

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 978-5-5321-0491-4

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 978-5-5321-0491-4

© Гребенников В., 2019
© ЛитРес: Самиздат, 2019

Содержание

Предисловие	5
1. Криптология до XX века	9
2. Изобретение «линейного» шифрования	21
3. «Чёрный кабинет» Ярдли	27
Конец ознакомительного фрагмента.	31

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 «*gupa*» означает «тайна» и происходит из древнего немецкого корня со значением «прятать». В современных языках это слово также присутствует: немецкое «*gaupen*» значит «нашёптывать», латышское «*gunat*» – «говорить», финское «*gupo*» – «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

достойн, кто понимал скрытый смысл этих символов. Посвящённые жрецы считали свято-татством 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: «А» выражало начало всех вещей; «У» – 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 «А», «Е», «Н», «I», «О», «У» и «Ω» отвечали 7 планетам (небесам). Буквы «В», «Г», «Δ», «Z», «K», «Λ», «М», «N», «П», «Р», «Σ» и «Т» приписывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Ф» и «Х» 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 «Е» (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 «А», «Е», «I», «О», «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 древнем 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 интересовало, 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 шифрованием. Шифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифротекстом. Шифровка позволяет спрятать информацию от тех, для кого она не предназначена, 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 определёнными инструментами дешифрования.

Криптографический алгоритм, или шифр – это математическая формула, которая описывает процессы шифрования и расшифрования. Секретный элемент шифра, который должен быть недоступным 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 1777 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 дожидаться 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 зашифрованных 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 зашифрованной 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 названного «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 «М-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 (номенклатуры) 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 приемлемым 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 26×33 .

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 $26 \times 33 = 858$ 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: $26 \times 33 = 858$.

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 зашифрованного 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 зашифрованного 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 зависело 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: $2263966 \times 9 = 20375694$, 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 обеих 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 чаще 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, содержащий 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 26х26 (число букв латинского алфавита).

Столбцы таблицы обозначались буквами латинского алфавита по порядку (А, В, С,..., 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.

Перед битвой под Шайлоу он послал генералу Джонстону словарь для использования в качестве кодовой книги. Приложением к словарю была инструкция, в которой указывалось, что слово «соединение» будет обозначаться как «146.Л.20», что означало, соответственно, номер страницы, левый столбец и номер слова.

Словари использовались в качестве кодовых книг также в ВМФ конфедерации. Его министр Стефан Мелори лично распорядился, чтобы командиры кораблей получили идентичные экземпляры разных словарей.

Распространёнными в то время были шифры типа Виженера. Сохранились даже образцы таких шифровальных устройств в виде медных шифровальных цилиндров. Шифрование осуществлялось с помощью двух указателей (на верхней планке устройства) на буквы открытого текста и соответствующие им буквы шифротекста.

Как уже говорилось ранее, при шифровании допускались многочисленные ошибки. Ошибками конфедератов успешно пользовались федералы для дешифровки перехваченных сообщений. В частности, при использовании книжных шифров в качестве исходных шифровеличин выбирались не буквы, а слова и целые выражения. При этом конфедераты часто использовали общедоступные коммерческие кодовые книги, согласно которым и делали замену шифровеличин.

Федералам не сложно было перебрать ограниченное число коммерческих кодовых книг и найти ключ. Для усиления кодирования конфедераты вводили простые правила типа: если шифруемое слово находилось на 18-м месте 29-й страницы книги, то оно заменялось 18-м словом на 19-й странице. Однако подобные модификации не смущали федералов.

Шифрованная связь федералов осуществлялась через Управление военного телеграфа, при котором была шифровальная служба. Начальником военного телеграфа был майор Томас Эккерт (Thomas Eckert), который позже стал председателем правления компании «Вестерн Юнион телеграф».

Управление располагалось в доме военного министерства, находившееся рядом с Белым Домом. Президент Авраам Линкольн (Abraham Lincoln) уделял большое внимание организации шифрованной связи и часто общался с тремя молодыми телеграфистами-шифровальщиками: Дэвидом Бейтсом (David Bates), Чарльзом Тинкером (Charles Tinker) и Альбертом Чендлером (Albert Chandler). Эти люди были главными криптоаналитиками Севера.

Криптоаналитическая служба федералов достигла достаточно серьёзных успехов. Так, например, в декабре 1863 года начальник почтового отделения Нью-Йорка Абрам Уэйкман (Abram Wakeman), пересматривая корреспонденцию перед отправкой, наткнулся на письмо, адресованное Александру Кейту в город Галифакс в Новой Шотландии. О Кейте было известно, что тот часто переписывался с агентами Юга. Поэтому, раскрыв конверт и установив, что письмо зашифровано, Уэйкман передал его военному министру.

В течение двух дней сотрудники Военного министерства напрасно пытались разгадать таинственные знаки перехваченной криптограммы. Поэтому она была передана шифровальщикам президента Линкольна, взявшие её прочитывать. Они быстро установили, что неизвестный автор письма использовал для его зашифрования как обычный алфавит, так и 5 разных шифралфавитов. Но он поступил опрометчиво, разделив слова письма запятыми и ограничившись одним алфавитом в пределах каждого слова.

Дешифровщики нашли слово, состоявшее из шести букв, в котором вторая и шестая буквы повторялись. Следом шло слово из четырёх букв, за которым в свою очередь следовала фраза, посланная клерком: «reaches you». Они решили, что за этой последовательностью шифрознаков должна скрываться фраза «before this». Бейтс допустил, что в письме использован шифр, подобный тому, что применялся для обозначения цен в магазине в Питсбурге, где он когда-то давно работал посыльным.

Эта догадка позволила значительно продвинуть процесс дешифровки криптограммы. Помогло и выявление знаков, обозначающих место отправления и дату – «Нью-Йорк, 18 декабря 1863 г.». Действуя таким образом, 3 шифровальщика в присутствии президента Линкольна, нетерпеливо ожидавшего результатов, за четыре часа прочитали шифрованное письмо, в котором было написано:

«Нью-Йорк, 18 декабря 1863 г. ... Два парохода отбудут отсюда примерно на Рождество... 12 тысяч нарезных мушкетов пришли точно по адресу и отправлены в Галифакс в соответствии с инструкциями. Мы сможем захватить еще два парохода, как намечено... прежде чем это дойдёт до вас. Цена 2000 долларов. Нам нужно больше денег... Пишите как прежде...»

Два дня спустя была перехвачена и быстро дешифрована ещё одна криптограмма, адресованная Кейту. В ней говорилось: «Передай Мемминджеру, что у Хилтона все станки нахо-

дятся в собранном виде и все матрицы будут готовы к отправке 1 января. Гравировка печатных форм превосходная».

Таким образом, из письма стало известно, что формы для печатания денег конфедератов изготавливались в Нью-Йорке. Гравёра Хилтона легко нашли в Манхеттене. 31 декабря 1863 года полицейские совершили налёт на его жилище, где захватили печатные станки и матрицы, а также уже напечатаны деньги на сумму в несколько миллионов долларов. Тем самым конфедерация утратила оборудование для изготовления бумажных денег, которых ей не хватало. Главную роль во всём этом деле сыграли криптоаналитические способности, проявленные тремя молодыми шифровальщиками Линкольна. За это каждый из них получил прибавку к жалованию в размере 25 долларов в месяц.

Всего за время войны Север передал приблизительно 6,5 миллионов телеграмм. Конфедераты осуществляли перехват их телеграфных сообщений, многие из которых, естественно, шифровались. Их кавалерия осуществляла налёты на пункты связи, что приводило к компрометации систем шифрования федералов и позволяло конфедератам получать ключи и информацию об открытых текстах, соответствующих известным шифрованным текстам. Кроме того, шифры федералов имели уязвимые места. Несмотря на всё это, конфедераты так и не научились раскрывать зашифрованные сообщения федералов.

Они иногда не могли правильно расшифровать и свои собственные сообщения, поэтому не удивительно, что им не удалось прочитать ни одного зашифрованного сообщения федералов. Этому факту было бы трудно поверить, если бы конфедераты сами не признали его, напечатав в своих газетах несколько зашифрованных сообщений с просьбой их дешифровки.

Федералы также захватывали шифры Юга и осуществляли перехват курьеров с шифрованными сообщениями. Так, например, в 1863 году во время осады города Висксберга войска У. Гранта захватили восемь повстанцев и у одного из них нашли криптограмму. Её отправили в Вашингтон криптоаналитикам Президента, которые успешно справились с очередной задачей. Хотя дешифровка этой телеграммы не помогла Гранту «взять» Висксберг, но она дала федералам один из ключей, которыми конфедераты пользовались во время войны.

Шпионы как федералов, так и конфедератов зашифровывали свои сообщения очень простыми шифрами. Так, сторонница Севера Элизабет Ван Лью (Elizabeth Van Lew) защищала свои агентурные донесения с помощью буквенно-цифрового шифра, основанного на квадрате Полибия. А сторонница Юга Роза Гринхоу (Rose Greenhow) защищала свои агентурные донесения с помощью шифра случайной замены.

После окончания гражданской войны и победы федералов разработкой кодов и шифров стал заниматься Государственный департамент США. В 1867 году госсекретарь Уильям Генри Сьюард (William Henry Seward) (1801-72) разработал код Госдепартамента на 148 страницах. Однако процесс кодирования и декодирования оказался для дипломатов очень сложным.

Поэтому в 1871 году начальник корпуса связи полковник Альберт Майер разработал для Госдепартамента код на 88 страницах, состоявший из одной части. Книга содержала коды для времени суток, дней, месяцев и – впервые у истории кодов – лет. Она стала первым кодом Госдепартамента, в котором одному кодовому слову соответствовала длинная фраза или целое предложение. Для обозначения времени суток в качестве кодовых слов использовались женские имена, а дней месяца – мужские. Названия городов и стран заменялись цифрами.

Следующую книгу государственных кодов разработал в 1876 году заведующий бюро каталогов и архивов Госдепартамента Джон Генри Хасвелл (John Henry Haswell) (1841-99), который к этому делу подошёл очень серьёзно. Много лет он занимался вопросами стойкости кодов и дороговизны телеграмм, изучал методы шифрования Майера и Стейджера времён Гражданской войны и коммерческие коды, в частности: телеграфный код Слэйтера в 1870 году.

В результате книга Хасвелла, получившая название «Шифр Госдепартамента (1876)», содержала наилучшие черты кодов того времени и имела одну часть на 1200 страницах.

Поскольку она имела красную обложку, позже код был назван «красным» (англ. red). Для повышения стойкости своего кода Хасвелл разработал также «Дополнение к шифру Госдепартамента: код, который не поддаётся декодированию». В этом дополнении перечислялись 50 правил, или способов перешифрования, которые могли применяться к закодированным сообщениям.

В 1878 году впервые в истории США решающую роль в американской политике был вынужден сыграть криптоанализ. Всё началось с сенсационной статьи, напечатанной 7 октября газетой «Трибуна Нью-Йорка» (англ. The New York Tribune). В заметке, размещённой под заголовком «Перехваченные шифрованные телеграммы», приводился открытый текст нескольких криптограмм.

Дело в том, что в результате подсчёта голосов, собранных на выборах президента в 1876 году, первым оказался кандидат от Демократической партии Самуэль Тилден (Samuel Tilden), получивший на четверть миллиона голосов больше, чем его соперник от Республиканской партии Рутерфорд Хэйс (Rutherford Hayes). Но как окончательно распределятся голоса избирателей, зависело от того, какие из противоречивых результатов голосования, проведённого дважды во Флориде, Луизиане, Южной Каролине и Орегоне, будут признаны действительными. Конгресс создал специальную комиссию для решения этого вопроса, которая постановила отдать все спорные голоса избирателей Хэйсу. Это обеспечило ему большинство всего в один голос в коллегии избирателей и должность Президента США.

На сессии Конгресса, состоявшейся после выборов Президента, была назначена ещё одна специальная комиссия для расследования распространяемых демократами слухов о «покупке» республиканцами голосов избирателей. В ходе расследования комиссия конфисковала более 600 шифротелеграмм, посланных разными политическими деятелями и их доверенными лицами во время избирательной кампании в четырёх штатах. Остальные американская телеграфная компания «Вестерн Юнион» к тому времени уже успела уничтожить, чтобы показать, что гарантирует тайну доверенной ей переписки.

В 1875 году 27 шифротелеграмм были тайно переданы в прореспубликанскую газету «The New York Tribune» в надежде на то, что будучи дешифрованными, они поставят демократов в трудное положение. Интересно, что редактор газеты Уайтлоу Рэйд решил не ограничиваться публикацией шифротелеграмм своих политических противников. Он лично взялся за «раскрытие» шифропереписки демократов с целью предания огласке их открытых текстов.

Много читателей, побуждаемые редакционными статьями газеты, предлагали свои варианты дешифровки опубликованных шифротелеграмм, но при проверке все они оказались неверными. Между тем газета «Detroit Post» сумела вывести у одного из демократов, каким именно шифром пользовались его партийные соратники во время предвыборной кампании в Орегоне. Шифровальщик отыскивал нужное слово в «Домашнем английском словаре», изданном в Лондоне в 1876 году, определял порядковый номер этого слова на странице, отсчитывал 4 страницы назад и брал на ней соответствующее слово как кодовое обозначение. Для дешифровки полученного сообщения его адресат делал наоборот.

4 сентября 1878 года один из редакторов «The New York Tribune» Джон Хассард, основываясь на информации газеты «Детройт пост», опубликовал несколько открытых текстов дешифрованных криптограмм, из которых стало известно, что в Орегоне демократы стремились подкупить одного республиканского избирателя, однако соглашение не состоялось только из-за задержки с передачей ему денег.

Но «Домашний английский словарь» мало помогал в дешифровке сообщений демократов, посланных из других трёх штатов. Не полагаясь больше на постороннюю помощь, Рэйд предложил своим сотрудникам заняться их дешифровкой. За дело взялись Джон Хассард (John Hassard) и Вильям Гросвенор (William Grosvenor), экономический обозреватель «The New York Tribune». Причём Хассард работал над криптограммами так рьяно, что простудился,

заболел туберкулёзом и последующие последние десять лет своей жизни думал лишь о своем выздоровлении.

Позже Рэйд вспоминал: «Оба они трудились чрезвычайно хорошо, работали независимо друг от друга, честно сравнивая результаты, замечательно сотрудничали вместе... Хассард немного раньше начал работать в этой сфере и заслужил особой похвалы. Гросвенор был также способным и, как я сейчас вспоминаю, достиг почти такого же успеха. Иногда он и Хассард подходили к дешифровке одной и той же криптограммы с разных сторон и после многократных неудач, наконец, находили верное решение в тот же вечер...»

Одновременно с Хассардом и Гросвенором над чтением криптограмм, обнаруженных в редакционных статьях «The New York Tribune», работал молодой математик из военно-морской обсерватории США в Вашингтоне Эдвард Холден. В своих мемуарах Холден написал по этому поводу: «До 7 сентября 1878 года я открыл закономерность, с помощью которой можно было безошибочно найти любой ключ к самым тяжёлым и замысловатым из этих телеграмм».

Он обратился к газете «Нью-Йорк трибюн», которой понравилась идея нанять профессионального математика. Хассард выслал Холдену большое количество криптограмм. Однако на то время Хассард и Гросвенор независимо от Холдена разработали свои криптоаналитические методы и сумели опередить его в чтении некоторых криптограмм.

Рэйд утверждал, что ни одной из дешифрованных Холденом криптограмм «The New York Tribune» не получила раньше, чем эти же самые криптограммы были прочитаны Хассардом и Гросвенором. Поэтому результаты работы Холдена рассматривались лишь как подтверждение правильности дешифровок Хассарда и Гросвенора.

Результат превзошёл все ожидания. Общественность была возмущена непорядочностью демократов и захвачена изобретательностью дешифровщиков. Тысячи читателей расшифровывали криптограммы с помощью ключей, опубликованных в «The New York Tribune», и с удовольствием отмечали правильность их дешифровки. К тому же до выборов в Конгресс оставалось всего несколько недель. На них республиканцы получили значительную победу.

Часть дешифрованных телеграмм адресовалась не Тилдену, а его племяннику У.Пептону. И хотя Тилден клялся, что совсем не знал, чем занимался его племянник и что всё было сделано без его ведома, репутация Тилдена была навсегда запятнана. Это разоблачение положило конец его надеждам стать президентом. Даже биограф Тилдена, который имел к нему большую симпатию, признал, что в результате дешифровки телеграмм демократов республиканцы получили преимущество, обеспечившее им победу на президентских выборах в 1880 году. Вот так криптоанализ помог избрать американского президента.

В ноябре 1899 года «красный» шифр Госдепартамента был заменён на новый – «голубой» (англ. blue), который опять был разработан Джоном Хасвеллом и назван по цвету своей обложки. Книга была более подробной, содержала наиболее употребляемые термины и фразы из корреспонденции посольств и консульств, поэтому имела уже 1500 страниц.

Для повышения стойкости своего кода Хасвелл разработал также «Дополнение к шифру Госдепартамента: код, который не поддаётся декодированию» на 16 страницах. В этом дополнении перечислялись дополнительно ещё 25 правил, или способов перешифрования, которые могли применяться к закодированным сообщениям, кроме указанных в дополнениях к «красному» шифру.

В 1910 году Госдепартамент принял на вооружение «зелёный шифр» (англ. green), состоявший из двух частей (кодирование и декодирование) и имел 1418 страниц.

В марте 1918 года был введён в действие «серый» (англ. grey) код, в котором для обозначения стандартных терминов и фраз использовались пятибуквенные группы. В мае 1919 года «зелёный шифр», который реально был только кодом, получил соответствующее ему название «Код Госдепартамента А-1».

Эти коды вместе использовались американскими государственными служащими даже в период Второй Мировой войны, когда было нужно внести изменения в дипломатические и военные криптосистемы с целью повышения их стойкости. Так, например, в 1940 году ещё «серым» кодом «закрывалась» трансатлантическая переписка, в том числе между руководителями США и Великобритании.

30 декабря 1937 года был введён в строй «коричневый» (англ. brown) код Госдепартамента, содержащий раздел для кодирования объёмом 954 страницы и раздел для декодирования объёмом 938 страниц. Подобно «А-1» и другим современным на то время кодам «коричневый» код имел многочисленные варианты замены для часто употребляемых слов. Он также положил начало системе кодирования дат и времени, что стало новшеством в конце 1930-х годов.

Месяцы обозначались первой буквой, дни – второй и третьей, время – четвёртой, а с помощью пятой буквы уточнялась половина дня – первая или вторая. И хотя этот код в 1939 году был похищен из американского консульства в Загребе (Югославия), им продолжали пользоваться даже во время Второй Мировой войны.

Кодом американских военных атташе в то время был «чёрный» (англ. black), получивший название также по цвету своего переплёта. В начале 1940 года он считался неуязвимым, поскольку дополнительную стойкость ему обеспечивали шифровальные таблицы. Но в действительности уже в начале войны он был скомпрометирован: его «взломала» немецкая служба радиоперехвата и криптоанализа.

2. Изобретение «линейного» шифрования

В истории криптологии упрощение процедуры ручного шифрования путём механизации этого процесса издавна интересовало многих специалистов. Любопытные умы изобретателей неоднократно пытались решить эту проблему. Попыток было много, но лишь некоторые смогли оставить в истории заметный след и заложить фундамент для будущей механизации, а затем и автоматизации шифровального дела.

Толчком к необходимости автоматизировать процесс шифрования послужили технические достижения конца XIX века, такие как телеграф, телефон и радио, при использовании которых для передачи криптограмм удалось существенно повысить оперативность шифрованной связи. Вслед за изменениями в технологиях связи изменялась и криптология, которая стала сначала электромеханической, а затем электронной. Скорость передачи информации очень выросла и все большие объёмы ее были подвержены перехвату и прочтению. Шифровальщики, которые вручную заменяли буквы и слоги специальными символами, уже не могли справиться с постоянно растущим потоком информации.

Радиосвязь оказалась более дешёвой и мобильной по сравнению с проводной. Появилась возможность активизировать общение между воинскими подразделениями, устанавливать связь с подвижными объектами (автомобилями, самолётами, кораблями). Однако при этом упростился перехват переданных таким образом сообщений, что, в частности, подтвердила практика Первой Мировой войны.

Несмотря на то, что все участники боевых действий постоянно разрабатывали новые коды и совершенствовали старые, обеспечить их сохранность удавалось далеко не всегда. В результате противник нередко был полностью проинформирован обо всём, что было в секретной переписке врага. С этим были связаны и некоторые трагические события, из которых вспомним в третьей части лишь разгром двух российских армий под командованием генералов Раненкампа и Самсонова в Восточной Пруссии в августе 1914 года. Причиной их разгрома была плохая организация «закрытой» связи, в результате чего переговоры по радио велись вообще без всякого шифрования.

Во время войны главным (и чаще всего единственным) средством засекречивания было кодирование. Коды часто применяли не только для того, чтобы обеспечить секретность переданной информации, но и, чтобы сократить длину сообщения или сделать его более понятным. Чаще всего код представлял собой набор символов (цифр или букв), которые заменяли конкретные названия.

Кстати, развитие технического шпионажа и, в частности, радиоперехвата, буквально ни на шаг не отставало от развития систем передачи сообщений, осваивая новые диапазоны и способы модуляции. Однако основная масса телеграфных и телефонных сообщений передавалась или после их закрытия шифрами простой замены, или просто открытым текстом.

Резкое увеличение объёмов зашифрованных передач и сравнительная простота радиоперехвата сообщений подтолкнули дешифровщиков к мысли о том, что исследование отдельной перехваченной криптограммы необходимо связать с анализом всего массива перехвата, в котором появилась эта криптограмма. Этот путь оказался достаточно плодотворным. Как справедливо отмечает Дэвид Кан (David Kahn), «телеграф создал современное шифровальное дело, радио – современный криптоанализ».

Шифрованный текст, переданный по радио, был доступен каждому, кто имел в своем распоряжении радиоприёмник. И даже, если этот текст нельзя было расшифровать сразу, его можно было использовать при анализе следующих сообщений. В этот период получили развитие методы дешифровки, основанные на парах открытых и шифрованных текстов; на нескольких шифровках, созданных с помощью одного ключа; на переборе вероятных ключей. Именно

эти методы применялись англичанами для чтения секретной переписки немцев во время Первой мировой войны.

Телеграф и радио начали постепенно вытеснять кодирование с целью защиты информации в интересах применения шифров. Громоздкие и малоудобные при использовании секретные кодовые книги могли стать и становились добычей противника, а их изменение порождало серьёзные проблемы. Шифры оказались намного более мобильными и более дешёвыми. Секретное кодирование начало уменьшаться, но не исчезло совсем. Коды стали применяться вместе с шифрами. Такое соединение оказалось достаточно эффективным и дошло до наших дней. Подчеркнем, что при компрометации шифра достаточно лишь изменить его ключи, а не все кодовые книги. Отметим также, что коды очень чувствительны к лексике и словарному запасу языка общения. Появление новых терминов и понятий приводило к необходимости восстановления кодовых книг. Шифры в этом плане намного более важны, потому что их применение не связано с содержанием открытого текста.

Кстати, в 1881 году была запатентована первая идея телефонного шифратора Д.Х. Роджерсом (D.H. Rogers). Идея состояла в передаче телефонного сообщения несколькими (в самом простом случае – двумя) линиями с помощью поочередных импульсов в некоторой последовательности, которая быстро изменялась и напоминала телеграфное сообщение. Предлагалось разнести такие линии на значительное расстояние друг от друга для того, чтобы устранить возможность подключения сразу ко всем одновременно. Подключение же к одной из них позволяло бы слышать только отдельные неразборчивые сигналы.

В XIX веке применялось, в основном, так называемое предварительное шифрование сообщений. В этом случае отправитель зашифровывал передаваемое сообщение (в котором шифротекст удовлетворял требованиям телеграфной передачи), после чего относил зашифрованное сообщение на телеграф. В XX веке такое замедление в передаче сообщений часто оказывалось неприемлемым. Нужно было разработать методы так называемой линейной передачи зашифрованных сообщений, при которой аппарат шифрования (шифратор) находился бы непосредственно в аппаратуре передачи сообщений. Таким образом, передача зашифрованного сообщения в принципе не отличалась бы от передачи несекретного сообщения.

Такую идею автоматического шифрования телеграфных сообщений в декабре 1917 года предложил американец Жильбер Вернам (Gilbert Vernam) (1890–1960), молодой инженер компании «АТ&Т» (англ. American Telephone and Telegraph) и талантливый изобретатель. Он работал в телеграфном отделении научно-исследовательского отдела компании, где занимались разработкой «телетайпа» – буквопечатающего телеграфного аппарата.

Ещё летом, через несколько месяцев после того, как Соединенные Штаты объявили войну Германии, в компании началась работа над секретным проектом по сохранению секретности сообщений, переданных телетайпом. Во время исследований оказалось, что колебания тока в линии связи могли быть записаны с помощью осциллографа и потом легко преобразованы в буквы переданного сообщения. Поэтому было решено внести изменения в соединение проводов печатающего механизма телетайпа. В результате текст сообщения шифровался методом одноалфавитной замены. В телеграфном отделении понимали, что такая защита была слишком слабой, однако ничего другого придумать не смогли и прекратили заниматься этой проблемой до тех пор, пока Вернам не рассказал им о своей идее.

Он предложил использовать особенности телетайпного кода Бодо, в котором каждый знак состоял из пяти элементов. Каждый из этих элементов символизировал наличие («+») или отсутствие («—») электрического тока в линии связи. Таким образом, были 32 разных комбинации «+» и «—». 26 из них должно было соответствовать буквам, а оставшиеся соответствовали «служебным комбинациям» (пробел между словами, переход с букв на цифры и знаки препинаний, обратный переход с цифр и знаков препинаний на буквы, возвращения каретки печатающего устройства, переход на новую строку и холостой ход).

Например, буква «А» отражалась комбинацией «++—», а переход на цифры и знаки препинаний отражался комбинацией «++—++». Закодированное сообщение набивалось на перфоленте: «+» были дырками, а «—» – их отсутствием. При считывании перфоленты металлические щупы проходили через дырки, замыкали электрическую цепь и посылали импульсы тока по проводам. А там, где на перфоленте находился «—», бумага не позволяла этим щупам замкнуть цепь, и в результате токовый импульс не передавался.

Вернам предложил готовить перфоленту со случайными знаками (так называемую «гамму») предварительно и потом электромеханически соединять её импульсы с импульсами знаков открытого текста. «Гамма» – это секретный ключ, созданный из хаотического набора букв того же алфавита. Полученная сумма представляла собой шифротекст, предназначенный для передачи по линии связи. Вернам установил такое правило сложения: если одновременно оба импульса были «+» или «—», то итоговый импульс будет «-», а если эти импульсы разные, то в результате выйдет «+».

Сложение, по современной терминологии, осуществляется «по модулю 2» («0» означает знак «—», а 1 – «+»): $0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$; $1 + 1 = 0$. Пусть, например, знак «гаммы» имеет вид: «+—+—» (10100). Тогда буква «А» – «++—» (11000) при шифровании переходит в двоичную комбинацию «- ++—»: $(01100) = (11000) \times (10100)$. При дешифровке ту же операцию необходимо повторить в обратном порядке: $(01100) \times (10100) = (11000)$ – буква «А».

Чтобы складывать электроимпульсы при шифровании, Вернам сконструировал специальное устройство, которое состояло из магнитов, реле и токосъёмных пластин. А поскольку процедура дешифровки была аналогична процедуре шифрования, этот же прибор мог быть использован и при дешифровке. Импульсы поступали в устройство сложения из двух счётчиков: один считывал «гамму», а другой – открытый текст. «Плюсы» и «минусы», которые получали на выходе, можно было передавать как обычное телетайпное сообщение. На приёмном конце устройство, изобретённое Вернамом, добавляло импульсы, считываемые с идентичной ленты с «гаммой», и восстанавливало исходные импульсы открытого текста.

Важность изобретения Вернама заключалась в том, что больше не нужно было осуществлять шифрование и дешифровку секретных сообщений в виде отдельных операций. Открытый текст поступал в аппарат, находившийся у отправителя сообщения, и такой же открытый текст выходил из аппарата, который находился у получателя этого сообщения. А если кто-нибудь перехватывал это сообщение по пути прохождения от отправителя к получателю, то в его распоряжении оказывалась ничего не значащая последовательность «плюсов» и «минусов». Теперь, чтобы зашифровать, передать, принять и расшифровать сообщение, было нужно приложить не намного больше усилий, чем при отправлении сообщения открытым текстом.

Основное преимущество изобретённого Вернамом метода засекречивания сообщений заключалось в отсутствии механического шифрования открытого текста со следующей печатью результата на бумаге, осуществлённое ещё в начале 1870-х годов французами Эмилем Винеем (Emil Viney) и Жозефом Госсеном (Josef Gossen). Вернам впервые сумел совместить два процесса – шифрование и передачу сообщения. Он создал то, что впоследствии назвали линейным шифрованием, чтобы отличать его от традиционного предварительного шифрования. Вернам освободил процесс шифрования от уз времени и ошибок, исключив из этого процесса человека. Выдающийся вклад, сделанный Вернамом в практику шифрования, заключается именно в том, что он привнёс в шифровальное дело автоматизацию, которая уже успела к началу XX века послужить людям во многих сферах их деятельности.

Вокруг идеи, изложенной Вернамом в кругу коллег, моментально развернулась активная деятельность. Сначала Вернама заставили изложить эту идею в короткой записке, которая была датирована 17 декабря 1917 года. Компания «АТ&Т» сообщила об изобретении Вернама американскому военно-морскому ведомству, с которым она поддерживала тесное сотрудниче-

ство. 18 февраля 1918 года состоялось совещание, в котором приняли участие Вернам и другие инженеры телеграфного отделения компании «АТ&Т», с одной стороны, и военные моряки, с другой.

27 марта эти же инженеры встретились со своими коллегами из американской компании «Вестерн Электрик», производственного филиала «АТ&Т», и договорились с ними об изготовлении первых двух линейных шифраторов с использованием как можно большего количества стандартных деталей. В лаборатории «Вестерн Электрик» изготовленные шифраторы были присоединены к телетайпам и осуществлены первые испытания процесса, которые называли «автоматическим шифрованием». Все устройства, входившие в его состав, работали без сбоев. Компания «АТ&Т» проинформировала об этом факте майора Джозефа Моборна (Joseph Mauborgne) (1881–1971), занимавшего тогда должность начальника отдела научно-исследовательских и конструкторских разработок войск связи Армии США.

Нерешённым оставался только один вопрос – откуда брать «гамму». Сначала «гамма» для устройства Вернама представляла собой склеенные петлёй короткие перфоленты, на которых были набиты знаки, взятые наугад из разных открытых текстов. Инженеры компании «АТ&Т» почти сразу обратили внимание на существенные изъяны такого процесса «автоматического шифрования», связанные с недостаточной длиной «гаммы». Поэтому, чтобы усложнить криптоанализ, они сделали перфоленты с «гаммой» более длинными. Но тогда эти перфоленты стало слишком трудно использовать.

Вернам предложил суммировать две короткие, имеющие разную длину «гаммы» так, чтобы одна «гамма» шифровала другую. Полученная в результате так называемая «вторичная гамма», более длинная, чем две исходные «первичные гаммы», использованные для её генерации, была применена для зашифрования открытого текста. Например, если одна закольцованная лента имела 1000 знаков, а другая – 999, то данное расхождение в длинах всего в один знак давало 999 тысяч комбинаций, прежде чем результирующая последовательность повторялась.

Однако Моборн понимал, что даже усовершенствованная система Вернама очень уязвима для криптоанализа. В свои 36 лет будущий начальник войск связи Армии США Моборн был незаурядным криптоаналитиком. Он обстоятельно изучил криптоанализ в армейской школе связи и был хорошо знаком с последними достижениями в этой сфере. Более того, за несколько лет до описываемых событий Моборн сам принимал участие в одной научно-исследовательской работе, в ходе которой специалисты армейской школы связи сделали вывод о том, что единственной стойкой «гаммой» была та, которая сравнима по длине с самим сообщением. Любое повторение в «гамме» подвергало огромному риску полученные с её помощью криптограммы и, скорее всего, привели бы к их раскрытию.

Проведённый Моборном анализ системы «автоматического шифрования» ещё больше убедил его в этом. Он понял, что не имеет никакого значения, находятся ли повторения в пределах одной криптограммы или они распределены по нескольким, выходят ли они путём комбинации двух первичных «гамм» или в результате простого повторения в единственной длине «гаммы». Важным было то, что повторений в «гамме» не должно быть ни при каких условиях. Необходимо, чтобы она была совсем уникальна и максимально хаотична.

Осознав это, Моборн объединил свойство хаотичности «гаммы», на что опирался Вернам в своей системе «автоматического шифрования», со свойством уникальности «гаммы», разработанным криптографами армейской школы связи, в системе шифрования, которую сейчас принято называть «одноразовым шифроблокнотом». Одноразовый шифроблокнот содержал случайную «гамму», которая использовалась только один раз. При этом для каждого знака открытого текста предусматривалось использование абсолютно нового непрогнозируемого знака «гаммы».

Это была стойкая шифросистема. Подавляющее большинство систем шифрования были абсолютно стойкими лишь на практике, поскольку криптоаналитик мог найти пути их раскры-

тия при наличии у него определённого количества шифротекста и достаточного времени для его исследования. Одноразовый же шифроблокнот был абсолютно стойким как в теории, так и на практике. Каким бы длинным не был перехваченный шифротекст, сколько бы много времени не уделялось на его исследование, криптоаналитик никогда не сможет раскрыть одноразовый шифроблокнот, использованный для получения этого шифротекста. И вот почему.

Раскрытие многоалфавитного шифра означало объединение всех букв, зашифрованных с помощью одного шифралфавита, в одну группу, которую можно изучать на предмет выявления её лингвистических особенностей. Методы такого объединения могли быть разными в зависимости от вида «гаммы». Так, метод Казиского заключался в выделении идентично «гаммированных» букв открытого текста при повторяемой «гамме». Связная «гамма» могла быть вскрыта путём взаимного восстановления открытого текста и «гаммы». А «гамма», использованная для зашифрования двух или больше сообщений, поддавалась раскрытию путем одновременного возобновления открытых текстов этих сообщений, причем правильность прочтения одного текста контролировалась чтением другого. Почти для всех разновидностей многоалфавитных шифров был разработан свой метод раскрытия, основанный на их отличительных чертах.

Совсем другой была ситуация с одноразовым шифроблокнотом. В этом случае криптоаналитик не имел отправную точку для своих исследований, поскольку в одноразовой шифросистеме «гамма» не содержала повторений, не использовалась более одного раза, не была связным текстом и не имела внутренние структурные закономерности. Поэтому все методы дешифровки, в той или иной степени основанные на этих характеристиках, не давали никаких результатов. Криптоаналитик заходил в тупик.

Оставался лишь метод тотального испытания. Ведь прямой перебор всех возможных ключей, в конечном счёте, обязательно приводил криптоаналитика к открытому тексту. Однако успех, достигнутый этим путём, был иллюзорным. Тотальное испытание действительно позволяло получить исходный открытый текст. Но оно также давало и каждый другой возможный текст той же длины, поэтому сказать, который из них является правильным, было невозможно.

Вместе с тем, этот совершенный шифр не нашёл широкого применения из-за огромного количества «гамм», необходимых при его использовании. Проблемы, возникающие при изготовлении, рассылке и уничтожении «гаммы», человеку, не осведомлённому во всех тонкостях организации шифросвязи, могут показаться пустяковыми, однако в военное время объёмы переписки становятся очень большими. На протяжении суток может понадобиться зашифровать сотни тысяч слов, а для этого нужно изготовить миллионы знаков «гаммы». И поскольку «гамма» для каждого сообщения должна быть единственной и неповторимой, то её общий объём будет эквивалентен объёму всей переписки за время войны.

Таким образом, практические проблемы не позволили применять одноразовые шифроблокноты в быстро меняющихся ситуациях, например, в ходе проведения военных операций. Этих проблем не существовало в более стабильных условиях: в генеральных военных штабах, дипломатических представительствах или агентурной переписке одноразовые шифроблокноты были достаточно практичными и нашли применение. Однако и здесь возникали непреодолимые трудности, если объём переписки был слишком большим.

Это и случилось, когда Моборн, устроив первое большое испытание шифросистемы Вернама, установил его машины сразу в трёх городах. Даже, при сравнительно небольшом объёме переписки (до 135 коротких сообщений ежедневно) оказалось невозможным изготовить достаточное количество качественной «гаммы». Поэтому, не найдя другого выхода из трудного положения, Моборн стал комбинировать с двумя относительно короткими «гаммами» с целью получения из них более длинной «гаммы», как это сначала и предлагал сделать сам Вернам.

В сентябре 1918 года Вернам отправился в Вашингтон и подал там заявку на патент. Первая Мировая война успела закончиться раньше, чем шифросистема Вернама сумела хоть как-то проявить свои достоинства на практике. Тем не менее, 22 июля 1919 года на неё был выдан патент № 1310719 – важнейший в истории криптологии. Эксперты из вашингтонского патентного бюро признали возможную полезность этого изобретения и в мирное время.

Хотя созданный Вернамом прибор несомненно был ценным результатом творческого инженерного мнения талантливого изобретателя, в коммерческом плане он испытал полный «провал». Телеграфные компании и коммерческие фирмы, которые, по мнению «АТ&Т», должны были массово закупать запатентованные шифроприставки Вернама к своим телетайпам, отдавали предпочтение старомодным кодам, существенно снижавшим длину сообщений, тем самым уменьшая телеграфные расходы и одновременно обеспечивая хоть какую-то, даже небольшую, безопасность переписки.

По окончании Первой Мировой войны бюджеты вооружённых сил всех стран были сокращены до минимума. Недостаток средств и недостаточность материальных ресурсов заставили армейских связистов опять вернуться к комбинации двух относительно коротких лент с «гаммой», а продемонстрированная военными криптоаналитиками слабая стойкость такой системы генерации «гаммы» привела к тому, что шифросистема Вернама на время была забыта.

Что касается самого Вернама, то он продолжал заниматься научно-исследовательской работой в компании «АТ&Т». Учёный усовершенствовал свою шифросистему, а также изобрёл прибор для автоматического шифрования написанного от руки текста во время его передачи фототелеграфом. В 1929 году Вернама со значительным повышением перевели в один из филиалов компании «АТ&Т». Однако через четыре месяца в США разразился финансовый кризис, и, поскольку Вернам ещё не успел наработать достаточного производственного стажа на новом месте, его вскоре уволили.

Он перешёл на работу в другую большую компанию, но резкие перемены в его личной судьбе, вероятно, действовали на него угнетающе. С каждым годом о Вернаме было слышно всё меньше и меньше, пока наконец 7 февраля 1960 года человек, который автоматизировал процесс шифрования, не умер практически в полном забвении.

3. «Чёрный кабинет» Ярдли

В 1912 году в Госдепартаменте в качестве шифровальщика начал работать Герберт Ярдли (Herbert Yardley) (1889–1958), один из выдающихся американских криптоаналитиков. В начале своей карьеры Ярдли обратил внимание на слабость шифров, использовавшиеся американским правительством. Он был потрясён, узнав, что Президент США Вудро Вильсон (Woodrow Wilson) пользуется кодом, применявшимся уже на протяжении более 10 лет. Так, когда Вильсону было передано закодированное сообщение из 500 слов от его советника Хауза, Ярдли был поражён тем, что раскодировал и прочитал это сообщение всего за несколько часов.

Полученный успех ещё больше повысил интерес Ярдли к криптоанализу, и он в мае 1916 года написал 100-страничный меморандум «Раскрытие американских дипломатических кодов», который передал своему руководству. Углубившись в проблему возможного раскрытия очередного кода, он первым поставил диагноз явлению, с тех пор известному среди американских криптоаналитиков как «симптом Ярдли»: «Просыпаясь, я сразу начинаю об этом думать. Засыпая, я всё равно продолжаю думать об этом».

6 апреля 1917 года американский Конгресс объявил о вступлении США в Первую Мировую войну против Германии. А 28 апреля в составе Управления военной информации «MID» (англ. Military Information Division) Генштаба Военного Департамента (англ. War Department General Staff) была создана кабельно-телеграфная секция (англ. Cable and Telegraph Section), получившая кодовое название «MI-8» (англ. Military Information, Section 8).

Для участия в боевых действиях Первой Мировой войны на территорию Франции было переброшено по морю экспедиционное соединение американских войск под командованием генерала Джона Першинга численностью более 175 тысяч человек. Ярдли был направлен в этот экспедиционный корпус в качестве офицера-шифровальщика. Уже в первые месяцы работы Ярдли на практике продемонстрировал свои выдающиеся криптоаналитические способности.

Участие в войне дало ему возможность убедить «отца» американской военной разведки «MID» майора Ральфа ван Демана (Ralph van Deman) в необходимости создать спецподразделение для «взлома» шифров других стран. Он добился успеха не только потому, что американской армии были нужны криптоаналитики, но и благодаря исключительному таланту убеждать людей в своей правоте. В результате в июне 1917 года Ярдли в звании второго лейтенанта возглавил «MI-8».

Учебное подразделение «MI-8», занимавшееся подготовкой криптоаналитиков, возглавил доктор Джон Менли (Jon Manley). 52-летний филолог, который был деканом факультета английского языка в Чикагском университете, а также давним и пылким почитателем криптоанализа, Менли стал одним из лучших криптоаналитиков «MI-8». Руководимое им учебное отделение вело обучение криптоанализу в военном колледже Армии США.

«MI-8» читала дипломатическую шифропереписку Аргентины, Бразилии, Германии, Испании, Коста-Рики, Кубы, Мексики, Панамы и Чили. Служба американской цензуры посылала в «MI-8» перехваченные шифрованные письма. Большинство из них оказывалось любовными посланиями, в которых применялись очень простые шифры. Многие из них были таким компроматом, что Ярдли часто повторял: «Меня раздражает тот факт, что мужчины и женщины доверяют свою секретную переписку таким слабым методам шифрования».

Важнейшая из разработок «MI-8» привела к обвинению Лотара Витцке (Lothar Witzke) – единственного немецкого шпиона, приговорённого в США к смерти во время Первой Мировой войны. 25 января 1918 года при обыске в его багаже было обнаружено шифрованное письмо, датированное 15 января. Оно попало в «MI-8» только весной и пролежало там в течение еще нескольких месяцев, пока криптоаналитики безуспешно пытались его дешифровать. В конечном итоге это письмо удалось прочитать Менли, который и выяснил, что оно было послано

немецким послом в Вашингтоне Эккардтом немецкому консулу в Мексике. Открытый текст письма был таким:

«Предъявитель сего является подданным Германской империи, который путешествует под именем Павла Ваберского. Он является немецким секретным агентом. Если он обратится к вам с просьбой, пожалуйста, обеспечьте ему защиту и окажите помощь. Также выдайте ему до тысячи песо золотом и посылайте его зашифрованные телеграммы в наше посольство в качестве официальных консульских депеш».

Когда Менли зачитал этот текст в зале суда на закрытом процессе по обвинению Витцке в шпионаже, сомнений в его виновности ни у кого не осталось. Шпион был приговорён к смерти через повешение. Однако Вильсон заменил смертный приговор пожизненным заключением. В 1923 году Витцке был помилован и выпущен на свободу.

9 февраля 1918 года «MID» было реорганизовано в Управление военной разведки (англ. Military Intelligence Division). В ноябре того же года «MI-8» насчитывала 18 офицеров, 24 гражданских криптологов, 109 машинисток и стенографисток. Однако к маю следующего года её штатная численность сократилась до 15 офицеров, 7 гражданских криптологов и 55 технических служащих.

После участия Ярдли в 1919 году в Парижской мирной конференции в качестве главного криптолога американской делегации руководство разведки объявило о будущем свёртывании дешифровальной работы из-за потери её актуальности. Ярдли категорически это отрицал и подготовил доклад под названием «Изучение и раскрытие кодов и шифров», в котором указывал, что Соединённые Штаты имеют достаточно врагов во всём мире, поэтому раскрытие их шифросистем позволит правительству заблаговременно получить информацию о возможных угрозах национальной безопасности.

Ярдли предлагал не прекращать эту работу, а реорганизовать «MI-8» в криптослужбу мирного времени с двойным подчинением Государственному департаменту и Генштабу Военного департамента. Эта аргументация настолько поразила начальника разведки генерала Мальборо Черчилля, что он уговорил госсекретаря сохранить «Бюро шифров» и финансировать его работу из секретного фонда.

Это «Бюро шифров», позже ставшее известным как «американский чёрный кабинет» (англ. american black chamber) (далее – АЧК), должно было совместно финансироваться двумя департаментами на сумму приблизительно в 100 тысяч долларов в год, но её фактические расходы никогда не достигали этой суммы. По закону платежи Госдепартамента, начавшие поступать в июне 1919 года, не могли быть на законных основаниях потрачены в пределах Вашингтона, и поэтому Ярдли вместе с подобранным из состава «MI-8» персоналом АЧК вскоре переехал в Нью-Йорк. Военным департаментом АЧК был впервые профинансирован лишь 30 июня 1921 года. Первоначальный бюджет Бюро составил 45 тысяч долларов вместо запрошенных 96 тысяч, а к 1929 году снизился до 19630 долларов.

Конечным продуктом криптослужбы был бюллетень, посылавшийся в Отдел военной разведки и Госдепартамент, в котором указывались все факты, заслужившие внимания, естественно, без ссылок на истинное происхождение информации.

Все сообщения начинались стереотипно: «Из источников, которые заслуживают доверия, установлено, что». При этом никакого информационно-аналитического подразделения в «Бюро шифров» не было, материалы отбирал лично его руководитель, часто по субъективным признакам.

Послевоенная дешифровка АЧК немецкой переписки базировались на полученных в Нидерландах в 1919 году ключах, предложенных американским представителям инициативником, известным под агентурным псевдонимом «Дачмен». Как обычно происходило в подобных случаях, «Дачмена» обманули: когда он оставил кодовые таблицы для изучения, их сфотографировали и вернули, якобы по ненадобности. Но на основании его данных американцы

сумели раскрыть немецкие коды с обозначениями «2500», потом «2970», «9700», «5300» и «1219». Всего АЧК прочитал 20 немецких кодов и шифров, однако на послевоенный период из них пришлось лишь 9, фактически представлявших собой вариации двух базовых систем.

Одной из основных задач, поставленных перед АЧК, было раскрытие кодов Японии, напряжённость в отношении с которой росла с каждым днём. В порыве энтузиазма Ярдли пообещал добиться их раскрытия на протяжении года или уйти в отставку. Он пожалел о своём обещании сразу, как только приступил к этому делу, поскольку моментально запутался в открытых текстах на японском языке, не говоря уже о самом шифротексте.

После длительного предварительного анализа Ярдли выяснил, что для своих телеграфных сообщений, передававшихся буквами латинского алфавита, японцы использовали немного видоизменённую форму иероглифической письменности, называемой «катакана». Но несмотря на тщательное изучение перехваченных шифротелеграмм, прочитать их так и не удалось. Он писал:

«К этому времени, я так долго работал с кодированными телеграммами, что каждая их строка, даже каждое кодовое обозначение неизгладимо отпечатались в моей голове. Я мог лежать на кровати с открытыми глазами и заниматься своими исследованиями в кромешной тьме... И вот однажды я проснулся в полночь, так как ушёл с работы рано, и откуда-то из темноты пришло убеждение, что определенная последовательность двухбуквенных кодовых обозначений должна абсолютно точно соответствовать слову «Ирландия». Затем передо мной заплесали, быстро сменяясь, другие слова – «независимость», «Германия», «точка»... Великое открытие! Сердце мое замерло, я не смел двинуться с места. Было ли это со мной во сне или наяву? Не сошёл ли я с ума? Решение? Наконец-то после всех этих месяцев! Я спрыгнул с кровати и в спешке (поскольку теперь я уже точно знал, что не сплю) почти скатился по лестнице. Дрожащими руками я открыл сейф, схватил папку с бумагами и торопливо начал делать заметки».

На протяжении часа Ярдли проверял свои гипотезы, а затем, убедившись, что начало успешному раскрытию положено, вернулся к себе домой и напился. Однако его радость была немного преждевременной. Ярдли встретился с неожиданными трудностями, пытаясь подыскать переводчика с японского языка. В конечном итоге он нашёл добродушного миссионера, который в феврале 1920 года сделал для Ярдли первые переводы открытых текстов японских шифротелеграмм. Через полгода миссионер-переводчик уволился, осознав шпионский характер своего труда. Однако в то время один из подчинённых Ярдли сделал поистине неслыханный подвиг, выучив за это время очень сложный японский язык.

В 1920 году Ярдли доложил о раскрытии четырёх японских кодов, но это утверждение было не полностью корректным, поскольку раскрытые системы были не кодами, а шифрами, причём достаточно невысокого уровня стойкости. Однако вскоре после этого «Бюро шифров» действительно достигло выдающихся успехов. Всего с 1917 по 1929 годы американцы сумели скомпрометировать 31 японскую шифросистему (условные обозначения от «JA» до «JZ» и от «JAA» до «JJJ») и прочитать 10 тысяч текстов, 1600 из которых относились к Вашингтонской конференции. Это было очень высоким показателем, особенно с учётом острого недостатка сотрудников со знанием языка.

Летом 1921 года АЧК прочитал японскую шифротелеграмму от 5 июля, направленную в Токио послом Японии в Лондоне и содержала первые упоминания о конференции по разоружению, которая должна была состояться в ноябре в Вашингтоне. После этого чтение японской дипломатической шифропереписки стало настолько регулярным, что за несколько месяцев до открытия конференции были введены ежедневные поездки курьеров между АЧК и Госдепартаментом. Одно официальное лицо в правительстве США с улыбкой заметило, что руководители Госдепартамента относились к работе криптоаналитиков АЧК с восхищением и каждое

утро читали дешифрованные ими японские криптограммы, попивая при этом апельсиновый сок или кофе.

Целью Вашингтонской конференции по разоружению было ограничение тоннажа больших военных кораблей. По мере того, как переговоры приближались к своему главному результату – договору пяти держав, устанавливавшему определённое соотношение тоннажа для Англии, Италии, США, Франции и Японии, персонал Ярдли читал всё большее количество секретных шифрованных инструкций, которые предназначались для стран, принимавших участие в переговорах.

Он писал: «Американский чёрный кабинет, глубоко спрятанный за надёжными запорами, всё видит и всё слышит. Хотя ставни закрыты и окна тщательно зашторены, его зоркие глаза видят, что творится на секретных совещаниях в Вашингтоне, Женеве, Лондоне, Париже, Риме и Токио. Его чуткие уши слышат даже самые слабые шёпоты в столицах иностранных государств».

Каждый участник переговорного процесса в Вашингтоне стремился добиться наиболее благоприятного для себя тоннажного соотношения. Самой агрессивной оказалась Япония, которая вынашивала широкомасштабные замыслы, связанные с экспансией в Азии, но побаивалась вызвать недовольство своими действиями со стороны США. В самый разгар конференции, когда Япония потребовала установить для себя соотношение 10 к 7 по сравнению с США, АЧК прочитал японскую шифротелеграмму от 28 ноября, которую Ярдли позже назвал важнейшей из дешифрованных им криптограмм.

«Вам надлежит удвоить усилия для достижения поставленных целей в соответствии с проводимой нами политикой, избегая при этом любых столкновений с Америкой по вопросу об ограничении вооружений, – телеграфировало японское МИД своему послу в Вашингтоне. – Вы должны добиться принятия предложения о соотношении тоннажа 10 к 6 с половиной. Если же, несмотря на все ваши усилия, ввиду сложившейся ситуации и в интересах нашей политики, возникнет потребность пойти на уступки, вам необходимо заручиться согласием всех сторон на ограничение права концентрации военно-морских сил и проведения манёвров на Тихом океане в обмен на нашу гарантию сохранить там статус-кво. В принятом соглашении вам также следует сделать соответствующую оговорку, из которой было бы совершенно ясно, что именно в этом состоит наше намерение, когда мы принимаем соотношение 10 к 6».

Уменьшение тоннажа ВМФ Японии на 0,5 условных единиц, о чём шла речь в этой японской шифротелеграмме, приблизительно отвечало двум большим боевым кораблям. Поскольку представители США на переговорах вовремя получили из АЧК информацию о том, что в случае давления японцы согласятся на увеличение тоннажного соотношения между Америкой и Японией, оставалось только осуществить это давление на практике. Что и сделал госсекретарь Чарльз Хьюз.

10 декабря Япония «капитулировала». В прочитанной АЧК шифротелеграмме японская делегация на переговорах в Вашингтоне получила инструкцию из Токио о том, что необходимо принять соотношение, предложенное США. В итоге договор, подписанный пятью государствами, установил для США и Японии соотношения тоннажа больших военных кораблей в размере 10 к 6. Японцы надеялись на большее. Однако добиться желаемого им помешал АЧК.

За время проведения конференции в АЧК было прочитано и переведено больше пяти тысяч шифросообщений. В результате перенапряжения несколько его сотрудников заболели на нервной почве. Один начал что-то бессвязно бормотать, а другой стал посвящать всё своё свободное время ловле бродячей собаки, у которой на боку якобы был записан японский дипломатический код. Третьему мерещился ужас, и он постоянно носил при себе огромную сумку с камнями, собранными на морском берегу. В результате все трое были вынуждены уйти с работы. Сам Ярдли также оказался на грани нервного расстройства и в феврале 1922 года получил четырёхмесячный отпуск для восстановления своего здоровья.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.