Вадим Гребенников

Американская криптология

История спецсвязи

Вадим Гребенников

Американская криптология. История спецсвязи

«ЛитРес: Самиздат»

2019

Гребенников В.

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

ISBN 978-5-532-10491-4

Книга рассказывает историю рождения и развития шифров и кодов, криптологии и специальных видов засекреченной связи в США, американских криптологических служб, техники шифрования и аппаратуры засекречивания; военных сетей спецсвязи; описывает шпионскую деятельность американских спецслужб по «охоте» за советскими шифрами, успехи и провалы в этой сфере, а также появление асимметричной криптологии и ее практическое использование сегодня.

ISBN 978-5-532-10491-4

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 елевсинские 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, языки американских индейцев неоднократно использовались в качестве системы засекре-

ченной радиосвязи. Во время Первой мировой войны индейцы племени «чокто (чахта)» были первыми, кто помогал Армии США шифровать военные сообщения, а в начале Второй мировой войны для ВМФ США это делали индейцы племени «навахо».

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 про-

извёл 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 (др. греч. κρυπτος – тайный и γραφω – пишу) 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 (греч. αναλυσις – разложение) – это мероприятия по анализу и раскрытию зашифрованной информации. Вместе криптография и криптоанализ создают науку криптологию (греч. λογος – слово, понятие).

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 американской криптологии…

1. Криптология до XX века

За океаном, в Северной Америке, в XVIII веке не было ни «чёрных кабинетов», ни каких-либо криптослужб. Вместе с тем, известно, что американские делегаты во Франции и государственный секретарь во время скандального дела «Икс-Игрэк-Зэт» (англ. X-Y-Z) в 1737 году, связанного с вымогательством французскими должностными лицами денежных «подарков» от американцев, шифровали свою переписку с помощью номенклатора.

В конце XVIII века началась война за независимость США (1775–1783) между королевством Великобритании и роялистами (сторонниками британской короны) с одной стороны и революционерами 13 английских колоний (патриотами) с другой, которые провозгласили свою независимость от Великобритании, как самостоятельное союзное государство. 29 ноября 1775 года патриоты образовали такой государственный орган как Комитет для секретной корреспонденции с друзьями колоний в Великобритании, Ирландии и других частях мира. В конце 1977 года он был реорганизован в Комитет иностранных дел (с 1789 года – Госдепартамент) США.

Повстанцы как могли боролись с английскими шпионами, однако перехватывать криптограммы англичан им удавалось очень мало. И только когда война приближалась к своему завершению, и было захвачено достаточное количество шифрованных сообщений, были организованы «разовые группы» по дешифровке. В одну из таких групп входил будущий вице-президент США Элбридж Джерри (Elbridge Gerry). Главным направлением работы этих групп было выявление английских шпионов и дешифровка переписки английских войск. Большинство криптограмм было дешифровано Джеймсом Ловеллем (James Lovell) (1737–1814), которого можно по праву назвать «отцом» американского криптоанализа.

В 1777 году Ловель был избран депутатом Конгресса, членом Комитета иностранных дел и вскоре стал известен благодаря своему усердию и трудолюбию. Одной из первых обязанностей Ловелля была расшифровка писем Чарльза Дюма (Charles Dumas), американского дипломата, который жил в Нидерландах и позже представлял интересы США в Европе. Именно Дюма изобрел первый дипломатический шифр Континентального Конгресса, который использовался американским дипломатом во Франции Бенджамином Франклином для переписки с агентами в Европе.

Осенью 1781 года американский командующий на юге Натаниэль Грин (Nathanael Greene) направил Конгрессу несколько перехваченных английских криптограмм, которые в его штабе никто не мог прочитать, добавив их к своему общему сообщению. Эта шифрованная английская корреспонденция оказалась перепиской между заместителем главнокомандующего английских войск в Америке Чарльзом Корнуолисом (Charles Cornwallis) и его подчинёнными.

Сообщение Грина было зачитано в Конгрессе 17 сентября. Четырьмя днями позже Ловель расшифровал приложения к сообщению. К сожалению, из-за быстрого развития событий добытая им информация не принесла много пользы. Но найденные Ловелем ключи могли пригодиться когда-нибудь в будущем. В своих письмах Джорджу Вашингтону (George Washington) он написал: «Не исключено, что противник намеревается и дальше зашифровывать свою переписку… Если это так, то Ваше превосходительство, возможно, пожелает извлечь для себя пользу, дав вашему секретарю указание снять копию ключей и замечаний, которые я через Вас направляю…»

Более проницательным Ловель быть не мог. Раскрытый им шифр действительно служил также и для связи между Чарльзом Корнуолисом и генералом Генри Клинтоном (Henry Clinton), который находился в Нью-Йорке. В то время Корнуолис отступил к Йорк-тауну, чтобы дождаться подкреплений от Клинтона. Кстати, Клинтон зашифровывал свои сообщения, используя номенклатор, алфавитную таблицу, ряд замен и решётку.

Но Вашингтон с 16-тысячным войском окружил город, а французский адмирал граф де Грасс (François Joseph Paul de Grasse) с 24 кораблями заблокировал помощь англичанам с моря. 6 октября Вашингтон написал Ловеллю: «Мой секретарь снял копии с шифров и с помощью одного из алфавитов сумел расшифровать параграф недавно перехваченного письма лорда Корнуолиса сэру Клинтону». Эта информация помогла Вашингтону оценить реальное состояние дел в английском лагере.

Между тем для связи с Корнуолисом Клинтон снарядил два небольших судна, которые он отправил из Нью-Йорка 26 сентября и 3 октября. Однако они были захвачены повстанцами. При этом одно из них прибило к берегу, где англичанин, который вез пачку шифрованных депеш, спрятал их под большим камнем, прежде чем его захватили в плен. Потом, как сказал один из очевидцев, «в результате непродолжительной беседы, пообещав прощение», повстанцы уговорили англичанина отдать спрятанные депеши.

Ловель получил эти депеши 14 октября и сразу приступил к делу. Успех не заставил себя долго ждать, потому что он выяснил, что депеши были зашифрованы тем же шифром, что и другая переписка Корнуолиса. Через пять дней после того, как Ловель закончил дешифровку, Корнуолис капитулировал.

Но победа повстанцев была не совсем полной. Вашингтон понял это, когда на следующий день наконец получил от Ловелля копии дешифрованных депеш. Не теряя ни минуты, Вашингтон переправил их де Грассу, корабли которого должны были помешать попытке предоставления помощи Корнуолису Грейвсом и Клинтоном. Будучи предупреждённым, французский адмирал обстоятельно подготовился к нападению англичан. 30 октября он заставил английский флот отступить и тем самым приблизил окончательную победу американцев в войне за независимость.

Позже Ловель изобрёл собственный многоалфавитный шифр. Этот шифр активно использовался Ловелем в его переписке. Однако, как выяснилось позже, шифр стал известен тем, что постоянно запутывал корреспондентов Ловелля. В его шифре корреспонденты формировали таблицу замен из согласованного ключевого слова.

Сначала в столбец записывались числа от 1 до 27, потом рядом с ним записывался столбец из 27 букв алфавита (A-Z и &), начиная с первой буквы ключевого слова. Потом записывался аналогичный столбец, начинавшийся со второй буквы ключевого слова, и т. д. При шифровании столбцы использовались по очереди, и каждая буква шифровалась числом. Однако если при шифровании допускалась ошибка, то есть, например, один столбец использовался дважды подряд, процесс дешифровки сразу же запутывался.

В целом, эффективность дешифровки повстанцев оказывалась достаточно высокой благодаря тому, что английские шифры и ключи не менялись длительное время. Кроме того, сеть шифрованной связи Англии в США имела существенный недостаток: все командиры воинских подразделений использовали для связи между собой и Лондоном те же шифры и ключи. В этих условиях дешифровка сообщений одного из абонентов приводила к компрометации переписки всех абонентов сети. В результате американцам удавалось получать информацию, достаточно важную для проведения своих военных операций.

Посланец США во Франции, член Комитета иностранных дел, учёный, дипломат и философ Бенджамин Франклин (Benjamin Franklin) (1706-90) для связи с Конгрессом разработал свой собственный шифр многозначной замены. Интересен был сам способ составления шифра. Он взял отрезок французского текста (682 буквы), пронумеровал в нём знаки и каждой букве латинского алфавита прибавил множество обозначений (чисел) в пронумерованном тексте. При шифровании каждая буква заменялась на произвольно выбранное число из множества обозначений.

В современном понимании он использовал шифр пропорциональной замены, в котором количество возможных шифробозначений пропорционально частоте повторяемости букв

в открытом тексте. При использовании такого шифра знаки зашифрованного текста появлялись приблизительно с одинаковой частотой. Разработав собственный шифр пропорциональной замены, Франклин воспроизвёл идею шифра, предложенного Габриэлем де Лавинда ещё в XV веке.

К сожалению для американцев, один из помощников Франклина – генеральный секретарь американской миссии во Франции Эдуард Банкрофт (Edward Bancroft) – был английским шпионом. В результате Франклин часто отправлял в Америку дезинформацию, предоставленную ему Банкрофтом. Другой помощник Франклина, Артур Ли (Arthur Lee), пользовался своеобразным книжным шифром. Открытый текст шифровался не по буквам, а по словам. Ключом шифра был заранее выбранный словарь, а все слова заменялись на соответствующие номера страниц и слов на странице. Однако этот шифр оказался достаточно неудобным в применении.

В 1779 году конгрессмен и офицер континентальной армии Бенджамин Толмадж (Benjamin Tallmadge) (1754–1835) разработал для связи с Вашингтоном номенклатор, который состоял из одного раздела и 760 элементов. Для этого он использовал наиболее употребляемые слова из «Нового орфографического словаря» Джона Энтика (John Entick). Выписав в столбец выбранные слова, Толмадж присвоил каждому из них определённое число, а географические названия и имена людей поместил в отдельный раздел. Слова в номенклаторе были расположены в буквенно-цифровой последовательности, а кроме того, номенклатор содержал также перемешанный алфавит для кодирования слов и чисел, не вошедших в список.

В 1781 году Секретарь иностранных дел США Роберт Ливингстон (Robert Livingston) (1746–1813) разработал номенклатор, который содержал упорядоченную по алфавиту группу слов и слогов на одной стороне и числа от 1 до 1700 на другой. Воспользовавшись системой Ливингстона, будущие госсекретарь и президент США Томас Джефферсон (Thomas Jefferson) (1743–1826) и Джеймс Мэдисон (James Madison) (1751–1836) разработали свою собственную систему защиты переписки. Она оказалась удобнее, поскольку позволяла вставлять буквы или числа в открытый текст при любых выбранных отправителем и адресатом кодовых комбинациях.

Кроме того, Мэдисон как член вирджинской делегации на Континентальном конгрессе пользовался номенклатором, состоявшим приблизительно из 846 элементов, чтобы отправлять частные письма губернатору штата Вирджиния Бенджамину Гарисону (Benjamin Harrison). Его система состояла из перечня чисел, букв, слогов и географических названий, таких как Вена и т. п.

С 1801 года Мэдисон, состоя в должности госсекретаря США, для переписки с Ливингстоном, который в то время был послом во Франции, пользовался номенклатором, состоявшим из 1700 элементов. С 1803 года Мэдисон переписывался со своими представителями Ливингстоном и Джеймсом Монро (James Monroe) уже новым кодом, получившим название «шифр Монро». Хотя эта система была названа шифром, она имела все свойства номенклатора, 1600 элементов которого были расположены в алфавитном порядке.

В 1790-х годах американская криптология обогатилась замечательным изобретением. Его автором был государственный деятель, первый госсекретарь, а затем и президент США Томас Джефферсон (Thomas Jefferson). Свою систему шифрования он назвал «дисковым шифром». Этот шифр реализовывался с помощью специального устройства, впоследствии названным «шифратором Джефферсона». Конструкция шифратора может быть кратко описана таким образом.

Деревянный цилиндр разрезался на 36 дисков (в принципе, общее количество дисков может быть и другим). Эти диски насаживались на одну общую ось так, чтобы они могли независимо вращаться на ней. На окружности каждого из дисков выписывались все буквы английского алфавита в произвольном порядке. Порядок следования букв на разных дисках был различным. На поверхности цилиндра выделялась линия, параллельная его оси.

При шифровании открытый текст разбивался на группы по 36 знаков, затем первая буква группы фиксировалась положением первого диска по выделенной линии, вторая – положением второго диска и т. д. Шифрованный текст получался путём считывания последовательности букв по любой параллельно выделенной линии.

Обратный процесс осуществлялся на аналогичном шифраторе: полученный шифротекст выписывался путём поворота дисков по выделенной линии, а открытый текст отыскивался среди параллельных ей линий путём прочтения возможного осмысленного варианта. Хотя теоретически этот метод позволял допустить появление разных вариантов открытого сообщения, но как показал накопленный к тому времени опыт, это было маловероятно: осмысленный текст читался только по одной из возможных линий.

Шифратор Джефферсона реализовывал ранее известный шифр многоалфавитной замены. Частями его ключа был порядок расположения букв на каждом диске и порядок расположения этих дисков на общей оси. Общее количество ключей было огромным.

Это изобретение стало предвестником появления так называемых дисковых шифраторов, которые нашли широкое применение в развитых странах в XX веке. Шифратор «M-94», который был аналогичен шифратору Джефферсона, использовался в армии США во время Второй Мировой войны. Однако при жизни Джефферсона судьба его изобретения сложилась неудачно.

Будучи госсекретарём, сам Джефферсон продолжал использовать традиционные коды (номенклаторы) и шифры Виженера. Он очень осторожно относился к своему изобретению и считал, что его нужно обстоятельно проанализировать. С этой целью он длительное время поддерживал связь с математиком Робертом Паттерсоном (Robert Patterson).

В результате обмена информацией Паттерсон предложил свой собственный шифр, который, по его мнению, был надёжнее, чем шифр Джефферсона. Он представлял собой шифр вертикальной перестановки с введением «пустышек». По своей стойкости он значительно уступал шифру Джефферсона, тем не менее тот принял доводы своего оппонента и признал его шифр более приемлимым для использования. Таким образом, Джефферсон сам не оценил всю значимость своего собственного изобретения.

В 1817 году полковник американской армии, начальник артиллерийско-технической службы армии США Джеймс Уодсворт (James Wadsworth) также предложил свой механический шифратор. Основными элементами устройства были два шифровальных диска. По окружности первого из них (верхнего), реализовывавшего алфавит открытого текста, по алфавиту были расположены 26 букв английского алфавита. На втором (нижнем) диске с алфавитом шифротекста в произвольном порядке располагались эти же буквы и цифры от 2 до 8. Таким образом, он содержал 33 знака. Буквы на диске были съёмными, что позволяло изменять алфавит шифротекста. Диски были соединены между собой шестерёнчатой передачей с количеством зубцов 26x33.

При вращении первого диска (с помощью кнопки) на один шаг второй диск вращался также на один шаг в другую сторону. Поскольку числа 26 и 33 были взаимно простыми, то при пошаговом вращении первого диска оба диска возвращались в изначальное состояние через 26x33=858 шагов. Диск открытого текста вращался только в одну сторону. Диски содержались в футляре, в котором были прорезаны окна.

С помощью специальной кнопки шестерни разъединялись, что позволяло независимо друг от друга возвращать диски в изначальное для шифрования положение (с помощью дополнительных кнопок). Долгосрочным ключом был алфавит шифротекста (их количество было 33), а разовый ключ состоял из двух букв (верхнего и нижнего диска) и устанавливался в окнах при независимом повороте дисков. Количество разовых ключей было: 26x33=858.

Шифрование производилась таким образом. Перед его началом диски устанавливались в начальные условные положения (например, LB). Потом шестерни соединялись, и с помощью

кнопки диск вращался до тех пор, пока в верхнем окне не появлялась первая буква открытого текста. С окна под ним выписывалась первая буква шифрованного текста. Другие буквы шифровались аналогичным способом. Если буквы повторялись (например, АА), то диск делал полный оборот, поэтому в шифротексте этой паре отвечали пары из разных знаков (например, 8В).

Расшифрование осуществлялось в обратном порядке. Буквы шифрованного текста устанавливались по нижнему окну, а с верхнего выписывалась соответствующая буква открытого текста. Данный шифр имел такие особенности:

– количество знаков в алфавите шифротекста (33) было больше количества букв в алфавите открытого текста (26);

– шифрование буквы открытого текста зависела от того, какой была предыдущая ей шифруемая буква.

Предложение Уодсворта заслуживало внимания, несмотря на то, что недостатком шифра была его особая чувствительность к неточностям (типа замены и пропуска знаков в шифротексте). Искажённая или пропущенная буква делала весь последующий текст при дешифровке непонятным. Однако исторический отказ от предложенной системы шифрования был связан с другими обстоятельствами.

В эти годы господствовали так называемые «ручные шифры», применение которых не требовало специальных приспособлений. Эти шифры были хорошо усвоены, им верили и их хорошо знали, в связи с чем предложение Уодсворта порождало лишние «заботы».

В начале XIX века американец Плини Чейз (Pliny Chase) предложил модификацию известного шифра Полибия (см. таблицу).

	1	2	3	4	5	6	7	8	9	0
1	X	U	A	C	O	N	Z	L	P	φ
2	B	Y	F	M	@	E	G	J	Q	ω
3	D	K	S	V	H	R	W	T	I	λ

Ключом шифра был порядок расположения букв в таблице. При шифровании координаты букв выписывались вертикально. Например, слово «UKRAINE» можно записать как двухстрочный цифровой шифротекст:

1 3 3 1 3 1 2

2 2 6 3 9 6 6

Чейз предложил ввести еще один ключ: заранее оговоренное правило преобразования нижней строки цифр. Например, число, определённое строкой, умножалось на 9: 2263966x9=20375694, после чего получался новый шифротекст:

1 3 3 1 3 1 2

2 0 3 7 5 6 9 4

Эта двухстрочная запись опять превращалась в буквы по указанной выше таблице, при этом первое число «2» определяло букву первой строки «U», затем «10» превращалось в «φ» и т. д. В результате получаем такой шифротекст: UφSWORPM.

Шифр Чейза был более стойким, чем шифр Полибия, однако распространения он не получил. Его недостатками были значительное осложнение процесса зашифрования-расшифрования и особая чувствительность к ошибкам (искажение в шифротексте).

Во второй половине XIX века произошла революция в военном деле. Появились новые средства вооружённой борьбы (паровые корабли, нарезные артиллерия и стрелковое оружие),

коммуникаций (железная дорога) и связи (телеграф). Появление телеграфа заметно повлияло на развитие криптологии.

Одной из войн, в которой были широко применены перечисленные новинки, стала гражданская война в США (1861–1865) между жителями Севера (далее – федералы) и Юга (далее – конфедераты). Победу в этой войне одержали федералы, что в результате привело к созданию США в их современном виде. В этой победе заметную роль сыграло преимущество федералов в криптологических методах. При этом федералы временами «изобретали» заново шифры, которые уже были хорошо известны в Европе.

В то время для передачи сообщений уже широко использовался телеграф. Чтобы телеграфист мог легко читать передаваемый текст, шифротексты должны были быть максимально приближены к обычным открытым текстам. При передаче шифротекстов, представлявших собой хаотический набор букв, телеграфисты делали многочисленные ошибки, что существенно осложняло последующую дешифровку.

Кроме того, ошибки возникали из-за сбоев в работе телеграфных аппаратов. Например, американскому аппарату «Морзе» были свойственны ошибки при передаче, в результате которых в тексте одна буква оказывалась лишней, или наоборот, одной буквы не хватало. В случае «хаотических» шифротекстов такие искажения нередко приводили к невозможности дешифровки.

Кроме телеграфа применялись и другие способы передачи информации, в частности, «флажковые» коды. В 1856 году офицер медицинской службы Альберт Майер (Albert Myer) (1828-80) предложил метод связи с использованием сигнальных флажков – флажковый семафор (англ. wig-wag).

Для обозначения разных букв использовались разные положения флажка, и таким способом солдаты передавали сообщение. «Флажковую» систему Майера применяли солдаты обоих сторон, как федералы, так и конфедераты. Для этого использовалась природная возвышенность. Если таких не оказывалось, то строились специальные вышки.

Теперь рассмотрим шифры, которыми пользовались федералы и конфедераты во время Гражданской войны в США. Наибольшее распространение у федералов имел шифр, включавший элементы кодирования и перестановки слов. Наиболее секретные слова текста заранее заменялись с помощью долгосрочного кода. Например, слово «COLONEL» заменялось на «VENUS». Аналогично, фраза «PRESIDENT OF USA» заменялась на слово «ADAM» и т. п. Замена на легко читаемые обозначения облегчала работу телеграфистов, передававших шифрованные сообщения.

Затем кодируемый текст выписывался по порядку слов в прямоугольник, содержавший определённое количество столбцов. Количество столбцов в открытом виде передавалось в зашифрованном тексте в виде какого-либо слова. Например, слово «GUARD», стоявшее в начале телеграммы, означало, что в прямоугольнике пять столбцов (количество букв в слове). Потом из полученного прямоугольника слова выписывались, например, по такому правилу: первый столбец – сверху вниз, второй – снизу вверх, третий – сверху вниз и т. п. В результате получался окончательный шифротекст, который и передавался телеграфом.

Этот шифр был предложен в 1861 году Ансоном Стейджером (Anson Stager), первым руководителем компании «Вестерн Юнион телеграф». После мобилизации он был назначен руководителем управления военного телеграфа в Огайо. Ещё до войны Стейджер предложил такой шифр для губернатора штата Огайо, который с успехом использовался последним в переписке со своими коллегами – губернаторами штатов Индиана и Иллинойс.

В 1862 году благодаря первому масштабному использованию телеграфа в военных целях шифр Стейджера начал применяться всей армией Севера. Опыт работы Стейджера на телеграфе, естественно, привёл его к системе, в которой шифротекст состоял, как и в новых теле-

графных кодах, с обычных слов, гораздо менее поддающимся искажениям, чем группы произвольно набранных букв.

В ходе войны в систему были введены некоторые элементарные усложнения, которые её заметно усилили. В написанный текст вставлялись «пустышки». Выписывание стало делаться по диагоналям и переменным столбцам в прямоугольниках, которые всё больше и больше увеличивались.

С.Бэквит (S.Beckwith), шифровальщик командующего войсками федералов Уиллиса Гранта (Willis Grant), предложил передавать важные термины тщательно отобранными кодовыми обозначениями, чтобы свести к минимуму телеграфную ошибку. Интересно отметить, что кроме военных этим шифром пользовался и руководитель разведки Алан Пинкертон (Allan Pinkerton), будущий основатель знаменитого детективного агентства.

В этом шифре использовались и простые словарные перестановки: слова открытого текста переставлялись по определённому закону (ключу). Тем не менее, этот шифр был достаточно слабым. Использовался ещё один вид шифров – многоалфавитные системы (относительно алфавита шифрованного текста), в котором строилась таблица размером 26x26 (число букв латинского алфавита).

Столбцы таблицы обозначались буквами латинского алфавита по порядку (A, B, C,…, Z). Строки таблицы были произвольными перестановками этих букв. Это был алфавит открытого текста, определявший верхнюю строку подстановки, по которой выбирались буквы открытого текста. Строки таблицы использовались в естественном порядке (первая, вторая и т. д.) и определяли нижнюю строку подстановки. Первая буква текста шифровалась по первой строке, вторая – по второй и т. д. Правило циклически повторялось (27-я буква текста шифровалась опять по первой строке, 28-я – по второй и т. д.).

В июле 1865 года сержант Э.Хоули предложил использовать для этого шифра веер, состоявший из 26 деревянных дощечек, на которых были записаны алфавиты шифротекста (строки таблицы). Этот веер оказался настолько эффективным в практическом применении, что впервые в истории США его автору был выдан патент на шифровальное устройство.

В то время как федералы внедрили централизованную организацию системы связи, конфедераты распространили принцип прав штатов и на сферу шифровального дела. Каждый командир мог по своему усмотрению выбирать собственные коды и шифры. Это привело к существенным негативным последствиям, поскольку местные командиры практически ничего не понимали в шифровальном деле.

Конфедераты использовали примитивные шифры вплоть до шифров простой замены. Например, перед битвой под Шайлоу 6 апреля 1862 года генерал Джонстон договорился со своим заместителем генералом Борегаром использовать в качестве военного шифра замену Цезаря. Изредка употреблялись книжные шифры. Книжным шифром пользовался президент конфедерации южных штатов Джефферсон Дэвис.

Конец ознакомительного фрагмента.