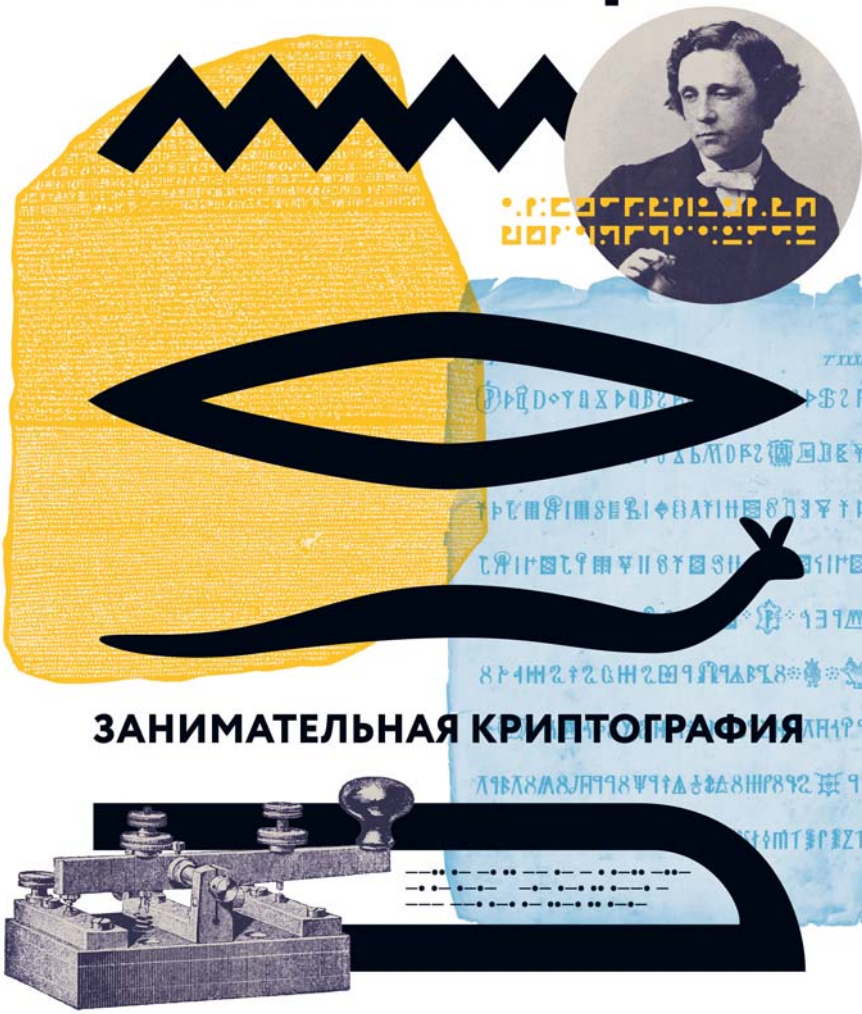
ИВАН ЕФИШОВ

ТАИНСТВЕННЫЕ СТРАНИЦЫ



ЗАНИМАТЕЛЬНАЯ КРИПТОГРАФИЯ

Содержание

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 переменке, 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 мусудресецаса в осодносом тасазусу
Пусустисилисись посо мосорюсю в гросозусу,
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 слоге. 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.

Этюд I

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.

ALE55IA. 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 Е. 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 — PI4 NER. Многие наверняка предположили, что это пионер. Но, увы, по-английски это слово пишется через О и с двумя буквами Е — pioneer. А может, владелец намекает, что его автомобиль PI4 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, датируемом приблизительно 740 годом до н. э. Оригинальный ее текст:

ΗΟΣΝΥΝΟΡΧΕΣΤΟΝΠΑΝΤΟΝΑΤΑΛΟΤΑΤΑ
ΠΑΙΖΕΙΤΟΤΟΔΕΚΛΜΙΝ

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 дипилонской 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.

издательство
МАНН, ИВАНОВ И ФЕРБЕР
Максимально полезные книги