Татьяна Соловьева

Власть тайной азбуки

Конструкция из двух вращающихся дисков с шифрами Цезаря может быть использована как для шифрования, так и для дешифрования

Секретная голова египетского раба

Писать и изобретать способы сокрытия от чужих глаз написанное человечество, похоже, научилось одновременно. Подтверждением этому могут служить зашифрованные тексты, которые археологи находят при раскопках ушедших цивилизаций Месопотамии, Египта, Индии, Китая. Древняя криптография, или тайнопись, как переводится с древнегреческого это слово, особой сложностью не отличалась. Писцы просто заменяли письменные знаки, которые мог прочесть любой, кто учился грамоте, условными символами, числами, геометрическими фигурами или рисунками, понятными лишь посвященным. Именно так был зашифрован рецепт изготовления знаменитой вавилонской синей глазури на глиняной табличке, найденной при раскопках на Евфрате и датируемой II тысячелетием до н. э. Ученым не только удалось расшиф-

ровать вавилонскую криптограмму, в которой использовались редко употребляемые клинописные знаки, современные химики смогли выполнить описанную операцию и воссоздать глазурь. Со времен Шумера и Аккада на Древнем Востоке существовал тайный язык «эме-саль», предназначенный для религиозных и магических ритуалов. Им пользовались жрецы, исполнители храмовых гимнов и предсказатели.

Тайнописью записывались заклинания и в Древнем Египте. Шифровали египтяне также медицинские рецепты, наблюдения над звездами, магические и религиозные ритуалы, а нередко даже надгробные эпитафии, предназначенные лишь для «прочтения» богами. Сами письменные знаки египтяне называли *«Mdue ntr»* – «слово бога». Не для чужих глаз предназначались и военные распоряжения правителей и полководцев. В «Истории» Геродота рассказывается о довольно своеобразных способах «пересылки» секретных фараоновых посланий: рабу обривали наголо голову и водостойкой растительной краской наносили на нее текст тайного письма. Когда волосы отрастали, раба отправляли к адресату, который, чтобы прочитать послание, снова брил его. Если, конечно, «ходячее письмо» не сбежало в пути или не было убито врагами и разбойниками.

В Древней Греции распространенным способом сокрытия информации был акростих, в котором начальные буквы каждой строки, читаемые сверху вниз, образовывали какое-либо слово или фразу. Это было не особо надежно, но возвышенные эллины ценили такое тайнописание за эстетичность. Из древнегреческих текстов известно, что письмо, понятное лишь избранным, использовали греческие философы Пифагор, Платон, Гераклит.

Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра. Он использовал шифр «скитала», известный со времен войны Спарты против Афин в V веке до н.э.

В Древней Спарте еще в V веке до н. э. для отправки и получения секретных сообщений было создано одно из первых шифровальных приспособлений – *скитала*. На жезл по спирали наматывалась узкая полоса пергамента, на которую наносился текст. Когда полосу разворачивали, написанное превращалось в бессвязный набор букв, и прочитать послание мог лишь обладатель *скиталы* аналогичного размера.

Особую важность криптография приобретала в условиях войны. Поэтому многие криптографические изобретения связаны с именами древнегреческих полководцев. Большинство придумок оказалось давно забыто. Но шифровальный диск, который создал в IV веке до н. э. политический деятель и полководец Аркадийского союза Эней Тактик, и «квадрат Полибия», носящий имя в честь своего изобрета-

теля, древнегреческого военачальника III века до н. э., пережив тысячелетия, использовались в Европе вплоть до XIX века.

Основой для греческих шифров служила замена и перестановка букв алфавита. Это оказалось настолько удобно, что позже этот способ был заимствован римлянами, с той разницей, что вместо греческих использовались латинские буквы. Собственная тайная азбука для передачи военных приказов и дипломатических сообщений была предметом особой гордости римских императоров Юлия Цезаря и Нерона. Цезарь, по утверждению древнеримского историка Светония, лично разработал шифр подстановки, в котором заменял одни буквы другими, в каждой строке сдвигая их на определенное число. Это число и было шифровальным ключом. Интересно, что, пройдя множество модификаций, алгоритм шифра Цезаря дошел до наших дней и сегодня его можно встретить даже в смартфонах!

А вот в средневековой Европе положение криптографии оказалось двойственным. С одной стороны, шифрование посланий широко использовалось в дипломатии и военном деле. С другой – тайные азбуки церковь отождествляла с черной магией, оккультизмом, алхимией, астрологией, и люди, владеющие криптографическими знаниями, считались еретиками. Чернокнижником был объявлен, например, Роджер Бэкон (1214—1292), монах-францисканец, выдающийся ученый, профессор Оксфордского и Парижского университетов. Церковный суд усмотрел крамолу в описании методов сокрытия текста при помощи тайных шифров, для которых Бэкон предлагал использовать метафоры, пропуск гласных букв, вставки букв из иностранных языков, за что ученый был осужден и провел 14 лет в заточении.

Бэкон был не единственным, кого не миновало пристальное внимание инквизиции, разве что из тех немногих, кому повезло. Чаще чернокнижников отправляли на костер.

Манускрипт Войнича

Долгое время на занятиях Роджера Бэкона криптографией основывалась и гипотеза о том, что именно его перу принадлежит рукописная книга, ставшая самой большой сенсацией криптографической науки – «Манускрипт Войнича» (название он получил по имени владельца, американского библиофила Вильфреда Войнича). Однако радиоуглеродный анализ рукописи, проведенный в XX веке, позволил установить, что к Роджеру Бэкону она не имела никакого отношения, так как создана позже – между 1404 и 1438 годами.

Главная же загадка этой рукописи была не столько в том, что неизвестен ее автор, анонимные книги в библиотеках и музеях составляют едва ли не большую часть литературного наследия европейского Средневековья. «Манускрипт Войнича» был написан на неизвестном языке и неизвестным алфавитом, который не относился ни к одной существующей системе письма и расшифровке не поддавался.

Не имели успеха и многочисленные попытки разгадать загадку необычных иллюстраций, сопровождающих текст рукописи. Так, в одной из частей книги, которая получила условное название «ботанической», более или менее узнаваемыми оказались лишь четыре растения, нарисованные в манере, характерной для травников средневековья: анютины глазки, чертополох, лилия и папоротник. Ни одно другое из изображенных растений сопоставить с земной флорой не удалось – науке они неизвестны. Мало того, что многие их них кажутся составными: корни одних соединены с листьями других и цветами третьих, на страницах рукописи изображено таинственное растение, явно напоминающее подсолнечник, о существовании которого автор рукописи просто не мог знать. Родина подсолнечника – Центральная Америка, в Европу он был привезен лишь в XVI веке, то есть после создания манускрипта.

Сбивают с толку и рисунки раздела, условно названного «биологичес-

ким», где водоемам и каналам с обнаженными купальщицами придана форма внутренних органов, соединенных скрупулезно продуманным трубопроводом. Скорее всего, это аллегорическое изображение организма с системой кровообращения. И снова

традиций – европейской или любых других – пока никто не смог.

У скептически настроенных ученых даже появилась мысль, не является ли рукопись подделкой или мистификацией. Одно время высказывалось мнение что это поддельная шиф-

Растение, напоминающее подсолнечник, – один из самых загадочных рисунков «Манускрипта Войнича»: это растение происходит с американского континента, о существовании которого во время создания рукописи известно еще не было. Библиотека редких книг и рукописей Йельского университета, Нью-Хейвен, США

«но»! Круги кровообращения английский ученый Вильям Гарвей открыл лишь два столетия спустя: в 1628 году. До этого времени в течение полутора тысяч лет господствовала теория Галена, согласно которой кровь образовывалась в печени из пищи, затем поступала в сердце, откуда по артериям и венам разносилась по органам и тканям, а движение крови происходило приливами – вперед и назад.

Неясны по содержанию и астрономические рисунки. За исключением двенадцати зодиакальных символов и изображений Солнечной системы, которые были известны в эпоху Античности и Средневековья, интерпретировать остальные иллюстрации в рамках известных астрологических

ровка XVI века, построенная с помощью «решетки Кардано», примененной для того, чтобы составить псевдослучайную бессмыслицу, в которой скрыт некий секретный текст. Но тогда нужно предположить и то, что кто-то почти двести лет хранил пергамент и чернила с целью создать когда-нибудь поддельную книгу. А принадлежность их к началу 1400-х годов исследованиями подтверждена однозначно.

Над расшифровкой загадочного текста трудились сотни исследователей, лингвистов, криптографов, в последние годы – еще и искусственный интеллект. Появляются новые теории, обнаруживаются новые характеристики структуры текста и слов,

ранее не замеченные детали рисунков. Но все напрасно: «Манускрипт Войнича» тайну самого загадочного шифра не открывает.

Инструмент гениев

С эпохой Ренессанса криптография обретает наконец научный статус. Совершенствуются известные со Средневековья способы составления тайных кодов с использованием букв латинского и греческого алфавитов, наряду с моноалфавитными, появляются шифры многоалфавитной замены, проводятся серьезные изыскания в области криптоанализа (т.е. расшифровывания сообщений или, попросту говоря, «взламывания шифров»). Все это способствует появлению новых, более сложных систем шифрования.

Первым, кто предложил вместо единственного секретного алфавита использовать два или более, был флорентийский ученый-гуманист Леон Баттиста Альберти (1404—1472), по праву считающийся отцом западной криптографии. Его труд «Трактат о шифрах», написанный в 1466 году по заказу Ватикана, стал своеобразной библией криптографии, а изобретенный ученым «диск Альберти» – основой для большинства будущих шифровальных устройств. «Диск Альберти» состоял из двух кругов, скрепленных в центре общим штифтом: *Stabilis* – неподвижного и *Mobilis* – подвижного. Каждый из них имел алфавит, написанный по краю, внешний (заглавный алфавит) для открытого текста, и внутренний (смешанный со строчными буквами) – для зашифрованного. Изобретение это произвело настоящую революцию в шифровании – такой шифр невозможно было взломать без знания специального кода, известного только тем, кто состоит в тайной переписке.

Еще одно знаменитое криптографическое устройство, появившееся в эпоху Возрождения, принадлежит итальянскому врачу и влиятельнейшему математику своего времени Джероламо Кардано (1501—1576). В историю он вошел как изобретатель кодового замка, лампы с автоматической подачей масла и механизма, широко известного всему миру как «карданный вал». В математике его имя носит «формула Кардано» для нахождения корней кубического неполного уравнения, а в криптографии – «решетка Кардано». Под этим названием известен специальный трафарет в форме прямоугольной или квадратной таблицы-карточки, с помощью которого можно закодировать секретное послание, сокрыв его внутри совершенно «невинного» текста. И хотя сам метод был довольно медленным и требовал некоторых литературных навыков, чтобы написанное не выглядело полнейшей абракадаброй, «решетка Кардано» на протяжении веков пользовалась в Европе неизменной популярностью.

Джероламо Кардано (1501—1576) был не только врачом, математиком и изобретателем знаменитой карданной передачи, без которой невозможен современный автомобиль. Он придумал еще и один из наиболее распространенных шифров тайнописи. Гравюра 1547 года.

Подобный способ шифрования относится к одной из форм стеганографии, предполагающей сокрытие самого факта существования тайного писания. Термин ввел в 1499 году аббат бенедиктинского монасты-

ря в Шпанхейме (Германия) Иоганн Тритемий (к слову, это ему принадлежат первые сведения о жизни астролога и хироманта Георга Сибелликуса Фаустуса, ставшего прообразом литературного Фауста).

В двух сочинениях из большого письменного наследия Иоганна Тритемия «Стеганография» и «Полиграфия» рассказывается о *«конкретных способах тайно писать, с помощью которых короли и властители, знатные и неизвестные, жрецы и простецы, ученые и неученые тайно, безопасно и без всяких сомнений... могли бы обмениваться письмами на расстоянии»*.

Подробно описывая разные системы тайнописи, Тритемий предлагает весьма оригинальный шифр многоалфавитной замены «Аве Мария», в котором для маскировки тайного письма буквы замещались заранее оговоренными словами религиозной лексики, чтобы шифровка, попавшая в чужие руки, воспринималась, как текст благочестивого содержания. Таким образом, одновременно реализовались оба метода защиты информации – криптография и стеганография, что для XV века было подлинным новаторством.

Вклад Тритемия в развитие тайнописания оценивается столь высоко, что наряду с Леоном Баттистой Альберти его неизменно называют одним из основоположников криптографической науки. Правда, самому аббату возделывание этой нивы стоило потери репутации и обвинений в ереси и чародействе со стороны церкви, которая внесла написанные им книги в список запрещенных. Причиной послужило увлечение Тритемия практической каббалой и «магическими» операциями над буквами для... общения с неземными силами. Своими мыслями на этот счет Тритемий поделился в одном из писем к другу Арнольду Бостию из Гентского монастыря. Но до адресата письмо не дошло – в Гент оно было доставлено, когда Бостия уже не было в живых. Послание вскрыл настоятель монастыря и, ошеломленный его содержанием, предал гласности. В результате Тритемий приобрел славу оккультиста, общающегося с демонами.

Сокрытые грамотицы

В ходу тайнопись была и на Руси. Секретными посланиями обменивались русские князья, отправляя их друг другу со специальным гонцом и помечая печатью с надписью «ДЬНЕСЛОВО», что означало: «скрытое, тайное слово». И хотя зашифрованные письма зашивали в одежду или прятали в подошве обуви, сохранить тайну это помогало не всегда – в пути гонцов перехватывали вражеские лазутчики, и письма отбирали.

В качестве шифров, известных по древним русским рукописям, использовались глаголица, вязь, греческая и латинская азбуки. Чтобы скрыть написанное от посторонних глаз, буквы писали в обратном порядке. В XV—XVI веках с тайнописными целями сокращались гласные, употреблялись перевернутые в обратную сторону и деформированные буквы. Популярна была и так называемая полусловица, когда вместо целой буквы писалась лишь ее часть. Известно, что полусловицей широко пользовался осужденный за ересь троицкий игумен Артемий.

Но особенно распространенной в XV веке была цифирь – тайнопись, основанная на употреблении букв кириллицы в качестве цифр. Еще один вид – описательная цифровая тайнопись представляла собой нечто вроде загадки или шарады.

В XVI веке в славянской тайнописи особенно часто стало применяться риторейское или литорейское письмо. Оно состояло в замене одних букв азбуки другими. Из рукописных источников того времени известно, что писцы знали десять видов «буквицы риторийской». И литореей, и цифирью пользовались для создания простых шифров профессиональные тайнописчики Посольского приказа при Иване Грозном и его сыне Федоре Иоанновиче, наказывавшем: *«Писать письма мудрою азбукою, чтоб оприч*

Флопяцевская азбука.
Тайнопись, описанная в рукописи, хранящейся в Санкт-Петербургской Публичной библиотеке. В этой тайнописи используется замена на буквы греческого и глаголического алфавита и специально придуманные знаки

Царского величества никто не разумел». Но окончательно на государственную основу тайнописное дело было поставлено лишь в Смутное время. Главную роль в этом сыграл отец царя Михаила Романова, патриарх Филарет. Он заведовал иностранными делами при молодом царе и лично занимался созданием «хитрого письма» – особой азбуки для дипломатической тайнописи.

Большим любителем «сокрытых грамотиц» был и внук патриарха, царь Алексей Михайлович, еще в детстве сочинявший простенькие шифры, в которых переставлял местами буквы. Позже, став правителем государства, он собственноручно разработал двенадцать азбук для шифрования, взяв за основу «тайную цифирь» Филарета.

В XVII веке специальные службы занимались тайнописью в Приказе тайных дел, Посольском приказе, в боярской думе, где каждый боярин старался изобрести свою собственную «тарабарскую грамоту». «Тарабарской грамотой» на Руси называли любые шифровки, используя их, где надо и где не надо – в личной переписке, в хозяйственных и даже таких простых и повседневных делах, как-то доставка птиц и лошадей или роспись дворов служилых людей.

На новый уровень криптография вышла при Петре Великом (1672–1725). За рубежом появились дипломатические представительства России, и шифрование стало основным средством защиты дипломатической информации. Обеспечения секретности переписки требовало и управление огромной внутренней территорией. Для организации связи были созданы ряд учреждений – Кабинет его императорского величества, Посольская канцелярия, Коллегия иностранных дел и т.д.– со строгим разделением функций: одни занимались созданием шифров для дипломатической тайнописи, другие – анализом перехваченных иностранных.

С каждым столетием человечество все дальше удаляется от того времени, когда для сохранения тайного сообщения гонцу древнеегипетского фараона брили голову или переставляли местами буквы алфавита. Сегодня криптографические системы стали частью повседневной жизни. Они широко используются в банках, бизнесе, цифровом телевидении, сотовой связи, мобильных приложениях, при общении в мессенджерах.