
Вадим Гребенников
Европейская криптология
История спецсвязи
KRYHA
LILIPUT
12+

Вадим Гребенников

Европейская криптология. История спецсвязи

«ЛитРес: Самиздат»

2019

Гребенников В.

Европейская криптология. История спецсвязи / В. Гребенников — «ЛитРес: Самиздат», 2019

ISBN 978-5-5321-0225-5

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.

ISBN 978-5-5321-0225-5

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 использоваться 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 «рунические 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 «A», «E», «H», «I», «O», «Y» и «Ω» отвечали 7 планетам (небесам). Буквы «B», «Г», «Δ», «Z», «K», «Λ», «M», «N», «П», «P», «Σ» и «T» приписывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Ф» и «X» 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 «E» (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 многочисленных 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», которое 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 скиталы, 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 скиталы того же диаметра, какой был и у скиталы 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 скиталы 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 достаточно 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 напитков, 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», совпадали 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 шифрах, 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. Наследник 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 алфавита, 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 5х5 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 применять 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 году 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 похо-

жий 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 алхимики 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 3х3, если не принимать во внимание его повороты. Магических квадратов 4х4 насчитывается уже 880, а их число размером 5х5 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 каждое 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 «третьей» 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 прочесть 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 криптоанализа. 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…».

Отметим, что такое задание Калкашанди выполнил бы не за 15 лет, а за несколько часов!

Неизвестно, была ли тесная связь между развитием европейской и восточной криптологии. Безусловно подобного рода контакты могли происходить в Испании и во время Крестовых походов, но утверждать, что европейская криптология в то время использовала арабский опыт, нельзя. Труды Калкашанди не были переведены с арабского языка, поэтому прямой связи европейской криптологии с восточной нет. Кроме того, если на востоке криптология была скорее частью лингвистики, то в Европе она была ближе к математике и естественным наукам, что также определило ее специфику.

Европейская цивилизация начала пользоваться криптологией со времен средневекового феодализма. Правда, сначала тайнопись находилась в зародышевом состоянии, её применяли редко. Даже церковные системы шифрования были простыми, хотя в ту эпоху церковь поль-

зовалась наибольшим влиянием в обществе. Интересно, что в то время, когда простые люди шифрование считали колдовством, основные работы в сфере криптологии выполнялись в лоне католической церкви.

В X веке монах Герберт Орильякский (Аврилакский), который правил католической церковью под именем папы Сильвестра II (около 946-1003) и изучал «магические» знания, вёл записи по стенографической системе, созданной Марком Туллием Тироном (103-4 до н.э.), вольноотпущенным и другом известного Цицерона.

В 1267 году английский монах-францисканец, профессор в Оксфорде, универсальный учёный, математик, оптик, астроном Роджер Бэкон (Roger Bacon) (1214-94) написал первую европейскую книгу, которая была посвящена криптологии и называлась «Послание монаха Роджера Бэкона о тайных действиях искусства и природы и ничтожестве магии» (лат. Epistola fratris Rogerii Baconis de secretis operibus artis et naturae, et de nullitate magiae). В предисловии он заметил: «Дурак тот, кто пишет о тайне каким-либо способом, но не так, чтобы скрыть её от простонародья».

В разделе «Семь способов сокрытия тайны» Бэкон привёл следующие методы шифрования: полная замена символов и знаков, использования загадочных и образных выражений, особенные способы записи, одновременное использование букв разных языков, применения разных рисунков, сокращения гласных букв и т. п. За свои научные труды он был осуждён за «черную магию» церковным судом и провёл 14 лет в заключении.

В 1379 году антипапа Климент VII, который за год до этого убежал к французскому Авинену, велел своей канцелярии ввести в действие новые шифры. Секретарь антипапы Габриэль де Лавинда, работавший в его представительстве в одном из северно-итальянских городов-государств, изготовил индивидуальные ключи для всех 24 корреспондентов антипапы. Ключи де Лавинда, которые были самыми древними среди сохранившихся на Западе, совмещали в себе элементы кода и шифра.

В своей книге «Трактат о шифрах» Габриэль де Лавинда описал новый тип шифра, использующий «омофоны», то есть допускал замену букв несколькими символами (знаками), количество которых было пропорционально появлению букв в открытом тексте. Имена, должности, географические названия он рекомендовал заменять специальными знаками. Кроме шифралфавита замены с «пустышками» почти каждый такой ключ включал небольшой список из десятка широко распространённых слов или имён, которым соответствовали двухбуквенные кодовые эквиваленты. Это был самый ранний образец «Номенклатора» (лат. nomen – имя и calator – раб, слуга) – гибридной системы шифрования, который в следующие 450 лет распространился по всей Европе.

Развитию европейской криптологии способствовало то, что средневековые ученые, сделав открытие, никоим образом не спешили описывать его в письмах коллегам, как это было тогда принято в условиях отсутствия периодических научных изданий. Нередко ту часть открытия, которое сейчас называют «Know how», они шифровали анаграммой, переставляя буквы сообщения по известному только им ключу. Например, названия древней и современной столиц Японии в русском написании также представляют собой анаграмму: КИОТО – ТОКИО.

Объясняя широкое распространение тайнописи среди учёных средневековья, Александр Иванович Герцен писал: «гонимые, скитальцы из страны в страну, окруженные опасностями, они не зарыли из благоразумного страха истины, о которой были призваны свидетельствовать; они высказывали её везде; где не могли высказывать прямо – одевали её в маскарадное платье, облекали аллегориями, прятали под условными знаками, прикрывали тонким флером, который для зоркого, для желающего ничего не скрывал, но скрывал от врага: любовь догадливее и проницательнее ненависти. Иногда они это делали, чтоб не испугать робкие души современников; иногда – чтоб не тотчас попасть на костёр».

Наибольшего расцвета криптология достигла в период Эпохи Возрождения. Творческие периоды жизни таких великих людей, как Леонардо да Винчи, кардинала Ришелье, Людовиков XII-XIV и других дали толчок к зарождению научного подхода к проблемам тайнописи. Именно в эти годы возникло понятие «кодирования» сообщений, то есть замены букв и цифр открытого текста на буквы, цифры и знаки в соответствии с заранее условленным правилом, законом.

Леонардо да Винчи (Leonardo da Vinci) (1452-1519) также шифровал большинство своих личных записей. Самым простым видом шифра, которым он пользовался, было обратное (зеркальное) написание текста так, что прочитать его можно было лишь в отражении зеркала, например: слово «UKRAINE» превращается в шифротекст «ENIARKU». Однако Леонардо иногда использовал и более серьёзные шифры, поэтому далеко не все его записи расшифрованы и изучены до сих пор. Неслучайно вышли в свет книга и фильм с названием «Код да Винчи».

Одним из ведущих европейских криптологов был известный английский писатель, астроном-любитель, таможенный чиновник Джефри Чосер (Geoffrey Chaucer) (1343-1400). В 1370-х годах он выполнял секретные дипломатические поручения своего короля в Италии и Франции. Всю тайную переписку Чосер осуществлял, используя шифр простой замены. Его книга «Экватор Планет», вышедшая в 1390 году, содержала отдельные шифрованные главы.

В 1401 году в Мантуанском герцогстве был найден шифр с использованием «омофонов» для гласных букв. Тот факт, что «омофоны» применялись не для всех букв, а только для гласных свидетельствовал о знании криптоаналитических методов, основанных на частоте появления знаков шифротекста.

Широкое развитие торговли в средние века спровоцировало появление специфических шифров, очень простых и удобных, которыми могли бы пользоваться купцы для передачи, например, даты приезда или цены товара. Это были простые шифры замены цифр на буквы, основанные на ключевом слове. Торговцы заранее договаривались об использовании общего ключевого слова, буквы которого соответствовали бы цифрам.

Например, для ключа «ШИФРОВАННЫЙ» цифра 0 означает букву «Ш», цифра 1 означает «И», 2 – «Ф», 3 – «Р» и т.д. Поэтому получив от корреспондента сообщение «ПРИБЫВАЮ ИФШАЙР», они его читали как «ПРИБЫВАЮ 12/06/93». Простота и удобство этой системы шифрования позволили ей дожить до начала XIX века без всяких изменений. Кроме этих шифров, чаще всего использовался шифр простой замены, заключавшийся в замене каждой буквы сообщения на соответствующую ей букву шифра.

В ручных шифрах того времени часто использовались таблицы, которые давали простые шифры перестановки. Ключом в них служил размер таблицы и фраза, которая задавала перестановку или специальную особенность таблиц. Простая перестановка без ключа – один из самых простых методов шифрования, соответствующий шифру «скитала».

Например, сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» записывалось в таблицу размером 4х4 по столбцам (см. таблицу).

В	Е	С	Е
С	Т	Я	С
Т	И	В	Т
Р	М	Ш	Ь

После того, как открытый текст был записан по столбцам, для образования шифровки он считывался по строкам. В результате получался шифротекст: «ВЕСЕСТЯСТИВТРМШЬ». Для использования этого шифра отправителю и получателю нужно было договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входило в ключ шифра и использовалось лишь для удобства записи текста.

Более практичным был метод шифрования, названный одиночной перестановкой по ключу. Он отличался от предыдущего лишь тем, что столбцы таблицы переставлялись по ключевому слову, фразе или набору чисел длиной в строку таблицы. Ключевое слово (например, «ШИФР») вписывалось в первую строку таблицы, после чего осуществлялась перестановка столбцов в соответствии с порядковыми номерами букв ключа (см. 2 квадрата).

Ш	И	Ф	Р
4	1	3	2
В	Е	С	Е
С	Т	Я	С
Т	И	В	Т
Р	М	Ш	Ь

▶

1	2	3	4
Е	Е	С	В
Т	С	Я	С
И	Т	В	Т
М	Ь	Ш	Р

В результате считывания по строкам сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» преобразовывалось в шифротекст «ЕЕСВТСЯСИТВТМЬШР».

Кроме одиночных перестановок использовались еще двойные перестановки столбцов и строк таблицы с сообщением в соответствии с заранее определённым порядком нумерации строк и столбцов таблицы, что и было ключом шифра. При этом перестановки определялись отдельно для столбцов и отдельно для строк. В таблицу вписывался текст по столбцам, после чего осуществлялись перестановки столбцов и строк (см. 3 квадрата).

	3	2	4	1
2	В	Е	С	Е
1	С	Т	Я	С
4	Т	И	В	Т
3	Р	М	Ш	Ь

▶

	1	2	3	4
2	Е	Е	В	С
1	С	Т	С	Я
4	Т	И	Т	В
3	Ь	М	Р	Ш

▶

	1	2	3	4
1	С	Т	С	Я
2	Е	Е	В	С
3	Ь	М	Р	Ш
4	Т	И	Т	В

В результате конечного считывания по строкам сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» превращалось в такой шифротекст: СТСЯЕЕВСЬМРШТИТВ. При расшифровывании порядок перестановок был обратным. Однако даже шифры двойной перестановки были слабым видом шифра, потому что легко читались при любом размере таблицы шифрования.

Новый этап развития криптологии начался во второй половине XV века с введением в практику многоалфавитных шифров замены. Отцом этого шифра оказался теоретик искусства Леон Баттиста Альберти (Leone Battista Alberti) (1404-72), который обобщил опыт гуманистической науки в изучении античного наследия, написал трактаты «О статуе», «О живописи», «О

зодчестве», 10 книг о зодчестве, построил палаццо Ручеллаи, церковь Иль Джезу и ряд других замечательных достижений зодчества средневековой Италии.

В 1466 году Альберти предоставил папской канцелярии также и трактат о шифрах, где осуществил анализ частоты букв, исследовал шифры замены и перестановки, коснулся вопросов стойкости шифров. Подмеченная Альберти разная частота появления букв в осмысленных текстах дала толчок к изучению синтаксических свойств письменных сообщений. При этом основное внимание уделялось буквам, которые чаще всего встречались в тексте.

Альберти впервые выдвинул идею «двойного» шифрования – текст, полученный в результате первого шифрования, поддавался повторному шифрованию. Он предложил использовать два или больше шифралфавитов, переходя от одного к другому в процессе шифрования и запутывая этим возможных криптоаналитиков (см. таблицу).

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

Здесь, например, есть два возможных шифралфавита, и мы можем зашифровать сообщение, используя по очереди то один, то другой. Таким образом, чтобы зашифровать слово «UKRAINE», зашифруем первую букву с помощью первого шифралфавита, так что «U» превратится в «Z», вторую же букву зашифруем, используя второй шифралфавит, при этом «K» станет «E». Для шифрования третьей буквы вернёмся опять к первому шифралфавиту (R – U), а, чтобы зашифровать четвёртую букву, опять обратимся ко второму шифралфавиту (A – U) и так далее: I – M, N – H, E – H. В результате получим такой шифротекст: ZEUUMHH.

Основное преимущество системы Альберти заключалась в том, что одинаковые буквы открытого текста не обязательно оставались одинаковыми в шифротексте. То есть повторяющиеся буквы шифротекста становились разными буквами открытого текста.

В своей книге Альберти предложил также свой собственный шифр с нескромным названием «шифр, достойный королей», который сделал шифровку очень стойкой к «взлому». Реализация шифра обеспечивалась с помощью механического шифровального диска, что было также одним из важнейших изобретений Альберти.

Шифровальный диск состоял из большого внешнего диска и подвижного внутреннего диска. Окружность внешнего диска была разделена на 24 ровных сектора, в которые были вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры. При этом из алфавита были изъято 6 букв, без которых можно было обойтись, – H, J, K, U, Y, W. Окружность внутреннего диска была разделена также на 24 сектора, в которые были вписаны буквы смешанного латинского алфавита.

Имея два таких прибора, корреспонденты договаривались о первой индексной букве на подвижном диске. При шифровании сообщения отправитель ставил индексную букву напротив любой буквы большого диска. Он информировал корреспондента о таком положении диска, записывая эту букву внешнего диска как первую букву шифротекста.

Очередная буква открытого текста отыскивалась на неподвижном диске, и буква меньшего диска, которая стояла напротив нее, была результатом ее шифрования. После того, как были зашифрованы несколько букв текста, положения индексной буквы менялось, о чем также сообщалось корреспонденту.

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

Так, например, для индексной буквы «L» одним из многих вариантов шифрования слова «PRESIDENT» может быть «ATQEIOZECX», а другим – «BHYZQBAZFI» и т.д.

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

Такой шифр имел две особенности, которые делали изобретение Альберти важным событием в истории криптологии. Во-первых, в отличие от шифров простой замены шифродиск использовал не один, а несколько алфавитов для шифрования. Такие шифры получили название многоалфавитных. Во-вторых, шифродиск позволял использовать так называемые коды с перешифрованием, которые получили широкое распространение лишь в конце XIX века, то есть через четыре века после изобретения Альберти.

Для этой цели на внешнем диске имелись цифры. Альберти составил код, который состоял из 336 кодовых групп, пронумерованных от 11 до 4444. Каждому кодовому обозначению соответствовала определённая фраза. Когда такая фраза встречалась в открытом сообщении, она заменялась соответствующим кодобозначением, а с помощью диска цифры шифровались как обычные знаки открытого текста, превращаясь в буквы.

В 1474 году был написан первый в мире трактат, посвящённый исключительно криптоанализу. Это сделал Чикко Симонетта (Cicco Simonetta), один из секретарей правителей Милана – герцогов Сфорца. В нём он изложил усовершенствованные шифры замены, в том числе шифр многозначной замены, в котором одной букве (гласной) соответствовало несколько шифробозначений. Он разработал 13 правил раскрытия шифров простой замены, в которых сохранены разделители слов.

Рукопись, написанная на трех кусках пергамента, начиналась со слов: «Первое необходимое условие заключается в выяснении того, написан ли документ латинским или местным языком, а это можно установить таким способом: выясните, имеют ли слова в данном документе только пять разных окончаний, меньше или больше. Если их только пять или меньше, вы правы, считая, что документ написан местным языком…».

Ч.Симонетта в своём трактате подробно описал шифры замены, в которых для выравнивания частоты появления букв в шифротексте гласной букве соответствовал не один знак, а несколько. Здесь же впервые было приведено описание так называемого «лозунгового» шифра, который в разных модификациях будет применяться и несколько веков позже. Правило замены букв в нём определялось так: под алфавитом писалась ключевая фраза – лозунг (например, «Ukraine») без повторяемых букв, а затем буквы, которые в лозунге не встречались, в естественном порядке.

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

В результате слово «UZHGOROD» превращается в шифротекст: «TZBELPLA».

3. Многоалфавитные шифры

В 1518 году появился первый печатный труд по криптологии «Полиграфия» (лат. Polygraphia). Она была написана Йоганном Гейденбергом (1462-1516), или Тритемием (Трисемусом), аббатом бенедиктинского монастыря Святого Мартина (г. Вюрцбург, Германия), которого многие историки считают отцом европейской криптологии. «Полиграфия» представляла собой сборник из 6 книг и содержала столбцы латинских терминов и слов, соответствующих буквам открытого текста, и первую квадратную таблицу, основу многоалфавитной замены.

Хотя в труде Тритемия были описаны много шифров – как существующих в то время, так и изобретённых самим автором, она была пронизана каббалистическими и оккультными аллюзиями.

В результате книга вызывала гнев многих монарших дворов Европы, которые думали, что Тритемий выдал в ней слишком много тайн. Кроме того, Римская католическая церковь считала труды Тритемия еретическими и в 1609 году внесла его книги в список запрещенных. Это запрещение длилось 250 лет.

В 1541 году книга была переиздана на французским языке, а вскоре был сделан её перевод на немецкий язык. В этой книге Тритемий сделал два новаторских предложения в криптологии: шифр «Аве Мария» и шифр, построенный на основе периодически сдвигаемого ключа.

Шифр «Аве Мария» основывался на принципе замены заранее оговоренных слов на буквы шифротекста. С таких слов складывалось внешне «невинное» сообщение. Например, заменим буквы «А», «К», «Т» на такие слова: «А» – ожидаю, мой; «К» – дома, ключ; «Т» – я, здесь. В таком случае позитивный тайный ответ на заданный вопрос может иметь несколько вариантов: «Я ожидаю дома» или «Здесь мой ключ».

Вторым более серьезным шифром была «таблица Тритемия» – квадратная таблица размером 24х24 со многими алфавитами, названная «tabula recta». Алфавиты были записаны в строки таблицы один под другим, причем каждый из них был сдвинут на одну позицию влево по сравнению с предыдущим.

Тритемий предлагал использовать эту таблицу для многоалфавитного шифрования самым простым из возможных способов: первая буква текста шифровалась первым алфавитом, вторая буква – вторым и т.д. В этой таблице не было отдельного алфавита открытого текста, для этой цели служил алфавит первой строки. Таким образом, слово «UKRAINE» превращалось в шифротекст «ULTDNSL».

Преимущество этого метода шифрования по сравнению с методом Альберти заключалась в том, что каждая очередная буква текста шифровалась новым алфавитом. Альберти изменял алфавиты лишь после трёх или четырёх слов. Поэтому его шифротекст состоял из отрезков, каждый из которых имел закономерности открытого текста, которые помогали расшифровать криптограмму. Побуквенное шифрование не давало такого преимущества (см. таблицу).

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

Кроме того, Тритемий предлагал также использовать одноалфавитное шифрование с помощью квадрата Полибия и ключевого слова – пароля. Выбиралось какое-либо слово, из него убирались повторяемые буквы, а оставшиеся записывались в первые клетки квадрата. Пустые клетки заполнялись оставшимися буквами алфавита по порядку.

Рассмотрим эту систему шифрования, таблица которой будет иметь размер не 5x5, а 5x6. Буква шифрования берётся из клетки, находившейся под клеткой буквы сообщения. Поскольку ключевое слово легко было запомнить, то такой подход упрощал процессы шифрования и дешифрования. Для ключа «ШИФРОВКА» таблица будет иметь такой вид (см. таблицу).

Ш	И	Ф	Р	О	В
К	А	Б	Г	Д	Е
Ж	З	Л	М	Н	П
С	Т	У	Х	Ц	Ч
Щ	Ь	Ы	Э	Ю	Я

Для вышеописанного шифра по данной таблице сообщение «УЖГОРОД» даёт шифровку «ЫСМДГДН». Такие табличные шифры были названы монограммами, потому что шифрование велось по одной букве.

Тритемий также первым заметил, что можно шифровать одновременно по две буквы, которые стояли рядом и были названы «биграммой». Такой шифр был назван «биграммным». Опишем его на примере той же таблицы. Открытый текст разбивался на биграммы, а текст шифровки выходил из него в соответствии с такими правилами:

1. Если обе буквы биграммы исходного текста принадлежали одному столбцу таблицы, то буквами шифра считались буквы, которые были под ними. Так, биграмма «БУ» давала текст шифровки «ЛЫ». Если буква открытого текста находилась в нижней строке, то для шифра бралась соответствующая буква из верхней строки: биграмма «ЯЩ» давала шифр «ВШ» (биграмма из одной буквы или пары одинаковых букв тоже подчинялась этому правилу).

2. Если обе буквы биграммы исходного текста принадлежали одной строке таблицы, то буквами шифра считались буквы, которые лежали справа от них. Так, биграмма «КА» давала текст шифровки «АБ». Если буква открытого текста была в правом столбце, то для шифра бралась соответствующая буква из левого столбца: биграмма «ВЕ» давала шифр «ШК».

3. Если обе буквы биграммы открытого текста лежали в разных строках и столбцах, то вместо них брались две буквы таким образом, чтобы вся их четверка составляла прямоуголь-

ник. При этом последовательность букв в шифре была отражением исходной пары. Например, «АЛ» шифровалось как «БЗ», а «ДУ» – как «БЦ».

При шифровании фразы «ОБЪЯВЛЕН СБОР» по биграммам получается шифровка «ФДИВФПДПУКВО»:

ОБ ЪЯ ВЛ ЕН СБ ОР

ФД ИВ ФП ДП УК ВО

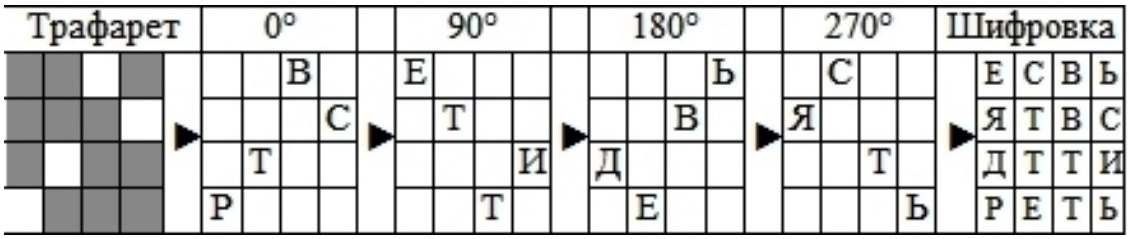
Шифрование биграммами резко усилила стойкость шифров к раскрытию.

Несмотря на то, что «Полиграфия» была достаточно доступной печатной книгой, описанные в ней идеи получили признание лишь тремя веками позже. Скорее всего это было вызвано непопулярностью Тритемия среди профессиональных криптологов, который был не криптологом, а богословом, библиофилом и основателем архивного дела.

Следующий шаг в развитии предложенного Тритемием способа шифрования был сделан итальянцем Джованни Баттиста Беллазо (Giovan Battista Bellaso). В 1553 году он опубликовал брошюру «Шифр сеньора Джованни Баттиста Беллазо» (итал. La cifra del. Sig. Giovan Battista Bellaso), где предложил использовать для многоалфавитного шифра буквенный ключ, который был назван им «паролем» и должен был легко запоминаться. Пароль выписывался под или над строкой сообщения. Буква пароля, что находились над (под) буквой сообщения, определяла номер строки таблицы Тритемия, то есть алфавит замены, в соответствии с которым и осуществлялась шифрование. Буква сообщения определяла номер столбца таблицы, а буква шифротекста находилась на пересечении строки и столбца таблицы.

Приблизительно в то же время итальянский математик и философ Джероламо Кардано (Gerolamo Cardano) (1501-76) предложил использовать в качестве ключа сам текст сообщения, то есть «самоключ» или «автоключ» (англ. autokey). Например, во фразе «СБОР СЕГОДНЯ» ключом было слово «СБОР» (см. таблицу). Шифрование осуществлялась с помощью таблицы Тритемия.

Кроме того, в 1556 году увлечение теорией магических квадратов привело Кардано к открытию нового класса шифра перестановок, названного решёткой или трафаретом. Он представлял собой квадратную таблицу, в которой четверть ячеек прорезана так, что при четырёх поворотах они покрывали весь квадрат. Вписывание в прорезанные ячейки текста и повороты решётки длились до тех пор, пока весь квадрат не был заполнен. Например, на рисунке ниже показан процесс шифрования решёткой 4x4. Трафарет имел 4 прорезанные клетки, а повороты осуществлялись по часовой стрелке на указанный ниже угол (см. таблицу).



В результате считывания по строкам сообщения «ВСТРЕТИТЬ В ДЕСЯТЬ» превращается в шифротекст: ЕСВЬЯТВСДТТИРЕТЬ.

Главное требование к трафарету – при всех поворотах «окна» не должны попадать на одно и то же место в квадрате, в котором образуется шифротекст. Если в квадрате после снятия трафарета образовывались пустые места, то в них вписывались любые буквы.

Количество подобных решёток быстро растет с их размером. Так, решётка 2x2 единственная, решёток 4x4 уже 256, а решёток 6x6 свыше 100 тысяч. Несмотря на определенную сложность, шифры типа решёток достаточно просто раскрывались, поэтому не могли использоваться в качестве самостоятельного шифра. Тем не менее они были очень удобными и ещё долго использовались в практике для усиления шифров замены.

Воскрешение смешанных алфавитов, применявшихся Альберти, и объединение идей Альберти с идеями Тритемия и Беллазо в современную концепцию многоалфавитной замены выпало на долю итальянца Джованни Баттиста Делла Порта (Giovanni Battista Della Porta) (1535-1615). Ему было 28 лет, когда он в 1563 году опубликовал книгу «О скрытой значимости отдельных букв» (лат. De Furtivis Literarum Notis). Её первые два раздела были посвящены криптографии, а в двух других излагались основы криптоанализа и рассматривались лингвистические особенности, которые помогали раскрытию шифров.

Книга Порты содержала первое в Европе описание того, как стоит раскрывать шифр простой замены, когда шифротекст не был разделён на слова или был разделён неправильно. Порта также описал то, что считалось вторым по значимости приёмом в современном криптоанализе:

«…Когда тема переписки известна, исследователь может сделать проницательные предположения относительно слов, которые обычно употребляются в таком контексте. Эти слова можно без большого труда обнаружить, подмечая в текстах количество знаков, а также сходство и различие букв… Каждой теме характерны некоторые общие слова, которые сопутствуют ей, будучи необходимы. Например, в любви – это страсть, сердце, огонь, пламя, сгорать, жизнь, смерть, жалость, жестокость; на войне – это солдат, командир, генерал, лагерь, оружие, бороться и т.д. Таким образом, этот прием вскрытия, который не основан на анализе самих документов или на попытке разбить текст на гласные или согласные, может облегчить задачу».

В своей книге Порта также дал один мудрый совет, который и сегодня полезен криптоаналитику в той же степени, в какой он был уместен в Италии эпохи Возрождения:

«Необходимы самая полная сосредоточенность и усердие, чтобы свободная от посторонних мыслей голова, когда все остальное отложено в сторону, была всецело занята единственной задачей доведения начатого дела до успешного завершения.

И все-таки, когда такая задача требует чрезмерного напряжения и необычных затрат времени, напряжение не должно быть непрерывным, не следует изнурять мозг сверх меры, ибо слишком большие усилия и продолжительная умственная нагрузка приводят к нервному истощению, после которого голова уже менее пригодна для подобных вещей и из нее уже не выжмешь ничего…»

А далее Порта поделился с читателем своим собственным практическим опытом работы: «Кроме того, далеко немаловажно, чтобы сообщение было написано рукой автора или искусного писца, ибо если перехваченное сообщение будет скопировано неправильно или если оно выйдет из-под руки человека незнакомого с искусством шифра, то в результате, поскольку правописание нарушено, любая интерпретация сообщения будет блокирована».

Подобный опыт приходил только к криптоаналитику, который имел дело с сообщениями, в которых буквы часто были пропущены, переставлены или заменены на другие. Это случалось лишь при обработке настоящих криптограмм. Задачи, которые встречались в книгах по криптоанализу того времени, всегда были безукоризненно составлены с точки зрения правописания и поэтому легко решались. Скорее всего, Порта регулярно занимался криптоанализом, выполняя поручение папской курии.

В полной мере замечательные способности Порты проявились при решении наиболее тяжелой проблемы криптоанализа эпохи Возрождения – раскрытии многоалфавитных шифров. Невзирая на высокую оценку этих шифров криптоаналитиками того времени, Порта отказался признать их неуязвимость и разработал для них методы раскрытия. Хотя эти методы

не были универсальными, их основная ценность состояла в примененном Портой смелом подходе, который и привёл его к успеху.

Для начала Порта попробовал прочитать шифротекст, который его современниками был зашифрован с помощью специального устройства. Это устройство состояло из двух дисков: внутреннего неподвижного диска, на который по часовой стрелке был нанесен алфавит открытого текста, и внешнего подвижного диска с рядом причудливых шифрознаков.

Внешний диск после шифрования очередной буквы поворачивался по часовой стрелке на один шаг. Порта заметил, что если в каком-либо слове открытого текста три буквы подряд стояли в алфавитной последовательности, тот же шифрознак троекратно повторялся в получаемом шифротексте. Это помогло ему прочитать криптограмму.

Потом Порта модифицировал разработанный им метод, чтобы дешифровать другую многоалфавитную криптограмму, которая была составлена по принципу Джованни Беллазо. По мнению Порты, в криптограмме троекратное повторение буквы шифротекста сигнализировало о том, что ключом из трёх букв, расположенных в обычном алфавитном порядке, был зашифрован открытый текст, в котором были три буквы в порядке, противоположном алфавитному.

Рассуждая по этому поводу, Порта вплотную подошёл к универсальному методу раскрытия многоалфавитных шифров, найти который он так стремился:

«Поскольку… между первыми тремя „M“ и этими же тремя буквами, повторенными в 13-м слове, находится 51 буква, я прихожу к выводу, что ключ повторен три раза, и правильно считаю, что он содержит 17 букв».

Однако Порта так и не воспользовался своим наблюдением. В итоге многоалфавитный шифр продолжал считаться надёжным в течение трёх следующих веков.

В своей книге Порта ввел свою таблицу многоалфавитного шифрования (см. таблицу).

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

Шифрование сообщения осуществлялась с помощью секретного лозунга-пароля, который периодически выписывался над открытым текстом. Буква лозунга определяла алфавит (заглавные буквы первого столбца), расположенная под ключом буква открытого текста искалась в верхнем или нижнем полуалфавите и заменялась соответствующей ей буквой второго полуалфавита.

Например, если в качестве лозунга использовать слово «UKRAINE», то шифрование слова «UZHGOROD» приведет к шифровке «LHQTKLMN» (см. таблицу).

Лозунг	U	K	R	A	I	N	E	U
Открытый текст	U	Z	H	G	O	R	O	D
Шифротекст	L	H	Q	T	K	L	M	N

За этот шифр Порта позже назвали отцом современной криптографии, но в то время этот шифр не нашёл широкого приложения. Причиной этого была необходимость постоянно иметь при себе указанную таблицу и сложность процесса шифрования. Вместе с тем, был дан импульс для появления других шифровальных систем (например, Виженера).

Также Порта предложил шифр простой биграммной замены с использованием квадратной таблицы со смешанным алфавитом и паролем. В нём пары букв (биграммы) обозначались одним специальным графическим символом. Например, биграмма «EA» заменялась греческим символом «Δ», биграмма «LF» – символом «Ψ» и т.д.

Они заполняли квадратную таблицу размером 20x20, строки и столбцы которой были пронумерованы буквами латинского алфавита. По сути дела это был тот же шифр простой замены, но на уровне двухбуквенных соединений. Криптостойкость при такой замене по сравнению с побуквенным шифрованием значительно повышалась.

Французский посол в Риме Блез де Виженер (Blaise de Vigenere) (1523-96), ознакомившись с криптологическими трудами и идеями Цезаря, Альберти, Тритемия, Беллазо и Порта, увлёкся криптологией. В 1585 году он написал книгу «Трактат о шифрах» (фр. Traite des chiffres), где изложил основы криптологии. В ней он выразил мнение о том, что «все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом». Позже эту мысль повторили и Блез Паскаль (Blaise Pascal), и отец кибернетики Норберт Винер (Norbert Wiener).

В своем трактате Виженер опять повторил идею Кардано по использованию «самоключа». Заранее оговаривалась одна ключевая буква алфавита, и первая буква сообщения шифровалась по строке таблицы Тритемия, соответствующей этой букве. Вторая буква сообщения шифровалась по строке, соответствующей первой букве шифротекста и т.д.

Второй вариант использования таблицы Тритемия, предложенный Виженером, заключался в применении ключа-лозунга. По сути Виженер, объединив подходы Тритемия, Беллазо и Порта к шифрованию открытых текстов, не внёс в них ничего оригинального.

Шифр Виженера содержал в себе алфавитную квадратную таблицу Тритемия, состоявшую из 24 пошаговых ротаций влево линии стандартного латинского алфавита. В этой таблице первая горизонтальная строка называлась «линией языка», а первый вертикальный столбец – «секретной линией». Ключом могло быть любое слово, буквы которого выписывались подряд над или под буквами открытого письма. Причем, когда оно заканчивалось, то записывалось опять, циклически повторяясь, пока не заканчивался текст.

Этот ключ и был «секретом», который Беллазо называл «паролем», а Виженер назвал «лозунгом». В наше время ключевая последовательность букв или цифр получила название «гамма» по аналогии с известным музыкальным термином. Таблица Виженера легко восстанавливалась перед самим процессом шифрования, после чего могла быть уничтожена.

Предложенная Виженером шифросистема стала первым большим открытием в криптологии со времён Юлия Цезаря, которая в течение 350 лет считалась одной из самых надёжных систем. Главным её преимуществом была простота (см. таблицу).

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

Сообщение шифровалось буква за буквой, для чего в таблице нужно было найти столбец, обозначенный той же буквой, что и соответствующая буква ключа, и строка, обозначенная той же буквой, что и буква открытого текста, которая находилась под данной буквой ключа. Буква, которая находилась в таблице на пересечении выбранных столбца и строки, и была нужным шифросимволом.

Например, если в качестве ключа использовать слово «UKRAINE», то шифрование слова «UZHGOROD» приведет к шифровке «PHWGYESZ» (см. таблицу).

Открытый текст	U	Z	H	G	O	R	O	D
Ключ	U	K	R	A	I	N	E	U
Шифротекст	P	H	W	G	Y	E	S	Z

Шифр Виженера имел также некоторые из преимуществ более раннего номенклаторного типа шифра. Каждая буква открытого текста могла обозначаться в шифротексте таким числом разных шифросимволов, сколько разных букв содержалось в ключе.

Кроме того, многоалфавитная замена позволяла скрыть повторяющиеся буквы и другие внутрисловные сочетания, характерные для данного открытого текста. При этом в окончательном шифротексте использовались только 24 обычных буквы алфавита, а какие-либо специальные символы или цифры были не нужны.

Астрологические увлечения Виженера привели его к шифру, в котором шифрознаками были положения небесных тел в момент шифрования. Тем самым он попробовал перевести свои послания на «язык неба».

В XIX веке британский адмирал сэр Френсис Бофорт (Francis Beaufort) (1774-1857) предложил свою разновидность шифра Виженера – квадрат Бофорта (Бьюфорта). Его строками были строки квадрата Виженера, но записанные в обратном (зеркальном) порядке (см. таблицу).

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

Эта таблица имела одно преимущество – правила зашифрования и расшифрования были одинаковы: и в том, и в другом случае буквы выбирались из верхней алфавитной строки.

Ради исторической справедливости необходимо отметить, что таблица Бофорта была предложена ещё в XVIII веке итальянцем Дж.Сестри. Однако его имя в истории оказалось забытым.

Человеком, который сумел сделать криптологию отдельной научной дисциплиной, стал английский философ и государственный деятель Френсис Бэкон (1561-1626), который был одним из умнейших людей в свое время и автором больше, чем два десятка работ, опубликованных и признанных современниками ещё при его жизни. Будучи лордом-канцлером при короле Якове I, он хорошо знал потребности государства в надёжных шифрах, поэтому его первая талантливая работа, относившаяся к 1580 году, в дальнейшем получила блестящее практическое развитие.

Посвятив криптологии специальные работы «Успех познания» и «О достоинстве и приумножении наук», он был не только теоретиком, но и талантливо применял на практике свои знания, благодаря чему занял почётное место среди выдающихся европейских криптологов. В частности, именно он в первый раз предложил свою систему тайнописи, назвав её «двухбуквенным» шифром. Практически это была «двоичная кодировка» букв латинского алфавита – то же, что используется в настоящий момент в компьютерах.

Двухбуквенный код Фрэнсиса Бэкона							
a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAABA	h	AABBB	o	ABBAB	u,v	BAABB
c	AAABB	ij	ABAAA	P	ABBBA	w	BABAA
d	AAABB	к	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

По сути, это была бинарная система стеганографии, поскольку с помощью шрифтов двух видов (например, «А» и «В») в буквы произвольного (нетайного) текста тайком вносилась дополнительная (тайная) информация. Каждой букве тайного послания соответствовало пять букв обычного открытого текста.

В начале XVII века Матео Ардженти (Mateo Argenti), криптолог папской канцелярии, составил пособие по криптологии на 135 листах, которое было издано в плетении из телячьей кожи. В этой книге он повторил идею Чикко Симонетти по использованию слова как ключа для получения смешанного алфавита. Например, ключевое слово «UKRAINE» даёт такой смешанный латинский алфавит: UKRAINEBCDFGHJLMOPSTVWXYZ.

Такие смешанные алфавиты часто использовались в качестве алфавита шифротекста в шифрах простой замены. С целью усложнения шифра простой замены Ардженти рекомендовал не разделять слова, использовать «омофонные» замены, вставлять в шифротекст большое количество «пустышек» (0), устранять пунктуацию, не вставлять в шифротекст открытые слова («клер») и т.д. Для букв, которые часто встречались в словах, он ввёл несколько обозначений, а для соединений букв, которые часто встречались в текстах, – отдельные обозначения. Позже подобные идеи получили широкое распространение.

Пример шифра Ардженти													
A	B	C	D	E	F	G	H	I	L	M	N	O	P
1	86	02	20	62, 82	22	06	60	3	24	26	84	9	66

Q	R	S	T	U	Z	ET	CON	NON	CHE	0
68	28	42	80	04, 40	88	08	64	00	44	5, 7

Слово «UZHGOROD» может быть зашифровано многими способами, например: 754078856070692859205577 или 0488600659289720.

Наибольшим достижением Ардженти считается разработанный им буквенный код (номенклатор), в котором 1200 букв, слогов, слов и целых фраз замещались группами букв.

В XVII веке наиболее ценным историческим трудом в сфере криптологии были произведения Густава Селена (псевдоним Августа II герцога Брауншвейг-Люнебурга, князя Брауншвейг-Вольфенбюттеля) (1579-1666) «Криптописьмо и криптография» (лат. Cryptomenytices et cryptographie): «Девять книг Густава Селена, в которых изъясняется учение о скрытии смысла и тайнописи, некогда написанное Иоганном Тритемием, настоятелем в Спенхейме и Хербиполене, мужа чудесного ума и скрытых магических способностей. Здесь же изложены важные способы и других авторов в 1624 г.». Эти книги, кстати, были учебными пособиями российского криптолога XVIII века Эпинуса.

Криптология уже была известна многим и применялась во многих слоях общества. Так, англичанин Самюэль Пепис (1633-1703) стал всемирно известен своим зашифрованным дневником, согласно которому историки пишут труды о переходе от Пуританства к Реставрации. Искусствоведы включили это произведение в мировую сокровищницу литературы.

Пепис закончил Кембридж благодаря кузену отца – адмиралу Монтегю и имел много друзей: ученого Исаака Ньютона, архитектора Кристофера Рена, поэта и драматурга Джона Драйдена. Пепис был лично свидетелем таких незабываемых для Англии событий, как возвращение короля Чарльза II в Англию, большая чума 1664 года, пожар Лондона 1666 года, революция 1688 года.

Свои мемуары Пепис зашифровал по системе криптолога Томаса Шелтона и дополнительно своим собственным шифром, поскольку содержали много скандальных фактов о великих современниках. Вместе с его личными книгами и бумагами дневник после смерти писа-

теля попал в Кембридж, где сразу же привлек внимание исследователей. Первый успех в его расшифровании был получен лишь в 1822 году, а полностью он был расшифрован в 1899 году.

4. Развитие криптоанализа

В 1506 году «секретарём по шифрам» Венецианской республики был назначен Джованни Соро (Giovanni Soro). Он прославился тем, что с успехом раскрывал шифры многочисленных европейских княжеств. Слава Соро была настолько великой, что начиная с 1510 года папская курия посылала ему для раскрытия шифры, с которыми не могли справиться в Риме. В 1526 году папа Климент VII дважды направлял Соро перехваченные депеши для дешифровки, и в обоих случаях Соро добился успеха. А когда одно из посланий Климента попало в руки его противников, тот выкрикнул: «Соро может раскрыть любой шифр!», – и направил Соро копию этого послания, чтобы выяснить, надежно ли оно зашифровано. Климент успокоился только тогда, когда Соро сообщил, что не может его прочитать. Хотя кто знает, не пытался ли Соро преднамеренно ввести папу в заблуждение ошибочным заявлением о надёжности его шифра.

В 1542 году Соро получил двух помощников. С этого времени Венеция имела уже три квалифицированных криптоаналитика. Их помещение находилось во дворце венецианского правителя, где они работали за закрытыми дверями. Никому не позволялось их тревожить, а им самим не позволялось оставлять своё рабочее помещение, пока не будет раскрыта очередная перехваченная криптограмма.

Криптоаналитики Венеции также писали трактаты, в которых разъясняли методы своей работы. Труд Соро о дешифровании переписки на латинском, итальянском, испанском и французском языках, написанный им в начале XVI века, к сожалению, не сохранился. Но уцелели отрывочные записи его наследника, а также исследование в этой сфере других венецианских секретарей по шифрам.

Джованни Соро стал первым, кто начал готовить профессиональные кадры для криптологии, и хотя это была достаточно примитивная форма «ученичества», лишенная достаточной теоретической базы, она была преобладающей в течение длительного времени. Дело в том, что люди, которые работали с шифрами того времени, были хорошо образованы, но успешно освоить криптологическое дело, которое постоянно эволюционировало и усложнялось, можно было только с помощью длинной практики, чем и занимался Соро со своими учениками.

Специальных учебных заведений, где учили бы криптологической деятельности в то время не существовало. Криптологов рекрутировали из наиболее образованных людей того времени, которые знали математику и иностранные языки. Соро был первым, кто попробовал специально учить молодых криптологов этой науке, но опять же на практике. С другой стороны, сама проблема кадров не стояла в то время так остро, а должность секретаря по шифрам была достаточно желаемой для многих одарённых людей того времени, потому что приносила славу, уважение и достаточно большие доходы.

Многие выдающиеся математики, начиная с тех времен, вовлекались в криптологические службы. Папы Римские всегда пользовались услугами криптологов, поэтому выдающийся итальянский математик и философ Джироламо Кардано (Gerolamo Cardano) в середине XVI века состоял у них на службе, а также был и астрологом. Кроме того, он изобрёл шарнирный механизм и метод решения уравнений третьей степени.

Опубликованный в 1550 году его труд «О тонкости вещей» (лат. De subtilitate libri XXI) и вышедший четырьмя годами позже «О разнообразии вещей» (лат. De rerum varietate libri XVIII) представляли собой наиболее полное энциклопедическое изложение естественных и физических наук XVI века.

Римский Папа Павел III, заменивший Климента VII, быстро понял, что не в его интересах посылать шифры для раскрытия за границу. В 1555 году в папской курии была основана должность секретаря по шифрам. Первый успех пришел только через два года, когда папские

криптоаналитики раскрыли шифр испанского короля Филиппа II, воевавшего тогда с Папой Римским. А в 1567 году выделился викарий собора Святого Петра в Риме, который меньше, чем за шесть часов сумел прочитать криптограмму, написанную турецким языком, на котором викарий не знал и четырех слов.

Во Флоренции Пиро Музефили, граф Сасетский, с 1546 по 1557 годы прочитал множество шифрованных сообщений, раскрыв среди других номенклаторы, которые использовались в переписке между французским королем Генрихом II и его послом в Дании. Криптоаналитическая экспертиза Музефили была настолько квалифицированной, что многие приезжали к нему, как и к Соро, с просьбой раскрыть для них шифры. Среди клиентов Музефили был и король Англии, который послал ему криптограмму, которая была найдена в подметках туфель, доставленных к его двору из Франции.

В XVI веке не только итальянские правители славились своими криптоаналитиками. Так, во Франции в дешифровке перехваченных депеш больше всего преуспел Филибер Бабу (1484-1557), который был первым государственным секретарем и казначеем короля Франциска I. Один наблюдатель описывал, как Бабу, «не имея алфавита, часто дешифровывал много перехваченных депеш на испанском, итальянском и немецком языках, хотя он не знал ни одного из этих языков или знал очень плохо, причем он рьяно работал над сообщением дни и ночи непрерывно в течение трех недель, прежде чем разгадывал одно слово. После того, как пролом был проделан, другое происходило очень быстро и напоминало разрушение стен».

Стоит заметить, что в то время, как Бабу не покладая рук работал на короля, король принимал у себя любовницу – чудесную жену Бабу. Бабу получил много милостей от короля, но трудно сказать, за что именно: за криптоаналитические успехи или за разрешение наставлять «рога».

В Голландии также работал блестящий криптоаналитик – фламандский дворянин Филипп ван Марникс, барон де Сент-Альдегонд (1538-98), автор мелодии современного национального гимна Нидерландов, правая рука Вильгельма Оранского, стоявшего во главе объединенного восстания голландцев и фламандцев против Испании. В 1577 году Голландией руководил испанский губернатор дон Хуан Австрийский, родной брат испанского короля Филиппа II. Его целью было свержение с трона королевы Англии Елизаветы, захват английской короны и бракосочетание с королевой Шотландии Марией Стюарт. Однако в июне того же года во Франции были перехвачены шифрованные письма дона Хуана.

Они были переправлены Марниксу, который через месяц раскрыл испанский шифр. После этого содержание писем через Вильгельма Оранского было доведено до сведения министра Елизаветы Френсиса Уолсингема. Уолсингем сразу же осуществил мероприятия по получению более полной информации и независимости от иностранных криптоаналитиков. С этой целью он направил в Париж талантливого юношу, который быстро расправлялся с шифрованными письмами. Это был Томас Фелипес, первый выдающийся английский криптоаналитик.

В результате проведенных мероприятий вся шифрованная переписка Марии Стюарт, в которой она давала согласие на заговор против Елизаветы и рекомендации относительно ее осуществления, расшифровывалось Фелипесом и поступало к Уолсингему. Эти письма и шифр, которым она пользовалась вместе с другими изменниками, послужили главным материалом для обвинения на заседаниях суда, который признал Марию Стюарт виновной в государственной измене. 8 февраля 1587 года в 8 часов утра она поднялась на эшафот, стала на колени и мужественно приняла от палача три удара топором. Таким образом, криптоанализ ускорил смерть Марии, королевы Шотландии.

В 1589 году королем Франции стал Генрих IV, который сразу же был вынужден вступить в ожесточенную борьбу со Священной лигой. Эта лига во главе с герцогом Майенским контролировала столицу и все другие большие города Франции, получая большие подкрепления в виде живой силы и денег от испанского короля Филиппа II. Генрих был со всех сторон окру-

жен противником. Но именно в это трудное для него время в его руки попала часть переписки Филиппа с испанским военачальником Хуаном Моро.

Письма Филиппа были зашифрованы, но у Генриха секретарем по шифрам в то время служил 49-летний математик Франсуа Виет (1540-1603), основатель современной элементарной алгебры. Его теорему о корне и коэффициентах квадратных уравнений доныне изучают в школе. Он также был членом тайного совета и занимался адвокатской практикой. В 1588 году Виет прочитал зашифрованную испанскую депешу, адресованную Олесандро Фарнезе, герцогу Пармы, который командовал испанскими войсками Священной лиги.

С тех пор Генрих передавал Виету все новые перехваченные депеши, чтобы выяснить, сможет ли тот повторить свой успех. Виет, работая вместе с голландским криптоаналитиком Филиппом ван Марниксом, сумел примерно за год раскрыть шифр короля Испании Филиппа II, который до этого времени считался неуязвимым не только в Испании, но и в Ватикане – одном из серьезных криптологических центров того времени.

Во Франции дешифровальное отделение было создано при Людовике XIII по предложению кардинала Ришелье. Его возглавил Антуан Россиньоль (1600-82), который создал дипломатический шифр, представлявший собой слогово-словарный код на 600 компонентов.

Антуан Россиньоль в первый раз приобрел популярность в 1626 году. Ему передали зашифрованное письмо, захваченное у курьера, который пробирался из осажденного города Реальмон, и до конца дня он дешифровал его. Из письма стало понятно, что армия гугенотов, удерживавшая город, находилась на грани гибели. Французы, которые к этому не подозревали об отчаянном положении гугенотов, вернули им письмо вместе с его расшифровкой. Теперь гугеноты знали, что их противник не отступит, и немедленно сдались. Так победа французов стала результатом дешифровки.

Могущество криптологии стало очевидным, поэтому Антуан Россиньоль и его сын Бонавентур получили высокие должности при дворе. Выдающееся мастерство и накопленный опыт по раскрытию шифров позволил Россиньолям понять, как создать более стойкий шифр, и они придумали так называемый «Великий шифр». Он применялся для шифрования наиболее секретных сообщений короля, скрывая детали его планов, замыслов и политических интриг.

В одном из этих сообщений вспоминалась одна из наиболее загадочных личностей во французской истории, человека в железной маске, но стойкость «Великого шифра» означала, что сообщение останется нерасшифрованным и непрочитанным в течение двух веков.

«Великий шифр» оказался настолько надёжным, что сумел противостоять усилиям всех криптоаналитиков той эпохи, пытавшихся выведать французские тайны, и даже следующих поколений дешифровщиков. К сожалению, после смерти отца и сына «Великий шифр» перестал применяться, а его подробности были быстро утеряны. Это привело к тому, что зашифрованные бумаги во французских архивах стало нечем расшифровывать.

Тем не менее этот шифр французская армия будет использовать более 100 лет. Известно, что даже Наполеон во время своих походов использовал шифры, которые были упрощенными вариантами шифра Россиньоля. Не менее известным был и «шифр Ришелье» – при его использовании текст сообщения разбивался на отрезки, буквы которых переставлялись в определенном порядке.

Россиньолю принадлежит также авторство известной доктрины о том, что «стойкость военного шифра должна обеспечить секретность сообщения в течение срока, необходимого для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение нескольких десятков лет».

Россиньоли чрезвычайно плодотворно работали в сфере криптоанализа как при дворе Людовика XIII, так и в свите Людовика XIV. Например, захват крепости Эден королевской армией был ускорен благодаря тому, что Россиньоли прочитали зашифрованную просьбу её

защитников о помощи, а после этого тем же шифром составили ответ, в каком жителе города извещались о бесполезности их надежд.

Они никогда никому не рассказывали о том, сколько других городов должны были сложить оружие и сколько измен раскрыли среди высшей знати. Из-за этой их таинственности некоторые придворные утверждали, что в действительности Россиньоли не раскрыли ни одного шифра, а кардинал распространял слухи об их способностях с целью предупреждения потенциальных заговорщиков.

На смертном одре Людовик XIII охарактеризовал Антуана Россиньоля как человека, от которого зависело благополучие его подданных. Не удивительно, что через два года, 18 февраля 1645 года, наследник Ришелье кардинал Мазарини назначил Россиньоля государственным советником. Как и Ришелье, Мазарини пересылал ему перехваченные шифровки.

Так, в 1656 году он направил зашифрованное письмо кардинала Реца с указанием Россиньолю прочитать его. При Людовике XIV Россиньоль часто работал в комнате, которая непосредственно прилегала к кабинету короля в Версальском дворце. Отсюда шёл весь поток дешифрованных им сообщений, которые помогали королю определять политику Франции.

Одним из лучших друзей Россиньоля был поэт Буаробер, инициатор идеи создания Французской академии. Когда Буаробер впал в немилость при дворе, он пожаловался на несчастье, которое свалилось на него, в стихотворении, адресованном своему влиятельному другу-криптоаналитику.

Россиньоль показал это стихотворение Мазарини, который во время следующей аудиенции при всем народе похвалил Буаробера. Позже из чувства благодарности Буаробер написал 66-строчное стихотворение, в котором воспевал Россиньоля. Это первая стихотворная ода, посвящённая криптоаналитику. Некоторые ее строки звучат так:

Как изумительно твое искусство и ярко.
И как важна сила твоего мастерства!
Ибо с его помощью приобретаются провинции,
Раскрываются секреты всех королей,
И с малыми усилиями оно
Вынуждает сдаваться города и форты…
Действительно, твоё мастерство выше моего понимания,
И я никогда не постигну
Твой секрет; но я сейчас могу сказать,
Что оно служит тебе очень хорошо,
Что ты заслуживаешь этого. Не опасайся,
Твоё мастерство будет благоприятствовать тебе годами
И судьба будет тебе улыбаться,
Пока войны омрачают землю.

Труд Россиньоля сделал его видной фигурой при дворе Людовика XIV. Именно ему удалось доказать правителям Франции чрезвычайную важность дешифровки депеш для формирования их политики. Его работа демонстрировала это настолько эффективно, что королевский военный министр Лувуа стал энергично поощрять каждого, кто мог предоставить полученную таким образом информацию. Сохранилось письмо Лувуа, в котором тот выражал благодарность за добытый шифр врага, заверяя, что человеку, способному прочитать несколько шифрованных писем, «его величество подарит всё, что он попросит».

Россиньоль стал первым человеком, который прославился исключительно благодаря своим криптоаналитическим способностям. Данью общего увлечения умению «взламывать» шифры было то, что слово «россиньоль» стало французским жаргонным названием отмычки. Шарль Пьеро, который больше известен как автор сказок, внёс биографию Россиньоля в свою книгу «Знаменитые люди Франции в нынешнем веке» вместе с жизнеописанием Ришелье.

После смерти Россиньоля в 1682 году «Великий шифр» уже не всегда применялся в королевской переписке, и эта неосмотрительность дорого обошлась Франции. Так, в 1774 году Людовику XV был доставлен пакет из Вены от секретаря французского посольства аббата Жоржеля. Когда французский король раскрыл его, то нашёл там копии открытых текстов своей шифрованной корреспонденции, которая была «раскрыта» в венском ЧК.

В то время также и Швеция уделяла внимание защите собственной дипломатической и военной переписки. Так, в 1676 году, за несколько дней до битвы между шведской и датской армиями под городом Лунд, шведский король Карл XI отправил генералу Фабиану фон Ферсену шифрованное письмо со своими рассуждениями о стратегии и тактике войск в будущей битве. Благодаря этой информации шведы одержали победу в битве, ставшей одной из самых кровавых в истории Скандинавии.

В XVII веке свой вклад в развитие криптоанализа сделал британец Джон Фальконер. В 1685 году он написал книгу «Раскрытие тайных посланий, или Искусство добывать тайные сведения без ключа» (англ. Cryptomensis Patefacta: or the art of secret information disclosed without a key), где изложил некоторые разработанные им методы дешифровки. В частности, он предложил использовать перебор возможных открытых слов по их длине (если в шифротексте слова разделялись).

Вообще, в XVI-XVII веках криптослужбы появились практически в каждом европейском государстве, причём в состав этих служб входила научная элита того времени: Франсуа Виет и Антуан Россиньоль во Франции, Джироламо Кардано в Риме, Джон Валлис и Френсис Бэкон в Англии, Вильгельм Лейбниц в Германии. Европейские правители нередко привлекали уже известных криптологов-иностранцев на службу, хотя это не всегда удавалось. По-видимому, наиболее неуспешным из таких криптологов был Готфрид Вильгельм Лейбниц (1646-1716) – выдающийся немецкий учёный, математик, основатель Берлинской академии наук.

Английский король Георг I хотел пригласить Лейбница, чтобы тот возглавил британскую криптослужбу, но натолкнулся на резкое противодействие в лице Джона Валлиса (1616-1703), который побаивался конкуренции со стороны своего немецкого коллеги и пригрозил королю перейти на сторону Испании, выдав ей все английские секреты, которых Валлис по характеру своей деятельности знал немало.

Активно выступал против подобного назначения и Исаак Ньютон (1642-1727) – председатель Королевского научного общества, отрицавший авторство Лейбница в дифференциальном вычислении. Не повезло Лейбницу и во второй раз, когда его пригласил в Россию Пётр I не только для организации Российской академии наук, но и для создания российской криптослужбы по европейскому образцу. Смерть Лейбница не позволила осуществиться планам Петра, вынужденного воспользоваться услугами менее именитых криптологов.

К тому времени повсеместно применявшиеся ручные методы шифрования были весьма трудоёмкими. Поэтому для ускорения процессов шифрования и дешифровки изобретались вспомогательные криптографические механические устройства типа сдвигающихся дисков, линеек и т.п. Как правило, они позволяли быстрее и надёжнее выполнять привычную для шифровальщиков операцию простой замены (подстановки) букв алфавита.

Только в новейшее время стало известно, что в 1670-х годах Лейбниц изобрёл механическую машину для кодирования и декодирования шифрованных сообщений. Принципы её построения он изложил в 1679 году герцогу Ганновера Джону Фредерику и в 1688 году императору Священной Римской империи Леопольду I, который часто находился в состоянии войны с Францией и Османской империей (впоследствии Турцией). Ни герцог, ни император не проявили заинтересованности к этой полуавтоматической шифромашине, полагая свои ручные шифры достаточно надёжными.

Шаговый барабан, который использовался в вычислительной машине Лейбница, с помощью клавиатуры производил нерегулярные перемещения, делая шифрование гораздо более

сложным и стойким. Шифромашина Лейбница на 250 лет предвосхитила изобретения механических роторных шифромашин шведа Арвида Дамма, голландца Гуго Коха, немца Артура Шербиуса и американца Эдварда Хеберна, сделанные в начале XX века.

В начале 1700-х годов по политическим мотивам приказом короля Георга I более 200 тысяч личных документов Лейбница были конфискованы. К счастью, эти документы сохранились после смерти Лейбница и постепенно публиковались немецкими учёными в течение нескольких последних десятилетий. Содержание меморандума 1711 года, написанного самим Лейбницем, позволило американскому философу и логику Николасу Решеру и помогавшим ему инженерам за два года реконструировать шифромашину Лейбница.

В Англии лорд-протектор Оливер Кромвель создал «Интеллидженс сёрвис» (англ. Intelligence service – служба разведки), в состав которой входило подразделение дешифровки. Его возглавлял известный математик Джон Валлис (Уоллис), который владел уникальными способностями. Так, бессонными ночами он высчитывал квадратный корень из 50-значных чисел с точностью до 20-30-го знака.

Английский король Карл II ценил искусство Валлиса и называл его «драгоценным камнем для короля…». Расцвет дешифровального искусства Валлиса пришелся на времена правления Вильгельма Оранского и его жены Марии. Он продолжал служить криптоаналитиком и составлял отчёты для графа Нотингемского, командующего морскими и сухопутными вооруженными силами Англии. Напряжение, с которым он работал в те годы, отразилось в одном из его писем: «…боюсь, что вообще обезумею».

В 1689 году Валлису удалось «раскрыть» шифр переписки короля Франции Людовика XIV и французского посла в Польше, тем самым осуществив значительное влияние на внешнюю политику Англии. В частности, он раскрыл намерения Людовика XIV втянуть Польшу в войну против Пруссии. В результате эффективное использование этой информации дипломатией Англии привело к тому, что французские посланцы были с позором изгнаны из Польши.

После смерти Валлиса Англия предприняла важный политический шаг: официально объявила о введении правительственной должности криптолога. В 1703 году первым официально объявленным дешифровщиком Англии стал внук Валлиса – Уильям Бленкоу. Он работал достаточно успешно, но не выдержал рабочего напряжения. В приступе временного безумия Бленкоу совершил самоубийство.

До конца XVII века криптология окончательно сложилась как научная дисциплина. Хотя в данный период господствовали «номенклаторы», которые не были шифрами в «чистом» виде, однако появление многоалфавитной замены, использования трафаретов, биграмм и цифровых обозначений стало огромным шагом вперёд по сравнению с самым древним периодом и означало наступление новой эры в развитии криптологии, вплотную приблизившейся к своему современному виду.

Развитие криптоанализа на Западе напрямую зависело от развития дипломатии. С тех пор, как государства стали поддерживать постоянные дипломатические отношения, их послы, которых иногда иронически называли «почётными шпионами», регулярно отправляли к себе на родину содержательные послания. Существующие между государствами соперничество и подозрительность вынуждали дипломатов зашифровывать свои депеши, поскольку их нередко перехватывали и вскрывали.

Появление постоянных дипломатических представительств и заострение политической борьбы стимулировало послов зашифровывать свои сообщения, побаиваясь, что они будут перехвачены противником. До конца XVI столетия криптоанализ стал играть настолько важную роль, что в большинства европейских государств были введены должности секретарей по шифрам, которые полный рабочий день занимались шифрованием и расшифрованием своих сообщений, а также дешифрованием перехваченных депеш.

5

. Эра «чёрных кабинетов»

XVII век вошел в историю криптоанализа как эра «Cabinets noirs», или «чёрных кабинетов» (далее – ЧК). В это время в разных странах начали появляться первые службы негласного вскрытия писем, или перлюстрации (лат. perlustro – осматриваю), и дешифровки перехваченной корреспонденции, которые были засекречены и работали в условиях полной конспирации.

Известно, что в августе 1620 года голландский посол в Англии Жан Баптиста Ван Мале старательно пытался подкупить правительственного шифровальщика Винсентио, который уже отсидел 6 лет в Тауэре за связи с испанской разведкой. Ван Мале хотел побуждать Винсентио отказаться расшифровывать важные письма испанского посла в Вене к голландскому правителю эрцгерцога Альберту, перехваченные английскими разведчиками.

Винсентио предлагались деньги – понятно, с прямо противоположной целью – также и от имени голландского посла. Все договорные стороны торговались при этом, как на рынке. А между тем английские власти спохватились и предложили Винсентио поторопиться с расшифровкой, если он не желает познакомиться с пыточной камерой.

В то же время испанский посол в Англии Гондомар узнал, что англичане читают его письма, которые он направлял в Мадрид. Там копии с них каким-то неизвестным путём снимал английский посол сэр Джон Дигби, расшифровывал закодированные места и пересылал свою добычу в Лондон Якову I.

Напрасно Гондомар менял шифры и курьеров, просил, чтобы в Мадриде его донесения попадали только в руки абсолютно доверенных лиц. Только через многие годы, уже вернувшись из Испании, Дигби, уступая настойчивой просьбе Гондомара, рассказал, что депеши перехватывались и копировались, пока курьер отдыхал на последней почтовой станции неподалеку от испанской столицы.

В XVIII веке ЧК уже стали распространённым явлением по всей Европе, а венский ЧК (Geheime Kabinets-Kanzlei) пользовался репутацией наилучшего среди них. Он функционировал очень эффективно. Мешки с почтой, которые должны были доставляться посольствам в Вене ежедневно в 7 часов утра, появлялись сначала в помещении ЧК. Там письма раскрывали, растапливая печати над свечой, отмечали порядок расположения страниц в конверте и передавали их помощнику директора. Тот читал их и давал указания о снятии копий с важнейших документов.

Длинные письма для экономии времени копировались под диктовку с использованием до четырёх стенографистов одновременно. Если письмо было на незнакомом для помощника директора языке, он передавал его служащему ЧК, который владел этим языком. Там были переводчики со всех европейских языков, а когда появлялась потребность в специалистах по неизвестным другим языкам, один из служащих в срочном порядке брался за его изучение. После копирования письма аккуратно помещались опять в конверты, которые опечатывались поддельными печатями и возвращались на почту не позже 09-30 утра.

Через полчаса в ЧК прибывала новая почта. Она обрабатывалась таким же образом, хотя и с меньшей поспешностью, поскольку была транзитной. Как правило, эта корреспонденция возвращалась на почтовую станцию до двух часов дня, хотя иногда её задерживали и до семи вечера. В 11-00 прибывала почта, перехваченная полицией. А в 16-00 курьеры привозили письма, которые отправляли заграничные посольства. Они опять вливались в поток почтовой корреспонденции, которая отправлялась из Вены в 18-30.

Скопированный материал попадал на стол директору ЧК, который отбирал особенно важную информацию и направлял её заинтересованным лицам, – правительству, полицейским чиновникам, дипломатам и военачальникам. Таким образом, венский ЧК со штатом всего в 10 человек обрабатывал в среднем сотню писем ежедневно.

Конец ознакомительного фрагмента.