Вадим Гребенников

Европейская криптология

История спецсвязи

Вадим Гребенников

Европейская криптология. История спецсвязи

http://www.litres.ru/pages/biblio_book/?art=42591458
SelfPub; 2019
ISBN 978-5-532-10225-5

Аннотация

Книга рассказывает историю рождения и развития шифров и кодов, криптографии (шифрования), криптоанализа (расшифрования) и специальных видов засекреченной связи в ведущих странах Европы (Великобритания, Германия и др.), образования их криптологических служб, шифровальной аппаратуры и вычислительных машин для дешифровки; описывает шпионскую деятельность европейских спецслужб по «охоте» за шифрами противника, успехи и ошибки в этой сфере.

Содержание

Предисловие

Философ Фридрих Вильгельм Шеллинг писал: «То, что мы называем природой, – лишь поэма, скрытая в чудесной тайнописи». Такую же мысль высказывает и современная поэтесса Юнна Петровна Мориц: «Тайнопись – почерк всего мироздания, почерк поэзии, кисти, клавира! Тайнопись – это в тумане перевода огненный шрифт современного мира».

Бесспорно, самые первые символы и знаки, написанные или выдолбленные в камне, или вырезанные на дереве имели магический характер. Самые древние свидетельства того относятся к 17-16-му тысячелетию до н.э. На этих памятниках письменности изображены фигуры, ставшие «праотцами» известных сегодня магических символов: крестов, рун, колёс, свастик. Впоследствии эти сакральные знаки накапливались, передавались в откровениях, устно и до 3-1 тысячелетия до н.э. уже были системами, начали образовываться первые магические алфавиты.

Эти алфавиты осмысливались в те времена именно как набор священных символов с присвоенными им фонетическими значениями, что позволяло использовать эти знаки для письменности. Так возникли родственные финикийский, греческий, латинский, этрусский и рунический алфавиты, но достаточно значительная часть древних символов осталась за пределами этих алфавитов и продолжала исполь-

зоваться исключительно с магической и художественной целью.

До нашего времени как магический дошел рунический алфавит. Руны (то есть знаки древнескандинавского алфавита) были разбиты на три группы по восемь штук в каждой. Основная система шифрования являла собой шифр (араб. sifr – ноль, ничто, пустота) замены – каждой руне отвечали два знака шифротекста (косые черточки разной длины). Число чёрточек сверху помечало номер группы, а снизу – номер руны в группе. Встречались и осложнения этой системы, например руны в группах перемешивались.

До наших дней сохранился даже памятник древней шведской криптографии – рекский камень. Этот камень высотой более четырёх метров находится на кладбище села Рек. На нём нанесено 770 зашифрованных рун.

Несмотря на то, что позже в странах Скандинавии стала применяться латинская азбука, руническое письмо использовалось в XIX веке. Однако в XVI-XVIII веках достаточно мало людей знали рунические алфавиты, поэтому руническая запись даже без шифрования обеспечивала сохранение тайны переписки. В частности руны для защиты информации использовал шведский генерал Якоб де ла Гарди во время тридцатилетней войны (1618–1646).

Готское слово «runa» означает «тайна» и происходит из древнего немецкого корня со значением «прятать». В современных языках это слово также присутствует: немецкое

«raunen» значит «нашёптывать», латышское «runat» – «говорить», финское «runo» – «стихотворение, заклинание». Ещё одним магическим алфавитом, который некоторые авторы относят к «руническим надписям», является огамический (ogam, ogum, ogham), распространенный в Ирландии, Шотландии, Уэльсе и Корнуоли в III-X веках н.э. В древнеирландских текстах было упоминание о том, что «ogam» служил для передачи тайных посланий, а также для мыслей.

Вообще магическим алфавитом можно назвать любой алфавит, потому что каждая буква каждого алфавита имеет собственно символическое значение. Особенно это касается еврейского иврита и индийского санскрита, которые рядом с греческим и латинским алфавитами до этого времени используются оккультистами. Однако, невзирая на наличие сакральных значений у символов двух последних, они все-таки стали впоследствии, в первую очередь, признаками учености и культуры тех, кто их употреблял.

Символизм, который был заложен в каждую букву, выполнял две функции: во-первых, он скрывал тайны от непосвященных, а во-вторых, напротив, открывал их тем, кто был этого достоин, кто понимал скрытый смысл этих символов. Посвящённые жрецы считали святотатством обсуждение священных истин высшего света или божественных откровений вечной Природы на том же языке, который использовался простым народом. Именно из-за этого всеми сакральными традициями мира разрабатывались свои тайные

алфавиты.

Иврит является одним из самых распространенных алфавитов в Западной магической традиции, а его буквы считаются вместилищем божественной силы. Например, буква еврейского алфавита «алеф» означает власть, человека, мага; буква «бет» – науку, рот, двери храма; «гимель» – действую, протягиваю для рукопожатия руку и т. п. В алхимии буквы были также многозначительны: «A» выражало начало всех вещей; «Y» – отношение между четырьмя основными элементами; «L» – разложение; «M» – андрогенную природу воды в ее первобытном состоянии и тому подобное.

Греческий алфавит, подобно ивриту для евреев, служил грекам одним из средств познания мира. У греков буквы «Α», «Ε», «Η», «Ι», «Ο», «Υ» и «Ω» отвечали 7 планетам (небесам). Буквы «Β», «Γ», «Δ», «Ζ», «Κ», «Λ», «Μ», «Ν», «Π», «Ρ», «Σ» и «Τ» приписывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Φ» и «Χ» являли собой 4 мировых элемента (стихии), а «Ψ» – «мировой дух». Алфавит использовался также для мысли и в разных мистериях. Да, например, пятая буква греческого алфавита «Ε» (эпсилон) служила символом «Духовного Солнца» в большом храме греческих мистерий в Дельфах, где в течение семнадцати веков проводились элевсинские посвящения.

В латинском алфавите гласные буквы «A», «E», «I», «O», «U» и согласные «J», «V» отвечали 7 планетам. Согласные буквы «B», «C», «D», «F», «G», «L», «M», «N», «P», «S» и

«T» руководили 12 астрологическими знаками. Буквы «K», «Q», «X», «Z» отвечали 4 стихиям, а «H» являла собой «мировой дух». Латинский алфавит использовался во многих оккультных знаковых фигурах.

В древних цивилизациях мы находим два вида письма: иератическое, или священное письмо, которое использовалось священнослужителями для тайного общения друг с другом, и демотическое письмо, которое употреблялось всеми другими. Изобретение первой системы скорописи, которая исконно служила как тайное письмо, приписывался Тулиусу Тиро, вольноотпущенному рабу Цицерона (106-43 года до н.э.).

По свидетельству Геродота в древнем Египте роль шифра играл специально созданный жрецами язык. Там параллельно существовали три алфавита: письменный, священный и загадочный. Первый из них отображал обычный разговорный язык, второй мог использоваться для изложения религиозных текстов, а третий применялся предсказателями или для сокрытия содержания сообщений. В древней Греции также существовали десятки достаточно отличных один от другого диалектов.

Диоген Лаэртский так объяснял одну из причин угасания философии пифагорейцев: «…записана она была по-дорийски, а поскольку это наречие малопонятно, то казалось, что и учения, которые на нём выкладывают, не настоящие и перекрученные…». В книге Э.Шюре «Великие посвящённые»

встречается фраза о том, что «с большим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свою учёбу иначе, как тайными знаками и под разными символами».

Фиванский алфавит используется и сегодня благодаря стараниям не только практиков средневековых гримуаров (фр. grimoire – книга, описывающая магические процедуры и заклинания для вызова духов), но и некоторых мистически настроенных личностей, которые именуют себя «язычниками». Равно как и любой другой из категории магических, фиванский алфавит используется для написания текстов заклинаний и служит в таких случаях шифром.

Ученый Блез Паскаль писал: «Языки суть шифры, в которых не буквы заменены буквами, а слова словами, так что неизвестный язык является шифром, который легко разгадывается». Так, в 1960 году ирландские вооруженные силы в Конго, направленные туда по решению ООН, осуществляли секретные переговоры по радио на гельском языке.

С развитием фонетического письма письменность резко упростилась. В давнем семитском алфавите во 2-м тысячелетии до н.э. было всего около 30 знаков. Ими обозначались согласные звуки, а также некоторые гласные и слоги. Упрощение письма стимулировало развитие криптологии и шифровального дела.

Правителям больших государств необходимо было осуществлять «скрытое» руководство наместниками в много-

численных провинциях и получать от них информацию о состоянии дел на местах. Короли, королевы и полководцы должны были руководить своими странами и командовать своими армиями, опираясь на надёжную и эффективно действующую связь. В результате организация и обеспечение шифрованной связи для них было жизненно необходимым делом.

В то же время все они осознавали последствия того, что их сообщения попадут не в те руки, если враждебному государству станут известны важные тайны. Именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров – способов сокрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано.

Стремление обеспечить секретность означало, что в государствах функционировали подразделения, которые отвечали за обеспечение секретности связи путем разработки и использования самих надёжных кодов и шифров. А в это же время дешифровщики врага пытались раскрыть эти шифры и выведать все тайны.

Дешифровщики представляли собой алхимиков от лингвистики, отряд колдунов, которые пытались с помощью магии получить осмысленные слова из бессмысленного набора символов. История кодов и шифров – это многовековая история поединка между «творцами» и «взломщиками» шифров, интеллектуальная гонка шифровального «оружия», ко-

торое повлияло на ход истории.

Шифр всегда является объектом атаки криптоаналитиков. Как только дешифровщики создают новое средство, обнаруживающее уязвимость шифра, последующее его использование становится бессмысленным. Шифр или выходит из применения, или на его основе разрабатывается новый, более стойкий. В свою очередь, этот новый шифр используется до тех пор, пока дешифровщики не найдут его слабое место, и т.д.

Борьба, которая не прекращается между «творцами» и «взломщиками» шифров, способствовала появлению целого ряда замечательных научных открытий. Криптографы постоянно прилагали усилия для создания все более стойких шифров относительно защиты систем и средств связи, в то время как криптоаналитики беспрестанно изобретали все более мощные методы их атаки.

В своих усилиях разрушения и сохранения секретности обе стороны привлекали самые разнообразные научные дисциплины и методы: от математики к лингвистике, от теории информации к квантовой теории. В результате шифровальщики и дешифровщики обогатили эти предметы, а их профессиональная деятельность ускорила научно-технический прогресс, причем наиболее заметно это оказалось в развитии современных компьютеров.

Роль шифров в истории огромна. Шифры решали результаты боёв и приводили к смерти королей и королев. Поэтому

я обращался к историческим фактам политических интриг и рассказов об их жизни и смерти, чтобы проиллюстрировать ключевые поворотные моменты в эволюционном развитии шифров. История шифров настолько богата, что мне пришлось опустить много захватывающих историй, что, в свою очередь, значит, что моя книга не слишком полна. Если вы захотите больше узнать о том, что вас заинтересовало, или о криптологе, который произвёл на вас неизгладимое впечатление, то я рекомендую обратиться к списку использованной литературы, которая поможет глубже изучить конкретные факты истории.

Шифрование – единственный способ защитить нашу частную жизнь и гарантировать успешное функционирование электронного рынка. Искусство тайнописи, которая переводится на греческий язык как криптография, даст вам замки и ключи информационного века. Чтобы в последующем вся изложенная ниже информация была понятной, рассмотрим основные понятия и термины этой науки.

Информация, которая может быть прочитана и понятна без каких-либо специальных мероприятий, называется открытым текстом. Метод перекручивания и сокрытия открытого текста таким образом, чтобы спрятать его суть, называется зашифрованием. Зашифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифротекстом. Шифровка позволяет спрятать информацию от тех, для кого она не предназначается, невзирая на

то, что они могут видеть сам шифротекст. Противоположный процесс превращения шифротекста в его исходный вид называется расшифровыванием.

Криптография – это мероприятия по сокрытию и защите информации, а криптоанализ – это мероприятия по анализу и раскрытию зашифрованной информации. Вместе криптография и криптоанализ создают науку криптологию.

Криптология – это наука об использовании математики для зашифрования и расшифровывания информации. Криптология позволяет хранить важную информацию при передаче её обычными незащищёнными каналами связи (в частности, Интернет) в таком виде, что она не может быть прочитанной или понятной никем, кроме определённого получателя. Криптоанализ являет собой смесь аналитики, математических и статистических расчётов, а также решительности и удачи. Криптоаналитиков также называют «взломщиками».

Криптографическая стойкость измеряется тем, сколько понадобится времени и ресурсов, чтобы из шифротекста восстановить исходной открытый текст. Результатом стойкой криптографии является шифротекст, который чрезвычайно сложно «сломать» без владения определенными инструментами дешифрования.

Криптографический алгоритм, или шифр – это математическая формула, которая описывает процессы шифрования и расшифрования. Секретный элемент шифра, который

должен быть недоступный посторонним, называется ключом шифра.

Чтобы зашифровать открытый текст или разговор, криптоалгоритм работает в сочетании с ключом – словом, числом или фразой. Одно и то же сообщение, зашифрованное одним алгоритмом, но разными ключами, будет превращать его в разный шифротекст. Защищённость шифротекста полностью зависит от двух вещей: стойкости криптоалгоритма и секретности ключа.

Самым простым видом шифровки является кодировка, где не используется ключ. Хотя в современной криптологии код не считается шифром, тем не менее он таким является – это шифр простой замены. Кодирование, как правило, содержит в себе применение большой таблицы или кодового словаря, где перечислены числовые соответствия (эквиваленты) не только для отдельных букв, но и для целых слов и наиболее используемых фраз и предложений.

Ну, а теперь перейдем к интересной и захватывающей истории криптологии в странах Европы…

1. Появление шифров

Вообще все шифры могут быть разделены на два вида: перестановка и замена. При перестановке буквы сообщения просто переставляются, образовывая анаграмму. Для очень короткого сообщения, которое складывается, например, из одного слова, такой способ достаточно ненадежный, поскольку существует крайне ограниченное число возможных способов перестановки букв. Так, 3 буквы могут быть расставлены всего лишь 6 разными способами. Однако по мере увеличения численности букв количество возможных перестановок стремительно растет, и возобновить исходное сообщение становится невозможно, если неизвестен точный способ шифрования. Например, если фраза состоит из 35 букв, то количество их разных перестановок составляет больше 50 000 000 000 000 000 000 000 000 000 000.

Если бы один человек смог проверять одну перестановку в секунду, и если бы все люди на Земле работали круглые сутки, чтобы проверить все возможные перестановки, нужно было бы времени в тысячу раз больше, чем срок существования Вселенной.

Создается впечатление, что случайная перестановка букв гарантирует очень высокую степень безопасности, поскольку для противника дешифровать даже короткое предложение окажется невыполнимым. Однако при перестановке может

образоваться невероятно сложная анаграмма, и если буквы случайно, ни с того, ни с сего перепутаются, то ни получатель, ни перехватчик не смогут ее расшифровать. Поэтому способ перестановки букв должен быть предварительно обсужден отправителем сообщения и его получателем, но вместе с тем сохраняться в тайне от противника.

Первым шифровальным устройством, которое дошло до нас и реализовывало шифр перестановки, была так называемая «скитала» или «сцитала» (около VI-V ст. до н.э.), которая использовалась в античный период спартанцами.

Скитала представляла собой деревянный цилиндр, вокруг которого наматывалась полоска кожи или пергамента. Отправитель писал сообщение по всей длине скитады, а затем разматывал полоску, на которой после этого оставался бессмысленный набор букв. Таким образом сообщение оказывалось зашифрованным. Вестник брал эту полоску и прятал сообщение, используя полоску как пояс, буквами вовнутрь, то есть кроме криптографии использовалась также и стеганография. Чтобы получить исходное сообщение, адресат просто наматывал полоску кожи вокруг скитады того же диаметра, какой был и у скитады отправителя.

В 404 году до н.э. к спартанскому полководцу Лисандру привели одного из 5-ти вестников, который остался живым после крайне опасного путешествия из Персии, был окровавлен и едва держался на ногах. Он передал свой пояс Лисандру, который намотал его вокруг своей скитады и прочитал,

что персидский военачальник Фарнабаз собирается напасть на него. Благодаря скитале Лисандр успел подготовиться к нападению и отбил его.

Греческий историк Плутарх так описал этот способ шифрования: «Отправляя к месту службы начальника флота или сухопутного войска, эфоры вручают отъезжающему круглую палку. Другую, совершенно одинаковой длины и толщины, оставляют себе. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, плотно, без промежутков наматывают ее на свою скиталу и пишут на нем текст. Затем снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение».

Это то же самое, что и буквы писать не подряд, а через определенное число, по кругу до тех пор, пока весь текст не закончится. Сообщение «ВЫСТУПАЙТЕ» при окружности палочки в 3 буквы даст шифровку «ВУТИПЕСАТЙ».

Для прочтения шифровки нужно было не только знать систему засекречивания, но и иметь ключ в виде палки определенного диаметра. Зная тип шифра, но не имея ключ, расшифровать сообщение было бы сложно. Шифр был до-

статочно популярен в Спарте и многократно совершенствовался в более поздние времена. О его важном значении и большом распространении говорит свидетельство Плутарха в «Сравнительных жизнеописаниях», когда историк сообщает о жизни греческого полководца Алкивиада: «Однако Лисандр обратил внимание на эти слова не раньше, чем получил из дома скиталу с приказанием отделаться от Алкивиада… »

Этот нехитрый способ часто использовался из-за своей простоты и возможности оперативного расшифровывания сообщений. В то же время стойкость данного шифра была небольшой, потому что позже Архимед предложил устройство («антискитала»), с помощью которого расшифровка подобного сообщения без нужного цилиндра была достаточно простой и быстрой. Ремень наматывали на коническое «копье» и двигали верх и вниз до тех пор, пока не находили нужный диаметр, а текст сообщения становился понятным.

Альтернативным шифру перестановки был шифр замены, в котором каждая буква в исходном тексте замещалась другой буквой. Одно из первых описаний шифра замены было приведено в трактате «Камасутра», написанном в IV веке н.э. священником-брамином Ватсьяяной Малланага, но основанному на манускриптах, которые относятся к IV веку до н.э.

В соответствии с «Камасутрой» женщины должны владеть 64 искусствами, такие как приготовление еды и напит-

ков, искусство одевания, массажа, приготовления ароматов. В этот список также входили менее очевидные искусства: колдовство, игра в шахматы, переплетное дело и плотничество. Под номером 45 в списке находилось искусство тайнописи «mlecchita-vikalpa», предназначенное для того, чтобы помочь женщинам скрыть подробности своих любовных связей.

Один из таких способов заключался в том, чтобы расположить попарно буквы алфавита случайным образом, а затем замещать каждую букву в исходном сообщении ее парной (симметричной). Если применить этот принцип к латинскому алфавиту, то можно составить такую таблицу (линейку) шифрования:

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

Тогда вместо слова «UKRAINE» отправитель напишет слово «QJNBGRS».

На Ближнем Востоке один из первых шифров замены был разработан древними евреями и назывался «темура» – «обмен». 22 буквы еврейского алфавита делились на две части, причем одна содержалась над другой; потом верхние буквы замещались на нижние или наоборот. Можно было установить всевозможные комбинации в зависимости от места деления алфавита и направления перемещаемых букв.

Самый простой способ заключался в делении алфавита посередине так, чтобы первые две буквы, «А» и «Б», совпа-

дали с двумя последними, «Т» и «Ш». Эти буквы и дали название методу шифровки – «Атбаш» (англ. Atbash). Это был простой шифр одноалфавитной замены для еврейского алфавита. Таблица (линейка) шифровки этим методом для латинского алфавита будет выглядеть таким образом:

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

Видим, что в этом шифре замена имеет симметричный вид. Таким образом слово «UZHGOROD» превращалось в слово «FASTLILW».

Другой шифр «Альбам» заключался в разбивке алфавита на две части и расположении одной части под другой, но применялось другое направление расстановки букв:

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

Слово «UZHGOROD» превращалось уже в слово «HMUTBEBQ».

Первое документально подтверждено использование шифра замены в военных целях появилось в «Записках о галльской войне» (лат. Commentarii de Bello Gallico) Гая Юлия Цезаря (I века до н.э.). Цезарь описывал, как он послал сообщение Цицерону, который находился в осаде и был на грани капитуляции. В этих листьях латинские буквы были заменены греческими, потому враг его не смог бы понять.

Цезарь так часто пользовался тайнописью, что Марко Валерий Проб написал целый трактат о применяемых им шиф-

рах, который, к сожалению, не дошел до наших дней. Однако благодаря произведению Гая Транквилла Светония «Жизнь 12 Цезарей», написанному во II веке н.э., у нас есть подробное описание одно из шифров замены, которые применялись Юлием Цезарем. Он просто замещал каждую букву в послании буквой, которая находилась в алфавите на три позиции дальше.

Вот как об этом сообщает Рощу Светоний: «Существуют и его письма Цицерону и письма к близким о домашних делах: у них, если нужно было сообщить что-либо негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не состояло ни одно слово. Чтобы разобрать и прочитать их, нужно читать каждый раз четвертую букву вместо первой».

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

Сначала выписывался алфавит в естественном порядке, а затем под ним выписывался тот же алфавит, но с сдвигом на 3 буквы влево. При зашифровании буква «A» замещалась буквой «D», «B» замещалась на «E», «C» – на «F» и так далее. Таким образом слово «UZHGOROD» превращалось в шифротекст «XCKJRURG», а «UKRAINE» – в «XNUDLQH». Получатель зашифрованного сообщения искал эти буквы в нижней строке и по буквам над ними возобновлял исходное слово. Ключом в шифре Цезаря была величина сдвига нижней строки алфавита, то есть цифра 3. На-

следник Юлия Цезаря – Цезарь Август – использовал тот же шифр, но с ключом сдвига 4.

Уже в IV веке до н.э. делались попытки «механизации» криптологического дела, связанные в первую очередь с именем древнегреческого полководца Энея Тактики, защитника Трои, друга Гектора. Он создал так называемый «диск Энея», который получил в Древней Греции широкое применение. В диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия, которые соответствовали буквам алфавита, через которые протягивалась нить в соответствии с буквами шифрованного текста. Для расшифровывания нить вытягивали, получая обратную последовательность букв. Этот примитивный на первый взгляд способ шифрования был достаточно эффективен, потому что противнику, который перехватил сообщение, было неизвестно, какая буква отвечает каждому отверстию. Кроме того, если возникала опасность перехвата сообщения, нить можно было легко порвать, тем самым уничтожив его.

Идея Энея была использована при создании и других оригинальных шифров замены. В частности, в одном из вариантов вместо диска использовалась линейка с количеством отверстий, равным количеству букв алфавита. Каждое отверстие соответствовало своей букве, а буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на нее нитью. Рядом с катушкой была прорезь.

При шифровании нить протягивалась через прорезь, а затем через отверстие, которое отвечало первой букве шифрованного текста, при этом на нити завязывался узелок в месте прохождения ее через отверстие. Потом нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и так далее.

По окончании шифровки нить вытягивалась и передавалась получателю сообщения. Тот, имея идентичную линейку, протягивал нить через прорез к отверстиям, обусловленным узлами, и возобновлял исходный текст по буквам отверстий.

Это устройство получило название «линейка Энея». Шифр, реализованный линейкой Энея, был одним из примеров шифра замены: когда буквы замещались на расстоянии между узелками с учетом прохождения через прорез. Ключом шифра был порядок расположения букв по отверстиям в линейке.

Противник, который получил нить (даже, имея линейку, но без нанесенных на ней букв), не мог прочитать переданное сообщение. Аналогичное «линейке Энея» «узелковое письмо» получило распространение у индейцев Центральной Америки. Свои сообщения они также передавали в виде нити, на которой завязывались разноцветные узелки, которые определяли содержание сообщения.

Еще одно изобретение древних греков – так называемый «квадрат Полибия». Греческий писатель Полибий (около

200 – 120 до н.э.) использовал систему сигнализации, которая была широко принята как метод шифровки. Он записывал буквы греческого алфавита в квадратную таблицу и замещал их числовыми координатами в таблице номером строки и номером столбца. Пары чисел передавались с помощью факелов. В варианте с латинским алфавитом для передачи, например, буквы «U» нужно было взять 4 факела в правую руку и 5 – в левую, или записать как цифру «45» (см. таблицу).

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

Например, слово «UKRAINE» можно записать как цифровой шифротекст «45254211243315» или «54522411423351».

Интересно, что шифр Полибия дошел до наших дней и получил своеобразное название «шифра узников». Для его

использования нужно было только знать естественный порядок расположения букв алфавита (как в вышеупомянутом примере для английского языка). Число 3, например, передавалось путем тройного стука. При передаче буквы сначала отстукивалось число номера строки, в которой находилась буква, а затем число номера соответствующего столбца. Например, буква «F» передавалась двойным стуком (вторая строка) и потом одинарным (первый столбец).

С применением этого шифра связаны некоторые исторические казусы. Да, российские «декабристы», которые были заключены после неудачного восстания, не смогли установить связь с князем Одоевским. Оказалось, что он (хорошо образованный при тех временах) не помнил естественный порядок расположения букв в российском и французском алфавитах (другими языками он не владел). «Декабристы» для российского алфавита использовали прямоугольник размера 5x6 (5 строк и 6 столбцов) и сокращен до 30 букв алфавит.

Позже буквы стали располагать в квадрате хаотически, но это требовало наличие такого квадрата у получателя сообщения, которое также было опасно. Выход был найден в применении так называемого ключевого слова, которое легко запоминалось. Избиралось недолгое слово (например, «UKRAINE»), из него забирались буквы, что повторялись, а те, которые оставались, записывались в первые клетки квадрата по строкам. Пустые клетки заполнялись буквами алфа-

вита, которые остались, в естественном порядке (см. таблицу).

	1	2	3	4	5
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

В результате такой шифровки слово «UZHGOROD» превращается в цифровой шифротекст «11553332414125».

Полибийский квадрат стал одной из наиболее широко распространенных криптосистем, которые употреблялись в то время. Этому способствовала его достаточно высокая стойкость (во всяком случае, к автоматизации дешифровальных систем): квадрат 5x5 для латинского алфавита содержит 155112100433310000000000000 (расчет достаточно приблизителен) возможных положений, что практически исключает его дешифрацию без знания ключа.

Ленивые и потому изобретательные римляне в IV веке до н.э., чтобы упростить процедуру шифрования, начали при-

менять два шифровальных диска. Каждый из дисков, размещенных на общей оси, содержал на своём ободе алфавит в случайной последовательности. Каждой букве первого диска отвечала буква второго, что и составляло шифр. Найдя на одном диске букву текста, из другого диска считывали соответствующую ей букву шифра. Такие приборы, которые создавали шифр простой замены, использовались вплоть до эпохи Возрождения.

Эти криптосистемы активно применялись в Древней Греции и Риме и надолго определили характер криптологии. В условиях необходимости ручного расшифровывания, полибийский квадрат был практически неуязвимым шифром, а скитала и диск Энея были достаточно простыми. Однако они позволяли оперативно зашифровывать и расшифровывать информацию, что делало их выгодными, скажем, в полевых условиях для оперативной передачи приказов.

С упадком античной цивилизации и образованием в Европе варварских государств, криптология обветшала. Большой вред её развитию был нанесён во времена средневековой инквизиции. Все лучшие достижения цивилизации, а вместе с ними и криптология, были утеряны. По свидетельству святого Джерома «весь мир окунулся в руины». В условиях, когда грамотность была крайне низкой, зашифровывать сообщение не было необходимости, потому и самих письменных сообщений практически не было.

Так, король франков Карл Великий, основавший в 800 го-

ду Священную Римскую империю, научился читать и писать только в 50 лет. Тем не менее он знал и использовал в переписке со своими генералами шифр замены букв алфавита группой символов.

Образование и грамотность в те времена сосредоточились в церкви, поэтому тайнопись стала её монополией. Церковь постановила, что простым парафиянам нельзя скрывать тайны от «Господа», а тайнопись – это «ересь». При использовании тайнописи предусматривались жестокие виды наказания, вплоть до казни.

Кроме вышеперечисленных причин, криптология находилась в упадке ещё и потому, что в ней видели элементы колдовства. Набор непонятных букв или символов, сам по себе похожий на заклинание, воспринимался как что-то магическое, а люди, понимавшие в этом наборе символов содержание, расценивались как колдуны или маги, что не могло не наложить свой отпечаток на отношение к ним в христианской Европе.

С первых дней своего существования криптология была нацелена на утаивание содержания важных разделов письменных документов, имевших отношение к таким сферам магии, как мысль и заклинание. В одной из рукописей о магии, которая датируется III веком н.э., был использован шифр для утаивания важных частей колдовских рецептов. Криптология часто служила магии во времена средневековья, и даже в эпоху Возрождения с помощью шифров алхи-

мики засекречивали важные части формул получения «философского камня».

К шифрованию информации «призывались» и мистические силы. Так, например, рекомендовалось использовать «магические квадраты». В квадрат размером 4 х 4 вписывались числа от 1 до 16. Его магия заключалась в том, что сумма чисел по строкам, столбцам и диагоналям равнялась одному и тому же числу, равному 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

Магический квадрат			
16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Для зашифрования слова «ЗАКАРПАТЬЕ» буквы вписывались последовательно в квадрат в соответствии с записанными в них цифрами, а в пустые клетки вписывались любые буквы (см. таблицу).

16Ж	3К	2А	13Г
5Р	10Я	11Б	8Т
9Т	6П	7А	12В
4А	15Е	14Д	1З

После этого буквы записывались в строку и получался такой шифротекст: ЖКАГРЯБТТПАВАЕДЗ. Данный шифр – это обычный шифр перестановки, но считалось, что особую стойкость ему придают свойства «магического квадрата».

На первый взгляд кажется, что магических квадратов очень мало. Однако их число очень быстро растёт с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты. Магических квадратов 4x4 насчитывается уже 880, а их число размером 5x5 около 250 тысяч. Поэтому магические квадраты больших размеров могли быть красивой основой для надёжной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

Подобие между магией и криптологией обусловливалась и другими факторами. Кроме криптологии, таинственные символы использовались и в таких сферах магических знаний, как астрология и алхимия, где каждая планета и каж-

дое химическое вещество обозначались своим специальным символом. Как и зашифрованные слова, заклинания и магические формулы напоминали бессмыслицу, но в действительности имели важное значение.

То, что писали или рисовали астрологи и маги, было похоже на кодограмму, где каждый символ или иероглиф имел свое как экзотерическое (материальное), так и эзотерическое (духовное) значение. Например, символ Солнца – это индивидуальность и духовность, Луны – мягкость и душевность, Меркурия – мышление и интеллектуальность, Венеры – женственность и любовь, Марса – мужество и активность, Юпитера – законопослушание и религиозность, Сатурна – одиночество и целенаправленность и т.д.

Даже места символов, где они были нарисованы, тоже определяли их влияние на события жизни и взаимоотношения с другими факторами судьбы. А то, что одним рисунком (гороскопом) можно было отобразить судьбу и всю жизнь человека или страны, казалось настоящей магией или колдовством.

Мысль о том, что криптоанализ является также по своей сути какой-то магией, складывалась в связи с поверхностным подобием криптоанализа и размышления. Добывание истинного содержания шифротекста казалось точно таким же делом, что и получение знаний путём изучения расположения звёзд и планет (астрология), длины линий и мест их пересечения на ладони (хиромантия), положения кофейного

осадка в чашке (гадание). Видимость брала верх над реальностью. Простодушные люди видели магию даже в обычном процессе расшифровывания. Другие видели её в криптоанализе, потому что раскрытие чего-то глубоко спрятанного казалось им непостижимым и сверхъестественным.

Не таким сильным был упадок криптологии в Византии, которая сохранила много античных традиций. Но и здесь криптосистемы очень упростились и были легко читаемыми. Очень часто сообщение просто писали в обратном порядке или замещали каждую букву на следующую по алфавиту. Для засекречивания сообщений также использовали малоизвестные иностранные языки, чаще всего армянский или древнееврейский. Но в целом, в сравнении с эпохой античности, криптология находилась на крайне низком уровне.

В китайском трактате «Основы классической военной науки», составленном в XI веке н.э., присутствовали лишь рекомендации по кодированию. В них рекомендовалось соотнести с разными простыми сообщениями первые 40 знаков какого-либо стихотворения, известного как отправителю, так и получателю. По первому знаку стихотворения, поставленному в условленном месте полностью невинного сообщения, получатель «считывал» информацию, например, что нужно послать больше провианта. Такие коды практически не поддавались расшифрованию, но могли использоваться лишь в очень ограниченном масштабе.

Некоторые религиозные организации использовали для

шифрования переписки свои алфавитные шифры замены. Так, шифры тамплиеров и розенкрейцеров были очень похожими и нашли своих почитателей в лице масонов (некоторые исследователи, в частности, Е.П. Блаватская, так их и называли – масонские). Масонский шифр использовался их «ложами» для тайной переписки между посвящёнными высших степеней.

В XVIII веке франкмасонами использовался для обеспечения секретности своих документов так называемый шифр «Pigpen». В нём каждая буква заменялась определённым символом: чтобы зашифровать букву, определялось её местонахождение в одной из четырех сеток, а затем рисовалась та часть сетки, которая отвечала этой букве.

2. Шифрование как наука

В арабском мире криптология не только не обветшала, но продолжала успешно развиваться и достигла значительных успехов. О тайнописи и ее значении говорилось даже в сказках «Тысячи и одной ночи». В 855 году арабский писатель, алхимик и египтолог Абу Бакр Ахмед ибн Вахш (Ахмад Бин Абубекр Бин Вахиши) описал известные ему классические шифралфавиты в своей «Книге о большом стремлении человека разгадать загадки древней письменности» (араб. Kitab Shawq al-Mustaham). Издание арабского текста с английским переводом появилось лишь в 1806 году.

Это была одна из первых книг о криптологии с описаниями нескольких шифров, в частности с применением нескольких алфавитов, где автор также обсуждает некоторые древние письменности и утверждает о дешифровке египетских иероглифов. Один из шифралфавитов, называемый «дауди» (по имени израильского царя Давида), использовался для зашифрования трактатов по «чёрной» магии. Он был составлен из видоизменённых букв древнееврейского алфавита.

Кроме того, самый ранний из всех известных методов использования частоты появления букв с целью «взлома» шифров принадлежал перу арабского ученого Абу Юсуф Якуб ибн Исхак ибн Сабах аль-Кинди (около 800-879) и был

датирован приблизительно 850 годом. Известный как «философ арабского мира», аль-Кинди был автором 290 книг по медицине, астрономии, математике, лингвистике и музыке.

Его знаменитый трактат, обнаруженный заново лишь в 1987 году в оттоманском архиве Сулаймания в Стамбуле, назывался «Трактат о дешифровке криптографических сообщений аль-Кинди». Хотя в нем был изложен подробный анализ статистики, фонетики и синтаксиса арабского языка, революционная система криптоанализа аль-Кинди вмещается в два коротких абзаца:

«Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, – это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву «первой», букву, которая по частоте появления стоит на втором месте, назовем «вторая», букву, которая по частоте появления стоит на третьем месте, назовем «третья» и так далее, пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его «первой» буквой незашифрованного текста, второй по частоте появления символ заменим «второй» буквой, третий по частоте появления символ заменим «тре-

тьей» буквой и так далее, пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать».

Но по-настоящему характеризует познание арабов в сфере криптологии энциклопедия из 14-ти томов «Шауба аль-Аша» (Светоч для незрячего в ремесле писаря), которая была написана ученым Шихабом ад-Дин Абу-л-Аббас Ахмад ибн Али ал-Калкашанди (1335-1418) в 1412 году. В разделе «Относительно сокрытия букв тайных сообщений», автор изложил все известные ему на то время существующие в арабском мире криптосистемы. Он содержал две части: одна касалась символических действий и намеков, а другая была посвящена симпатическим чернилам и криптологии.

В работе предлагалось семь систем шифрования, которые повторяли неопубликованные идеи его предшественника Ибн ад-Дурайхима (1312-1361), который был первым, который использовал частотный анализ букв:

– заменять одну букву другой;

– писать слово в обратном порядке;

– переставлять в обратном порядке буквы слов;

– заменять буквы на цифры согласно принятой замене арабских букв числами;

– заменять каждую букву открытого текста на две арабских буквы, которые используются и как числа, и сумма которых равна цифровой величине шифруемой буквы открытого текста;

– заменять каждую букву именем какого-либо человека;

– использовать словарь замены, описывающий положение Луны, названия стран (в определенном порядке), названия фруктов, деревьев и тому подобное.

Первый раз за всю историю шифров в энциклопедии приводился список как систем перестановки, так и систем замены. Более того, в пятом пункте списка впервые вспоминался шифр, для которого была характерна более, чем одна замена букв открытого текста. Однако каким бы замечательным и важным этот факт не был, он затмевается первым в истории описанием криптоаналитического исследования шифротекста.

Его источники, по-видимому, стоит искать в интенсивном и скрупулезном изучении Корана многочисленными школами арабских грамматиков. Вместе с другими исследованиями они занимались подсчетом частоты появления слов, пытаясь составить хронологию глав Корана, изучали фонетику слов, чтобы установить, были ли они действительно арабскими или были заимствованы из других языков. Большую роль в выявлении лингвистических закономерностей, которые привели к возникновению криптоанализа у арабов, сыграло также развитие лексикографии. Ведь при составлении словарей авторам фактически приходилось учитывать частоту появления букв, а также то, какие буквы могут стоять рядом, а которые никогда не встречаются по соседству.

Калкашанди писал в своей книге: «Если вы хотите про-

честь сообщение, которое вы получили в зашифрованном виде, то прежде всего начните подсчет букв, а затем сосчитайте, сколько раз повторяется каждый знак, и подведите итог в каждом отдельном случае. Если изобретатель шифра был очень внимателен и скрыл в сообщении все границы между словами, то первая задача, которая должна быть решена, заключается в нахождении знака, разделяющего слова. Это делается так: вы берете букву и работаете, исходя из предположения, что следующая буква является знаком, делящим слова. И таким образом вы изучаете все сообщение с учетом различных комбинаций букв, из которых могут быть составлены слова…

Если получается, тогда все в порядке; если нет, то вы берете следующую по счету букву и т. д., пока вы не сможете установить знак раздела между словами. Затем нужно найти, какие буквы чаще всего встречаются в сообщении, и сравнить их с образцом частоты встречаемости букв, о котором упоминалось прежде.

Когда вы увидите, что одна буква попадается чаще других в данном сообщении, вы предполагаете, что это буква «Алеф». Затем вы предполагаете, что следующая по частоте встречаемости будет буквой «Лам». Точность вашего предположения должна подтверждаться тем фактом, что в большинстве контекстов буква «Лам» следует за буквой «Алеф»…

Затем первые слова, которые вы попытаетесь разгадать

в сообщении, должны состоять из двух букв. Это делается путем оценки наиболее вероятных комбинаций букв до тех пор, пока вы не убедитесь в том, что вы стоите на правильном пути. Тогда вы глядите на их знаки и выписываете их эквиваленты всякий раз, когда они попадаются в сообщении.

Нужно применять точно такой же принцип по отношению к трехбуквенным словам этого сообщения, пока вы не убедитесь, что вы на что-то напали. Вы выписываете эквиваленты из всего сообщения. Этот же принцип применяется по отношению к словам, состоящим из четырех и пяти букв, причем метод работы прежний.

Всякий раз, когда возникает какое-либо сомнение, нужно высказать два, три предположения или еще больше и выписать каждое из них, пока оно не подтвердится на основании другого слова».

Дав это четкое объяснение, Калкашанди приводит пример раскрытия шифра. Дешифрованная криптограмма состоит из двух стихотворных строк, зашифрованных с помощью условных символов. В заключение Калкашанди отметил, что восемь букв не было использовано и что это именно те буквы, которые находятся в конце перечня, составленного по частоте появления.

Он подчеркнул: «Однако это простая случайность: буква может быть поставлена не на то место, которое она должна занимать в вышеупомянутом перечне». Такое замечание свидетельствует о наличии большого опыта в сфере крипто-

анализа. Чтобы расставить все точки над «i», Калкашанди приводит второй пример криптоанализа достаточно длинной криптограммы. Этим примером он и закончил раздел по криптологии.

Арабы первыми обратили внимание на возможность использования стандартных слов и выражений для дешифровки. Так, первый широко известный филолог среди арабов Халиль ибн Ахмад аль-Фарахиди (около 718-791), дешифровавший криптограмму на греческом языке, посланную ему византийским императором, заявил:

«Я сказал себе, что письмо должно начинаться со слов «Во имя Бога» или как-нибудь в этом роде. Итак, я составил на основе этого первые буквы, и все оказалось правильным». На основе открытого им метода дешифрования он написал книгу «Китаб аль-Маумма» («Книга тайного языка»).

История замалчивает то, как арабы использовали свои блестящие криптоаналитические способности, которые продемонстрировал Калкашанди, для раскрытия военных и дипломатических криптограмм, или какое влияние это оказало на мусульманскую историю. Однако понятно, что вскоре эти знания перестали применяться на практике и были забыты. Один эпизод, который состоялся почти 200 лет спустя, ярко демонстрирует эту деградацию в сфере криптоанализа.

В 1600 году марокканский султан Ахмед аль-Мансур направил к английской королеве Елизавете I посольство во главе с доверенным человеком – министром Абдель Вахид ибн

Масуд ибн Мухаммед Ануном. Посольство должно было заключить с Англией союз, направленный против Испании. Анун отправил на родину зашифрованную простой заменой депешу, которая вскоре после этого каким-то образом попала в руки одного араба. Араб тот был, возможно, умным человеком, но, к сожалению, он ничего не знал о большом арабском наследстве в сфере криптоанализа. Свидетельство тому – памятная записка, в которой он написал:

«Хвала Аллаху! Относительно письма министра Абдель Вахид ибн Масуд ибн Мухаммед Ануна. Я нашел письмо, написанное его рукой, в котором он с помощью тайных знаков изложил некоторые сведения, предназначенные для нашего покровителя Ахмеда аль-Мансура. Эти сведения касаются султанши христиан (да покарает их Аллах!), которая жила в стране под названием Лондон… С того момента, как это письмо попало ко мне, я постоянно время от времени изучал содержавшиеся в нем знаки. Прошло примерно 15 лет, пока не наступило то время, когда Аллах позволил мне понять эти знаки, хотя никто не обучал меня этому…».

Конец ознакомительного фрагмента.