ЛАБОРАТОРНАЯ РАБОТА № 3

ИЗУЧЕНИЕ УСТРОЙСТВА И ПРИНЦИПА РАБОТЫ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»

Цель работы: изучение принципов шифрования/расшифрования информации, используемых в шифровальной машине «Энигма». Ознакомление с общими принципами действия шифровальной машины «Энигма» на примере эмулятора. Предварительно необходимо установить программу-эмулятор Enigma3S.

Описание лабораторной работы. «Энигма» (*Enigma*)[1] — портативная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений (рис. 1.9). Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с 1920-х гг. «Энигма» использовалась в коммерческих целях, а также в военных и государственных службах во многих странах мира, но наибольшее распространение получила в Германии во время Второй мировой войны. Именно «Энигма» Вермахта (Wehrmacht Enigma), немецкая военная модель, чаще всего является предметом изучения.

Рис. 1.9. Внешний вид шифровальной машины «Энигма»

Хотя шифр «Энигмы», с точки зрения криптографии, был достаточно слаб, но на практике лишь сочетание этого фактора с другими, такими как ошибки операторов, процедурные изъяны и захваты экземпляров «Энигмы» и шифровальных книг, позволило английским криптоаналитикам вскрывать сообщения, зашифрованные шифром «Энигмы».

На рисунке 1.10 показана электрическая схема машины «Энигма» для двух последовательно нажатых клавиш — ток течет через роторы,

[1] Эмуляторы машины «Энигма». http://www.attlabs.att.co.uk/andyc/enigma.

«отражается» от рефлектора, затем снова возвращается через роторы. Буква «A» заменяется в шифротексте по-разному при последовательных нажатиях клавиши, сначала на «G», затем на «C». Сигнал идет по другому маршруту за счет поворота ротора.

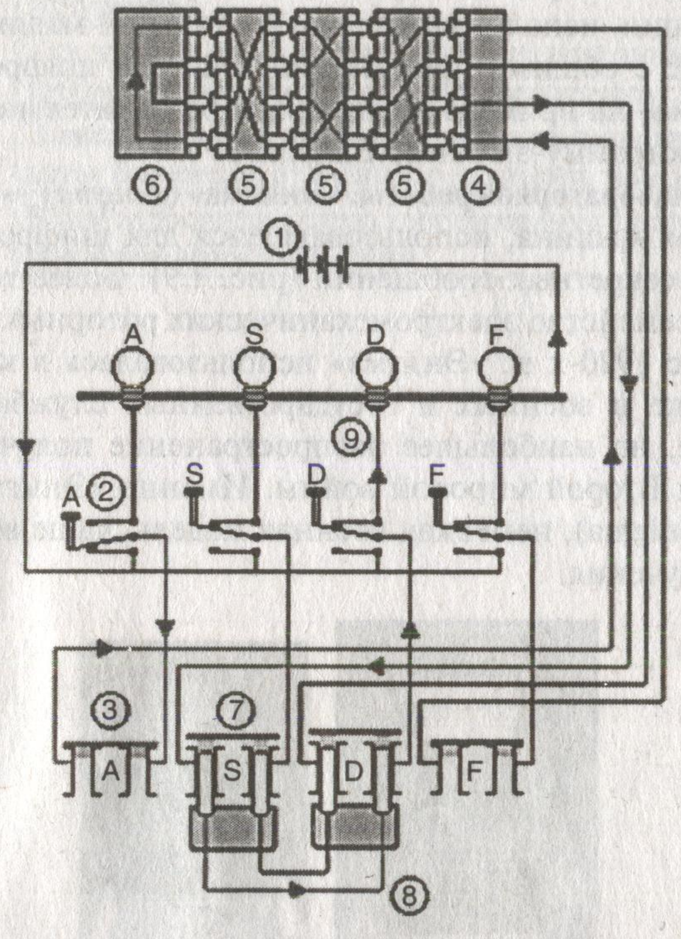


Рис. 1.10. Электрическая схема машины «Энигма» (замена в тексте буквы «A» буквой «D»)

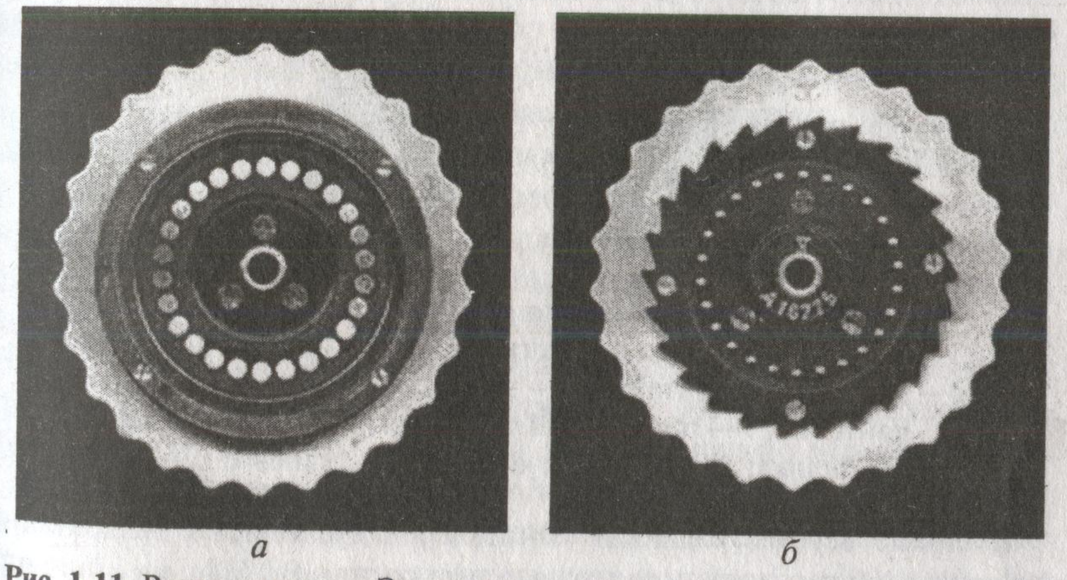
Как и другие роторные машины, «Энигма» состояла из комбинации механических и электрических систем. Механическая часть включала клавиатуру, набор вращающихся дисков (роторов), расположенных вдоль вала, и ступенчатого механизма, обеспечивающего движение одной или более роторов при каждом нажатии клавиши. Движение роторов приводит к различным вариантам подстановки символов при каждом следующем нажатии клавиши на клавиатуре.

Механические части двигались, образуя меняющийся электрический контур, т.е. фактически шифрование осуществлялось электрически. При нажатии клавиш контур замыкался, ток проходил через

различные компоненты и в итоге включал одну из множества лампочек, отображавшую выводимую букву. Например, при шифровании сообщения, начинающегося ANX..., оператор вначале нажимал кнопку «A», и загоралась лампочка «Z», т.е. «Z» становилась первой буквой криптограммы. Оператор продолжал шифрование, нажимая на клавиатуре «N» и т.д., до конца исходного сообщения.

Постоянное изменение электрической цепи, через которую протекал ток, вследствие вращения роторов позволяло реализовать многоалфавитный шифр подстановки, что давало высокую стойкость шифрования для того времени.

Роторы. Роторы — это сердце машины «Энигмы» (рис. 1.11). Каждый ротор представляет собой диск примерно 10 см в диаметре, сделанный из твердой резины или бакелита, с пружинными штыревыми контактами на одной стороне ротора, расположенными по окружности; на другой стороне ротора находится соответствующее количество плоских электрических контактов. Штыревые и плоские контакты соответсвуют буквам в алфавите; обычно это 26 букв «A» — «Z». При соприкосновении контакты соседних роторов замыкают электрическую цепь. Внутри ротора каждый штыревой контакт соединен с некоторым плоским. Порядок соединения может быть различным.



а *б*

Рис. 1.11. Ротор машины «Энигмы»: *а* — левая сторона(видны плоские электрические контакты); *б* — правая сторона (видны штыревые контакты)

Сам по себе ротор воспроизводит шифрование простой заменой символов. Например, контакт, отвечающий за букву «E», может быть соединен с контактом буквы «T» на другой стороне ротора. При использовании нескольких роторов в связке (обычно трех или четырех)

за счет их постоянного движения получается более стойкий тип многоалфавитного шифрования.

Ротор может занимать одну из 26 позиций в машине. Он может быть повернут вручную при помощи рифленого пальцевого колесика, которое выдается наружу, как показано на рис. 1.12. Чтобы оператор всегда мог определить положение ротора, на каждом ободе находится алфавитное кольцо; одна из букв видна через окошко. В ранних моделях «Энигмы» алфавитное кольцо было фиксировано, в более поздних версиях ввели усложненную конструкцию с возможностью его регулировки. Каждый ротор содержит выемку (или несколько выемок), используемых для управления движением роторов. Три последовательно соединенных ротора изображены на рис 1.13.

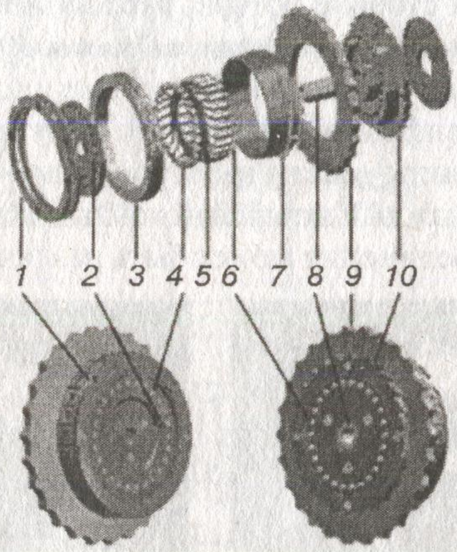


Рис. 1.12. Ротор в разобранном виде: *1* — кольцо с выемками; *2* — маркирующая точка для контакта «А»; *3* —алфавитное кольцо; *4* — залуженные контакты; *5* — электропроводка; *6* — штыревые контакты; *7* — пружинный рычаг для настройки кольца; *8* —втулка; *9* —пальцевое кольцо; *10* —храповое колесо

Военные версии машины «Энигма» выпускались с несколькими роторами; первая модель содержала только три. В 1938 г. их стало пять, но только три из них одновременно использовались в машине. Эти типы роторов были маркированы римскими цифрами I, II, III, IV, V, и все они были с одной выемкой, расположенной в разных местах алфавитного кольца. В военно-морских версиях Wehrmacht Enigma содержалось большее количество роторов, чем в других: шесть, семь или восемь.

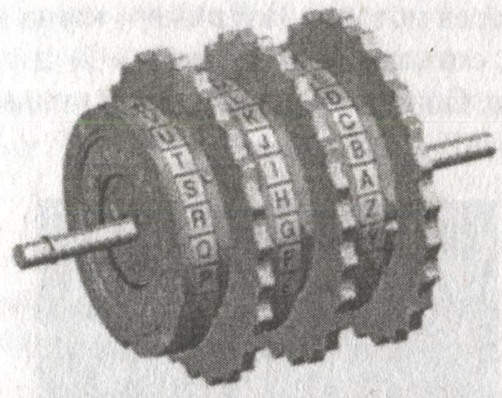


Рис. 1.13. Три последовательно соединенных ротора

Входное колесо. Входное колесо (нем. Eintrittswalze) машины «Энигма», или входной статор, соединяет коммутационную панель или (в случае ее отсутствия) клавиатуру и ламповую панель с роторами. Коммерческая версия «Энигмы» соединяла буквы в порядке их следования на клавиатуре: QA, WB, EC и т.д. Однако в военной модели они соединялись в прямом алфавитном порядке: AA, BB, CC и т.д.

Рефлектор. За исключением ранних за последним ротором устанавливался рефлектор (нем. Umkehrwalze) — запатентованная деталь, отличавшая семейство машин «Энигма» от других роторных машин, разработанных в то время. Рефлектор соединяет контакты последнего ротора попарно, коммутируя ток через роторы в обратном направлении, но по другому маршруту. Рефлектор гарантирует, что преобразование, реализуемое машиной, инволюция, т.е. процесс расшифрования, симметричен процессу шифрования. Кроме того, рефлектор гарантирует, что никакая буква не может быть зашифрована собой же. Это оказалось серьезным концептуальным недостатком, впоследствии использованным дешифровальщиками.

Коммутационная панель. Коммутационная панель, позволяющая оператору варьировать соединения проводов, впервые появилась в немецких военных моделях в 1930 г. и вскоре успешно использовалась и в машинах для военно-морских войск (рис. 1.14). Коммутационная панель внесла огромный вклад в усложнение шифра «Энигмы», даже больший, чем введение дополнительного ротора. С «Энигмой» без коммутационной панели дешифровальщик может справиться практически вручную, однако при использовании коммутационной панели взломщики были вынуждены конструировать специальные дешифровальные машины. Кабель, помещенный на коммутационную панель, соединяет буквы попарно, например «E» и «Q» могут быть соединены в пару. Эффект состоит в перестановке этих букв до и после про-

хождения сигнала через роторы. Например, когда оператор нажимал клавишу буквы «E», сигнал направлялся в «Q» и только после этого уже во входной ротор. Одновременно могло использоваться несколько таких пар (до 13).

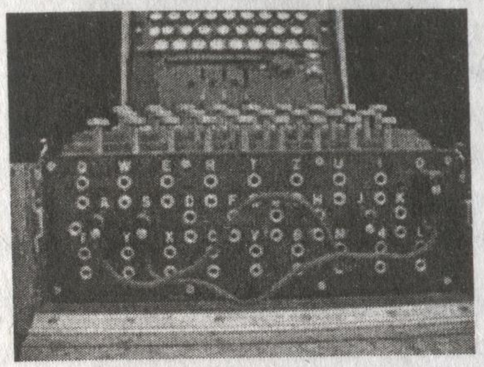


Рис. 1.14. Коммутационная панель «Энигмы»

Аксессуары. Удобной деталью, установленной на модели M4 «Энигма», был «*Schreibmax*» — маленькое печатающие устройство, которое могло печатать все 26 букв на небольшом листе бумаги.

Процедуры использования «Энигмы». Во время Второй мировой войны немецкие операторы использовали шифровальную книгу только для установки роторов и настроек колец. Для каждого сообщения они выбирали случайную стартовую позицию, например WZA, и случайный ключ сообщения, например SXT. Затем оператор устанавливал роторы в стартовую позицию WZA и шифровал ключ сообщения SXT. Предположим, что в результате шифрования ключа получится UHL. Далее оператор ставил ключ сообщения SXT как начальную позицию роторов и шифровал сообщение. После чего отправлял стартовую позицию WZA и зашифрованный ключ UHL вместе с сообщением. Получатель устанавливал стартовую позицию в соответствии с первой трехграммой WZA и, расшифровывая вторую триграмму UHL, распознавал исходный ключ SXT. Далее получатель использовал этот ключ как стартовую позицию для расшифровки сообщения. Обычно срок действия ключей составлял один день.

Военная модель «Энигма» использовала только 26 букв. Прочие символы заменялись редкими комбинациями букв. Пробел пропускался либо заменялся «X». Символ «X» также использовался для обозначения точки либо конца сообщения. Некоторые особые символы использовались в отдельных вооруженных частях, например, Wehrmacht заменял запятую двумя символами ZZ и вопросительный знак — FRAGE либо FRAQ, а Kriegsmarine заменяла запятую — «Y»

и вопросительный знак — UD. Два, три или четыре нуля заменялись CENTA, MILLE и MYRIA соответственно.

При выполнении лабораторной работы для исследования шифра «Энигмы» используется программа-эмулятор Enigma3S.

Задание

1. Запустить эмулятор Энигмы Enigma3S из папки, указанной преподавателем. Ознакомиться с файлом справки: опция меню HELP/HELP.

2. В меню программы выбрать пункт SETTINGS/RESET (рис. 1.15).

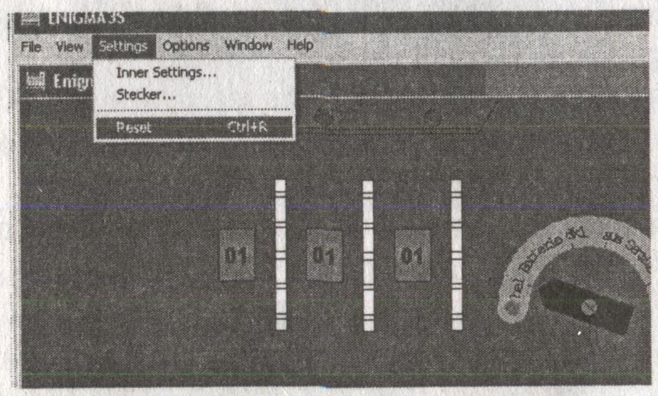


Рис. 1.15. Начальные установки эмулятора «Энигмы»

3. Установить значения для колец 01 01 01 путем выбора пункта меню VIEW/OPEN COVER. В меню SETTINGS/INNER SETTINGS установить следующие значения Reflector — B, Left — I, Middle — II, Right — III, Ringstellung — A-A-A (рис. 1.16, 1.17). Будем считать данное положение начальным.

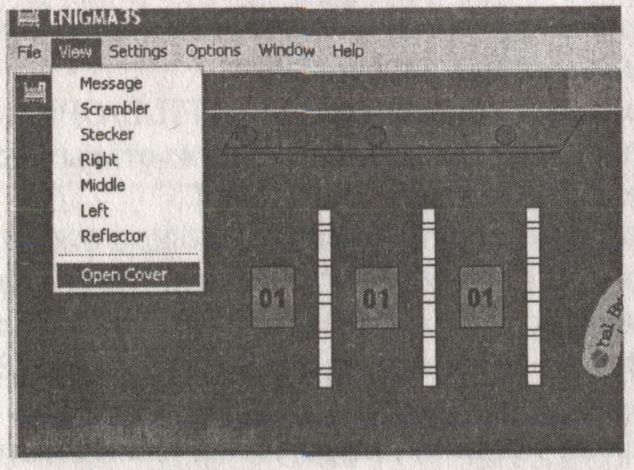


Рис. 1.16. Просмотр начальных установок

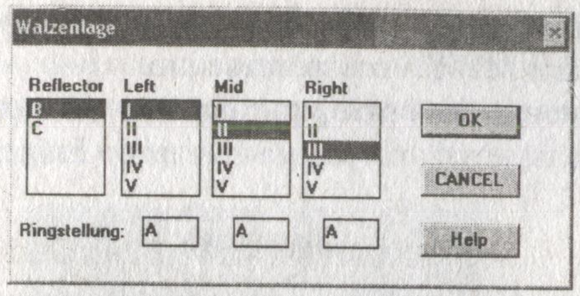


Рис. 1.17. Установки Reflector, Left, Mid, Right

4. Ввести на клавиатуре «Энигма» сообщение SECRET MESSAGE. Какое сообщение получено на выходе?

5. Повторить п. 3, изменив настройки Ringstellung — A-A-A на Ringstellung — A-B-C.

6. Ввести на клавиатуре «Энигма» сообщение SECRET MESSAGE. Какое сообщение получено на выходе? Насколько оно отличается от сообщения, полученного в п. 4?

7. Сохранить полученный в п. 6 шифротекст при помощи опции меню FILE/SAVE CT AS (рис. 1.18).

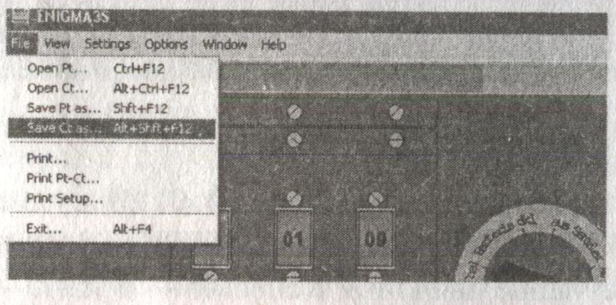


Рис. 1.18. Сохранение шифротекста

8. Создать в корне папки с программой эмулятором файл с расширением .pln, открывать его для редактирования в блокноте и записать в него открытый текст для шифрования.

9. В меню программы выбрать опцию FILE/OPEN PT и файл, созданный в пункте 9. Получить шифротекст из открытого текста, выбрав опцию меню OPTIONS/ENCIPHER TEXT.

10. Установить эмулятор в начальное положение. В меню программы выбрать пункт WINDOW/SCRAMBLER. Ввести при помощи клавиатуры произвольное сообщение из 22 символов (варианты указаны в табл. 1.3), обращая внимание на положение колец. Ввести последовательность из 22 символов еще раз. Как изменилось положение колец? Отличается ли новая зашифрованная последовательность от начальной? Почему изменилась выходная последовательность?

11. Используя окно SCRAMBLER, проследить за тем, как изменяется шифротекст в зависимости от настройки положения контактных колес. Что дает возможность настройки порядка следования контактных колес?

12. В окне программы выбрать опцию VIEW/RIGHT (рис. 1.19).

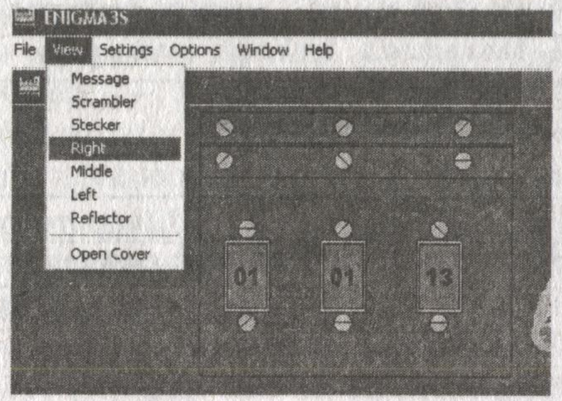


Рис. 1.19. Просмотр установок для выполнения задания

Заполнить таблицу соответствия для пяти букв (варианты указаны в табл. 1.4) для 12 первых угловых положений правого колеса.

13. Зная, что эмулятор установлен в начальное положение, расшифровать текст в соответствии с номером варианта, указанным преподавателем (варианты контрольных заданий указаны в табл. 1.5,.1.6.

Таблица 1.3

Номер варианта	Исходный алфавит
1, 5, 9, 13, 17	QRTYU FBNAK GHERL ADLKE DS
2, 6, 10, 14, 18, 22	UIERT PAEVC DSNCY OPLKD BV
3, 7, 11, 15, 19, 23, 27	UIFGH KLBVQ FDIIT QKJLS DB
4, 8, 12, 16, 20, 24, 28	LLWER TYYWV BAFDP WRTOPF JK
21, 25, 29, 26, 30	OPJHG JFDPJ GFDSK LDFHU BX

Таблица 1.4

Буквы на входе	Угловые положения колеса											
	1	2	3	4	5	6	7	8	9	10	11	12

Таблица 1.5

Номер варианта	Шифротекст
1, 5, 9, 13, 17	ABCDE
2, 6, 10, 14, 18, 22	FGHIJK
3, 7, 11, 15, 19, 23, 27	LMNOP
4, 8, 12, 16, 20, 24, 28	QRSTU
21, 25, 29, 26, 30	VWXYZ

Таблица 1.6

Номер варианта	Шифротекст
1, 5, 9, 13, 17	FQGAH WABUN NL
2, 6, 10, 14, 18, 22	QIKOL RCRJS EGBSS X
3, 7, 11, 15, 19, 23, 27	OOKWE PRFMI M
4, 8, 12, 16, 20, 24, 28	KIXDI ACTHJ L
21, 25, 29, 26, 30	XLXOO EABUN NL