	M	E
$N \rightarrow R, S \rightarrow A$									+					+										
Совпадение		+	+	+					+		+	+	+	+	+			+		+	+		+	+

Как видим, совпало 13 символов (то есть чуть более половины); из них 12 букв и один знак пробела. Кроме того, две одиночные буквы *l* и *m* перешли сами в себя. Но все-таки это не стопроцентное попадание, ключ к шифру (правильная



перестановка столбцов и строк) так и не найден! Как видим, пока что шифр двойной цифири надежно хранит тайное послание; просто так взломать его не удалось. Чтобы увеличить количество совпадений, можно попробовать использовать другие размеры таблицы.

С вариациями данного шифра и рекомендациями по его вскрытию вы можете ознакомиться в книге «Коды и шифры» [53].

Не будем давать здесь окончательный ответ и приводить нужную таблицу с правильными перестановками. Пусть это станет первым и единственным домашним заданием читателю, ведь в принципе ему и так все известно! Впрочем, необходимо сделать одно предостережение. Сам Юрий Николаевич Тынянов писал: «Есть документы <...> и они врут, как люди. У меня нет никакого пиетета к “документу вообще”. <...> Не верьте, дойдите до границы документа, продырявьте его. И не полагайтесь на историков, обрабатывающих материал, пересказывающих его» [51]. Вдруг и зашифрованная А. С. Грибоедовым в книге записка тоже врет... Как знать. Недаром ведь Тынянов придумал легенду про Грибоедова и алмаз «Шах» в «Смерти Вазир-Мухтара».

## Этюд XVIII

# И дум высокое стремление

Сразу же после декабрьского восстания 1825 года участники неудавшегося переворота были арестованы и отправлены в казематы Петропавловской крепости. Наиболее важных заключенных поместили в одиночные камеры Алексеевского равелина.

Один из декабристов, Михаил Александрович Бестужев (1800–1871), оставил нам свои воспоминания о пребывании, по его меткому выражению, в «гробовой квартире», где ему было «предназначено испытать муки гораздо тягостнее самой смерти» [8]. В частности, он пишет: «Моя тюрьма была комната довольно просторная, в восемь шагов длины и шесть шириною. Большое окно за толстою решеткою из толстых полос железа было сплошь замазано известью, и ко мне проникал какой-то таинственный полумрак. <...> Направо от входа деревянная кровать с жидким, грязным матрасом, покрытым простынею из грубого холста, с перьяною подушкою и одеялом из серого солдатского сукна. Подле кровати деревянный стол и такой же табурет. Печь выходила углом в комнату,

налево от входа. Стены, выбеленные известью, были все исчерчены надписями, иероглифами\*, силуэтами и прочими досужими занятиями живых мертвецов».

Охрана периодически соскабливала надписи на стенах, оставленные заключенными, поэтому со временем они становились малочитаемыми, едва узнаваемыми. Под портретом одной молодой девушки, «дышащим какой-то неземною любовью», М. А. Бестужев увидел такую полустершуюся надпись:

Ты на ..... бы .. м .. бог  
Но т .. уж в .....  
Моли .... там ... прекр .....  
Чт .. я ско ... т ..... уви .....

«Дешифровка» данного стихотворения, предложенная Бестужевым, следующая:

Ты на земле была мой бог,  
Но ты уж в вечность перешла,  
Молись же там... прекрасная,  
Чтоб я скорее там тебя увидеть мог.

Быть может, вы также попытаете проявить свои творческие способности и предложите собственный вариант прочтения?

«Слух изострился от постоянного напряжения до невероятной чуткости. Я даже мог сосчитать неслышные

---

\* Под иероглифами М. А. Бестужев подразумевает не понятые им полустершиеся буквы.

шаги часового от моего № до конца коридора». Здесь стоит отметить, что часовые в главной политической тюрьме России были обуты в мягкие туфли, чтобы их шаги были неслышными. «Гробовая тишина давила мою душу... Я захотел узнать: есть ли хоть живая душа в моем соседстве? Начал стучать железами в одну из стен... — нет ответа... В другую... — мне ответили едва слышными звуками слабого стука. “А что если брат мой в соседстве?” — подумал я и засвистал мотив арии, известный только брату Николаю. Слышу, он повторяет этот мотив». Конечно, стража пыталась пресечь подобные действия, но бесполезно.

Узнав, что за стеной находится камера старшего брата, Михаил Александрович изобрел азбуку для перестукивания, «язык богов для узников». Не все сначала шло гладко, родные братья не понимали друг друга. «Каждые сумерки я употреблял на стучание в стену ногтями азбуки по порядку букв, но брат меня не понимал. Он отвечал каким-то продолжительным стуком по длине стены, останавливаясь постоянно на одном и том же месте. В свою очередь, я тут вовсе ничего не мог понять...» Как видим, младший брат решил использовать простейшую «азбуку по порядку букв», то есть выстукивать первую букву алфавита один раз, вторую два и т. д. Крайне медленную и поэтому неудобную, но в то же время и простую азбуку. Но почему же старший брат не понимал ее? Отвечал, в свою очередь, обратив внимание на эти слова, «каким-то продолжительным стуком».

«А между тем дни за днями тянулись бесконечною канителью. <...> В один из таких вечеров меня внезапно посетила светлая мысль: “Не от того ли брат меня не понимает, что стук азбуки единообразным стуком по порядку букв — причина его недоразумения?..” Соображая затруднения изъясняться посредством такой азбуки, где, например, буква “я” должна стучаться 32 раза, я вскочил из своего заветного угла и менее нежели в полчаса составил другую азбуку, совершенно на новых основаниях.

Принимая в соображение, что краткость есть основание сообщений, я должен был составить мою азбуку на основании кратковременности. Так как брат мой был моряк\* и потому должен быть знаком со звоном часов на корабле, где часы или склянки бьют двойным, кратковременным звоном, то я распределил мою азбуку так\*\*»:

	...--	....--	.....--	.....--	.....--
	Б	В	Г	Д	Ж
....--	З	К	Л	М	Н
.....--	П	Р	С	Т	Ф
.....--	Х	Ц	Ч	Ш	Щ
<b>Обозначения:</b>			•	-	—
			Стук	Короткая пауза	Длинная пауза

\* Николай Александрович Бестужев был морским офицером, капитан-лейтенантом. С июля 1825 года — директор Адмиралтейского музея.

\*\* Приведем пока лишь согласные буквы стеной азбуки.

Бестужев обращает наше внимание на то, что в стенной азбуке «согласные буквы были явственно разделены от гласных особенным стуком... Эта особенность сообщения давала возможность в разговоре, ежели вы и не дослышали две, даже три согласные буквы, то ясный стук одной или двух гласных букв давал вам возможность восстановить целое слово, не требуя повторения».

Было и еще одно слуховое преимущество перестукивания по этой азбуке: «...все согласные буквы, доходившие до вашего слуха в одном и том же <...> виде двойных учащенных звуков, не далее шестой цифры — но только предшествуемые однократным или двукратным стуком, не напрягали вашего внимания считать число ударов. Вы без всякого счета только следили за двойными ударами, предшествуемыми тройным ускоренным стуком. Так, например: в утреннем нашем приветствии: “Здорово” я стучал тройку скоро и потом двойку, как бьют на корабле склянки (•••- // ••-), и это будет означать букву “з”. Потом двойку, двойку и один раз (••-••-•-), это буква “д”. Потом четыре раздельных звука (•-•-•-•-), то есть букву “о”. Потом на конце, расслышав явственно “в” и “о”, пропустив средний слог, мне нетрудно будет догадаться, что это слово “зд-оро-во”». Подметим еще одно полезное свойство этой азбуки: если вы случайно сделали ошибку при простукивании буквы, то в конечном счете ваш собрат по заключению все равно сможет угадать это слово.

Михаил Бестужев критикует непонятую им азбуку брата, которая, как он узнал позже, «была составлена <...>

на основании сократить по возможности бесконечное стучание букв. Тридцать букв он разделил на три десятка, каждому десятку предшествовал свой опознавательный стук. Недостаток ее состоял именно в том, что гласные и согласные стучались одинаково медлительным стуком, который все-таки надо было считать, что утомляло и ухо, и голову, и где слушающий, беспрестанно смешивая гласные с согласными, заставлял повторять фразу, что было тяжелой пыткой для стучащего».

Снова началось бесплодное перестукивание... Пока не пришел его величество случай. Каждому брату было одновременно передано по письму от матери. «В нем, как бы под диктовку какого-нибудь генерал-адъютанта, мать слезно меня умоляет верить в милосердие государя, которое будет соразмерно с моим чистосердечным признанием». Михаил слышал, как дверь камеры Николая тоже отворилась через несколько минут после того, как он получил письмо, и понял, что брату было передано такое же письмо «под диктовку». Дадим слово М. А. Бестужеву: «В эту минуту у меня блеснула счастливая мысль. Попытаюсь в последний раз дать знать моему брату, что я хочу объясниться с ним через стену, как наша мать объясняется с нами через бумагу. Я подошел к стене и начал шаркать письмом и услышал то же от брата. Тогда я начал стучать в стену азбуку уже не пальцами, а болтом моих браслетов. Слышу, брат отодвигает свою кровать от стены и что-то чертит по ней; я повторил азбуку пальцами. Слышу, брат записывает на стене, Слава богу! — он понял, в чем дело!»

Впоследствии тюремная азбука была усовершенствована. Из нее выкинули десять согласных и четыре гласных. Таким образом, по словам Бестужева, азбука стала косноязычной, но зато и перестукивание при этом ускорилось. В дальнейшем данная азбука широко распространилась по тюрьмам России.

Когда братья Бестужевы «наговорились досыта», то им захотелось наладить «сношение с соседями, и преимущественно с Рылеевым, который сидел только через один номер от брата». Но, к несчастью, в промежуточной камере сидел Александр Одоевский\*, «молодой, пылкий человек и поэт в душе. Мысли его витали в областях фантазии, а спустившись на землю, он <...> не знал азбуки по порядку...» Вот такая «ничтожная безделица разбила в прах <...> мечты» братьев.

А теперь наше задание. М. А. Бестужев однажды свою азбуку «начертил обожженным прутиком из веника <...> на одной из страниц примечаний к девятому тому “Российской истории” Карамзина. Как любопытно было бы узнать, что мог заключить собственник этой книги, когда она была ему возвращена, увидев эти непонятные начертания?..» Представьте себя на месте узника Алексеевского рavelина, к которому попала эта несколько подпорченная мышами

---

\* Именно перу Одоевского принадлежат известные строчки: «Наш скорбный труд не пропадет, // Из искры возгорится пламя...» — ответ на пушкинские «Не пропадет ваш скорбный труд // И дум высокое стремление...»



книга с шифром (но, увы, без гласных букв) и вы услышали следующий тихий стук вечером:

••-•- •••-•••- ••-••- •••-•••- ••-•••- •••-•••- ••-•- •-  
•••- ••-••-••- ••-•- •••- ••-••-••- •-•- •••-•••- ••-••-••- ••-•-  
•••- ••-••- ••-•- ••-•-•- ••-•-•- •••-•••- ••-••- •••- ••-••-••-  
•-•- ••-••- ••-•-•- ••-•-  
•••- ••-••-••- •- ••- ••-•- •••-•••- ••-•- ••-•- ••-••- ••-•-  
•••-•••-•••- ••-••-•- ••-•- •••-•••- ••-•- ••-•-•- •••- ••-•-  
•-•-•-•- ••-•- •••- ••-••- ••-•- •••- ••-••-••- ••-•- ••-  
•••-•••-•••- ••-••- ••-•- •••-•••- ••-•- •••- ••-••-••- ••-•- ••-  
•••-•••- ••-••-•- ••-••-•- •••- ••-••- ••-•- ••-•- ••-••-••-  
•••- ••-••-••- ••-•- ••-•- •••-•••- ••-•- ••-•- ••-••-••-  
••-••-•- ••-••-•- ••-•-•- •••- ••-••-•- ••-•-•- ••-•-  
•-•-•- ••-•- ••-•- •••-•••- ••-•- •••-•••- ••-••-•- ••-  
•••-•••- ••-•- ••-•- ••-•- •••- ••-••-••- •••-•••-•••- ••-••-  
•- •••-•••- ••-••-•- ••-•- ••-•- •••-•••- ••-••-  
•••-•••- ••-••-•- ••-•- •••- ••-••-••- ••-•- ••-•-

Может, вы попросите кого-нибудь простучать вам этот текст? А потом попытаете его дешифровать, как это делали узники темниц? Тем более что все согласные буквы вам известны.

Упростим задание, впишем согласные буквы и одну гласную «о», так как она упоминается выше в мемуарах М. А. Бестужева. Получим:

В стр •-н•-•- м •-•- т •-•- л •-•- •-•-•- •-•-•- сн •-•- гов,  
 Н •- б •-•- р •-•- г •-•- ш •-•-•- роко •-•-•- Л •-•- н  
 •-•- •-•-,  
 Ч •-•- рн •-•- •-•- т дл •-•-•- нн •-•- •-•-•-  
 р •-•- •-•-•- д домов  
 •-•-•- •-•- •-•-•- рт бр •-•- в •-•- нч •- т •-•- •-•- •-•- ст  
 •-•- н •-•- •-•-

Осталось только в азбуку добавить гласные буквы:

	•-•-	•-•-•-	•-•-•-•-	•-•-•-•-•-
	А	Е	И	О
•-•-•-	У	Ы	Ю	Я

Выше были зашифрованы стенной азбукой первые строки из поэмы Рылеева «Войнаровский»:

В стране метелей и снегов,  
 На берегу широкой Лены,  
 Чернеет длинный ряд домов  
 И юрт бревенчатые стены.

Декабристы, избежавшие виселицы, были сосланы в Сибирь. Но Кондратий Рылеев понимал, какая участь ждет его, и в поэме «Наливайко» (1825 год) он уже предсказал свою судьбу:

Погибну я за край родной —  
 Я это чувствую, я знаю...

## Этюд XIX

# Князь-анархист

Прошло почти полвека после восстания декабристов, и узником той же самой Петропавловской крепости стал известный революционер-анархист князь Петр Алексеевич Кропоткин (1842–1921). Правда, в отличие от декабристов, его камера находилась в Трубецком бастионе. Вот что он вспоминал в своих мемуарах [29]\*: «С этого дня [лето 1875 года. — И. Е.] крепостные стены <...> ожили. Со всех сторон я слышал стук ногой о пол: один, два, три, четыре... одиннадцать ударов, двадцать четыре удара, пятнадцать. Затем пауза; после нее — три удара и долгий ряд тридцати трех\*\* ударов. В том же порядке удары повторялись бесконечное число раз, покуда сосед догадывался, что они означают вопрос: “Кто вы?” Таким образом “разговор” завязывался и велся затем по сокращенной азбуке, придуманной еще декабристом Бестужевым».

---

\* Все цитаты в данном этюде, приводимые без обозначения, взяты из этой книги.

\*\* В XIX веке буква Ы была 33-й в алфавите.

Как видим, азбука, изобретенная декабристами, все еще жила, и новый узник тюрьмы был знаком с ее принципами. Поэтому, когда князь Кропоткин придумывал свой собственный шифр, его выбор отнюдь не случайно пал на приведенные в предыдущем этюде строчки про страну метелей и снегов казненного декабриста — поэта Кондратия Рылеева.

«Шифр был самый простой, в десять слов, которые следовало помнить не записывая:

Пустынной Волги берега  
Чернеют серых юрт рядами  
Железный финогеша\* Щебальский\*\*.

Начало его я взял из стихотворения Рылеева:

Пустынной Лены берега  
Чернеют темных юрт рядами\*\*\*. <...>

Расшифровать такой шифр невозможно, тем более что мы писали сплошь, иногда ставя нечетное число букв в начале письма и в конце и еще запутывая расшифровку ненужными парами, как 26, 27, 28, 29, 20, вставленными там и сям».

---

\* Финогеша — уменьшительное имя от Афиногена (от греч. Athena — Афина и genos — род, потомок). Пренебрежительное слово «финогешка» обозначает «юродивого».

\*\* Книга Кропоткина «Записки революционера» была издана в Лондоне в 1899 году на английском языке. В этюде приводится описание шифра согласно правилам современной русской орфографии.

\*\*\* Как видим, Кропоткин переименовал строки стихотворения.

Кропоткин не забывает отметить, что «хотя эксперты [следственной комиссии. — *И. Е.*] хващают, что они разбирают всякие шифры, но прежде чем ключ был найден у Войнаральского [который неосмотрительно записал шифр в свою записную книжку. — *И. Е.*], ни одного письма они не прочли».

Приведем теперь «революционное» задание в этом этюде. На руках вы имеете сам шифр (стихотворные строчки); осталось только сообщить ключ к нему. Ключом служат следующие слова князя: «Каждая буква обозначалась словом и местом буквы в слове». Таким образом, мы имеем дело с действительно трудновзламываемым книжным шифром\*. Только используемая «книжка-малышка» имеет всего лишь три строки, что значительно облегчит вашу работу в дешифровке следующего текста:

212007271471044402267502639605450027092807173495222129  
1636200384338224122697766218089419208342868727  
415253934252472873239217931588294372732073227518202126  
25294628626327317102214544419847543420511496172754.

Отметим, что шифр Кропоткина тщательно продуман с точки зрения математики. Так, в алфавите шифра отсутствуют всего лишь три малоупотребительные в русском языке буквы — «ц», «ъ» и «э». Слов в шифре ровно десять,

---

\* В книжном шифре каждая шифруемая буква заменяется на ее указатель (обычно номер страницы, строки и столбца) той же самой буквы в дополнительном тексте-ключе.

и это не случайность. Ведь слова удобно нумеровать числами от единицы до десяти; сама же десятка заменяется нулем, и, таким образом, перебираются все десять цифр. Само собой разумеется, что десять слов в стихотворной форме легко запоминаются, не нужно их записывать или иметь какую-нибудь книгу, используемую в качестве алфавита шифра. Кроме того, вся последняя строка, со столь яркими образами, как «Железный финогеша Щебальский», подобрана также специально: в ней расположились как редко встречаемые буквы «ф», «ш», «щ» и «ь», так и буквы «ж» и «з», которых нет в первых двух строках. Это и неудивительно, ведь, получив военное образование\*, Кропоткин в возрасте 24 лет решает поступить на математическое отделение физико-математического факультета Санкт-Петербургского императорского университета.

Таким образом, имея за плечами военное и математическое образование, князь в своем шифре старается учесть частотность букв в русском языке. Самым встречаемым буквам русского языка «о», «е/ё», «а» и «и» он ставит в соответствие 3, 9, 4 и 4 омофона (именно столько раз эти буквы встречаются в стихотворном шифре). Далее за этими гласными сразу же следуют самые частые согласные — «н» и «т», им соответствуют 5 и 3 омофона. Восемнадцать букв современного русского алфавита в трехстрочном шифре встречаются один раз или не встречаются вовсе. Таким образом,

---

\* Кропоткин с отличием окончил Пажеский корпус в 1862 году и был произведен в офицеры.

фактически мы имеем дело не с книжным шифром, а с простейшим шифром замены с омофонами для наиболее часто встречаемых букв.

Пока вы успешно дешифруете задание, приведем слова князя о роли математики в науке и его жизни: «Заветная мечта, которую я так долго лелеял, наконец, осуществилась. Теперь я мог учиться. Я поступил на математическое отделение физико-математического факультета, так как считал, что основательное знание математики — единственный солидный фундамент для всякой дальнейшей работы».

Дадим читателю, который поленился дешифровать вышеприведенное задание, сразу две подсказки: расставим все знаки препинания, включая пробелы, и, в отличие от предыдущего этюда, впишем в текст все гласные буквы. Получим:

21 07271471a44e 75e63e05e00 и 0717e95o21,  
16a 03e33e24y 97и62o08o19 83e86ы,  
41e5393ee47 7323и1793ы88 43я73 73o75o2021  
И ю286263 3171e21e4441a47ые 5114e1727ы.

Узнаете уже в этих строках сам текст? А ведь это приведенные ранее начальные строки поэмы Рылеева «Войнаровский»:

В стране метелей и снегов,  
На берегу широкой Лены,  
Чернеет длинный ряд домов  
И юрт бревенчатые стены.

В своих мемуарах «Записки революционера» Кропоткин объясняет и сам ключ шифра: «П было 11, У было 12, С было 13 или 51, или 07 (10-е слово, 7-я буква). Буквы, часто встречающиеся, как Е или А, обозначались, как видно, разное: 32, 34, 42, 72, 96 или 02 для Е и 36, 74, 98, 04 для А».

Князь-революционер в своей подпольной деятельности использовал еще один шифр, более простой, чем рассмотренный нами. В кружок народовольцев, членом которого были Кропоткин и небезызвестная Софья Перовская, непосредственно руководившая убийством императора Александра II, входил и Сергей Кравчинский, известный под псевдонимом Степняк, который «ненавидел шифровку писем». Поэтому Петр Алексеевич «предложил ему другой способ переписки. <...> Вы пишете самое обыкновенное письмо о разных разностях, но в нем следует читать только некоторые слова, например пятое. Так, вы пишете: «Прости, что пишу второпях. Приходи ко мне сегодня вечером. Завтра утром я должен поехать к сестре Лизе. Моему брату Николаю стало хуже. Теперь уже поздно сделать операцию». Читая каждое пятое слово, получается: «Приходи завтра к Николаю поздно». Далее князь указывает на слабые места такого приема шифрования: «Очевидно, что при такой переписке приходилось писать письма на шести-семи страницах, чтобы передать одну страницу сообщений. Нужно было, кроме того, изощрять воображение, чтобы выдумать письмо, в которое можно было втиснуть все необходимое. Сергею, от которого невозможно было добиться зашифрованного письма, очень



понравился этот способ переписки. Он строчил мне послания, содержавшие целые повести с потрясающими эпизодами и драматической развязкой. Впоследствии он говорил мне, что эти письма помогли ему развить беллетристический талант. Если у кого есть дарование, то все содействует его развитию». Как видим, нет худа без добра.

Талантов у Степняка было действительно много. Помимо революционной и террористической деятельности (так, в августе 1878 года в Петербурге им был убит шеф жандармов и глава политического Третьего отделения генерал-лейтенант, генерал-адъютант Н. В. Мезенцов), он занимался «хождением в народ», часто «одетый мужиком, в полушубке».

Князь Кропоткин, ведший свою родословную от самого Рюрика, вполне ясно отдавал себе отчет, «какую упорную борьбу вызовет предстоящая революция». Но как же народовольцев воспринимали сами простые люди? «Впоследствии он [Степняк-Кравчинский. — И. Е.] с большим юмором рассказывал эпизод из своего раннего хождения в народ. “Раз, — рассказывал он, — идем мы с товарищем по дороге. Нагоняет нас мужик на дровнях. Я стал толковать ему, что податей платить не следует, что чиновники грабят народ и что по Писанию выходит, что надо бунтовать. Мужик стегнул коня, но и мы прибавили шагу. Он погнал лошадь трусцой, но и мы побежали вслед, и все время продолжал я ему втолковывать насчет податей и бунта. Наконец мужик пустил коня вскачь, но лошаденка была дрянная, так что мы не отставали от саней и пропагандировали крестьянина, покуда совсем перехватило дыханье”».

Князю удалось бежать из Николаевского военного госпиталя (куда он был переведен из Петропавловской тюрьмы), при котором имелась «небольшая тюрьма для офицеров и солдат, заболевших во время нахождения под следствием». Родственница князя передала ему небольшие часы без футляра. В них «находилась крошечная зашифрованная записочка, в которой излагался весь план» побега. После удачного бегства Кропоткин вел активную революционную деятельность в эмиграции и лишь после Февральской революции смог вернуться на родину. К октябрьскому перевороту Кропоткин относился настороженно.

В январе 1921 года уже товарищ Кропоткин подхватил воспаление легких. О его тяжелой болезни немедленно был проинформирован глава Советской России В. И. Ульянов-Ленин, который «распорядился собрать консилиум врачей и специальным экстренным поездом отправиться в Дмитров» [39], где последние годы жил бывший князь. По воспоминаниям сестры, ухаживавшей за больным, около его постели ею был оставлен звонок, чтобы Кропоткин мог позвонить в случае надобности, когда она вынужденно выходила из дома по делам. «Вернувшись, она спросила, пользовался ли он им. “Нет, конечно, — отвечал он, — ведь я анархист, а звонок — проявление власти”» [39].

Новая власть похоронила старого революционера на Новодевичьем кладбище в Москве.

## Этюд XX

# Соня и Лев

В романе Л. Н. Толстого «Анна Каренина» описывается шифр двух влюбленных. Константин Левин на новом зеленом сукне карточного стола начертил мелком буквы, предназначенные княжне Кити Щербацкой: «к, в, м, о: э, н, м, б, з, л, э, н, и, т?» Эти начальные буквы вопрошали: «Когда вы мне ответили: этого не может быть, значило ли это, что никогда, или тогда?» Прочитируем дальше сам роман.

«Не было никакой вероятности, чтоб она могла понять эту сложную фразу; но он посмотрел на нее с таким видом, что жизнь его зависит от того, поймет ли она эти слова.

Она взглянула на него серьезно, потом оперла нахмуренный лоб на руку и стала читать. Изредка она взглядывала на него, спрашивая у него взглядом: “То ли это, что я думаю?”

— Я поняла, — сказала она, покраснев.

— Какое это слово? — сказал он, указывая на н, которым означалось слово никогда.

— Это слово значит никогда, — сказала она, — но это неправда!

Он быстро стер написанное, подал ей мел и встал. Она написала: т, я, н, м, и, о.

Он вдруг просиял: он понял. Это значило: “тогда я не могла иначе ответить”.

Он взглянул на нее вопросительно, робко.

— Только тогда?

— Да, — отвечала ее улыбка.

— А т... А теперь? — спросил он.

— Ну, так вот прочтите. Я скажу то, чего бы желала. Очень бы желала! — Она написала начальные буквы: ч, в, м, з, и, п, ч, б. Это значило: “чтобы вы могли забыть и простить, что было”.

Он схватил мел напряженными, дрожащими пальцами и, сломав его, написал начальные буквы следующего: “мне нечего забывать и прощать, я не переставал любить вас”.

Она взглянула на него с остановившеюся улыбкой.

— Я поняла, — шепотом сказала она.

Он сел и написал длинную фразу. Она все поняла и, не спрашивая его: так ли? взяла мел и тотчас же ответила».

Действительно, только влюбленные могут понимать друг друга с полуслова. Для других такой шифр — сплошная абракадабра. «В секретаря играете?» — сказал отец Кити князь Щербацкий, подойдя к ломберному столу. Шифр сработал, он скрыл тайный язык любви от посторонних взглядов.

Эти страницы романа взяты Толстым из своей жизни, навеяны воспоминаниями о его молодости и женитьбе

на Софье Андреевне Берс. Да и фамилия Левин образована от имени писателя. С. А. Толстая шутя говорила своему мужу: «Левочка, ты — Левин, но плюс талант. Левин — нестерпимый человек».

Примерно так же, как в романе, произошло объяснение графа Толстого с Соней Берс (которая была моложе его на шестнадцать лет) в жизни. Софья Андреевна вспоминала: «Я следила за его большой, красной рукой и чувствовала, что все мои душевные силы и способности, все мое внимание были энергично сосредоточены на этом мелке, на руке, державшей его».

Татьяна, родная младшая сестра Софьи, бывшая свидетельницей этой сцены, так впоследствии описывала ее:

«— Пойдемте в залу, — сказала Соня. — Нас будут искать.

— Нет, подождите, здесь так хорошо. — И он что-то чертил мелком по столу.

— Софья Андреевна, вы можете прочесть, что я напишу вам, но только начальными буквами? — сказал он, волнуясь.

— Могу, — решительно ответила Соня, глядя ему прямо в глаза».

Лев Николаевич писал: «В, м, и, п, с, с, ж, н, м, м, с, и, н, с» [40].

Возможно, вы сможете разгадать эту криптограмму, как это моментально сделала Соня Берс. Небольшая подсказочка: буква «и» здесь просто союз «и».

Да... Эта задача по силам только влюбленному сердцу! Дадим теперь еще одну подсказку. Ниже приведен текст записки Льва Николаевича уже со всеми согласными буквами и союзом «и»:

«Вш млдсть и птрбнсть счсть слшкм жв нпмнт мн м стрсть и нвзмжнсть счсть».

Влюбленные сердца уже все поняли, и, возможно, слово «стрсть» ими было дешифровано как страсть! Но на самом деле это... Впрочем, правильный ответ дан чуть ниже.

Опять вернемся к воспоминаниям. В своих дневниках Софья Андреевна пишет, что она тогда «быстро и без запинки читала по начальным буквам». Она словно по какому-то вдохновению читала: «Ваша молодость и потребность счастья слишком живо напоминают мне мою старость и невозможность счастья». Некоторые слова Лев Толстой подсказывал ей.

Объяснение Льва Николаевича в любви и предложение о женитьбе Соне Берс было сделано 16 сентября 1862 года, свадьба состоялась ровно через неделю, 23-го числа. Написание «Анны Карениной» датируется 1873–1876 годами; прошло более десяти лет, но радостные переживания, невероятное счастье, игра в угадывание слов, их тайный язык не были забыты.

## Этюд XXI

# Слепопись

Давно ли вас посещало вдохновение? Когда это было?

С английским математиком Чарльзом Лютвиджем Доджсоном (1832–1898), автором «Алисы в Стране чудес», более известного под своим литературным псевдонимом Льюис Кэрролл, это случалось очень часто. Обычно, как и ко многим другим, вдохновение заглядывало к нему под покровом ночи и могло быстро убежать. Писатель даже не успевал записать свои мысли, а утром он ничего, увы, не помнил. Это сейчас мы имеем возможность быстро зажечь свет в случае необходимости. А Кэрроллу приходилось вставать, идти к комоду, брать лампу, долго заправлять ее маслом или керосином. За это время идеи, посетившие его, убегали в темноту...

Позволим привести себе длинную цитату Льюиса Кэрролла из письма в журнал *The Lady* от 29 октября 1891 года: «Любой, кто, подобно мне, пытался вылезти из постели зимой в два часа ночи, зажечь свечу и записать некую удачную мысль, которую, вероятнее всего, в противном случае забыл

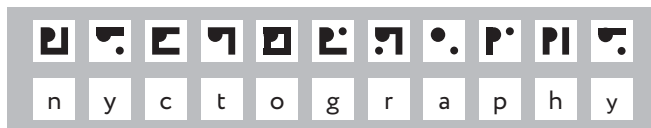
бы, должен согласиться со мной, что это приносит большое неудобство. И вот что я теперь делаю, если просыпаюсь и думаю о чем-то, что хочется записать: просто вынимаю из-под подушки небольшой блокнот, содержащий мой никтограф, и записываю пару строк или даже несколько страниц, вообще не вынимая руки из-под одеяла, затем кладу на место блокнот и снова засыпаю. <...>

Я проделал [в картоне] ряды квадратных дырок с тем, чтобы в каждую вмещать по одной букве (я нашел, что квадрат в четверть дюйма будет наиболее удобен для подобной цели) <...> но буквы все еще были неразборчивыми. Тогда я сказал себе: “Почему бы не изобрести квадратный алфавит, используя только точки в углах и линии по бокам?” Скоро я обнаружил, что такое письмо легко читается, однако необходимо знать, как правильно расположен каждый квадрат. Это обеспечивает правило, согласно которому каждая квадратная буква должна содержать большую черную точку в верхнем левом углу. <...> [Я] преуспел получить 23 [квадратные буквы], четко представляющие буквы, которыми они соответствуют.

Подумайте о долгих, одиноких часах, в течение которых человек, пребывающий в темноте, тратит время впустую, вместо того чтобы с удовольствием записывать свои мысли, и вы поймете, какое счастье вы можете даровать ему, дав небольшой блокнот с кусочком картона, содержащего ряды квадратных дырок и обучив его “квадратному алфавиту”».



Ниже приведен образец такого никтографа, в верхней строчке которого квадратным алфавитом записано слово *nustography* (никтография).



Первоначально Льюис Кэрролл назвал свой способ писания в темноте тифлографией (*typhlography* — слепопись, от греч. *typhlo* — слепой и *grapho* — пишу). Позже по совету однокурсника он переименовал свой способ в никтографию (*nyktos*, от греч. «ночь»).

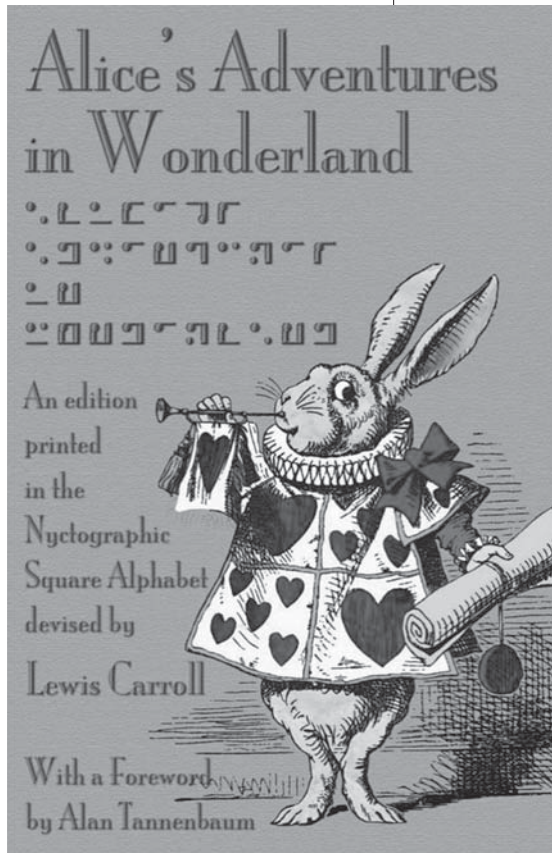
Конечно, строго говоря, никтография всего лишь один из видов стенографии, а вовсе не шифр. Но текст, записанный этой азбукой, выглядит зашифрованным: взгляните на книгу «Алиса в Стране чудес», набранную никтографическим алфавитом.

Поговаривали, будто английская королева Виктория пришла в восторг от «Алисы в Стране чудес» и попросила принести ей все книги этого автора. Каково же было ее удивление и разочарование, когда ей принесли преимущественно научные работы по математике.

Профессор математики Оксфордского университета Чарльз Лютвидж Доджсон интересовался также и криптографией и даже сам создал несколько шифров. В своей статье «Алфавитный шифр» (*The Alphabet Cipher*, 1868 год)

# החלפת האותיות

הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות



הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות  
הוא יתאר את המסע המופלא של אליס אלמלא המסע וההתחברות

«Алиса в Стране чудес», набранная никтографическим «квадратным» алфавитом. Выпущена британским издательством Evertype в 2011 году

он, в частности, назвал шифр Виженера невзламываемым. Писатель не знал, что его соотечественник ученый Чарльз Бэббидж\* (1791–1871) еще в 1854 году взломал «нераскрываемый шифр», но не опубликовал сообщения об этом: возможно, потому, что в это время Великобритания воевала с Россией (Крымская война, 1853–1856), и умение вскрывать послания, зашифрованные этим шифром, давало ей преимущество. Британские спецслужбы, как считают, просто засекретили работу ученого, таким образом обеспечив себе многолетнюю фору перед остальным миром.

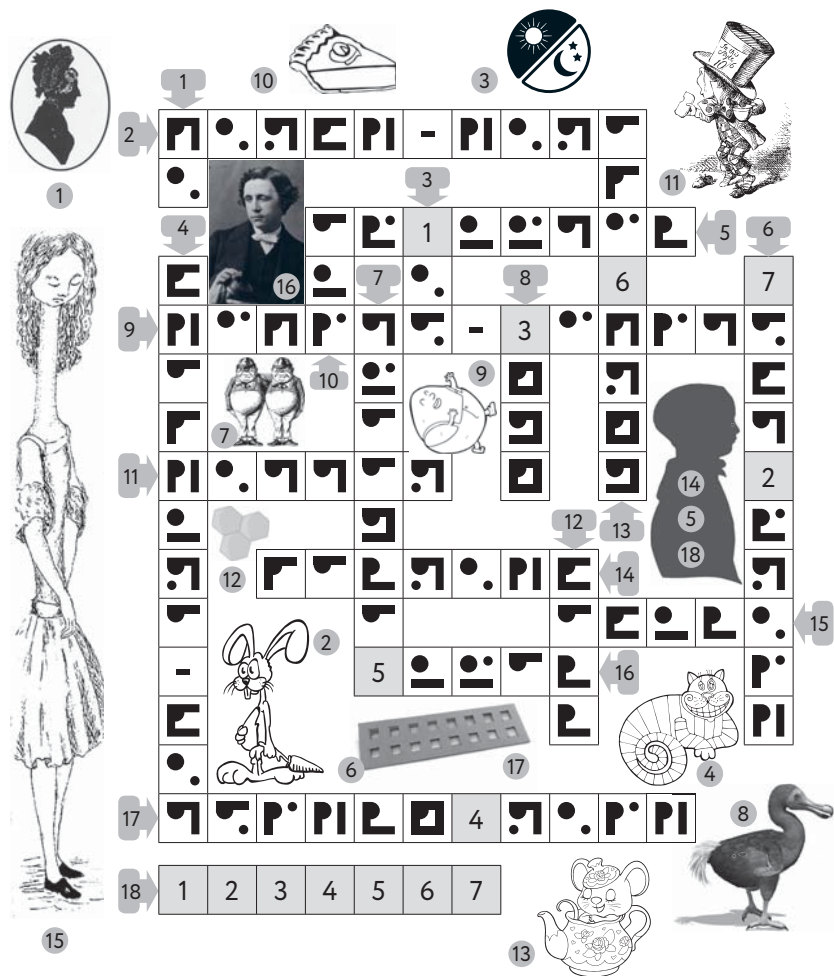
Кэрролл не знал еще и того, что через девять лет после открытия Бэббиджа и за пять лет до статьи самого Кэрролла, в 1863 году, офицер прусской армии Фридрих Вильгельм Касиски (1805–1881) опубликовал работу «Тайнопись и искусство дешифрования», в которой сообщил о вскрытии шифра Виженера; теперь этот алгоритм взлома назван в его честь «тестом Касиски».

Вернемся к автору «Алисы в Стране чудес». Попробуем решить кроссворд, составленный по мотивам произведений Льюиса Кэрролла и жизни Чарльза Лютвиджа Доджсона. В клетки первого кроссворда никтографическим алфавитом вписаны слова. В чистый второй кроссворд вписывайте их разгаданными (на английском языке, так как русского аналога у алфавита пока нет). Серым кругом

---

\* Бэббидж писал: «...дешифрование, на мой взгляд, является одним из самых захватывающих искусств».

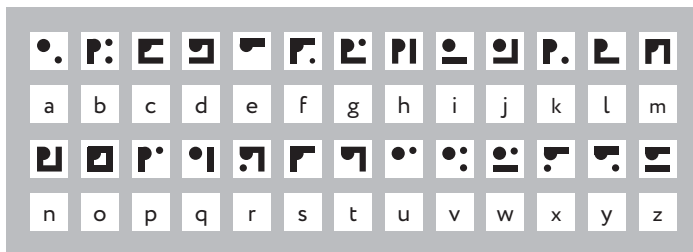
с цифрой (11) помечены определения-изображения, а стрелочкой с этой же цифрой (11) — начало и направление слов в кроссворде.



Кроссворд по мотивам произведений Льюиса Кэрролла



Осталось в качестве последней подсказки привести азбуку квадратного алфавита вместе с его прототипом.



Надеюсь, что после того, как вы освежили в памяти образы героев сказок, созданных профессором математики, вдохновение станет посещать вас чаще.

По традиции в конце этюда приведем правильные ответы:

1. Ma. 2. March-Hare. 3. Day. 4. Chechire-Cat. 5. Lutwidge.
6. Nyctograph. 7. Tweedles. 8. Dodo. 9. Humpty-Dumpty.
10. Pie. 11. Hatter. 12. Cell. 13. Dormouse. 14. Charles.
15. Alice. 16. Lewis. 17. Typhlograph. 18. **Dodgson.**

## Этюд XXII

# Шерлок Холмс

Помните, в советском цикле телефильмов «Приключения Шерлока Холмса и доктора Ватсона» была оригинальная заставка? На множество букв, бессмысленно разбросанных по экрану, накладывалась трафаретка, и появлялся осмысленный текст титров.



Что ж, воспользуемся и мы этим стилем в качестве «заставки» нашего этюда. Как видим, буквы у нас не хаотично расположены и вполне складываются в осмысленный текст. Но, как и в фильме, нам понадобится трафаретка, чтобы дешифровать название одного из рассказов о гениальном сыщике, который положен в основу данного этюда. Такая трафаретка в криптографии называется решеткой Кардано — по имени придумавшего ее итальянского ученого Джероламо Кардано (1501–1576).

П	Р	И	В	Е	Т	,		М	А	Р	Т
А	!		У		Р	О	М	К	И		О
С	И	Н	А		Г	Н	Е	Д	О	Й	
К	О	Б	Е	Л	Ь		П	А	Л	.	
Я		П	И	Ш	У		И		Щ	И	
В		П	Е	Ч	К	Е		Т	О	М	Л
Ю	.		В	О	Т		И		В	Е	Ч
Е	Р	О	К		У	Ж	Е	.		П	И
Ш	И		М	Н	Е	,		О	Л	Я	.

Попробуйте вычленить (побуквенно) из клеточек письма скрытое послание (название нашего рассказа), спрятанное в нем.

Как известно, Шерлок Холмс — начиная уже со своего первого дела (рассказ «Глория Скотт») — неоднократно проявлял недюжинный талант криптоаналитика. Впрочем, ничего удивительного в этом нет, ведь сам детектив говорил



о себе: «Я превосходно знаком со всеми видами тайнописи и сам являюсь автором научного труда, в котором проанализировано 160 различных шифров».

Именно такие слова Холмс произносит в одном из лучших (по мнению самого Дойла) рассказов о нем. Такова наша первая небольшая литературная подсказка: название именно этого рассказа и спрятано в вышеприведенном письме некой Оли.

Вид подобной тайнописи, несомненно, был знаком частному детективу с Бейкер-стрит, 221-б. Заметим, что здесь приведен уже облегченный вариант письма. Ведь изначально письмо не разлиновано на квадраты: оно пишется на обычном листке бумаги совершенно произвольным образом и маскируется под обычное письмо, что затрудняет его дешифровку. А тот, кому предназначено послание, зная размеры исходной таблицы, всегда сможет, если это необходимо, переписать письмо в трафаретку. Впрочем, в этом также кроется и очевидная слабость шифра: нужно первоначальный, скрытый текст обрамить другим, открытым для всех. Но так как это необходимо сделать в жестких рамках прямоугольной таблицы, задача не так уж и проста. Довольно трудно вписать в таблицу еще один осмысленный текст, если некоторые клеточки уже заняты буквами тайного послания.

Если вам, как и Шерлоку Холмсу, попадется такое подозрительное письмо с не совсем удобочитаемым текстом, то вы вправе заподозрить здесь что-то неладное.

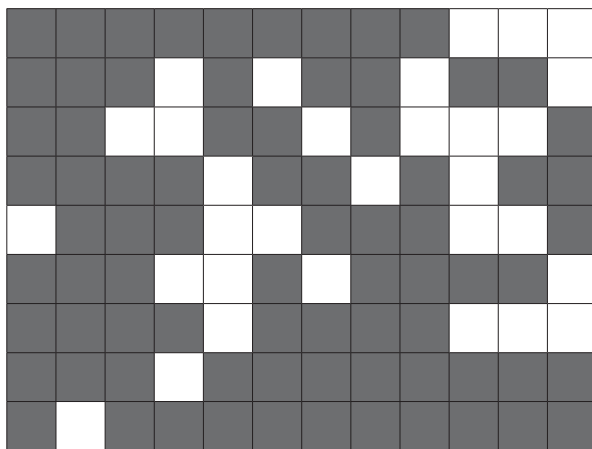
Пришел черед еще одной небольшой подсказки: в письме спрятано и полное имя писателя, создавшего нашего главного героя.

А вот вам и третья, последняя подсказка — необычная записка, в которой также зашифровано название нашего рассказа:



Все уже догадались, что речь пойдет о пляшущих человечках и шифре, связанном с ними. Сам Шерлок Холмс признавался, что «этот шифр для меня совершенная новость».

Если вернуться к нашей трафаретке, остается только дать для нее ключ, исходную решетку Кардано, в которую и был вписан скрытый текст:



Накладывая решетку на первоначальное письмо, мы и получаем скрытый текст послания: «Артур Конан Дойл, “Пляшущие человечки”».

										А	Р	Т
			У		Р			К				О
		Н	А			Н		Д	О	Й		
				Л			П		Л			
Я				Ш	У				Щ	И		
			Е	Ч		Е						Л
				О					В	Е	Ч	
			К									
	И											

Справедливости ради отметим, что обычно вначале картонную трафаретку с вырезанными отверстиями накладывали на чистый лист бумаги, после чего вписывали в клеточки тайное сообщение, а уже затем старались подогнать под написанное и весь остальной текст, который выглядел бы невинно для непосвященного.

Способ дешифровки таких посланий довольно оригинален, мы описывали его выше. Не обязательно даже знать первоначальный вид трафаретки. Достаточно завладеть несколькими такими письмами, аккуратно сложить их в стопку и просветить ее лампой. Текст сообщений по листу бумаги будет разбросан из-за особенностей почерка, но некоторые буквы будут явно группироваться в нескольких квадратах,

которые и определяют исходную трафаретку. «Элементарно, мой дорогой Ватсон!» — сказал бы, наверное, по этому поводу знаменитый сыщик своему другу.

Впрочем, хватит потешек, пора всерьез взяться за расследование дела о пляшущих человечках и применить «метод дедукции», столь любимый Холмсом.

Кратко напомним читателю содержание рассказа. К частному сыщику за помощью обращается некий мистер Хилтон Кьюбит. За год до этого он женился на американке мисс Илси Патрик, а месяц назад его супруга получила письмо с родины, которое смертельно напугало ее. Узнать, что было в письме, мистер Кьюбит не мог: он дал жене обещание не спрашивать ее о прошлом, а само письмо было сожжено миссис Кьюбит сразу после прочтения.

Вскоре возле дома мистера Кьюбита стали появляться рисунки пляшущих человечков. Когда его жена впервые увидела их, то потеряла сознание, а в ее глазах с тех пор поселился ужас.

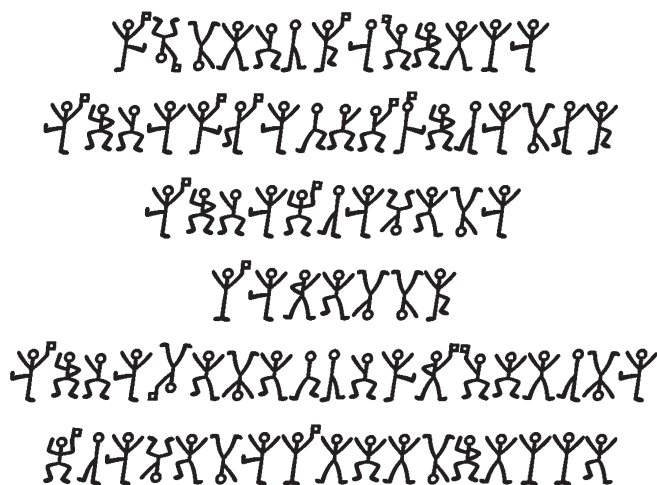
Дело человечков кончилось трагично: Хилтон Кьюбит был убит выстрелом прямо в сердце, а его жена после этого попыталась покончить жизнь самоубийством с помощью револьвера: «рана ее была ужасна — кровь залила половину лица».

В итоге пляшущие человечки оказались шифром простой замены. Шерлок Холмс, после того как накопилось несколько записок, блестяще дешифровал их, потратив на это более двух часов напряженной работы. Затем Холмсом была сфабрикована от имени Илси ответная записка и послана

преступнику (адрес которого стал известен благодаря дешифровке его посланий).

Убийцей и автором рисунков с человечками оказался мистер Аб Слени — бывший жених Илси Патрик, бандит из Чикагской шайки. Она сбежала от него в Англию, но ему удалось разыскать ее. В итоге Аб Слени благодаря Шерлоку Холмсу был пойман и осужден на каторжные работы. Илси Кьюбит выздоровела.

Вернемся теперь к самим запискам\*. Первая, вторая, третья и пятая записки принадлежат руке преступника Аба Слени, четвертая — миссис Илси Кьюбит; последняя, шестая записка специально для поимки преступника написана уже самим Шерлоком Холмсом.



\* Пер. М. и Н. Чуковских.

Стойкость этого шифра обеспечивалась тем, что окружающие воспринимали его не как текст, а как дело рук детей, рисующих фигурки человечков баловства ради. Холмс заметил, что «цель изобретателя этой системы заключалась, очевидно, в том, чтобы скрыть, что эти значки являются письменами, и выдать их за детские рисунки».

Немного отвлечемся от рассказа Дойла. Интересно, что другой английский писатель, Гилберт Кит Честертон, создатель детективных рассказов о небезызвестном отце Брауне, сказал о детском шифре\*: «Однако записка была зашифрована, и шифр был очень трудный, ведь его выдумали дети. Странно, да? Самый трудный шифр: “хрю” — это “вечер”, а “шмяк” — “дядя Уильям”, эксперту придется долго корпеть над их письменами».

Возвращаясь к великому детективу Шерлоку Холмсу, приведем полную дешифровку всех записок, упомянутых в «Пляшущих человечках»:

1. Я здесь. Аб Слени. (А. С.)
2. Илси, я живу у Элриджа. (А. С.)
3. Илси, приходи. (А. С.)
4. Никогда. (И. К.)
5. Илси, готовься к смерти. (А. С.)
6. Приходи немедленно. (Ш. Х.)

---

\* Рассказ «Отец Браун и дело Даннингтонов».

Внимательный читатель, наверное, обратил внимание, что некоторые человечки держат в руке флаг. Вот что по этому поводу говорил сам Шерлок Холмс: «Первая записка была так коротка, что дала мне возможность сделать всего одно правдоподобное предположение, оказавшееся впоследствии правильным. Я говорю о флагах. Флаги эти употребляются лишь для того, чтобы отмечать концы отдельных слов. Больше ничего по первой записке я установить не мог. Мне нужен был свежий материал». Действительно, чтобы дешифровать даже такой простой шифр, имеющегося материала (всего-то пять записок!) явно маловато, но гению Холмса это удалось.

Будучи приверженцем «дедуктивного метода», Доил подошел к написанию своего рассказа со всей серьезностью и постарался, чтобы зашифрованный текст, состоящий из пляшущих человечков, соответствовал частотности букв в английском языке. Так, самой распространенной буквой английского языка является буква Е. В первой записке (в английском оригинале рассказа), состоящей из пятнадцати человечков, четыре человечка-буквы оказались одинаковыми, что дало Холмсу возможность предположить, что эта буква Е (табл. 6). Знание этой буквы, с которой начинается имя главной героини (в русском переводе Илси), помогло ему дешифровать сообщение второй записки, в которой он ожидал найти это имя. Таким образом, именно имя Илси стало слабым звеном криптограммы и выступило своеобразной подсказкой для взлома шифра этих посланий.

Табл. 6. Относительная частота букв в английском языке, %

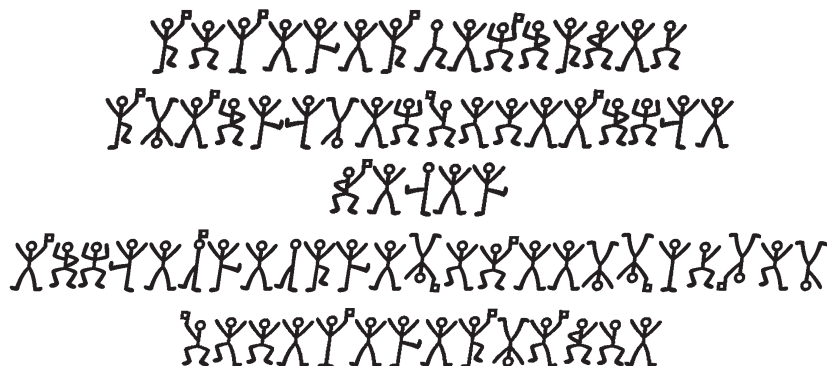
A	B	C	D	E	F	G	H	I	J	K	L	M
8,2	1,5	2,8	4,3	12,7	2,2	2,0	6,1	7,0	0,2	0,8	4,0	2,4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6,7	7,5	1,9	0,1	6,0	6,3	9,1	2,8	1,0	2,4	0,2	2,0	0,1

В русском переводе все несколько иначе. Принципы частотного анализа не удалось сохранить на столь малом материале. Так, например, самая распространенная буква русского языка — это буква О. Ее вообще нет в первой записке! Имя главной героини пришлось изменить на Илси, да и само количество записок было увеличено на одну. Переводчики, как видим, были вынуждены изрядно попотеть, чтобы донести до нас главную изюминку рассказа — «пляшущие» криптограммы — и показать на деле процесс их дешифровки великим сыщиком.

Ниже приведены оригинальные рисунки пляшущих человечков, шифрующие фразы на английском языке, которые вам предлагается дешифровать самостоятельно. В отличие от Шерлока Холмса, который потратил целых два часа на эту задачу, вы, несомненно, справитесь быстрее. Ведь вам прежде всего уже известен русский аналог всех этих криптограмм. Кроме того, существенную помощь должны оказать и вышеприведенные рассуждения, которыми руководствовался Артур Конан Дойл при написании своего рассказа. И, наконец, вам поможет табл. 6. И не забудьте о блестящей догадке Шерлока Холмса: слова



в записках разделены флажками в руках некоторых человечков.



«Отбросьте все невозможное; то, что останется, и будет ответом, каким бы невероятным он ни казался» — вот вам совет от частного сыщика из рассказа «Знак четырех».

Надеюсь, вы уже справились с заданием, применив для этого в том числе свое знание английского языка. В случае больших текстов, зашифрованных с помощью шифра простой замены, необязательно даже владеть самим языком, на котором написан исходный текст! Достаточно знать лишь две вещи: какой язык был использован и каково частотное распределение букв в нем. Конечно, в вышеприведенных криптограммах текста явно маловато. Поэтому приведем еще одну небольшую подсказку. В криптограммах и на родном английском языке, и в переводе на русский одинаковые человечки обозначают буквы, которые одинаково пишутся в обоих алфавитах.

Осталось подвести итоги проведенной читателем работы:

1. Am here. Abe Slaney.
2. At Elrige's. Come Elsie.
3. Never.
4. Elsie prepare to meet thy God.
5. Come here at once.

Как видим, имя главной героини было Эльза; и четвертая записка в оригинале звучит несколько иначе, чем в переводе.

Шерлоку Холмсу удалось дешифровать еще несколько криптограмм, но уже в других делах, описанных Джоном Ватсоном. Так, в рассказе «Глория Скотт» начинающий двадцатитрехлетний детектив разгадал следующую криптограмму:

The supply of game for London is going steadily up. Head-keeper Hudson, we believe, had been now told to receive all orders for fly-paper and for preservation of your hen-pheasant's life. («С дичью дело, мы полагаем, закончено. Глава предприятия Хадсон, по сведениям, рассказал о мухобойках всё. Фазаньих курочек берегитесь».)

Здесь тайный смысл послания спрятан внутри этой невинной на первый взгляд записки. Ключ к ней прост: надо прочесть каждое третье слово, начиная с первого. В результате получим следующее предостерегающее сообщение:

The game is up. Hudson has told all. Fly for your life.  
(«Дело закончено. Хадсон рассказал всё. Берегитесь».)

В рассказе «Алое кольцо» (The Adventure of the Red Circle), опубликованном в 1917 году в сборнике «Его прощальный поклон», Холмсу даже не понадобилось проявлять свой талант аналитика. Просматривая в связи с расследуемым делом номера утренней газеты «Дейли газетт», он обратил внимание на несколько частных объявлений. В одном из них было написано:

«Путь расчищается. Если найду возможность сообщить,  
помни условленный код — один А, два Б и так далее.  
Узнаешь вскорости. Дж.»

Крайне неосмотрительно подобным образом выдавать шифр, и без того крайне простой.

Холмс устанавливает, что подозреваемые, мужчина и женщина, подают сигналы с помощью свечи.

«— В той комнате кто-то ходит, — прошептал Холмс... — Да, я вижу его тень. Вот он опять. У него в руке свеча... Начинает подавать сигналы. Принимайте и вы, Ватсон, чтобы мы могли сверить наши данные. Одна вспышка, — разумеется, А. Ну, сколько вы насчитали? Двадцать? Я тоже. Должно означать Т. Т — вполне вразумительно! Снова Т. Это, разумеется, начало второго слова. Получается ТЕНТА. Кончилось. Неужели всё, Ватсон? АТТЕНТА — бессмысленно. Нет смысла и в том случае, если считать за три слова — АТ, ТЕН, ТА... Что же это такое? ...Как вы это объясните, Ватсон?

— Зашифрованное сообщение.

Неожиданно Холмс хмыкнул, будто что-то сообразив.

— И шифр не такой уж головоломный, Ватсон. Ведь это на итальянском! “А” в конце обозначает, что адресовано женщине. “Берегись!”... Что скажете, Ватсон?

— Полагаю, что вы попали в точку».

Крайне трудоемкий шифр, да еще и ненадежный: легко можно сбиться со счета, передавая буквы пламенем свечи! Но тем не менее Холмсу удалось выманить из убежища женщину, которой было адресовано послание «Берегись!», сообщив ей тем же самым способом слово *viene* (ит. «приходи»).

В повести «Долина ужаса» знаменитому детективу удалось справиться и с более сложным книжным шифром. Вот текст криптограммы:

534 C2 13 127 36 31 4 17 21 41 Douglas  
109 293 5 37 Birlstone 26 Birlstone 9 47 171.

О том, что был использован книжный шифр, Шерлок Холмс догадался по краткому виду послания и по тому, что некоторые слова написаны открытым текстом. Видимо, «открытые» слова не удалось найти в используемой для шифра книге.

Обычно книги для шифрования подбирают таким образом, чтобы они не вызывали никаких подозрений своим видом и самим фактом присутствия на книжной полке. Стараются использовать книги, изданные большими тиражами, наличие которых у двух разных людей (у того, кто шифрует,

и у того, кому предназначена криптограмма) не вызовет вопросов у посторонних.

Для дешифровки вышеприведенной криптограммы Холмсом совместно с доктором Ватсоном был использован широко распространенный «Альманах Уайтэкера»\*. Впрочем, передадим слово сэру Артуру Конану Дойлу: «Браво, Ватсон! Ежегодник! Возьмем номер “Альманаха Уайтэкера”. Он очень распространен. В нем имеется нужное количество страниц. И отпечатан он в два столбца... Теперь посмотрим, на что нам укажет страница пятьсот тридцать четвертая... столбец второй... Тринадцатое слово — “имею”, сто двадцать седьмое — “сведения”. Это сулит многое...» Окончательный текст записки следующий:

«Имею сведения. Опасность может угрожать  
очень скоро. Некий Дуглас, богатый помещик,  
теперь в Бирлстоун, замок Бирлстоун.  
Уверять, она настоящая».

Последнее неловкое предложение вызвано, видимо, тем, что автор записки торопился и не подобрал (или не смог подобрать) нужные слова, ограничившись близкими по смыслу словами. «Уверен, что эта опасность очень близка» — именно так понял это предложение Холмс.

---

\* Политический, финансовый и статистический ежегодник, издаваемый в Англии с 1868 года по настоящее время. Основан удачливым издателем Джозефом Уайтэкером (1820–1895).

Ну а для того, чтобы вспомнить, к каким приключениям Шерлока Холмса и Джона Ватсона привела дешифровка этих криптограмм, вам придется обратиться уже к самим рассказам.

Последнее дело знаменитого сыщика, относящееся к 1914 году, описано в рассказе «Его прощальный поклон». Этим делом Холмса заканчивается викторианский век английского детектива — когда был создан его канон — и начинается его золотой век.

## Этюд XXIII

# Английский детектив

Обычно под золотым веком английского детектива подразумевают период между мировыми войнами. Королевой детектива в это время становится Агата Кристи (1890–1976). Ей полностью будет посвящен следующий этюд. Пока же устроим небольшой тест и проверим, насколько хорошо вы знакомы с творчеством английской писательницы.

Из списка выберите главного героя рассказа А. Кристи «Изумруд раджи» (The Rajah's Emerald, 1926 год):

- глубокомысленный отец Браун;
- король сыщиков Нат Пинкертон;
- непревзойденный Эркюль Пуаро;
- отважный Джеймс Бонд.

Конечно, это не отец Браун, созданный воображением английского писателя Г. К. Честертона. Это, само собой разумеется, и не Нат Пинкертон. Но это также и не Эркюль Пуаро, ведь такой ответ был бы слишком очевиден!

«Проклятье!» — пробормотал Джеймс, скрежеща зубами». Итак, похищенный «знаменитый изумруд размером

с голубиное яйцо» был возвращен законному владельцу не кем иным, как Джеймсом Бондом!

В отличие от Артура Конана Дойла и Агаты Кристи, следующий наш герой, Жак Фатрелл (1875–1912), не был британцем. Но этот американский писатель путешествовал с супругой по Англии и Европе. В 1912 году он возвращался в Америку на печально знаменитом «Титанике». Когда произошло крушение корабля, писатель успел посадить жену в спасательную шлюпку, а сам остался на борту, сказав, что покинет корабль на следующей шлюпке. Но спастись ему не удалось [34].

Сыщик, созданный Фатреллом, — профессор Аугустус С.-Ф.-К. ван Дузен, по прозвищу Мыслящая Машина. «Этим громким именем его наградили газеты во время знаменитого шахматного турнира; тогда он доказал, что даже незнакомый с игрой человек может с помощью неумолимой логики выиграть у чемпиона, целую жизнь посвятившего шахматной премудрости».

В детективном рассказе «Загадка тринадцатой камеры» (The Problem of Cell № 13, 1905 год) ММ (эта аббревиатура фигурирует в самом рассказе; надеюсь, читатель понял, каким образом она появилась) также доказывает, что для гения не составит труда выбраться из одиночной камеры смертника в течение недели. Помещенный на пари в тюрьму, как обычный арестант, он выбрасывает из своего решетчатого окна записку, завернутую в пятидолларовую бумажку. В тексте записки содержится просьба передать ее адресату



и взять себе пять долларов за эту услугу. Кроме того, в записке есть зашифрованный текст:

У гебу ямыр-от окбос оп-стотен от. Э.

Что это за слегка исковерканное, но узнаваемое первое слово «убегу»? Далее можно разобрать «от собак», неужели это о начальнике тюрьмы!? Ясно видно число «сто» или чуть искаженное «сотен» — может, это цена побега? Огромная сумма по тем временам\*. И в конце записки либо подпись «от. Э.», либо намек на сообщника в деле побега.

Начальник тюрьмы, которому часовой отнес записку, напрасно потратил целый час, пытаясь понять, что это за шифр.

Вот и вы попробуйте разгадать его. Только не заглядывайте в ответ, сообщаемый в конце абзаца, следующего за подсказкой ниже! Шифр очень простой, очевидный; он вполне вам по силам.

Возможно, поможет следующая подсказка? Приведем текст записки в оригинале:

Epa cseot d'net niiy awe htto n'si sih. "T".

Позже профессор пояснил: «Я рассчитывал, что записка отвлечет внимание начальника тюрьмы, как оно и вышло.

---

\* Международная организация рабочих (Industrial Workers of the World), созданная в июне 1905 года в Чикаго (США), боролась за восьмичасовой рабочий день с оплатой в 4,5 доллара. Средняя зарплата в США и вовсе составляла 22 цента в час. Простой рабочий зарабатывал от 200 до 400 долларов в год.

А если бы начальник догадался, что там на самом деле написано, это было бы вроде дружеской шутки».

Правильный ответ: «Это не тот способ, которым я убегу» (англ. This is not the way I intend to escape). Криптограмму всего лишь надо прочитать задом наперед. То есть записка представляла собой простейший вид анаграммы, палиндромон (от др.-греч. *πάλιν*-δρομος — движущийся обратно, возвращающийся).

Заметим, что профессору ММ впоследствии удалось-таки благополучно сбежать из тюрьмы.

Различные виды анаграмм часто использовались авторами детективов. Современные писатели с успехом применяют этот прием в своих книгах. Достаточно назвать Дэна Брауна с его «Кодом да Винчи».

Писатель Эдгар Жепсон (Edgar Jepson, 1863–1938), член знаменитого Детективного клуба, почетным председателем которого одно время была Агата Кристи, часто писал под псевдонимом R. Edison Page. Это анаграмма от его имени и фамилии, за исключением одной буквы. Какой?

Ответ очевиден: первая буква фамилии *j* превратилась в псевдониме в соседку по алфавиту — букву *i*.

Генри Бейли (1878–1961) в межвоенный период был самым знаменитым детективным писателем Великобритании. Его слава затмевала даже славу самой Агаты Кристи [50]! Он создатель частного детектива Реджинальда Фортуна, врача, знатока древностей, специального советника Скотланд-Ярда по медицинским вопросам.

В рассказе «Длинный курган» (The Long Barrow, 1925 год) симпатичная преступница Изабелла Вудолл (настоящая фамилия Штульц), знающая древнегреческий язык, вместе со своим мужем Джорджем Штульцем решила завладеть состоянием старика-археолога Джозефа Ларкина. Она устроилась работать секретаршей у археолога и пытается стать его женой. Ларкин оказался очень ревнив и просматривает все письма своей помощницы.

Действие происходит в глухой деревеньке, где археолог совместно со своей помощницей раскапывает курган. Чтобы держать связь с сообщником, мисс Вудолл придумывает оригинальный способ. На ее имя приходят каталоги букиниста. Некоторые названия книг из списка помечены; в них подчеркнута одна из букв. В этом не было бы ничего необычного, если бы только помеченные таким образом книги не «демонстрировали странный вкус». В особняке Ларкина этот каталог попался на глаза Фортуну. Его внимание привлекло то, что спектр помеченных книг простирался от «чьих-то проповедей до истории авиации».

«Реджи задумался, подчеркнутые буквы образовывали сочетание SKUTHAI». Будучи знатоком древних языков, он понял, что это написанное по-гречески слово «скифы». Намек, по его мнению, был очевиден: в Древних Афинах полиция состояла из скифов. Муж мисс Вудолл ясно давал ей понять, что за ними следит полиция.

Во втором каталоге, который был найден в мусорной корзине, подчеркнутые буквы образовывали слово

TAPHONOIGEIN: taphon oigein — открыть могилу; очередной намек, уже на раскопки длинного кургана. Краткость посланий, очевидно, связана с тем, что с помощью подчеркивания одной буквы в названии трудно составить более длинное послание. Кроме того, подчеркивание нескольких букв и составление длинной фразы приведет к быстрой потере секретности переписки.

Еще было сообщение TUCHEAPELTNE: tuche apelthe — фортуна ушла; намек на то, что детектив Фортун покинул место раскопок.

Почта начала отслеживать каталоги на имя мисс Вудолл и присылать подчеркнутые буквы в полицию. Однажды и сама Изабелла отправила букинистической каталог почтой. Но почтовый служащий по недосмотру прислал детективу буквы не в том порядке, в котором они были в каталоге (он не знал древнегреческого языка, и для него подчеркнутые буквы были сплошной абракадаброй), а в виде статистического отчета:

A, B, G, H, L, M, N, P, R, T, U — 1 буква,  
I, S — 2 буквы, E — 4 буквы.

Таким образом, волею случая получилась анаграмма. Р. Фортун догадался, что это: PRESBUS GAMEIN THELEI.

На русском языке анаграмма выглядела бы следующим образом:

А, Ж, К, Н, О, Р, Х, Ч, Ь, Я — 1 буква,  
Е, И, С — 2 буквы, Т — 3 буквы.

Попробуйте и вы ее дешифровать!

Обратите внимание на второе слово в оригинальном тексте. Не напоминает ли оно вам слово «Гименей»? В греческой мифологии это божество брака. Вспомним, что мисс Вудолл устроилась секретаршей к старому археологу с намерением женить его на себе! Это вам намек на то, что в тексте русскоязычной анаграммы присутствует слово «жениться».

Тогда анаграмма упростится до

А, Е, И, К, О, Р, С, Х, Ч — 1 буква, Т — 2 буквы.

Как вы уже, несомненно, догадались, анаграмма дешифруется следующим образом: «Старик хочет жениться»: в оригинальном тексте PRESBUS (старик) GAMEIN (жениться) THELEI (хочет). Изабелле удалось претворить в жизнь свой преступный план. Она обманом стала миссис Ларкин, женой старика археолога. Но она не успела, как задумывала, убить Джозефа Ларкина в первую брачную ночь и спрятать тело в раскопанном длинном кургане. Полиция и Реджинальд Фортун помешали планам преступников.

# Christie for Christmas

Более полувека английская писательница Агата Кристи, удачно обыгрывая свою фамилию (Christie for Christmas, то есть Кристи к Рождеству), ежегодно делала рождественский подарок своим читателям — выпускала очередной детективный роман.

В развязках своих романов Агата Кристи нередко использует всем известные факты: некоторые имена могут быть как женскими, так и мужскими; одинаковые уменьшительные имена могут образовываться от первоначально разных полных имен; зеркало не только отражает, но и преворачивает изображение...

В записных книжках писательницы можно найти страницы, на которых она экспериментирует с симметричными английскими буквами: H, M, A, W, I, O, T, U, V, Y [26]. В романе «Немой свидетель» (Dumb Witness) брошь с инициалами владелицы ТА служит ключом к установлению убийцы. Эркюль Пуаро разгадает этот ребус и поймет, что на самом

деле инициалы были АТ, ведь свидетельница видела эту брошь отраженной в зеркале.

В рассказе «Случай с мячиком для собаки», который позже и был переработан в вышеупомянутый роман, Пуаро говорит: «Это напоминание о том, *mon ami*, что никакими мелочами не следует пренебрегать».

Вы заметили «мелочь» в вышеприведенной строке с симметричными буквами? Там нет буквы Х! Писательница не рассматривала ее всерьез, видимо, потому, что английские имена редко начинаются с этой буквы.

Агата Кристи в своих записных книжках оставила нам следующую головоломку:

The quick brown fox jumps over gladly  
(«Проворная бурая лиса радостно прыгает»).

Наверняка она рассматривала ее не просто так. Эта фраза, несомненно, могла бы стать важным ключом к разгадке очередного преступления. Догадайтесь, что в этой фразе не так? Какой намек в ней содержится?

Данная словесная головоломка называется панграммой, или разнбуквицей. При ее составлении необходимо использовать все буквы алфавита; желательно при этом использовать как можно меньшее их количество. Панграммы находят и практическое применение; так, они используются при проверке передачи текста по линиям связи, а также при подборе шрифтов в дизайне.

В версии Агаты Кристи отсутствует буква z, самая редкая буква английского языка!\* Возможно, писательница думала использовать данную разнобуквицу как заголовок очередной книги. Ведь она не раз мастерски использовала всевозможные детские стихи и считалочки в названиях своих книг. А можно использовать эту легко запоминающуюся фразу и как бегущий автоключ в шифре Виженера или как тайный алфавит в шифре простой подстановки, когда каждой букве обычного алфавита мы ставим в соответствие букву из тайного алфавита.

В своих произведениях Кристи не раз упоминает различные загадочные шифровки («Глупость мертвеца»; «Цветы смерти»). В этюде IX автором уже был приведен пример из рассказа «Цветы смерти», в котором использованы названия сортов цветов для шифрования.

Давайте посмотрим еще на один забавный ребус от Агаты Кристи, найденный в ее черновиках:



Отгадайте, название какого своего литературного произведения зашифровала писательница? Вспомним, что Агата Кристи часто использовала для названий своих произведений детские считалки и стихи. Может, это «Раз, два, три, туфлю

---

\* Аналогичная разнобуквица со всеми буквами английского алфавита: The quick brown fox jumps over the lazy dog («Проворная бурая лиса перепрыгивает ленивого пса»).



застегни» (One, Two, Buckle My Shoe)? Как-никак, в начале ребуса видна цифра три. А может, это буква *z* в устаревшем написании? Нет, на этот раз Агата Кристи взяла название другого стишка\* из детского сборника «Сказки матушки Гусыни».

Три слепых мышонка  
Бегали сторонкой.  
Хозяйка острый нож взяла,  
Взмахнула раз,  
Взмахнула два.  
Отрубила хвостики  
Малышам она.  
Видели такое?  
Ах, какое горе!

Конечно, в ребусе зашифровано название самой популярной пьесы писательницы «Три слепых мышонка»\*\* (радиопьеса, 1947 год; рассказ, 1948 год; позднее пьеса «Мышеловка»\*\*\*, 1952 год).

---

\* Стихотворение «Три слепых мышонка» (англ. Three Blind Mice).

\*\* Даже на позднем этапе своей театральной карьеры А. Кристи продолжала экспериментировать в постановках своих пьес. Как ни странно, она хотела, чтобы занавес падал или свет гас прежде, чем был разоблачен убийца. А потом запись ее собственного голоса спрашивала бы у зрителей, кого они считают убийцей [26].

\*\*\* Детективная пьеса «Мышеловка» (англ. The Mousetrap) и по сей день успешно идет в театрах Лондона. К настоящему моменту сыграно более 26 000 спектаклей, что является абсолютным рекордом непрерывности постановок. В конце каждого спектакля зрителей просят не рассказывать другим, чем заканчивается пьеса.

Надеемся, что, разгадывая эти головоломки, вы использовали «свои маленькие серые клеточки мозга» должным образом и смогли почувствовать себя Эркюлем Пуаро или хотя бы его верным помощником капитаном Артуром Гастингсом.

# Игры Клода Шеннона

Американский инженер и математик Клод Шеннон (1916–2001) в начале 1940-х годов приступил к работе в исследовательском центре известной телекоммуникационной корпорации Bell Telephone Laboratories. Кроме того, во время Второй мировой войны он занимался разработкой криптографических систем, в том числе и правительственной связи, которая обеспечивала переговоры Черчилля и Рузвельта через Атлантический океан. Позже эти разработки помогли Шеннону разработать методы кодирования с коррекцией ошибок. Как говорил сам ученый, работа в области криптографии подтолкнула его к созданию теории информации.

В лаборатории Белла помимо криптографических задач Клод Шеннон работал и над конкретной задачей: сколько телефонных разговоров или телеграмм можно одновременно передавать по проводу и как этот поток увеличить? Шеннон стал определять количество информации как «степень

удивления получателя». В полученном сообщении тем больше информации, чем больше новизны для получателя. Если вы заранее всё знали, то никакой полезной и новой информации для вас в сообщении не содержится.

В свободное время Шеннон предлагал своей супруге Бетти угадывать связный текст постепенно, буква за буквой, и таким образом определял степень новизны текста (для супруги) [30].

Попробуйте и вы сыграть в эту игру. Угадайте фразу из двух слов, первая буква которой «э». Конечно, сделать это весьма затруднительно; с этой буквы начинается очень большое количество слов: «Эфиопия», «Эйнштейн», «эволюция», «эллипс», «эхо», «экзамен», «эбонит», «эврика», «экипаж», «эксперимент», «элегия», «Этна» и многие другие. Вторая буква — «н». Слова можно перечислять и дальше: «Энигма», «энциклопедия», «энергия», «Энгельс», «энцефалит»... Нужна еще одна буква? Пожалуйста, это буква «т». Набор слов начинает постепенно сужаться: среди них как хорошо известные «энтузиаст» и «энтомолог», так и редкие — «энтерлак» (техника вязания) и «энтерит» (воспаление тонкой кишки). Последняя подсказка: четвертая буква «р», и ряд подходящих слов: «энтризм» (тактический прием, активно используемый троцкистами), «Энтрокаменту» (город в Португалии), «Энтро» (коммуна в Италии), «энтроп» (N-карбамоилметил-4-фенил-2-пирролидон).

Загаданное первое слово фразы — «энтропия»\*. Если вы угадали его с четвертой буквы, то можно считать, что ровно наполовину оно было вами не узнано; вероятность угадывания равна пятидесяти процентам.

Но в загаданной фразе есть еще и второе слово. Его первая буква «ш». Можно начать перечислять буквы, как и для первого слова, но посмотрите на фотографии ниже.



Здесь тоже постепенно «вырисовывается» второе загаданное слово, но уже не в виде букв, а в виде ряда фотографий с различной степенью четкости изображения. При передаче информации могла произойти частичная ее потеря. Как вы помните, Шеннон создал методы кодирования с коррекцией ошибок, чтобы информация при ее передаче по каналам связи и дешифровании не пропадала. Итак, задуманная фраза: «Энтропия Шеннона». По всеобщему мнению, именно работы Шеннона в области теории кодирования и передачи информации придали криптографии статус науки.

---

\* Информационная энтропия — мера неопределенности или непредсказуемости информации, неопределенность появления какого-либо символа первичного алфавита. При отсутствии информационных потерь численно равна количеству информации, приходящемуся на символ передаваемого сообщения.

В 1952 году Клод Шеннон опубликовал научную статью, в которой и описал эксперименты по определению количества информации в связном тексте. А ведь все начиналось с игры в угадывание слов с женой.

Вы можете сыграть в «угадайку» с кем-то из знакомых: предложите угадать какую-нибудь пословицу. Далее сделайте «ход конем». Предложите отгадать следующую фразу: Back to the Future («Назад в будущее»). Вряд ли кто-то сразу догадается, что предложенная фраза написана на английском языке. Если же вы напишете всю фразу прописными буквами, чтоб постараться скрыть английское начертание строчных букв *k* и *h*, BACK TO THE FUTURE, то мера неопределенности увеличится. В последовательности букв, составляющих какое-либо предложение на русском языке, разные буквы появляются с разной частотой, поэтому неопределенность появления для некоторых букв меньше, чем для других. Если же учесть, что некоторые сочетания букв встречаются очень редко, то неопределенность еще сильнее уменьшится. Когда игрок увидит начальные буквы BACK русского, как он думает, слова, то у него останется не так много вариантов для отгадывания всего слова. Большинство вспомнят о португальском мореплавателе Васко да Гаме, некоторые эрудиты — о васкулите; другие же догадаются, что заданная фраза не на русском языке.

Шеннон как инженер создал несколько механических игровых устройств. Среди них: устройство, которое собирало кубик Рубика; мини-компьютер для настольной

математической игры гекс, который всегда побеждал соперника; механическая мышка, которая могла находить выход из лабиринта. Кроме того, Шеннон вывел математическую формулу жонглирования мячиками и создал целый ряд механических кукол, которые жонглировали различным количеством мячиков. Клод Шеннон и сам умел жонглировать; известна его фотография, где он жонглирует клубнями картофеля. Действительно, делу время, но и потехе час!

## Этюд XXVI

# Дешифровка линейного письма Б

В сборнике задач для олимпиад по криптографии и математике для школьников [36] приведен следующий фигурный цифровой кроссворд:

	5		2		0		0	1		2		1
		5		3			3			5		
3		4							6			4
			5	3		3				5		
				2		3	3	3	2			1
2		2								0		
	0		3		5				3			0
						3				1		
	1	3										
0				9			7		8		2	
		6			6							
	3									6		0
0				6			5					

Условия задачи таковы: числа, расположенные в клетках таблицы, указывают, сколько соседних по горизонтали,



вертикали и диагонали клеток (может быть включена и та клетка, в которой находится само число) должны быть окрашены. Восстановите картинку, которой соответствуют эти числа.

Наверное, это одна из самых легких задач в этом сборнике. Но при чем тут криптография? На рисунке, конечно, изображено что-то, что может ассоциироваться с секретами, тайнами.

Дадим вам ключ к решению этого кроссворда — на картинке в том числе изображен самый обычный ключ для запирания двери.

Эта задача тренирует пространственное мышление. Постепенно «откапывая» куски, «орнаменты» кроссворда, вы будете формировать из зрительных образов закономерности, предугадывая рисунок. Однажды такой способ мышления пригодился для разгадывания критского линейного письма Б.

Линейное письмо Б — позднейшая форма критского письма (XV–XII века до н. э.), которая использовалась для записи текстов на древнегреческом языке в эпоху микенской культуры.

Микенские тексты — слоговая фонетическая письменность, каждый знак которой является слогом типа «согласный звук плюс гласный звук». Единственный нефонетический знак — словоразделитель (пробел), он играет очень важную роль в ходе любой дешифровки.

В 1900 году первооткрыватель линейного письма Б археолог сэр Артур Эванс (1851–1941) заметил на одной из глиняных табличек слово, состоящее из двух слоговых

знаков и третьего знака-детерминатива\* «лошадь без гривы»: 𐤆𐤕𐤍. Это слово было похоже по написанию на 𐤆𐤕𐤍 из кипрского силлабария\*\*, которое было уже дешифровано как ро-ло\*\*\* (третий слог se здесь немой). Эванс сопоставил ро-ло с греческим ρῶλος (жеребенок, родственно англ. foal). Такое прочтение оказалось правильным. Но после этого прогресс в деле дешифровки застопорился.

Дело сдвинулось с мертвой точки только через тридцать лет благодаря работам профессора классической филологии Алисы Кобер (1906–1950) из Бруклинского колледжа, США. Еще будучи студенткой, А. Кобер занималась исследованиями в различных направлениях, от астрономии и математики до естественных наук, никогда не ограничивая себя изучением только классических языков [64]. Видя, что филологи застопорились в деле дешифровки линейного письма Б, она применила статистический подход, анализируя символы табличек. Алиса не пыталась установить фонетические значения знаков, не пробовала угадать смысл отдельных слов, не делала даже предположений о языке письма. Зато она обратила внимание, что часть слов образует «тройки», то

---

\* Детерминатив — знак на письме, служащий для обозначения грамматических категорий слов в логографическом письме. Детерминативы облегчают чтение, но ни один из них не произносится. Обычно это символы для обозначения божеств, животных, растений и т. д.

\*\* Силлабарий — слоговая азбука.

\*\*\* Слово написано по слогам, так как линейное письмо Б, напомним, является слоговым.

есть одно и то же слово встречалось в тексте в трех слегка различающихся формах. Корень слова всегда был неизменным, но существовало три разных окончания.

**Табл. 7. Два склоняемых слова в линейном письме Б**

	Слово № 1	Слово № 2
Падеж 1	𐎶𐎵𐎠𐎥𐎶	𐎶𐎵𐎠𐎥𐎶
Падеж 2	𐎶𐎵𐎠𐎥𐎶	𐎶𐎵𐎠𐎥𐎶
Падеж 3	𐎶𐎵𐎠𐎥	𐎶𐎵𐎠𐎥

Как видим, первые два знака в обоих словах в табл. 7 образуют корень. Трудности начинаются с третьим символом. Если он часть корня, то должен быть одинаковым во всех падежах (но в третьем падеже его нет!). В противном случае, если третий символ не является частью корня, он должен быть частью окончания. Но ведь для разных слов окончания должны быть одинаковыми во всех падежах. А мы видим, что рассмотренные в табл. 7 слова совпадают в окончаниях только для первых двух падежей, но для третьего падежа это не так. Парадокс: третьи символы не являются ни частью корня, ни частью окончания.


Кобер разрешила эту проблему. Она предположила, что третий слог соединительный, то есть является и частью корня, и частью окончания слова. В качестве примера (табл. 8) она рассмотрела слово из аккадского языка — *sadanu*, имеющее корень *sad* и окончание *anu* в первом падеже.

Табл. 8. Соединительные слоги в аккадском слове *sadanu*

	Sadanu
Падеж 1	SA-Da-nu
Падеж 2	SA-Da-ni
Падеж 3	SA-Du

Здесь второй, соединительный слог меняется от -da к -du (корень для наглядности выделен заглавными буквами).

Продолжил дело Алисы Кобер английский архитектор Майкл Вентрис (1922–1956). Еще четырнадцатилетним школьником Вентрис побывал на популярной лекции Артура Эванса, посвященной в том числе и линейному письму Б. Майкл всерьез увлекся этой темой и решил дешифровать линейное письмо, но все же «ему самому казалось, что изучение старинных загадочных письмен не дело, а интересное и увлекательное времяпрепровождение, вроде *решения кроссвордов* [выделено мной. — И. Е.]. Поэтому, окончив школу, он <...> поступил в архитектурный институт в Лондоне, так как и архитектура его с детства очень интересовала» [31].

Майкл Вентрис окончательно, в июне 1951 года, дешифровал каждый символ, установил, что язык письма — греческий, и сопоставил каждому символу (слогу) его фонетическое звучание. Так, слово  — столица минойского Крита, город Кносс, по слогам линейного письма Б читается как ko-no-si-ja.

Так что же предопределило успех английского гения Вентриса в деле дешифровки? Несомненно, ему помогло то, что он свободно говорил на шести европейских языках (и кроме того, немного знал русский), владел древнегреческим и латынью. Он применил математические методы для анализа текста глиняных табличек. Но было еще кое-что, что помогло ему.

Соратник Вентриса, преподаватель классических языков в Кембридже Джон Чедвик писал о нем: «Его мозг работал с поразительной быстротой... Микенцы были для него не смутной абстракцией, а живыми людьми... [Он] настолько хорошо знал [неразгаданные] тексты, что большие куски запечатлелись в его мозгу просто как зрительные образы... и вот тут-то пригодилось его *архитектурное образование* [выделено мной. — И. Е.]. Глаз архитектора видит в здании не единственно лишь внешнюю сторону — беспорядочную мешанину декоративных элементов <...> он способен разглядеть то, что находится за ней: важные части орнамента, элементы конструкции и корпус здания. Так и Вентрис сумел разглядеть среди приводящего в замешательство многообразия загадочных символов и рисунков закономерности, которые раскрыли лежащую за ними внутреннюю структуру. Именно этим качеством — способностью разглядеть порядок в кажущемся беспорядке — характеризуются деяния всех великих людей».

Таким образом, как зрительное восприятие, так, возможно, и увлечение кроссвордами немало поспособствовали

Майклу Вентрису в окончательной дешифровке линейного письма Б.

Осталось только привести решение фигурного кроссворда:

	5		2		0		0	1		2		1
		5		3			3			5		
3		4								6		4
			5	3		3				5		
				2		3	3	3	2			1
2		2								0		
	0		3		5				3			0
						3				1		
	1	3										
0				9			7		8		2	
		6			6							
	3									6		0
0				6			5					

## Этюд XXVII

# О пользе знания языков

Глиняные таблички с клинописью шумеров и эгейской слоговой письменностью, папирусы с иероглифами древних египтян и многие другие дошедшие до нас письмена мертвых языков долгое время хранили в тайне смысл написанных на них текстов. Никто не мог в них ничего понять, хотя изначально эти тексты писались с прямо противоположной целью: чтобы любой грамотный человек мог их прочесть.

Постепенно их удалось расшифровать. Во многом этому способствовали найденные билингвы — двуязычные представления одного и того же текста в одном источнике. Например, иероглифы, как уже рассказывалось в этюде XVI, были расшифрованы благодаря Розеттскому камню, на котором один и тот же текст был записан как неразгаданными еще иероглифами, так и на хорошо известном древнегреческом языке. Но чтобы окончательно разобраться со структурой языка, понять его законы, одной только билингвой не обойтись: необходимо знать родственные языки, нередко также вымершие.

Так, Жан Франсуа Шампольон с детства мечтал первым прочесть загадочные иероглифы Древнего Египта. Мальчиком он начал учить древнееврейский и арабский языки. Далее последовали коптский (который оказался родственным древнеегипетскому языку), латынь, древнегреческий, эфиопский, китайский, персидский, арамейский и некоторые другие.

Майкл Вентрис, который расшифровал линейное письмо Б, свободно говорил на шести европейских языках. Знал он также древнегреческий и латынь, немного понимал и по-русски.

Георг Гротенфенд (1775–1853) в 1802 году на пари всего за несколько недель дешифровал неизвестную ему ранее систему письма — древнеперсидскую клинопись. Гротенфенд был учителем классических языков и случайно узнал о персепольской надписи, над дешифровкой которой ученые бились уже несколько десятилетий. Он предположил, что язык надписи древнеперсидский и клинописные таблички относятся к династии Ахеменидов (VI–IV века до н. э.). Древнеперсидский к тому времени был мертвым языком. Гротенфенд знал, что цари (шахиншахи) из персидской династии Сасанидов, правившие уже в III–VII веках (от Ахеменидов их отделяло более 750 лет), дословно себя величали титулатурой «Такой-то, царь великий, царь царей, такого-то царя сын, Сасанид». Парфянский (среднеперсидский) язык державы Сасанидов являлся наследником древнеперсидского языка, но тексты записывались не клинописью, а значками арамейской письменности и собственными идеограммами.



Гротенфенд решил искать вышеприведенный громоздкий титул и в клинописных табличках. Ключом к дешифровке оказалось слово «царь», повторяющееся в титуле четыре раза. Определив клинышки, соответствующие этому слову, Гротенфенд сумел дешифровать древнеперсидский язык. Более того, зная историю Древней Персии, он сумел по именам царей Ксеркса и Дария прочесть, озвучить древнюю клинопись. Заметим, что имена Ксеркс и Дарий мы знаем из греческих источников. Используя собрание древних священных зороастрийских текстов «Авеста», Гротенфенд реконструировал имена древних царей как Хшарша (Ксеркс) и Дархейш (Дарий).

Повторимся, Гротенфенд, когда приступал к разгадыванию персепольской надписи, не владел ни одним из восточных языков. Тем не менее он сумел подметить в них общие черты. Думается, что ему помогли хорошее знание истории, греческого и латыни, понимание общих принципов грамматики, а также «культурного кода» исчезнувшего языка.

Дешифровщику древних надписей важно знать, в каком значении слова употреблялись в прежние времена: язык постоянно развивается, меняется его лексический состав, происходят грамматические и фонетические изменения. Так что формально расшифрованный текст нужно еще «переводить» на современный язык.

Попробуем выполнить достаточно простое задание: определить значения всего лишь одного слова русского языка в тексте, которому нет еще и двух сотен лет. Напомним

читателю, что иногда благодаря одному правильно определенному слову были дешифрованы некоторые давно забытые языки.

В стихотворении А. С. Пушкина «Брожу ли я вдоль улиц шумных» есть такие строки:

День каждый, каждую *годину*  
Привык я думой провождать,  
Грядущей смерти *годовщину*  
Меж их стараясь угадать.

Вопрос: что здесь значит слово «година»?

В современном русском литературном языке слово «година» употребляется для обозначения времени, в течение которого происходят какие-либо значительные события: с оттенком торжественности, приподнятости. У Пушкина же это слово сопровождается словом «каждая», то есть употреблено в каком-то другом, бытовом значении.

Вы думаете, это год? Не спешите.

Иногда, чтобы понять слово родного языка, нужно посмотреть, что оно означает в других языках — родственных и не очень.

Для оценки степени генетического родства между двумя языками часто сравнивают схожесть их словарного запаса. Так, лексическое сходство русского языка с английским составляет только 24%, в то время как с польским оно уже в три раза больше — 77%, а с украинским и белорусским языками оно максимально и равно 86%.

Пусть на помощь вам придут строки из близкородственного нам польского языка. В нем это слово пишется как *godzina* (произносится ближе к «годжина») и до сих пор употребляется в том же значении, в котором использовал его наш великий поэт:

Slonce wbiegło w te sama nieba okolice,  
*Godzina* uderzyła! gdzież sa jej zrenice?

Строчки принадлежат Адаму Мицкевичу и взяты из стихотворения, которое называется дешифруемым нами словом *Godzina* (Elegia).

Можно уловить (экстраполируя польский язык на родной русский), что речь идет о некоем промежутке времени. И это явно не год.

Окончательно разобраться с реконструкцией этого слова и восстановить его истинный смысл поможет стихотворение «Вечірня година» украинской поэтессы Леси Украинки:

Вийду в садочок та погуляю,  
При місяченьку та й заспіваю.  
Як же тут гарно, як же тут тихо,  
В таку *годину* забудеш лихо!

В близком нам украинском языке слово «година» произносится как «годына» и обозначает до сих пор то же, что и польское *godzina*.

Наверняка вы, сравнив все три текста близкородственных языков, уже окончательно реконструировали смысл слова

«година» в пушкинских строках: это не что иное, как «час». Нам осталось только привести литературный перевод строк А. Мицкевича, принадлежащий перу его современника, русского поэта Владимира Бенедиктова:

Теперь... светило дня на том же месте вновь; —  
Бьет тот же самый час... Но где ж твой взор, любовь?

В древнерусском письменном языке слово «година» обозначало и время, и год, и час. Отметим, что «час» в украинском и *czas* в польском и теперь обозначают слово «время».

Как же могло получиться, что год и час обозначались одним словом? Чтобы понять эту взаимосвязь, нужно немного углубиться в историю. И слово «час», и слово «год» этимологически связаны с глаголами, обозначающими ожидание: «чаять» и «годить».

Если же заглянуть еще на несколько сотен лет назад, то можно докопаться и до более любопытных вещей. Слово «год» (годъ) приблизительно до XVI века обозначало в нашем языке благоприятный промежуток времени или ожидание такого момента (отсюда и корень в словах «погоди», «погода», «годный»), а отрезок времени от весны до весны раньше называли летом; однако «год» вытеснил «лето» в этом значении. А в английском, немецком и шведском языках слово, произошедшее от того же древнего корня «год», потеряло значение ожидания и стало означать просто что-то хорошее: в английском оно преобразовалось в *good*, немецком — *gut* и шведском — *god* [54].

Хорошее знание грамматики родного языка также помогало в делах криптографии. Так, сотрудник тайной канцелярии папской курии (напомним, что официальными языками Ватикана являются латинский и итальянский) итальянец Чикко Симонета еще в 1474 году издал трактат, в котором «систематически излагались принципы вскрытия шифров, основанные на знании некоторых лингвистических особенностей языка [латинского и итальянского. — *И. Е.*], на котором был написан открытый текст сообщения. Появление такого руководства <...> было вызвано необходимостью не единичного, а массового обучения соответствующих служащих курии основам криптоанализа. Создание такого трактата свидетельствует не только о том, что использование шифров <...> приобрело массовый характер, но и о том, что <...> вскрытие шифров стало возможным и реально осуществляемым на практике явлением» [44].

## Этюд XXVIII

# Аэропорт

Еще до недавнего времени всем путешественникам приходилось видеть, как меняются надписи перекидного табло в аэропорту или на железнодорожном вокзале. Сначала табло пустое. Потом вдруг появляется некая абракадабра, например:

**М Я У Ф И М У М Ж А К Х В Е Д А Т .**

Догадаться, тем более «дешифровать» такое сообщение вряд ли возможно. Но буквы опять приходят в движение, привлекая внимание своими щелчками, и надпись меняется:

**М А К Т И М Э М Д Е Л У В Е К А С .**

По-прежнему непонятно, что написано на табло; глаз выхватывает невероятные сочетания, вроде ДЕЛУВЕК, однако мелькание букв продолжается, возникают пробелы между словами:

**Р А К С — Н Ю — Ч Е Л О В Е К К С .**

Вы уже справились с этой задачей? «Дешифровали», какой город появится на табло?

Сменяются еще три буквы:

Р Б К С — Н Я — Ч Е Л О В Е К С С .

Те, кто собрался поехать в этот город, уже догадываются, другим нужна еще пара замен, чтобы понять надпись:

Р Б К С — Н Я — Ч Е Л Я В И Н С К .

И уже все догадываются, что за сообщение появится:

Р Е Й С — Н А — Ч Е Л Я Б И Н С К .

Примерно по тому же принципу работают автоматические камеры хранения багажа на вокзалах, которые открываются лишь тогда, когда набрано некоторое «тайное слово» или тайный набор цифр. Это слово (пароль) набирают с помощью одного или нескольких дисков, на которые нанесены буквы или цифры.

Пусть число букв и цифр на каждом диске равно двенадцати, а число дисков — пяти. Сколько неудачных попыток может быть сделано человеком, не знающим секретного слова и подбирающим его наудачу?

Воспользуемся комбинаторикой, чтобы решить задачу о подборе пароля для вскрытия ячейки.

Из условия задачи видно, что порядок выбираемых букв играет существенную роль. Одно дело набрать на первом диске букву А, а на втором Б, и совсем другое дело — набрать их в обратном порядке. Поэтому здесь мы имеем дело с размещением с повторениями. Тогда полное количество комбинаций для подбора пароля вычисляется по формуле  $n^k$ , где  $n = 12$  — число способов, которыми мы выбираем букву или цифру на каждом диске,  $k = 5$  — количество таких дисков. Получаем, что число комбинаций равно  $12^5 = 248\,832$ . Следовательно, число неудачных попыток может достигнуть 248 831, поэтому (считая по шесть секунд на одну попытку) в худшем случае получаем, что для открытия сейфа понадобится более 400 часов (почти семнадцать дней) непрерывной работы. Это неплохая стойкость пароля для обычной камеры хранения. Пассажир наверняка быстрее вернется за своим багажом, чем взломщик подберет пароль.



## Этюд XXIX

# Лепет

Рассмотрим несколько необычный этюд. Ученых давно интересуют вопросы: как появился язык, как он развивался? Детским лепетом называют стадию доречевого развития ребенка. Здесь же мы рассмотрим «лепет» шимпанзе и карликовых шимпанзе (бонобо): люди давно пытаются понять и дешифровать различные сигналы и звуки, с помощью которых общаются эти животные [37].

Обезьяны владеют множеством жестов для общения друг с другом. Среди последних мы можем наблюдать: почесывание головы и подбородка, обнимание, поцелуи, оскал клыков и даже улыбку, сцепление рук в кулак и просто кулак и многое другое. С помощью подобного языка жестов они многое могут рассказать друг другу. Но один жест им все же неведом. Как вы думаете, что это за жест, который является уникальным видовым признаком человека? Это указательный жест пальцем; лишь в редких случаях ему удается обучить обезьяну в условиях неволи.

Но люди пошли дальше. Они начали обучать шимпанзе человеческому языку глухонемых, так как из-за особенностей

своего речевого аппарата обезьяны не могут издавать человеческие звуки. Конечно, ученые надеялись, что таким образом им удастся наладить общение с подопечными.

После полутора лет обучения шимпанзе Уолшо, которая жила в семье исследователей и воспитывалась как человеческий детеныш, стала переходить от употребления однословных слов языка глухонемых («фрукт», «слушать» и т. п.) к использованию «двухсловных» комбинаций. Точно так же происходит становление речи и у детей примерно такого же возраста. Для того чтобы получить желаемое лакомство, которое хранилось в холодильнике, шимпанзе подходила к нему и на глазах воспитателей воспроизводила подряд три знака: «открыть — ключ — пища». Однажды, когда Уолшо каталась на лодке со своим воспитателем, она увидела лебедя и по собственному почину просигналила последовательно следующие знаки «пить — жидкость» и «птица», что было интерпретировано как «водяная птица».

Попробуйте разобраться, о чем «говорила» исследователям в разных ситуациях умная шимпанзе. В левой колонке — подаваемые ею знаки, в правой — расшифровка. Расставьте их по местам.

пить — фрукт	зерна злаков
холодный — фрукт	изюм
запах — фрукт	арбуз
цветок — пища	персик
кричать — больно — фрукт	лимон (грейпфрут)
пища — фрукт	чашка красного цвета

пахучая — пища  
красный — стекло

мороженная земляника  
редиска

Самая известная обезьяна, которую обучали человеческому языку, — самец бонобо Канзи. Его приемную мать, самку бонобо Матату, включили в программу обучения языку, когда Канзи исполнилось шесть месяцев. Способности Канзи оставались нераскрытыми на протяжении целых двух лет, в течение которых американский исследователь Сюзанна Севидж-Рамбо безуспешно пыталась научить работать с символами (лексиграммами\*), нарисованными на карточках или экране компьютера, его приемную мать. Случайно получив доступ к клавиатуре компьютера Мататы, юный Канзи тут же продемонстрировал свои выдающиеся способности в оперировании символами. В первые дни он использовал всего лишь семь лексиграмм: «апельсин», «арахис», «банан», «яблоко», «спальня», «гоняться» и «Остин» (его друг по играм; как видим, и тут не обошлось без игр!). Через год молодой бонобо знал уже 35 слов. В возрасте 29 лет он использовал 400 слов.

Популяция бонобо, обитающая только в лесах Конго, быстро сокращается. Тридцать лет назад их было около 30 тысяч, и уже тогда говорили, что надо применять меры по их сохранению. Теперь осталось меньше 10 тысяч особей:

---

\* Лексиграммы для разговора с бонобо С. Севидж-Рамбо были взяты из языка глухонемых в США и Канаде амслен. Лексиграммы были адаптированы для карликовых шимпанзе, кроме того, были добавлены новые рисунки.

местным жителям, *Homo sapiens*, пришлось по вкусу мясо бонобо.

Ну а теперь ответ на вопрос, что «говорила» шимпанзе:

пить — фрукт	арбуз
холодный — фрукт	мороженая земляника
запах — фрукт	лимон (грейпфрут)
цветок — пища	зерна злаков
кричать — больно — фрукт	редиска
пища — фрукт	персик
пахучая — пища	изюм
красный — стекло	чашка красного цвета

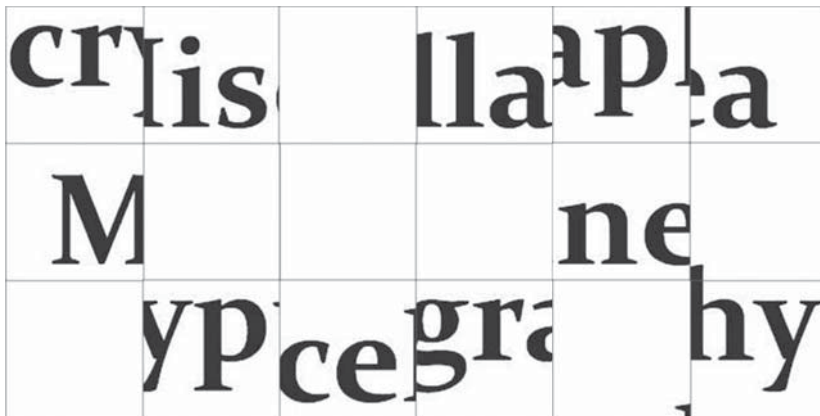
Шимпанзе знала и просто слово «чашка», но словами «красный — стекло» она особо выделял свою любимую чашку красного цвета.

## Этюд ХХХ

# Криптографическая смесь

В этом этюде собраны различные небольшие истории или задачи, образующие пеструю смесь развлекательных головоломок, так или иначе связанных с сокрытием информации.

Нижеприведенная головоломка похожа на пазл, мозаику; здесь нужно составить сообщение из множества фрагментов квадратной формы.



Скопируйте это задание на чистый лист бумаги\*, разрежьте на 18 квадратиков и попробуйте собрать правильный текст.

Внимательный читатель уже заметил, что все квадраты ориентированы на плоскости верным образом, то есть их не надо поворачивать ни влево, ни вправо. Кроме того, четыре квадрата абсолютно пусты. Нетрудно заметить, что квадрат с буквой «М» — единственный с заглавной буквой. Следовательно, в дешифруемой надписи этот квадрат будет стоять в начале. Таким образом, вам останется методом перебора правильно подобрать 13 квадратов. Если делать это бездумно, то у вас будет целых 6 227 020 800 (то есть свыше шести миллиардов!) вариантов подбора правильной картинки. Конечно, на самом деле вы справитесь с задачей гораздо быстрее, осмысливая текст.

Небольшая подсказка: вариантов подбора на порядок меньше, так как у задачи есть свой ключ! Вам надо на первоначальной картинке сдвигать столбцы вверх или вниз на один-два квадрата (либо оставлять их на месте). Если, к примеру, квадрат вылез вниз за первоначальную границу мозаики, то вы его аккуратно ставите первым вверху, на освободившееся место; и наоборот.

Подвигали, хотя бы мысленно? Правильный ключ сдвига столбцов:  $\uparrow = \downarrow = \uparrow =$ . Сдвигаем только нечетные столбцы

---

\* Либо скачайте готовым на странице книги: [www.mann-ivanov-ferber.ru/books/tainstvennye-stranicy/](http://www.mann-ivanov-ferber.ru/books/tainstvennye-stranicy/).

в указанных направлениях, четные не трогаем. В результате получаем ответ *Miscellanea cryptography*, то есть название нашего этюда на латыни. В данном контексте *miscellanea* означает смесь, всякая всячина. Иногда научные (и не только) сборники трудов выходят под этим звонким словом.

А теперь мы поговорим о своеобразном речевом пароле — шибболете. Пароли нужны не только для защиты писем в вашем электронном почтовом ящике от нежелательных гостей; надобность в них возникла раньше. Приведем цитату из Библии, Книга Судей Израилевых, 12:5–6. «...И перехватили Галаадитяне переправу чрез Иордан от Ефремлян, и когда кто из уцелевших Ефремлян говорил: “позвольте мне переправиться”, то жители Галаадские говорили ему: не Ефремлянин ли ты? Он говорил: нет. Они говорили ему “скажи: шибболет”, а он говорил: “сибболет”, и не мог иначе выговорить. Тогда они, взяв его, закололи у переправы чрез Иордан. И пало в то время из Ефремлян сорок две тысячи...»

В ефремском диалекте еврейского языка не было звука «ш», и его носители не могли правильно сказать требуемое слово, в отличие от галаадитян. Буквально «шибболет» означает «стремнину»\*, а вот «сибболет» — «бремя». Выбор данного слова для пароля был далеко не случаен. Ефремлянина ведь не просто просили сказать одно слово, а требовали от него

---

\* Стремнина — порожистый участок реки с большим падением воды, быстрым и бурным течением.

произнести целую фразу: «Позвольте мне переправиться через стремнину», и слово «шибболет» в этом контексте казалось ему нормальной составляющей. «И человек, думая, что его просят сказать “волшебную фразу”, некий код, не сосредоточивался на произнесении этого одного слова, которое отдельно он, может быть, и смог бы произнести правильно. И он говорил “сибболет”, — тогда-то его и убивали» [19].

Сорок две тысячи жизней — цена попадания этой истории об условном слове-пароле, «волшебной фразе», на страницы Библии.

В интернете можно найти и даже прослушать\* следующую скороговорку на чешском и словацком языках:

Strč prst skrz krk.

Трудная для нас скороговорка; в ней отсутствуют гласные буквы. Буквально она означает «просунь палец сквозь горло».

Попробуйте вслед за фонограммой ее произнести — пройти, так сказать, сквозь этот шибболет.

Существует даже птичий пароль [57]! Прекрасные расписные малюры, обитающие в Австралии, нашли способ борьбы с незваными кукушатами в своем гнезде.

Самка малюра приближает голову к каждому яйцу и исполняет короткую трель. Птичка начинает петь на десятый день высиживания яиц; у ее родных птенцов есть всего пять суток, чтобы выучить песню-пароль. Подкидыши-кукушата

---

\* [https://ru.wikipedia.org/wiki/Strč\\_prst\\_skrz\\_krk](https://ru.wikipedia.org/wiki/Strč_prst_skrz_krk)

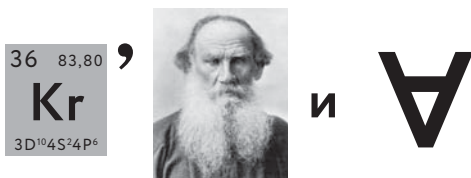


вылупляются на три дня раньше и просто не успевают запомнить мелодию.

Когда же наступает время кормления, птенчик должен повторить выученную песню матери, тем самым попросив родителей покормить его. Но кукушонок не может точно воспроизвести песенку и поэтому не получает пищи. Поняв, что в гнезде остался только птенец кукушки (ведь кукушонок выбрасывает из гнезда все имеющиеся там яйца и птенцов), малюры отправляются строить другое гнездо. Хотя птичий пароль не помогает малюрам сохранить своих птенцов, зато он дает шанс обустроить новое гнездо и вырастить родное потомство.

Под конец этюда приведем несколько несложных загадок — попробуйте отгадать задуманный предмет, который будет изображаться посредством другого, имеющего с ним какое-нибудь, возможно отдаленное, сходство. Ответы ко всем загадкам будут приведены в самом конце этюда.

Первый вид загадки — хорошо знакомый всем ребус. Слово, зашифрованное в нем, неоднократно встречалось вам на страницах книги; оно есть и в этом этюде.



Немного побалуемся шарадой, позаимствованной из книги Акентьева [2]. Кстати, иногда словом «шарада» называют тайну, загадку вообще.

Первый слог говорит:  
— Я живу на стене,  
Вечерами горит  
Ярко лампа во мне!..  
Перебил его второй:  
— Я живу на крыше,  
Ввысь взлетаю я стрелой,  
Всех антенн повыше!  
— Это все не так уж ново —  
Двум слогам сказало слово, —  
Я живу на корабле,  
Якорь поднимаю,  
Хоть и оба вы во мне,  
Я вас знать не знаю!

Итак, что это за слово, состоящее из двух слогов, каждый из которых также является полноценным словом?

И последняя загадка. «Лиза прочла стихотворение “На птичку” и радостно воскликнула, что знает, как птичка пищит. — Как же? — А вот так...» [9]. Устами младенца глаголет истина. Так как же пищит державинская птичка? Ответ на виду.

Поймали птичку голосисту  
И ну сжимать ее рукой.  
Пищит бедняжка вместо свисту,  
А ей твердят: «Пой, птичка, пой!»

*Гаврила Романович Державин,  
«На птичку»*

Приведем отгадки к загадкам. В первой отгадке чередованием цветов выделены соответствующие слова, из которых складывается ребус:

## КРИПТОГРАФИЯ

Второе слово — это брашпиль. Его слога «бра» и «шпиль» также являются самостоятельными словами.

Ответ к третьей загадке — «пи-па». Это стихотворение, по мнению автора упомянутой книги, — акrostих, в котором начальные буквы каждой строки образуют скрытую фразу, не слышимую на слух, зато ясно видимую.

# Послесловие

Вот и перевернута последняя страница. Прочитаны все тридцать этюдов, навеянных криптографическими играми. Конечно, по сравнению с самими играми этюды претерпели некоторое изменение: передать на бумаге динамику живой игры довольно затруднительно. Но в то же время это оставляет желающим простор для создания игр в своем собственном стиле.

Изучение секретов криптографии — нелегкая работа; немного занимательности в этом деле никому не помешает. Надеемся, что прочитанные этюды увлекут вас в этот необычный мир.

Как писал Ницше, зрелость — «это новое обретение той серьезности в игре, которая была у ребенка» [35]. Возможно, некоторым читателям захочется стать настоящими криптологами или в зрелом возрасте профессионально заняться дешифровкой еще не расшифрованных древних текстов, и данная книга станет первым маленьким шагом на этом пути.

В заключение приведу слова одного «несерьезного» немецкого поэта Иоганна Вольфганга Гете, которые он написал, когда ему было уже за шестьдесят, в романе «Годы учения Вильгельма Мейстера»: «Только не видеть в своих занятиях профессию, это мне претит. Все, что я могу, я хочу делать играя, как мне придется, и пока я испытываю от этого удовольствие. Так я бессознательно играл в молодости, так я хочу сознательно действовать всю жизнь».

# Благодарности

Хочу выразить благодарность своему другу Игорю Батуре, первому читателю этой книги, который помог исправить шероховатости изложения, указал на малопонятные места в тексте. В результате его усилий мне удалось упростить изложение, сделать его более доступным для понимания.

Также благодарю своих студентов Института прикладной математики и информационных технологий БФУ имени Иммануила Канта, с которыми я играл в шифры. Благодаря их живому отклику этюды постепенно доводились до ума и вылились в эту книгу.

# Литература

1. Аберт Г. В. А. Моцарт / пер. с нем., вступ. статья, коммент. К. К. Саквы. — 2-е изд. — М.: Музыка, 1987. — Ч. 1, кн. 1.
2. Акентьев В. В. Со второго взгляда. — Л.: Лениздат, 1969.
3. Акройд П. Исаак Ньютон. Биография. — М.: КоЛибри, Азбука-Аттикус, 2011.
4. Аристотель Риторика // Античные риторика / под ред. А. А. Тахо-Годи. — М.: Изд-во Моск. ун-та, 1978.
5. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России: учебно-практическое пособие по криптографии. — М.: КДУ, 2013.
6. Бабаш А. В., Шанкин Г. П. История криптографии. — М.: Гелиос АРВ, 2002.
7. Бенекс М. Прикольная наука 2. Из тайных архивов Шнобелевской премии. — М.: Книжный Клуб 36.6, 2011.
8. Бестужев М. А. Алексеевский равелин // Алексеевский равелин: секретная государственная тюрьма России в XIX веке. Кн. 1 / сост. А. А. Матышев. — Л.: Лениздат, 1990.
9. Бирюков С. Е. РОКУ УКОР: поэтические начала. М.: Рос. гос. гуманитар. ун-т, 2003.

10. Бэкон Ф. Сочинения: в 2 т. — 2-е изд., испр. и доп. / сост., общ. ред. и вступит. статья А. Л. Субботина. — М.: Мысль, 1977. — Кн. 6. Гл. I.
11. Виленкин Н. Я., Виленкин А. Н., Виленкин П. А. Комбинаторика. — М.: ФИМА, МЦНМО, 2006. — Гл. VII, п. 94, № 7.
12. Витковски Н. Сентиментальная история науки. — М.: КоЛибри, 2007.
13. Володарский А. И. Очерки средневековой индийской математики. — М.: Наука, 1977.
14. Вольфганг Амадей Моцарт. Полное собрание писем / пер. на рус. яз. И. С. Алексеевой, А. В. Бояркиной, С. А. Кокошкиной, В. М. Кислова. — М.: Международные отношения, 2006.
15. Галуев Г. А. Математические основы криптографии: учебно-методическое пособие. — Таганрог: Изд-во ТРТУ, 2003.
16. Гарднер М. Шифр Бэкона // Научно-популярный физико-математический журнал «Квант». — 1992. — № 8. — С. 21–26.
17. Гиндикин С. Г. Рассказы о физиках и математиках. — 3-е изд., расшир. — М.: МЦНМО, НМУ, 2001.
18. Гордон С. Г. Забытые письма. Открытие и дешифровка. — СПб.: Издательская группа «Евразия», 2002.
19. Дашевский З. Лекции по Книге Шофтим (Судьи). Лекция 21. 12:1–12:15. — Режим доступа: [http://www.machanaim.org/tanach/\\_da\\_sho/sho\\_21.htm](http://www.machanaim.org/tanach/_da_sho/sho_21.htm)
20. Диккенс Ч. Письмо Д. Бейнбриджу от 6.09.1864 // Диккенс Ч. Собрание сочинений: в 30 т.; под общ. ред. А. А. Аникста и В. В. Ивашевой. — М.: Гос. изд-во худ. лит., 1960. — Т. 30.
21. Диккенс Ч. Старые лампы взамен новых // Диккенс Ч. Собрание сочинений : в 30 т. / под общ. ред. А. А. Аникста и В. В. Ивашевой. — М.: Гос. изд-во худ. лит., 1960. — Т. 28.
22. Емельянов Г., Ларин Д., Бутырский Л. Франц Эпинус: дольше всех во главе отечественной криптослужбы // BIS Journal — Информационная безопасность банков. — 2014. — № 1 (12).



23. Жельников В. Криптография от папируса до компьютера. — М.: АБФ, 1996.
24. Злобин Н. В. Америка... Живут же люди. — М.: Эксмо, 2012.
25. Кан Д. Взломщики кодов. — М.: Центрполиграф, 2000.
26. Карран Д. Агата Кристи: секретный архив. — М.: Эксмо, 2010.
27. Кондорсе М. Ж. А. Н. Похвальное слово Эйлеру, 1786 г. // Портреты. Леонард Эйлер, Даниил Бернулли, Иоганн Генрих Ламберт / сост. и пер. О. Б. Шейнин. — Берлин: NG Verlag, 2009.
28. Кристи А. Автобиография. — М.: Эксмо, 2007.
29. Кропоткин П. А. Записки революционера. — М.: Московский рабочий, 1988.
30. Лейбов Р., Манин Д. Революционный держите шаг // Вокруг света. — 2011. — № 12. — С. 181–194.
31. Лурье С. Я. Заговорившие таблички. Неугомонный. — М.: ЗАО «МК-Периодика», 2002.
32. Миронов В. Б. Древние цивилизации. — М.: Вече, 2006.
33. Мордухай-Болтовской Д. Д. Философия. Психология. Математика / сост., предисл., библиогр., прим. А. В. Родина. — М.: Серебряные нити, 1998.
34. Не только Холмс. Детектив времен Конан Дойла (Антология викторианской детективной новеллы) / пер. с англ.; сост. А. Борисенко, В. Сонькина; предисл. А. Борисенко; послесл. С. Чернова. — М.: Иностранка, Азбука-Аттикус, 2012.
35. Ницше Ф. По ту сторону добра и зла // Ницше Ф. Полное собрание сочинений: в 13 т. — М.: Культурная революция, 2005. — Т. 5. — С. 82.
36. Олимпиады по криптографии и математике для школьников / А. Ю. Зубов, В. Н. Овчинников, А. В. Зязин, С. М. Рамоданов. — М.: МЦНМО, 2006.

37. Панов Е. Н. Знаки, символы, языки: коммуникация в царстве животных и в мире людей. — Изд. 6-е, испр. и доп. — М.: Изд-во ЛКИ, 2011.
38. Пересветов Р. Т. Тайны выцветших строк. — СПб.: Авалон, Азбука-классика, 2006.
39. Пирумова Н. М. Петр Алексеевич Кропоткин. — М.: Наука, 1972.
40. Полнер Т. И. Лев Толстой и его жена. История одной любви. — М.: У-Фактория, Наш дом — L'Age d'Homme, 2000.
41. Полное собрание сочинений А. С. Грибоедова: т. 1–2 / под ред. приват-доцента Императорского С.-Петербургского университета И. А. Шляпкина. — СПб.: Издание И. П. Варгунина: Типография И. Н. Скороходова, 1889. — Т. 1. — С. III. — С. 332–334.
42. Прудников В. Е. Русские педагоги-математики XVIII–XIX веков. — М.: Учпедгиз, 1956.
43. Риксон Ф. Б. Коды, шифры, сигналы и тайная передача информации. — М.: АСТ: Астрель; Владимир: ВКТ, 2011.
44. Русецкая И. А. История криптографии в Западной Европе в раннее новое время. — СПб.: Центр гуманитарных инициатив; Университетская книга-СПб, 2014.
45. Самые красивые цветы мира: иллюстрированная энциклопедия / сост. А. И. Пантлеева. — М.: Белый город, 2010.
46. Сдвижков Д. А. Пейзаж после битвы. Цорндорф, или Русские в 1758 г. // Германский исторический институт в Москве: доклады по истории XVIII века. — 2010. — № 7. — Режим доступа: <http://www.perspectivia.net>.
47. Сингх С. Книга шифров: тайная история шифров и их расшифровки. — М.: АСТ: Астрель, 2009.
48. Соболева Т. А. История шифровального дела в России. — М.: ОЛМА-Пресс, 2002.

49. Сперанский М. Н. Тайнопись в юго-славянских и русских памятниках письма. — Изд. 2-е. — М.: Книжный дом «Либроком», 2011.
50. Только не дворецкий. Золотой век британского детектива: новеллы / пер. с англ.; сост. А. Борисенко, В. Сонькина. — М.: Астрель: Corpus, 2012.
51. Тынянов Ю. Н. Как мы пишем // Как мы пишем: сборник научных трудов / А. Белый, М. Горький [и др.]. — М.: Книга, 1989.
52. Филиппов М. М. Готфрид Лейбниц. Его жизнь, общественная, научная и философская деятельность. — СПб.: Типография Высочайше утвержд. товарищества «Общественная польза», 1893.
53. Черчхаус Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. — М.: Весь Мир, 2005. — С. 55–59.
54. Шанский Н. М. Лингвистические детективы. — М.: Дрофа, 2010.
55. Эйлер Л. Письма к ученым / сост. Т. Н. Кладо. Ю. Х. Копелевич, Т. А. Лукина; под ред. акад. В. И. Смирнова. — М.-Л.: Издательство Академии наук СССР, 1963.
56. Юшкевич А. П., Копелевич Ю. Х. Христиан Гольдбах. 1690–1764. — М.: Наука, 1983.
57. Colombelli-Negrel D., Hauber M. E., Robertson J., Sulloway F. J., Hoi H., Griggio M., Kleindorfer S. Embryonic learning of vocal passwords in superb fairy-wrens reveals intruder cuckoo nestlings. *Current Biology*. Vol. 22. Issue 22. 2012. pp. 2155–2160.
58. Dickens Ch. Letter to W. Sandys 13.6.1847. — *The letters of Charles Dickens*, edited by his sister-in-law and his eldest Daughter. Leipzig, B. Tauchnits, 1880, vol. 1, p. 190.
59. Fuss P.-H. Correspondance mathématique et physique de célèbres géomètres de XVIIIe siècle. — St.Pétersbourg, 1843, Tome 1, pp. 278–293.
60. Rescher N. *Leibniz and Cryptography*. Pittsburgh: University Library Systems, University of Pittsburgh, 2012. pp. 96.

61. Rescher N. On Leibniz: Expanded Edition. University of Pittsburgh Press, 2013. Leibniz and Cryptography.
62. Rohrbach H. The Logogryph of Euler. Journal für die reine und angewandte Mathematik (Crelles Journal). Vol. 262/263, 1973. pp. 392–399.
63. Speziali P. Le logogriphe d'Euler. Stultifera navis, Bulletin de la Societe Suisse des bibliophiles, 10 me annee, № 1/2 (April), 1953. pp. 6–9.
64. Voight L. A. Biography of Alice Kober at Breaking Ground: Women in Old World Archaeology. [www.brown.edu/research/breaking\\_ground](http://www.brown.edu/research/breaking_ground).

*Научно-популярное издание*

Иван Иванович **Ефишов**

## **ТАИНСТВЕННЫЕ СТРАНИЦЫ** Занимательная криптография

Главный редактор *Артем Степанов*

Ответственный редактор *Юлия Потемкина*

Литературный редактор *Дарья Сальникова*

Арт-директор *Алексей Богомолов*

Дизайн обложки *Сергей Хозин*

Верстка *Надежда Кудрякова*

Корректоры *Лев Зелексон, Юлия Молокова*