Вадим Гребенников

Европейская криптология. История спецсвязи

ЛитРес: Самиздат
Москва

УДК 355
ББК 68
Г79

Гребенников В.

Европейская криптология. История спецсвязи / В. Гребенников — Москва: ЛитРес: Самиздат, 2019. — 268 с.

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

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 «руническим надписям», является огамический (ogam, ogum, ogham), распространенный в Ирландии, Шотландии, Уэльсе и Корнуоли в III-X веках н.э. В древнеирландских текстах было упоминание о том, что «ogam» служил для передачи тайных посланий, а также для мыслей.

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

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

использовался простым народом. Именно из-за этого всеми сакральными традициями мира разрабатывались свои тайные алфавиты.

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

Греческий алфавит, подобно ивриту для евреев, служил грекам одним из средств познания мира. У греков буквы «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 уси-

лия 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…