Германия. «Энигма» (Enigma)

В данной книге будет рассказано о шифрмашинах Германии и её союзников, которые были в основном дешифрованы советскими специалистами и союзниками, а также криптоаналитиками нейтральной Швеции (при этом как отмечалось выше, благодаря советской разведке, результаты работы криптоаналитиков Великобритании и Швеции были известны в СССР). Рассмотрим эту аппаратуру подробнее.

Первые механические криптографические машины (относящиеся к классу роторных) для шифрования текстов были независимо изобретены шестью инженерами в период 1915–1919 годов в Голландии, США, Швеции и Германии (T. A. van Hengel, R. P. C. Spengler, E. Hebern, A. Damm, H. Koch, A. Scherbius)[1]. Одним из этих изобретателей, чья роторная криптомашина получила впоследствии наибольшую известность, был Альберт Шербиус, который получил патент 23 февраля 1918 года и в этом же году в Берлине основал фирму Scherbius & Ritter. Коммерческого успеха шифрмашина не имела и в 1918 году Шербиус предложил её германскому флоту, указывая, что 7-ми роторное устройство создаёт 6 миллиардов комбинаций, а при 13-ти роторах — 100 триллионов. По расчётам Шербиуса, если даже враг похитит 8-мироторную машину, а также оба текста — открытый и шифрованный, потребуется непрерывная круглосуточная работа 1000 дешифровальщиков в течение 14,5 лет, чтобы найти ключ.

Но военные предложение отвергли и специалисты компании начали улучшать шифрмашину. Роторы, отличавшиеся между собою комбинацией внутренних проводных соединений, были модифицированы так, что могли извлекаться из машины и устанавливаться в различном порядке. Другое изменение состояло в том, что вращающееся кольцо на каждом из роторов могло быть зафиксировано в любой из 26-ти позиций, номера которой ранее наносились непосредственно на роторы. Оператор справлялся по таблице внутри корпуса, чтобы перевести буквы в числа, например J=10. Теперь вместо того, чтобы буква определяла начальное положение ротора, принимающему оператору необходимо было знать также положение алфавитного кольца на роторе, то есть зубец, который приводил в движение на один шаг соседний ротор, мог смещаться относительно роторного кольца.

Не получив заказов от военных Шербиус предложил свою разработку немецкой компании Gewerkschaft Securitas. Компания Chiffriermaschinen AG (Берлин) позднее в июле 1923 года развернула производство и продажу шифрмашины, которая получила название «Энигма» (Enigma, по гречески — «загадка») и предназначалась для шифрования телеграфной связи между банками.

В 1918 году шифратор «Энигма» имел вес 18 кг и габариты 34×28×15 см. С начала 1920 годов немцы начали активно рекламировать её коммерческий вариант, а Шербиус развернул энергичную деятельность с целью повышения спроса на «Энигму». В 1923 году он выставил свой шифратор в Берне, а затем в 1924 году на съезде Международного почтового союза

в Стокгольме. «Энигма» стала широко рекламироваться на радио и в прессе, были выпущены рекламные буклеты на немецком и английском языках, в которых, в частности, говорилось: «Естественному любопытству конкурентов сразу же будет положен конец, так как „Энигма“ позволяет вам хранить содержание ваших документов, или, по крайней мере, их самых важных частей, в полной тайне от любопытных глаз без каких-либо существенных затрат. Один хорошо защищенный секрет поможет разом окупить все затраты на приобретение этой машины»[2].

Однако, несмотря на активную рекламную кампанию, дела у Шербиуса шли неважно. Потенциальных покупателей отпугивала слишком высокая цена «Энигмы». Считанные экземпляры шифратора были приобретены армиями различных государств и компаниями связи, но с массовыми закупками никто не спешил.

Английские криптоаналитики ознакомились с устройством «Энигмы» в июне 1924 года, когда немецкая компания Chiffriermaschinen AG, производившая этот шифратор, предложила британскому правительству закупить партию аппаратов по цене около 200 долларов за штуку (весьма крупная сумма в то время, сравнимая с ценой небольшого автомобиля). В ответ правительство Великобритании предложило немцам зарегистрировать сначала аппарат в Британском патентном бюро. Германская компания согласилась и предоставила в Бюро полную документацию с описанием работы шифратора. В результате криптографическая спецслужба Британии получила полный доступ к криптосхеме коммерческой версии «Энигмы».

Германскими фирмами впоследствии было произведено беспрецедентное количество «Энигм» — более 100 000 шифрмашин. Но не все шифрмашины назывались так и имели этот логотип. Большинство шифрмашин имело только серийный номер и фабричный код. Машины производились на различных фабриках и в различных городах: Ertel-Werk fur Feinmechanik (Мюнхен), Olympia Buromashinenwerke (Эрфурт),

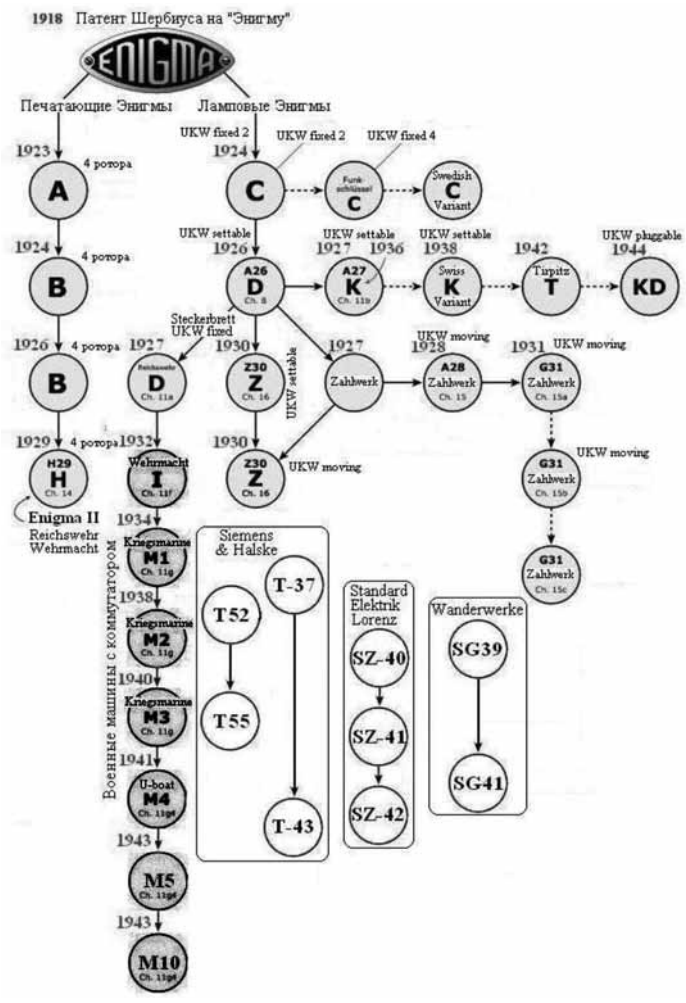

Рис. 1. Хронология разработок немецких шифраторов.

Chiffriermaschinengesellschaft Heimsoeth & Rinke (Берлин), Atlas-Werke Maschinenfabrik (Бремен), Konski & Kruger (Берлин). После приобретения необходимых патентных прав или лицензий эти компании производили машины «Энигма» и в военный период. Учитывая это, некоторые источники приводят цифру в ~200 000 шифраторов, изготовленных в 1920–1940 годах, из которых до конца войны вермахт закупил более 30 000 машин.

В течение Второй мировой войны бренд «Энигма» был весьма распространенным шифратором, который использовался в Германии и в странах-союзниках Германии — Италии, Японии, а также в Норвегии и Швейцарии. К концу войны количество конструктивных модификаций «Энигмы» составило обширное семейство из более, чем 30 шифрмашин: Enigma-A, -A26, -A27, -A28, -B, -B',-C, -D, -E, -F, -G31, -H29 (Enigma II), -Z30, -I, -K, -KD, -K932, -T, -M1–M5, -M10 и др. (см. рис. 1.)[3]. По окончании Второй мировой войны союзнические силы продавали трофейные машины, по прежнему считавшиеся на тот момент надёжными, в различные развивающиеся страны.

Основной механизм шифраторов Энигма представлял собой обычную клавишную пишущую машинку, которая укладывалась в деревянный футляр. Шифровальный механизм состоял из роторов (барабанов) шириной около ½ дюйма, с выбитыми по их окружности буквами алфавита и располагавшихся рядом на горизонтальной оси. На каждой стороне ротора по окружности располагалось 26 электрических контактов (по числу букв в классическом латинском алфавите). Контакты с обеих сторон барабана соединялись попарно *случайным образом 26 проводами* (перепайками), формировавшими замену символов. Эти «случайно» выполненные соединения в каждом из роторов являлись долговременным секретным криптографическим ключом, возможность определения которого противником должна быть исключена. Роторы были связаны шестеренками. При нажатии клавиши один из роторов приходил в движение, другие тоже начинали вращаться, но с разными скоростями. Зашифрование каждой буквы осуществлялась с помощью электроимпульсов, которые, проходя последовательно через все роторы, отражались от последнего и выходили через зигзагообразные промежутки, образованные разными положениями роторов по отношению друг к другу. Роторы касались друг друга подпружиненными контактами, которые и обеспечивали прохождение электрического тока сквозь весь пакет (3, 4 и более в различных моделях) роторов. Результат шифрования фиксировался лампочкой, засвечивавшей соответствующую букву (рис. 2.).

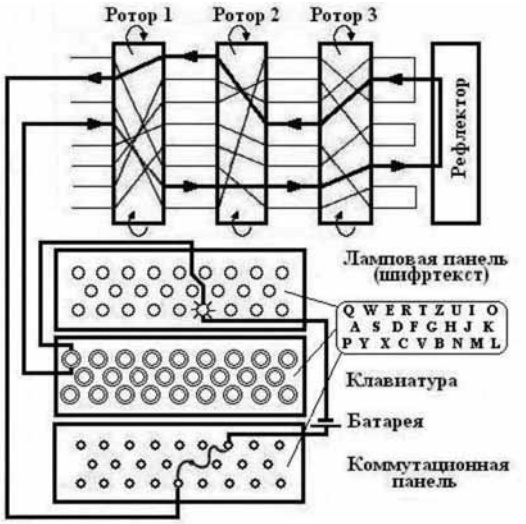

Рис. 2. Блок-схема 3-хроторного «лампового» шифратора «Энигма». Показаны коммутации при шифровании одной буквы (Q→B)

Ключ к шифру на определенный период, например на 24 часа, определялся исходным положением каждого ротора, которое легко менялось. Перед началом работы роторы поворачивались так, чтобы устанавливалось выбранное кодовое слово (пароль) из 3-х букв, а при нажатии клавиши и кодировании очередного символа правый ротор поворачивался на один шаг. После того как он делал полный оборот, на один шаг поворачивался следующий ротор — как в электросчетчике. Таким образом, получался ключ заведомо более длинный, чем текст сообщения. Для 3-хроторной машины период составлял $26 \times 26 \times 26 = 17\,576$ и, так как сообщения обычно не превышали нескольких сотен символов, не было риска повтора позиции роторов при шифровании одного сообщения.

Такой механизм обеспечивал миллионы вариантов шифра простой замены, определяемого текущим положением роторов. Для затруднения дешифрования роторы периодически переставлялись местами или заменялись на другие, имевшие отличавшиеся перепайки внутренних соединений. Дальнейшие усовершенствования машины заключались в замене регулярного вращения роторов на более хаотичное и в увеличении их числа сначала до 4, а потом до 5, 6, 8-ми и более. Все устройство могло поместиться в портфеле и было настолько простым, что

обслуживалось обычными связистами. Оно не обладало особой скоростью, но, безусловно, задавало большую работу криптоаналитикам.

В 1930 году для увеличения стойкости в конструкции военной версии «Энигмы» стала применяться дополнительная коммутационная панель из двадцати шести пар розеток и штепселей. С помощью этой панели осуществлялась дополнительная замена знаков перед тем, как знаки открытого текста в виде электрических сигналов поступали с клавиатуры на систему роторов и после того, как они ее покидали. У коммерческих вариантов шифратора такая панель отсутствовала.

После смерти Шербиуса[4] дальнейшим постоянным совершенствованием «Энигмы» занимался инженер Вилли Корн (Willi Korn), который и предложил для повышения стойкости к взлому 3-хроторной шифрмашины новый коммутирующий элемент — 4-й «половинный» ротор «*Umkerwalze*» (или UKW), выполнявший роль «рефлектора» (см. рис. 8.2. вверху справа). Рефлектор представлял собой тринадцать проводников, соединявших пары различных контактов на задней стороне третьего ротора. С его помощью сигнал шел обратно через роторы, но уже по другому пути. Когда сигнал выходил из набора роторов, он поступал на лампочку-индикатор, которая указывала на букву шифрованного текста.

Принцип рефлектора был изобретен Хьюго Кохом и означал следующее: при любом положении ротора если данная буква, например, A зашифрована как W, то W может также шифроваться в A. То есть каждый шифралфавит, генерируемый машиной, в принципе является обратимым. При наличии рефлектора машине не требуется переключателя на расшифрование. Необходимо только поставить роторы в том же порядке и стартовые позиции. Тогда буквы шифртекста преобразуются в открытый текст, а электрические лампочки укажут этот результат на табло. Более совершенные версии рефлектора B и C использовались на моделях для Вермахта и Люфтваффе (сухопутные войска и ВВС фашисткой Германии), а также на модели Кригсмарине (ВМС фашисткой Германии) Enigma M3. Этими же рефлекторами комплектовалась 4-хроторная Enigma M4, но с другими перепайками. В конце войны в 1944 году германское командование пыталось внедрить новый тип переключающегося рефлектора UKW-D, что создавало существенные проблемы для дешифровальщиков союзников, поскольку рефлектор мог меняться ежедневно. Но проблемы с абонентским распределением этого рефлектора и ключевых таблиц к нему воспрепятствовало его широкому распространению.

С целью повысить стойкость Энигмы с июля 1944 года ВВС Германии стали использовать небольшую приставку Enigma Uhr. Эта небольшая деревянная коробка подключалась к коммутационной панели Энигмы 20-ю проводами. С помощью большого поворотного переключателя оператор мог быстро выбрать одну из 40 возможных конфигураций соединения панели.

Ещё одной попыткой повысить безопасность Энигмы был похожий на штатный ротор, так называемый «*Luckenfullerwalze*», который содержал 26 переключателей, выбираемых пользователем. С помощью этого приспособления число и комбинации соединений в каждом роторе могли часто изменяться. «*Luckenfullerwalze*» предполагалось использовать совместно с UKW-D, но подобно Enigma Uhr, да и UKW-D этот переключатель появился слишком поздно.

Первая шифрмашина под названием Enigma-A появилась на рынке в 1923 году. Машина была тяжёлой и очень большой, имела электропривод и внешний вид электрической пишущей машинки. Её размеры составляли $65 \times 45 \times 35$ см, а вес около 50 кг. Шифрование осуществлялось со скоростью 300 символов в минуту, а шифртекст разделялся на 50-тирядные группы по 5 букв. По желанию даже в середине процесса шифрования можно было перейти в режим обычной открытой печати текста. В машине использовалось 4 ротора с 28-ю контактами в соответствии с выбранным вариантом алфавита на 28 букв. Последовательность состояний 4-х вращающихся роторов с различным числом зубцов имела период $11 \times 15 \times 17 \times 19 = 53\,295$ шагов[5].

Во втором варианте Enigma-B, разработанном в 1924 году и модернизированном в 1926 году машина представляла собой модифицированную электрическую пишущую машинку, с правой стороны которой было встроено шифровальное устройство с 4-мя сменными роторами. На смену вращающейся печатающей головке, применявшейся в Enigma-A, пришел набор плоских поворачивающихся рычагов с литерами аналогично распространенным моделям канцелярских пишущих машин. Внешне Enigma-B выглядела очень хорошо, но в её производстве возник ряд проблем, и к тому же выяснилось, что она плохо работает при высо-

кой скорости печати. Поэтому в 1926 году она была заменена модифицированной и улучшенной версией.

На смену весьма непрактичным моделям Enigma-A/-B в конце концов в 1929 году пришла ещё более громоздкая и тяжелая 8-мироторная H29, которая стала последней моделью в ряду буквопечатающих машин «Schreibende Enigma». В Рейхсвере (предшественнике Вермахта) она была названа Enigma-H. Иногда эта машина использовалась в качестве принтера для модифицированных моделей Enigma-G или Enigma-I.

Модели Enigma-A/-B/-H были совсем не похожи на более поздние версии. Коммерческого интереса к ним проявлено не было, вероятно потому, что машины были дорогими и сложными в обслуживании. Ни ВМС, ни МИД не приняли предложений изобретателя по буквопечатающим вариантам «Энигмы», поэтому он попробовал предложить эти громоздкие шифровальные машины в гражданские секторы экономики для эксплуатации в стационарных, офисных условиях. В армии и МИДе продолжали пользоваться шифрованием по кодовым книгам.

Тем не менее, в 1925 году Шербиус приступил к массовому производству своего шифратора, а военные стали постепенно проявлять интерес к «Энигме». Начиная со следующего года ими стал оснащаться немецкий флот, а с 1928 года вооруженные силы и спецслужбы Германии. Наиболее востребованными «Энигмы» стали после прихода Гитлера к власти в Германии в 1933 году, когда началось серьезное перевооружение армии. До Второй мировой войны и во время нее было выпущено около двухсот тысяч экземпляров шифраторов «Энигма» различных версий, они применялись во всех видах германских вооруженных сил, в Абвере (немецкая военная разведка) и в службе безопасности СД.

Ещё в 1924 году была создана 3-хроторная Enigma-C — более дешевая переносная альтернатива большим и тяжелым пишущим машинам типа Enigma-A. Она была первой моделью, в которой использовались миниатюрные электрические лампочки для подсвечивания выходных букв шифртекста. Модификация Enigma-C могла выполнять как шифрование, так и расшифрование и не требовала сложного обслуживания. Благодаря замене буквопечатающего устройства ламповой панелью она стала существенно меньше и легче. Она не отличалась большой стойкостью к взлому поскольку в её создании не участвовали профессиональные криптологи. Эта модель использовалась Кригсмарине с 1926 по 1934 годы, а позднее немецкий флот начал применять очередную модификацию Enigma-I (или Wehrmacht Enigma), которая стала базой для всех последуюших версий, предназначенных для вооруженных сил. Вначале Enigma-I имела 3 ротора, но с 1939 года была переоборудована на 5 роторов (в шифратор устанавливались 3 из них, то есть производилась выборка 3 роторов из 5 и их взаимная перестановка, эта ключевая установка менялась раз в месяц).

Массовое производство 3-хроторных машин «Энигма» началось только в 1925 году и они использовались в коммерческих целях, а также в военных и государственных службах многих стран мира. Как и другие роторные машины этого периода, «Энигма» состояла из комбинации механических и электрических систем, которые позволяли реализовать многоалфавитный шифр замены, что давало высокую стойкость шифра для того времени. Ключ к шифру на определенный период, например сутки, определялся положениями каждого из 3-х роторов, которые легко менялись. При нажатии клавиши и кодировании очередного символа крайний ротор поворачивался на один шаг. После того, как он делал оборот, на один шаг поворачивался следующий ротор. Таким образом, для повышения стойкости позднее был использован специальный коммутатор — «рефлектор», а тяжелая буквопечатающая машинка заменена на панель сигнальных лампочек, что привело к созданию компактной модели под названием — «ламповая Энигма-C».

Трехроторная Энигма предназначалась для сухопутных и военно-воздушных сил. Её размеры составляли 34 × 28 × 15 см и вес около 11 кг. Позади клавиатуры с 26-тью буквами (без цифр и знаков пунктуации) обычной немецкой пишущей машинки располагалась панель с такими же буквами, под которыми зажигались электрические лампы от батареи 4,5 В.

Как правило, с армейским вариантом трехроторной «Энигмой» работали три человека. Один зачитывал открытый текст, другой набирал его на клавиатуре, третий считывал шифртекст с ламп и записывал его. «Энигма» была портативной (размером с пишущую машинку), работала от батареи, имела деревянный футляр. Одним из недостатков шифратора было то, что он не печатал шифртекст. Впоследствии появились модификации «Энигмы», дающее такую возможность.

Рис. 3. Трехроторная армейская «ламповая» шифрмашина Энигма

Чтобы сообщение было правильно зашифровано и расшифровано, машины отправителя и получателя должны были быть одинаково настроены. Идентичными должны были быть: выбор роторов, начальные позиции роторов и соединения коммутационной панели. Эти настройки оговаривались заранее и записывались в специальных шифровальных книгах. В военно-морских силах эксплуатировалась как 3-х, так и 4-хроторные Энигмы — модели M3 и M4.

Семейство шифровальных машин «Энигма» насчитывает огромное количество моделей и вариаций дизайна. Ранние модели были коммерческими, начиная с 1920-х годов. Начиная с середины 1920-х различные немецкие военные службы стали использовать эти машины, внося большое количество собственных изменений для повышения безопасности. Кроме того, другие страны использовали чертежи «Энигмы» для создания своих собственных шифровальных машин. Модель Enigma-D, выпущенная в 1927 году широко использовалась в Нидерландах, Великобритании, Японии, Италии, Испании, США, Польше, Швейцарии. В 1928 году германская армия внедрила собственную 4-хроторную модель Enigma-G («Энигма» Абвера), модифицированную в 1930 году в модель Enigma-I («Энигма» вермахта — размеры $28 \times 34 \times 15$ см, вес около 12 кг). Существовала также большая 8-мироторная печатающая модель Enigma-II, которая использовалась для связи высших армейских структур, но вскоре Германия прекратила её использование из-за ненадежности механизмов.

Следует отметить, что сами немцы допускали возможность взлома шифра «Энигмы». Ещё в 1930 году ведущий немецкий криптоаналитик Георг Шредер продемонстрировал такую возможность, вполне по-немецки заметив при этом: «Энигма — дерьмо!»[6]. Однако из-за постоянного усложнения моделей были периоды, когда английские криптографы из Блетчли-Парк не могли с ней справиться. Так, в Германии считали абсолютно надежным шифрование 4-хроторной Enigma-M4 поскольку возможен был выбор из огромного числа способов кодирования текстовых сообщений — 2×10^{145}(!)

Рис. 4. Четырехроторная машина Enigma-D

В 1927 году появилась Enigma-D в нескольких коммерческих версиях с тремя роторами и одним рефлектором, который мог быть установлен в одно из 26 положений. За этой машиной последовала 4-хроторная Enigma-D, на базе которой была разработана серия специальных 4-хроторных машин Enigma-K. К этому семейству принадлежали и другие машины, такие, как Tirpitz (T), Enigma-KD и Swiss-K. С 1935 года в модель Enigma-D стала устанавливаться коммутационная панель. Эта модель имела коммерческий успех и её версии с различными перепайками в роторах продавали в Европе военным и дипломатам, в частности в Испании и Италии, а впоследствии с 1940 года «Railway Enigma» — клон Enigma-D широко использовался на железнодорожном транспорте в оккупированных районах Восточной Европы. Итальянский флот купил коммерческую версию «Энигмы» так же, как и Испания во время гражданской войны. Армия Швейцарии

использовала серию «специальных» машин Enigma-K. Япония использовала Enigma-T или Tirpitz Enigma — адаптированная Enigma D с видоизмененными соединениями внутри роторов. Также Япония разработала собственную версию «T» с горизонтальным расположением роторов. Все перечисленные выше модели в определенной мере также подверглись криптографическому взлому.

Четырехроторная модель Zahlwerk Enigma (Zahlwerk — clock-work) с улучшенным механизмом использовалась различными коммерческими пользователями и немецкой военной разведкой Абвер под наименованиями Enigma-G и Abwehr Enigma. 4-хроторная Enigma-G, использовавшаяся исключительно германской разведкой, называлась также «Counter Machine» (Счетная Машина) поскольку встроенный справа над панелью ламп счетчик увеличивал свои показания при каждом нажатии клавишей. Вес её составлял 12 кг. 5-тироторные версии Энигмы появились в 1938 году, а накануне Второй мировой войны также модификации с числом роторов от 6-ти до 8-ми (рис. 5.).

В 1942 году германский флот получил модифицированную 4-хроторную Энигму с новым рефлектором и добавлением второго зубцового кольца вокруг ротора, что значительно усложнило криптоанализ, постоянно проводившийся в Блетчли-Парк (Англия). Кроме того на базе Enigma-D и Zahlwerk Enigma были разработаны довольно странные варианты 4-хроторных ламповых машин, которые имели только 10 индикаторных ламп и 10 печатающих клавишей, оцифрованных от 0 до 9 и были предназначены для передачи различных цифровых сводок. Одна из версий такой машины — Enigma Z.

Рис. 5. Восьмироторная печатающая «Энигма» (1945г.)

Дешифрованием немецких радиосообщений, зашифрованных «Энигмой» пытались заниматься польские криптологи, но немецкая разведка сообщила об этом своим специалистам и те поменяли шифры. Когда выяснилось, что полякам не удается взломать сообщения от Enigma-I (адаптированная версия Enigma-D, в которой впервые был применен коммутатор) эту шифрмашину начал применять Вермахт, а после некоторого совершенствования именно эта машина стала основной во Второй мировой войне. С начала февраля 1942 года довольно внезапно ВМС Германии ввели в эксплуатацию новую 4-хроторную версию Enigma-M4, что

DARWIN ENIGMA CHALLENCE 1942 01.txt

GEHEIM! SONDER-MASHINENSCHLUSSEL : DARWIN ENIGMA C JANUAR 1942

Tag	UKW	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	C	I III V	21 19 06	AW BG CZ DJ FD HT KP MX QY SV	WWP OSB ZQX NWQ
30	B	II V III	10 03 13	AD FG HO IX JZ KU LN MS PV QW	HQG AXV WDY RQB
29	C	IV I V	01 12 21	AR BY CI DX EN FV GW HO JQ KT	QGL IXI VIT SGU
28	B	II IV I	26 03 21	AD BP CY FL GI HS KN OU RZ VX	UGZ DMD OTV PPL
27	B	II III IV	26 22 04	AD BP CE FK GY HQ JO LV NW SZ	SYI CGY NBY RHC
26	B	III V I	16 08 17	AH BG CZ DX FS IQ MU NQ PR TY	KYJ BMH TYW CNG
25	B	III IV II	24 06 19	AB CV DH EN FZ GI JL MT OU QW	UBO DTM OPH KGK
24	C	II IV I	09 06 21	AP BS GW HZ JV LR MN OY QU TX	JKO TAO ZDE OCR
23	C	II III IV	22 10 23	AU BF CM GO HS IN JZ KX LQ PY	MBI DTC AFR FGZ
22	B	V III II	17 20 17	AL BP CH DG FQ IZ JX KR SY TU	ESL ZGV FMK PLK
21	B	V I II	19 03 15	AD EG FW HR IZ KO NU QX SV TY	KRH AKV PIC KFJ
20	B	I V III	08 07 20	AZ BN CI DH EU FG JS MR OX TY	BSW KNT NIN HUJ
19	B	II IV V	15 10 16	AY BM DN FS GZ HW JX KQ LU PV	ZNG RXA JKC ZVI
18	C	II IV I	11 10 11	CV DJ EI FN GL HP KQ MZ RS TW	WXK IYY OKL PJV
17	C	V III I	26 21 17	AV BF CD EZ GH IM KO LU PQ SX	HSC ESL DTI WGL
16	B	II V IV	26 15 19	BC DT EU FV GK HM IR JL PX SZ	REO PES YRG XMA
15	C	IV V II	02 08 06	AZ BF CU ER GJ HI LP MS NT XY	PPC VWB TPL YPY
14	C	IV III II	18 10 06	BS CW DQ GH IL JP KR MX OZ TV	UDY AOH DXC SAT
13	B	I II III	02 17 14	AV CN DW EF IT JR KS LU MX QZ	HRW KTU JPL BUC
12	B	V II I	20 07 11	AU BT DY EL FK GS IZ MV NQ PX	KUU VSD VQP TRG
11	C	V II III	23 22 01	AT BV CG EF HU IX LM NZ QW RS	EFI QKE RAI NRK
10	B	IV V II	20 02 01	AG BJ CH DW EI FX KL NT OV QZ	KZH XJJ QWW YCA
09	C	IV III II	21 15 01	AV DM EG FS HN IQ JW KP LX RZ	SID BDF CRA NLV
08	C	IV V III	22 16 09	BF CP EG IL KY MU NW OQ RX ST	LPW ~~VKI HBB KDS~~
07	C	V IV II	10 13 09	AL CF DH ES GI IP KZ MR NW UY	WKZ LKO IYH AXO
06	C	I III IV	07 01 13	AO DI EQ FY GS HT JP LX RV WZ	OES RZT RBE IVB
05	B	IV II V	01 19 25	BD CZ EK FY HO IP LN MV QT RW	KKD GOS DMJ ZNC
04	C	II V IV	03 06 25	AL CV EQ FR GT HO IZ KN MW PS	YME BTD JQB LDF
03	C	II III I	23 22 01	AI BZ DJ FX HL MN OU PY RW ST	YXO ICF SYL DSF
02	C	III IV I	10 18 03	BF CH DJ ES IK MQ NR OZ TX UW	COQ VKN HPX VFG
01	C	I II IV	24 04 22	AB CR DH FX GN LT MV PQ SU WZ	FKD SLA OSW VVZ

Рис. 6. Таблица криптографических установок для шифрмашины. «Darwin Enigma-C» на январь 1942 года

причинило большие хлопоты криптоаналитикам союзников. Модель Enigma-M4 использовалась исключительно на подводных лодках в то время как надводные корабли и береговая инфраструктура Кригсмарине применяли модель Enigma-M3.

Шифрмашины семейства Энигма производились не только до и во время войны, но и позднее в довольно больших количествах. Так, если модель Schlusselkasten 43 в городе Хемнице в октябре 1945 года была произведена в количестве 1000 штук, то в январе 1946 года — уже 10 000. Впоследствии в послевоенные годы дешифровальные службы ряда стран добились успеха в дешифровании гражданских и военных версий, основанных на Enigma-D.

Криптографические установочные данные для шифрмашин Энигма подготавливались в форме текстовых секретных («geheim») ежемесячных страниц из кодовой книги. Такая таблица, действовавшая в январе 1942 года, представлена на рис. 6.[7].

Расшифрование содержания таблицы и перевод специфических криптографических терминов приданы ниже.

Tag	число месяца;
UKW	код рефлектора;
Walzenlage	выбор и взаимное положение роторов;
Ringstellung	начальные установки кольца на роторах;
Steckerverbindungen	соединения на коммутационной панели;
Kenngruppen	пароль

Данные для оператора из кодовой книги на 08.01.1942.

Тип шифрмашины:	Wehrmacht Darwin Enigma-C
Рефлектор:	B
Роторы:	IV, V, III
Начальные установки:	22, 16, 09
Коммутации на панели:	BF CP EG IL KY MU NW OQ RX ST
Пароль сообщения:	LPW

Пароль или идентификатор ассоциировался с определённым ключом для запутывания потенциального дешифровальщика. В одной радиосети разными корреспондентами могли использоваться разные ключи. Принимающий оператор, получив сообщение с неизвестным ему идентификатором, не производил расшифрования понимая, что информация предназначается другому корреспонденту сети.

Ключами шифратора являлись следующие элементы:

Долговременный ключ; количество возможных коммутаций для одного ротора равно числу возможных перестановок символов — $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ вариантов.

Суточный ключ: выбор взаимного расположения трех роторов из стандартной комплектации шифратора в 5 роторов; количество различных вариантов выбора этих трех роторов равно 10. Число возможных перестановок выбранных трех роторов равно 6; всего $10 \times 6 = 60$ вариантов.

Сеансовый ключ: начальное положение роторов; для каждого ротора 26 вариантов и для трех роторов $26^3 = 17\,576$.

Коммутация штепсельной панели: согласно кодовой книге.

MPXBB	AHKDM	AZHCT	QVAFP	TGCKZ
KTGHU	CWNDF	QIXDK	QJFYM	SAWGA
VADCM	NRMKE	KYDHL	ZDNVE	QNWFS
WGYVD	YJRIE	QCJAF	LVGXB	HQFRS
IMCMC	SEZGI	QCFOS	QVQJW	XMJTX
PSCXZ	QCBNV	PSFDN	JUIKU	OZRZQ
LXSAO	VKVJF	UYEGW	NSTFN	DHDPW
IXFVM	ZMREN	WAEZF	BODHI	HATTX
ZLDDB	QBWXC	HJRIX		

Рис. 7. Шифртекст радиоперехвата 08 января 1942 года.

Семейство моделей знаменитой немецкой криптографической машины под кодовым наименованием «Энигма», предназначавшихся для шифрования текстовых сообщений, отличилось завидным долголетием практического применения от эксплуатации первых образцов в середине 1920-х годов до краха гитлеровского рейха в 1945 году. История создания «Энигмы» и беспрецендентной тайной войны за добычу её образцов и разработки подходов к дешифрованию отражена в сотнях публикаций, а также в ряде документальных и художественных фильмов.

Другие немецкие шифрмашины довоенного и военного периода не получили и тысячной доли популярности в сравнении с «Энигмой». Ниже приблизительно в хронологическом порядке излагаются краткие сведения о некоторых немецких шифрмашинах, применявшихся до 1945 года.

В качестве исторического курьеза необходимо отметить, что американцами после войны

была проведена серьезная реклама «Энигмы», как очень устойчивого алгоритма. И множество стран приняли его на вооружение. Правительство США только «забыло» сообщить союзникам, что его разведслужбы давно научились успешно «ломать» эти шифры. Результаты, надо полагать, не замедлили сказаться на успехах внешнеполитического ведомства США[8].

Другие шифрмашины

Одна из крупнейших электротехнических немецких фирм Siemens & Halske в 1929–1932 годах разработала первый вариант «Der Geheimfernschreiber» (патент под наименованием «Anordnung zur Nachrichtenübermittlung in Geheimschrift über Telegraphenanlagen» — устройство для передачи шифрованных сообщений по телеграфу). Общим наименованием для целой серии подобных механических секретных буквопечатающих телеграфных аппаратов впоследствии стало «Geheimfernschreiber» или «Schlüsselfernschreibmaschine» (SFM). Алгоритмы формирования шифрующей гаммы реализовывались механически с помощью вращающихся кодирующих элементов, имевших одинаковое или различное число возможных положений. Так, если трех роторная (число возможных положений каждого ротора — 26) модель «Энигмы» тактического применения имела общее число возможных ключей 26×26×26=17 576, то 10 роторов наиболее секретной версии «Geheimschreiber» (русский перевод — «личный секретарь») вращались с периодами 47, 53, 59, 61, 64, 65, 67, 69, 71 и 73, генерируя шифрующую гамму с периодом $47 \times 53 \times 59 \times 61 \times 64 \times 65 \times 67 \times 69 \times 71 \times 73 = 893\,622\,318\,929\,520\,960 = 8{,}9 \times 10^{17}$. Таким образом, общее число ключей было значительно больше.

Все немецкие буквопечатающие телетайпшифраторы работали в режиме реального времени. При печати текстов оператором на передающей машине тот же текст сразу получался на принимающей машине, а операторы никогда не видели шифрованного варианта.

Стандартная скорость передачи информации по радио составляла 50 импульсов в секунду (скорость 50 бод). Возможны 2 режима работы шифратора. В реальном масштабе времени открытый текст вводится с клавиатуры и шифруется машиной, которая передает шифрованные комбинации вместо букв открытого текста в линию связи. В режиме предварительного шифрования шифртекст создается на перфоленте или ином носителе, высвечивается лампами, как в «Энигме» и т. п. для последующей передачи в канал связи. Засекречивание осуществляется суммированием по модулю двух пятиразрядных двоичных комбинаций, соответствующих буквам открытого текста и случайной гамме, зафиксированной на другой бумажной перфоленте. В канал связи передаются посылки из семи импульсов. Первый из них является стартовым, заставляя приемник принять следующие за ним шесть импульсов. Из них пять импульсов передают информацию о кодированной букве, а последний является стоповым сигналом.

Рис. 8. Модель Geheimzusatz T52.

Geheimschreiber постепенно развивался, и в ВМС и ВВС Германии нашли применение различные его модели. Первой машиной, которую начали использовать немецкие военные, была модель T52A/B (разработка 1937 года под наименованием «Geheimzusatz»)[9]. На борту военно-морских судов машины T52 могли присутствовать только в то время, когда они находились в своей гавани. Тогда они подключались к развитой телеграфной сети, которая покрывала большинство оккупированной немцами территории. Такая же ситуация была характерной для шифрмашин, используемых ВВС Германии. Со временем шифрмашины семейства T52 стали использоваться на радиорелейных линиях и КВ каналах связи.