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.

Для увеличения качества приёма сигналов один и тот же сигнал передавался по двум или более каналам (частотное распределение), а на приёме использовались две или более горизонтально разнесенных антенны. Это радиооборудование получило наименование Sagefish и основными его производителями были фирмы Telefunken и Siemens & Halske[10].

Позже были введены в эксплуатацию T52C, T52CA, T52D и T52E. Существовали также разновидности каждой модели.

Последняя разработанная модель этого семейства шифраторов таинственная T52Y (ясности с Y-машиной нет; возможно, что это была машина фирмы «Siemens & Halske» типа T-43 с одноразовой лентой, о ней ниже).

Тем не менее, все они основывались на схожих принципах. После войны, для своей секретной переписки, модернизированные захваченные машины типа T52 использовала полиция Норвегии.

В шифраторах T52a/b имеется коммутационная панель, которая позволяет менять местами выходные данные роторов (место пробивки каждого элемента кода), то есть осуществляется операция перестановки. Для этого использовались 5 роторов, а оставшиеся другие 5 роторов использовались для создания гаммы и дальнейшего суммирования. После зашифровывания каждого символа все десять роторов перемещались вперед на одну позицию (надо помнить, что периоды вращения роторов имели разную величину), и формировалась новая гамма для суммирования с открытым текстом и новая перестановка. Поскольку периоды вращения роторов были взаимно просты, битовая последовательность начинала повторяться только после зашифровывания текста длиной $47 \times 53 \times \ldots \times 71 \times 73 = \approx 8{,}93 \times 10^{17}$ символов. Это же значение соответствовало и числу возможных ключевых установок роторов.

Таким образом, основными элементами ключа являются, начальные угловые положения десяти роторов и коммутационная панель.

Разработчики «Geheimschreiber» T52 полагали, что применение шифра гаммирования и шифра перестановки при использовании ключевой последовательности большой длины приведет к тому, что в линии связи будет передаваться нечитаемая криптограмма с гарантированной стойкостью. Количество возможных коммутаций роторов и их начальных положений до изобретения компьютеров считалось чрезвычайно большим числом. Однако T52a/b и T52c оказались криптографически уязвимыми и их место заняла модель T52d.

В отличие от модели T52c, в T52d использовалась не сумма показаний нескольких колес, а значение на каждом отдельном колесе. Движение колес стало нерегулярным. Сдвигать или не сдвигать каждое конкретное колесо после зашифровывания символа, определялось по двум другим колесам, но таким образом, чтобы все одновременно никогда не простаивали. Кроме считывания показаний колес в основной (шифрующей) точке вывода, их показания также снимались в точке на 25, 24, 23, 23, 22, 22, 20, 20, 18, и 16 позиций раньше, соответственно. И эта дополнительная информация управляла перемещением колес.

Все операции суммирования и перестановки осуществлялись с использованием электромеханических реле. Смена полярностей при наложении гаммы осуществлялась пятью реле, а пять других реле отвечали за перестановку. Реле управлялись кодирующими колесами, которые, через набор штифтов и пазов, могли соединять реле случайным образом.

Окончательная версия машины, T52e, включила в себя все улучшения, которые прежде появлялись отдельно в других моделях шифратора, однако, в ней остались и прежние недостатки. Например, невозможность изменять положения штифтов[11].

Машине T52 предшествовала экспериментальная модель «Schluesselgeraet 39» (SG-39), изготовленная в трех экземплярах фирмой Telefonbau & Normalzeit. Эту 3-хроторную полностью автоматическую шифрмашину с электромоторным приводом изобрел Фриц Мензер из контрразведки Абвера в 1939 году. Функционально она была подобна модели Enigma-M4. Предполагалось, что она заменит «Энигму» т. к. период шифргаммы новой машины более чем в 15 000 раз ($2{,}7 \times 10^8$ символов) превышал количество возможных ключей «Энигмы». По словам оператора, работавшего на одной из них, военные не сочли её приемлемой из-за несоответствия специальным эксплуатационным требованиям.

К шифрмашинам SFM (Schlusselfernschreibmaschine) фирмы Siemens & Halske, работавшим в режиме использования одноразовой случайной шифрующей ключевой перфоленты следует отнести модели T37-ICA и T43. Шифрмашина T-37 ICA была разработана «Siemens & Halske» во второй половине 1930-х годов. По существу к стандартному коммерческому телетайпу

Т-37 был добавлен внешний шифрблок с механическим приводом от Т-37, представлявший собою считыватель информации с бумажной «ключевой» перфолентой, содержавшей гамму шифрования в коде Бодо. Принцип шифрования — суммирование по модулю 2 ключа и открытого текста. На левой стороне Т-37 ICA загорались большие сигнальные лампы красного или зеленого цвета при нажатии кнопок соответственно режимам работы — «открытая» или «шифрованная» передача.

Рис. 9. Шифрмашина Т-37 ICA.

Аппарат Т-37 ICA не являлся секретным. Однако это не относилось к ключевой перфоленте, которая была секретной и находилась в специальной кассете. Существовали строгие правила её хранения и передачи двум операторам, осуществлявшим установку и извлечение кассеты из шифрмашины перед и по окончании работы. На ключевых лентах имелись специальные маркеры, позволявшие операторам на передаче и приеме осуществить строго одинаковую установку лент в считывающие устройства и обеспечить синхронную работу двух шифрмашин. Ключевые ленты использовались однократно и затем уничтожались. Машины Т-37 ICA располагались в рабочих бункерах. Эти шифраторы были очень шумными, причем, вплоть до того, что операторы боялись оглохнуть, т. к. звуки работающей аппаратуры напоминали стрельбу из пулемётов по стальным бочкам. Кроме этого, шифрмашины устанавливались на мягкие маты, в середине которых размещалось 100 грамм мощной взрывчатки, предназначенной для уничтожения машины в случае внезапного нападения или экстренной эвакуации, что дополнительно создавало весьма нервную обстановку для обслуживающего персонала. Т-37 ICA были выведены из эксплуатации в 1980-х годах.

В конце войны по рекомендации немецких операторов была создана новая шифровальная машина, конструктивно похожая на Т-37 ICA. Об этом шифраторе ничего не было известно вплоть до ноября 1944 года, когда упоминание о нем появилось в перехваченном и дешифрованном шведами сообщении к немецкому воздушному атташе в Стокгольме[12].

Это была поздняя модель фирмы «Siemens & Halske» Т-43, использовавшая одноразовую ключевую перфоленту, что в принципе обеспечивало гарантированный уровень зашифрования. После того как очередной знак гаммы был считан, для автоматического уничтожения использованных знаков на одноразовой шифрующей ключевой перфоленте сразу же пробивались пять отверстий немного большего диаметра чем у стандартного телеграфного оборудования[13].

При использовании «хорошего» генератора случайных импульсных последовательностей в производстве ключевых перфолент и соблюдении всех установленных нормативных правил эксплуатации криптографической техники шифрмашины Т-37 ICA и Т-43 могли считаться стойкими против известных методов дешифрования. «Thrasher» — кодовое имя для трафика шифратораТ-43, который использовался на нескольких выделенных линиях в Норвегии в последний период войны и считался недешифруемым по мнению английских специалистов из Блетчли-Парк[14].

К середине войны количество шифраторов «Энигма», использовавшихся немцами было весьма велико. Однако определенные сомнения в гарантированной стойкости засекречивания сообщений этим роторным шифратором появились у немецких ученых-криптографов ещё в конце 1930-х годов. В 1941 году в компании Wanderwerke, специализировавшейся на пишущих машинках, Ф. Мензер начал разработку шифрмашины Schluesselgeraet 1941/Cipher Device 1941/SG-41, получившей впоследствии жаргонное кодовое наименование «Hitlermuhle» (мельница Гитлера, т. к. сленговым словом для пишущих машинок в немецком языке было именно «muhle»).

Рис. 10. Шифратор Schlusselgerat SG-41 (Hitlermuhle).

Функционально и конструктивно SG-41 имела некоторое сходство с американской машиной M-209 и шведской BC-38, конструктором которых был знаменитый шведский криптограф Борис Хагелин[15]. Фирма Хагелина не имела патентов в Германии и поэтому его недовольство предполагаемым заимствованием осталось неудовлетворенным. И хотя отдельные удачные конструктивные решения действительно были скопированы с BC-38 в целом SG-41 была новой конструкцией с рядом преимуществ по сравнению с шифраторами Хагелина. В середине 1944 году германское Верховное командование заказало 11 000 машин SG-41 для армии и ещё 2000 машин SG-41Z для шифрования сводок метеорологической службы ВВС Германии. Но из-за нехватки цветных металлов таких, как магний и алюминий и победного шествия советских войск к границам Германии к концу войны было поставлено по разным данным от 500 до 1000 экземпляров, которые использовалась Абвером и немецкими дипломатами с 1944 года. В настоящее время криптографическое превосходство SG-41 в сравнении с машинами Хагелина не доказано, хотя сохранилось два музейных работоспособных экземпляра этого шифратора.

Первая шифрмашина из семейства SZ-40/-42/-43 была разработана в конце 1930-х годов фирмой «Standard Elektrik Lorenz», а обозначение «SZ» означало «SchlusselZusatz» (вставная шифрующая приставка), поскольку наиболее секретный механизм шифратора помещался в блоке, который мог извлекаться из машины в случае опасности. В то время как «Энигма» использовалась полевыми подразделениями на кораблях и подводных лодках, шифрмашина фирмы Lorenz предназначалась для связи высшего руководства Вермахта и Люфтваффе, которое могло использовать тяжелую машину, телетайп и обслуживаемые стационарные линии связи.

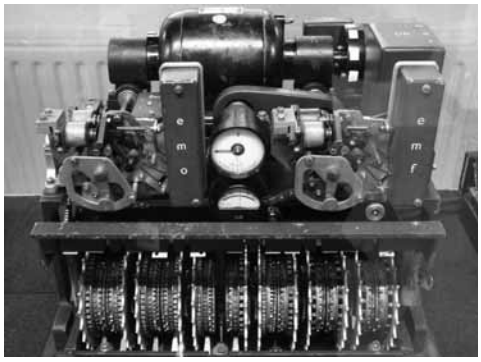

Рис. 11. Шифратор Lorenz SZ-42.

Lorenz использовался в качестве дополнения к телетайпу или коротковолновому радиопередатчику. Габариты сконструированной 12-тироторной машины составляли 51 × 46 × 46 см. Машина фирмы Lorenz вырабатывала псевдослучайный битовый поток группами по 5 битов для суммирования по модулю 2 со знаками кодов Бодо, считываемых с перфорированной ленты телетайпа. Псевдослучайная гамма генерировалась десятью роторами, пять из которых назывались «χ-роторами» и двигались регулярно, а другие пять «ψ-роторов» вращались нерегулярно. Шаговые перемещения «ψ-роторов» управлялись двумя «моторными роторами». Отдельно от перемещений пяти нерегулярных роторов (которые либо двигались вместе или стояли) по сути шифрмашина реализовала пять псевдослучайных генераторов т. о., что не существовало какой-либо связи между пятью линиями. Числа зубцов на всех роторах были взаимно простыми.

Союзники Германии

Подписанный в 1940 году пакт трех держав — Германии, Италии и Японии — гласил: Япония признает и уважает руководство Германии и Италии в деле создания нового порядка в Европе. Германия и Италия признают и уважают руководство Японии в деле создания нового порядка в великом восточно-азиатском пространстве. Помимо Италии в числе европейских государств, принявших сторону Германии, во Второй мировой войне оказались: Болгария, Венгрия, Румыния, Словакия, Финляндия и Хорватия. В боях на Восточном фронте на стороне нацистов участвовали воинские подразделения из Испании и ряда оккупированных Германии стран.

Рассмотрим криптографическую деятельность японцев. История появления японских шифрмашин весьма поучительна. После того как в конце 1920-х годах американский госсекретарь Стимсон (сказав знаменитую фразу о том, что джентельмены чужих писем не читают) ликви-