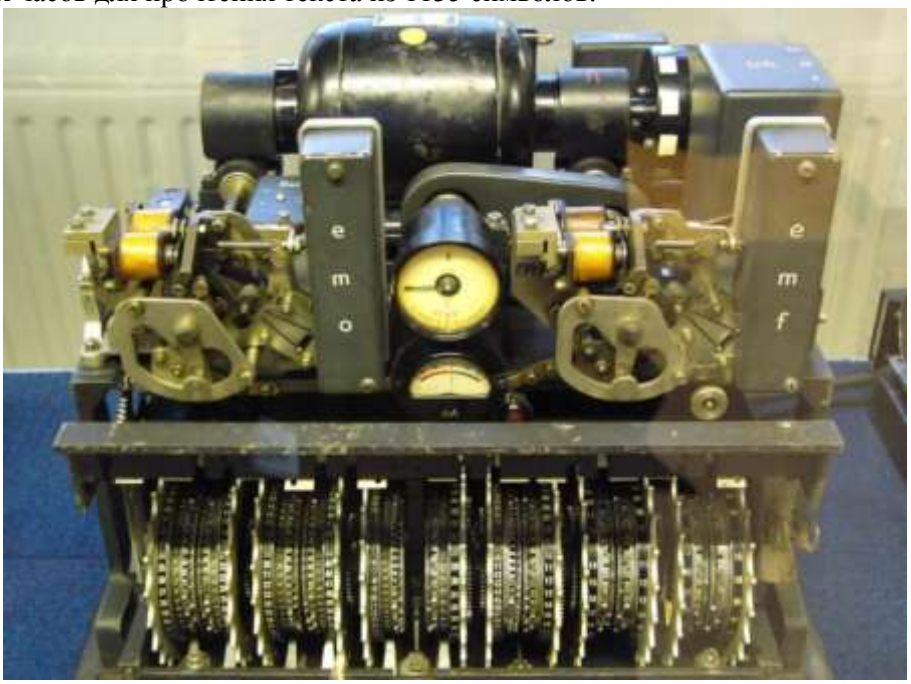
Шифровальные устройства

Германия



Шифровальная машина Kryha

Портативная механическая шифровальная машина «Kryha» была разработана в начале 1920-х годов для шифрования и дешифрования документов дипломатических работников. Известны, как карманные модели машины, так и большие электрические. Механическая машина весила около 5 кг. Машина имела низкую криптографическую стойкость. Группе американских криптоаналитиков понадобилось чуть более двух часов для прочтения текста из 1135 символов.



Шифровальная машина Lorenz SZ-42

Машина «SZ» выпускалась фирмами «Lorenz» и «Siemens» с 1940 г. и являлась дополнением к стандартному телетайпу Лоренца. Она использовалась в стационарных условиях и обслуживалась высококвалифицированным персоналом. В 1942 г. машина была модернизирована и получила обозначения «SZ-42A» и «SZ-42B». Машина использовала 5-битовый код с использованием аддитивного метода для шифрования. Ротор машины состоял из 12 дисков, на каждом из которых располагалось различное число контактов. Шифровальная машина генерировала псевдослучайный поточный шифр, который объединялся с помощью функции XOR с исходными символами, что формировало выходные символы. Габариты – 480x390x430 мм. В 1942 г. англичане, а в 1943 г. и шведы взломали код.



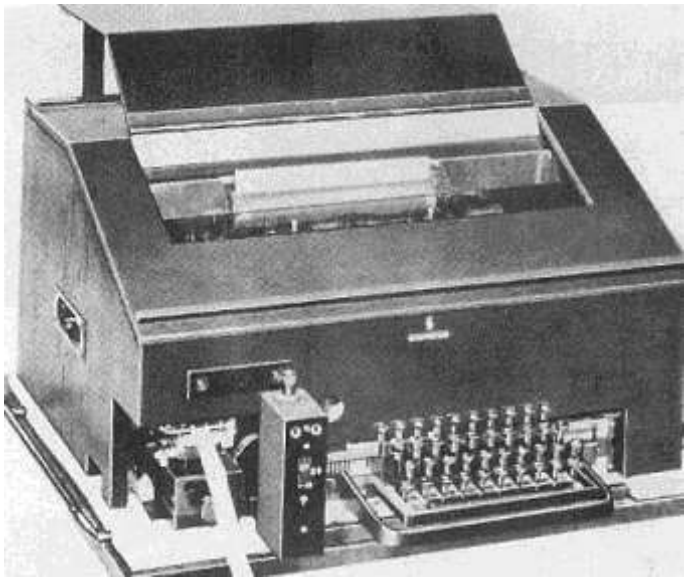
Шифровальная машина-телетайп T-37 ICA Fjernskriver

Машина выпускалась фирмой «Siemens-Halske» в двух вариантах: «T-37» и «T-37 ICA». Машина могла работать в двух режимах, в обычном и с шифратором. Для работы в закрытом режиме машина требовала ручной синхронизации с получателем сигнала.



Шифровальная машина-телетайп Geheimfernschreiber (T-52)

В 1940 г. фирмой «Siemens & Halske» для частей военной авиации и флота была создана стационарная электромеханическая шифровальная машина аналогичная «Lorenz SZ-40». Это устройство обеспечивало автоматическое шифрование текста, набираемого на клавиатуре, с одновременной передачей его в линию телеграфной связи. Машина была также снабжена буквопечатающим аппаратом. Существовало несколько версий машин: «T-52a», «T-52b», «T-52c», «T-52d» и «T-52e». Всего было изготовлено 1200 машин. Машина весила около 100 кг. Специалистам Швеции удалось взломать код машины и в течении 1940-1942 гг. более 0,5 млн. сообщений были расшифрованы. Однако после очередной модернизации машины в 1943 г. код был утрачен. Расшифрованные телеграммы попали в руки советской разведки, в результате чего криптоаналитики самостоятельно взломали код «T-52».



Шифровальная машина-телетайп Т-43

Т-43» была создана компанией «Siemens & Halske» в 1944 г. на базе «Т-52» и «Lorenz SZ-42». Машина совмещала функции шифратора с телетайпом. В качестве ключа служила перфорированная бумажная лента, которую можно было использовать только один раз, что исключало ошибки персонала. Она использовалась на флоте, верховным командованием Вермахта и в Министерстве иностранных дел. Всего было выпущено около 50 машин. Подтверждения взлома кода даже на сегодняшний день нет.



Шифровальная машина Schlüsselgerät 41 (SG-41) в транспортном положении



Шифровальная машина Schlüsselgerät 41 (SG-41) в рабочем положении

Механическая компактная шифровальная машина была разработана в 1941 г. на основе американской «М-209». В отличие от американской машины, немецкая, имела одно печатное устройство, оснащенное

двумя бумажными лентами – для зашифрованного и дешифрованного текста. В связи с отсутствием легких металлов, машина получилась достаточно тяжелой для мобильного использования. Всего было выпущено около 5 тысяч машин для замены «Enigma», из них около тысячи использовалось в Абвер.



Шифратор SG-41Z

Устройство являлось модификацией шифровальной машины «SG-41». Клавиатура его имела только 10 цифровых клавиш. Оно предназначалось для сообщений о погоде в Люфтваффе. Всего было выпущено 2 тысячи машин.





Мобильный пост связи с использованием «Enigma»



Использование «Enigma» в полевых условиях

«Enigma» (загадка) — это собирательный образ названия однотипных портативных электромеханических роторных шифровальных машин, идеология которых применялась Германией в годы войны, а также копировалась многими странами уже после войны. «Enigma» производилась корпорацией «Chiffriermaschinen AG» с 1923 г. для коммерческого рынка. Под впечатлением от ее безопасности, основанном на статистическом анализе, немецкое правительство приобрело, все права на машину и адаптировало ее к потребностям вооруженных сил. С 1929 г. она стала стандартной шифровальной машиной армии, воздушного и морских флотов, немецких дипломатов и тайной полиции. Машина использовалась в стационарных и полевых условиях, на сухопутном и морском транспорте и даже на подводных лодках.

По приблизительным оценкам, было выпущено около 100 тысяч машин различных моделей. Машина состояла из комбинации механических и электрических систем. Постоянное изменение электрической цепи, через которую шёл ток, вследствие вращения роторов позволяло реализовать многоалфавитный шифр подстановки, что давало высокую, для того времени, устойчивость шифра. Сообщение, подлежащее шифровке, набиралось на клавиатуре машины, а затем зашифрованный текст передавался традиционным путем (радио, телефон, телеграф). Расшифровка полученного сообщения производилась обратным путем – оператор набирал зашифрованные символы на клавиатуре, а декодируемый символ отображался на клавиатуре путем зажигания лампочки, расположенной под буквенным символом. Зажигание лампочек записывал второй оператор. Военные модели машины выпускались с различным количеством роторов. Первая модель содержала только три ротора, с конца 1938 года их стало пять. В военно-морских моделях находилось большее количество роторов, чем в других: шесть, семь или восемь. Так, 4-роторная военно-морская модель «M-4» имела один дополнительный ротор, хотя была такого же размера, что и 3-роторная. Настройки машины (ключи) регламентировались в специальных шифровальных книгах. Большинство ключей хранилось лишь определённый период времени, обычно сутки. Для каждого нового сообщения задавались новые ключи. Армейская версия машины использовала только 26 букв. Шифровальщики в армии и люфтваффе отправляли сообщения группами по пять символов. Военно-морские шифровальщики, использующие, 4-рёхроторные машины, отправляли сообщения группами по четыре символа.



Шифровальная машина Enigma I



Клавиатура и панель сигнальных ламп машины Enigma



Коммутационная панель машины Enigma



Вал с тремя роторами машины Enigma

Собственная разработка Вермахта шифровальной машины на базе «Enigma» была внедрена в 1928 г. под обозначением «Enigma G», модифицированная в 1930 г. в модель «Enigma I». Основное различие между коммерческой и военной машиной заключалось в наличии у последней коммутационной панели клавиатуры для замены пар букв, что существенно увеличивало уровень защиты шифрограмм. Эта модель использовалась армейскими частями, военными службами и другими государственными организациями. Размеры машины составляли 280×340×150 мм. Весила она около 12 кг.



Шифровальная машина Enigma M-4

В 1934 г. ВМФ взял на вооружение военно-морскую модификацию армейской «Enigma», которая была названа «Funkschlüssel M» или «M3». Люфтваффе стали использовать машину в 1935 г., а с 1942 г. 4-роторная «Enigma» под обозначением «M4» устанавливалась и на подводные лодки. Коммерческий вариант «Enigma» использовали и другие страны – Италия, Испания, Швейцария. Однако код таких машин был взломан польскими, французскими, британскими и американскими дешифровальщиками.



Шифровальная машина Enigma M-4 с печатным устройством «Schreibmax»

Устройство «Schreibmax» позволяло ограничить доступ оператора машины к незашифрованному тексту, поскольку оно могло устанавливаться в удалении от шифратора. При его установке с машины снимались индикаторы (лампочки) дешифратора. Например, на подводных лодках «Schreibmax» размещался в каюте капитана. При этом оператор на своем посту вводил в машину зашифрованный текст, а его дешифрованный вариант распечатывался в каюте капитана.



«Enigma» с удаленным пультом дешифратора



Удаленный пульт дешифратора

Для усиления режима секретности с машины демонтировались индикаторы (лампочки) дешифратора, а сама машина комплектовалась удаленным пультом дешифрования – клавиатурой с лампочками. Пульт мог устанавливаться как в удалении от оператора, так и рядом, создавая удобства для работы второго оператора.





Шифровальная машина Enigma T

Специально для осуществления связи между немецким и японским военными флотами на базе «Enigma K» в 1942 г. была разработана модификация шифратора под обозначением «ENIGMA TIRPITZ» (Enigma T). Она была оснащена одним отражателем и 8 роторами, что обеспечивало большую криптологическую устойчивость в сравнении с прототипом. Не менее 244 машин было изготовлено и частично отправлено в Японию. Часть машин при транспортировке была потеряна, а некоторые составляющие — захвачены войсками США.



Фрагмент восстановленной американской версии криптоаналитической машины «Bombe»

Для дешифрования информации «Enigma» Великобританией был создан специальный криптографический центр «Station X». К концу войны численность его сотрудников составляла более 12 тысяч. В 1940 г. компанией «British Tabulating Machines» была построена криптоаналитическая машина «Bombe», для расшифровки сообщений «Enigma». Впоследствии за время войны было выпущено 210 таких устройств, работавших в Англии и США. Начиная с 1939 г. Великобритания с несколькими перерывами, после очередной модернизации «Enigma», могла дешифровать большинство информации, проходившей в сетях «Enigma». С лета 1941 г. британское правительство предоставляло СССР некоторую информацию, снятую с «Enigma» без указания источника ее получения.