Лабораторная работа № 4

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (рассчитана на 4 часа аудиторных занятий).

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.
2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства Энигма.
3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе Энигма, реализованной в виде симуляторов.
4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе Энигма.
5. Результаты выполнения лабораторной работы оформить в виде отчета проведенных исследованиях, методики выполнения практической части задания и оценки криптостойкости шифров.

4.1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

4.1.1 Краткая историческая информация

Идея создания шифровального устройства высказана голландцем Гуго Кох де Дельфтю (в некоторых источниках – Гуго Александр Кох, Hugo Alexander Koch) еще в 1919 г. В 1920 году он же изобрел первую роторную шифровальную машинку. Параллельно с этим немец Артур Шербиус (Arthur Scherbius) изучал проблему криптостойкости (в нашем современном понимании) шифровальных машин. Он же получил патент на такую машину, которая получила название «Enigma» (от греч. – загадка). Основная особенность Энигмы – все знали в то время алгоритм шифрования, но никто не мог подобрать нужный ключ.

Первая шифровальная машина, *Enigma A*, появилась на рынке в 1923 году. Это была большая и тяжелая машина со встроенной пишущей машинкой и ве-

сом около 50 кг. Вскоре после этого была представлена *Enigma B*, очень похожая на *Enigma* A. Вес и размеры этих машин сделали их непривлекательными для использования в военных целях.

По достоинству шифровальную машину оценили в немецкой армии. В 1925 году её принял на вооружение сначала военно-морской флот (модель *Funkschlussen* C), а в 1930-м – и Вермахт (*Enigma* I). Общее количество шифраторов, произведённых до и во время Второй мировой войны, превысило 100 тысяч. Применялись они всеми видами вооруженных сил Германии, а также военной разведкой и службой безопасности.

Идея коллеги А. Шербиуса, Вилли Корна (Willi Korn), позволила создать компактную и намного более легкую *Enigma* C. Особенностью этой модели было наличие ламповой панели. В 1927 году *Enigma* D была представлена и коммерциализирована в нескольких версиях с различными роторами и продана военным и дипломатическим службам многих стран Европы. В *Enigma* D было три обычных ротора и один отражатель (рефлектор), которые можно было установить в одном из 26 положений (по числу букв используемого алфавита). Именно эта модель стала основным прототипом многих известных версий машин Энигма, которые использовала Германия в годы Второй Мировой войны.

4.1.2 Конструкция и принцип функционирования Энигмы

Машина Энигма – это электромеханическое устройство. Как и другие роторные машины, Энигма состоит из комбинации механических и электрических подсистем.

Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, – которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состояла из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

На рис. 4.1 показана фотография одной из моделей Энигмы с указанием месторасположения основных модулей машины. Как видно на этом рисунке, Энигма состоит из 5 основных блоков:

- панели механических клавиш, 1 (дают сигнал поворота роторных дисков);

- трех (или более) роторных дисков, 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;

- рефлектора, 3 (имеет контакты с крайним слева ротором);

- коммутационной панели, 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);

- панели в виде электрических лампочек, 5; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифрования.

Рисунок 4.1 Одно из моделей (трехроторная) Энигмы [18]

Конкретный механизм мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигается на одну позицию, а при определённых условиях сдвигаются и другие роторы. Движение роторов приводит к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре, т.е. зашифрование/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим. Идея А. Шербиуса состояла в том, чтобы добиться этих подстановок электрическими связями.

Механические части двигались и замыкая контакты, образовывали меняющийся электрический контур. При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную (для зашифрования/расшифрования одного конкретного символа сообщения) цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифртекста (или расшифрованного сообщения). На рис. 4.2 показаны упрощенная конструкция ротора (а) и рефлектора (б). Замыкание цепи происходило за счет рефлектора.

На рис. 4.3 схематично показано, как некоторая буква (например, «a») будет зашифрована другой буквой (например, «g»), а следующая за ней буква сообщения (также «a») – уже буквой «c».

а) б)

Рисунок 4.2 Упрощенная конструкция ротора (а) и рефлектора (б) Энигмы

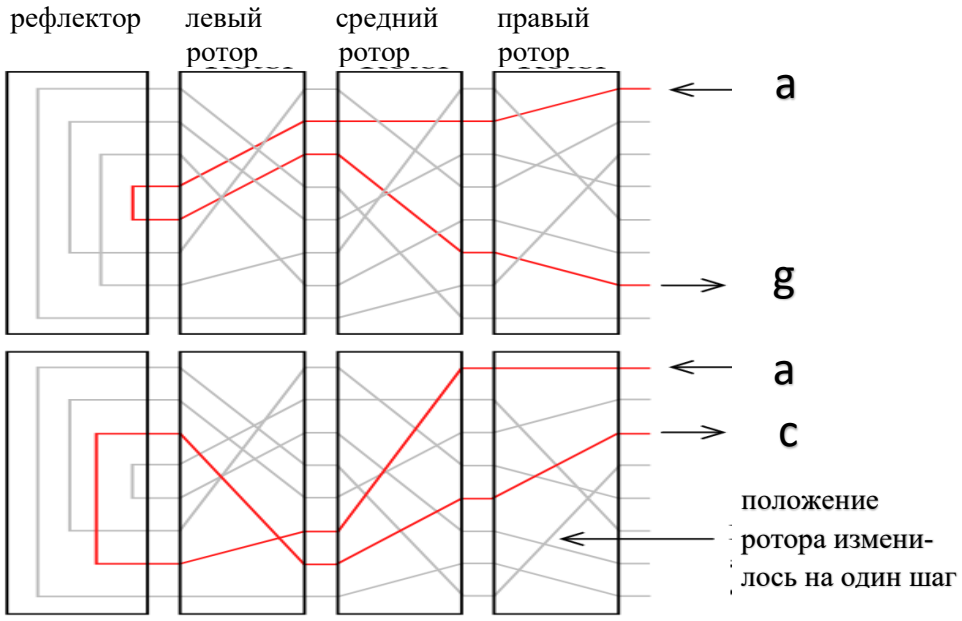

Рисунок 4.3 Пояснение к принципу шифрования путем формирования электрической цепи [19]

Отметим, что на рис. 4.3 электрическая цепь не представлена в виде замкнутой, поскольку не показаны части коммутационной панели и электрическая лампочка. Замкнутые электрические цепи хорошо иллюстрирует рис. 4.4.

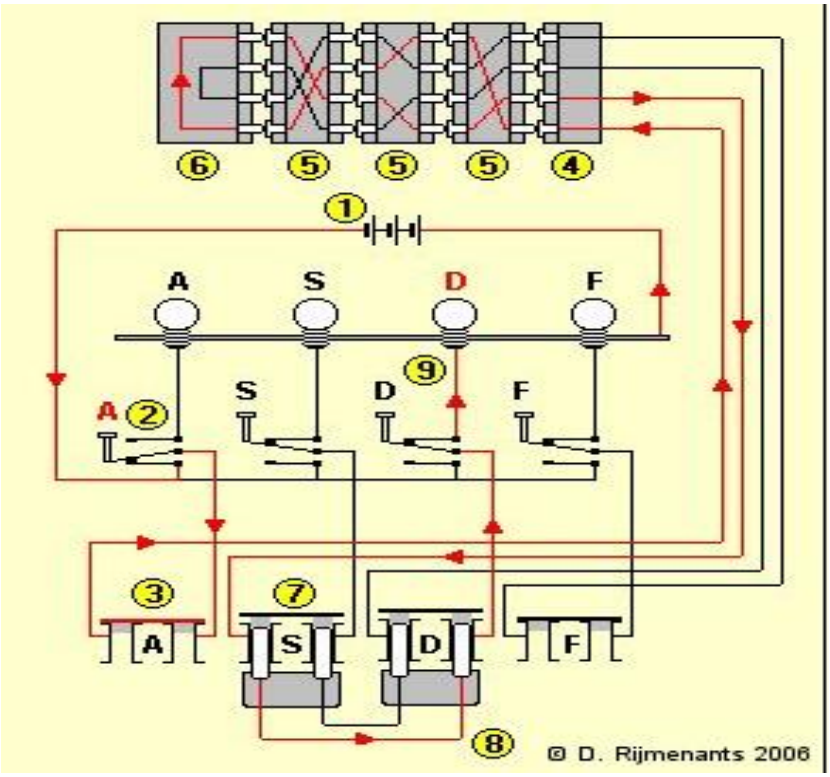

Рисунок 4.4 Пояснение к принципу формирования зашифрованного символа с помощью замкнутой электрической цепи [18]

Замкнутую цепь составляют: батарея 1 (это могут быть и иные источники питания), нажатая двунаправленная буквенная клавиша, 2, разъем коммутационной панели, 3 (как видим, в одном случае – буква «а» – коммутационного перехода на другую букву нет), входной разъем (входное колесо) 4 роторного модуля, роторный модуль 5 (состоит из трех роторов, как в версии Энигмы для Вермахта, *Wehrmacht Enigma M3*, или четырех – в версии Энигмы для военно-морского флота, *Kriegsmarine Enigma M4*), рефлектор 6. Последний возвращает ток (цепь) по другому пути через узлы те же узлы, «зажигая» на ламповой панели букву «D», к другому полюсу батареи. Обратим внимание, что обратная часть цепи уже проходит с учетом выполненной коммутации (7 и 8).

Отметим также, что клавиатура соответствовала немецкой раскладке *QWERTZ.*

4.1.3. Шифры Энигмы

Во время Второй мировой войны немецкие операторы использовали специальную (тайную) шифровальную книгу для установки роторов и настроек колец.

Операторы Энигмы (шифровальщики и дешифровальщики выполняли следующие основные операции.

Пример 1.

Зашифрование сообщения.

1. Установить начальную стартовую позицию роторов (предположим, их 3), согласно текущей кодовой таблице (коду дня). Например, *WZA*.

2. Выбрать случайный ключ сообщения, например, *SXT*. Затем оператор устанавливал роторы в стартовую позицию *WZA*.

3. Зашифровывать ключ сообщения *SXT*. Предположим, что в результате зашифрования ключа получится *UHL*.

4. Далее оператор ставил ключ сообщения (*SXT*) как начальную позицию роторов и зашифровывал собственно сообщение. После этого он отправлял стартовую позицию (*WZA*) и зашифрованный ключ (*UHL*) вместе с сообщением.

Расшифрование сообщения.

1. Установить стартовые позиции роторов в соответствии с первой трехграммой (*WZA*).

2. Расшифровывая вторую треграмму (*UHL*) и извлечь исходный ключ (*SXT*).

3. Далее получатель использовал этот ключ как стартовую позицию для расшифрования шифртекста. Обычно срок действия ключей составлял одни сутки.

Пример 2.

Зашифрование сообщения.

1. Установить стартовую позицию роторов согласно коду дня. Например, если код был "*HUA*", роторы должны быть инициализированы на "*H*", "*U*" и "*A*" соответственно.

2. Выбрать случайный код с тремя буквами, например, *ACF*.

3. Зашифровать текст "*ACFACF*" (повторный код), используя начальную установку роторов шага 1. Например, предположим, что зашифрованный код – "*OPNABT*".

4. Установить стартовые позиции роторов к *OPN* (половина зашифрованного кода).

5. Присоединить зашифрованные шесть букв, полученных на шаге 2 (*OPNABT*), в конец к начальному сообщению.

6. Зашифровать сообщение, включая код с 6 -ю буквами. Передать зашифрованное сообщение.

Расшифрование сообщения.

1. Получить сообщение и отделить первые шесть букв.
2. Установить стартовую позицию роторов согласно коду дня.
3. Расшифровать первые шесть букв сообщения, используя начальную установку шага 2.
4. Установить позиции роторов на первую половину расшифрованного кода.
5. Расшифровать сообщение (без первых шести букв).

Военная модель Энигмы использовала только 26 букв. Прочие символы заменялись редкими комбинациями букв. Пробел пропускался либо заменялся на «*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 – словом *FRAGE* либо буквосочетанием *FRAQ*, а *Kriegsmarine M4* запятой соответствовала буква «*У*».

Как мы отмечали выше, Энигма строится на основе подстановочных шифров, подобных на шифр Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра Энигмы лежит *динамический шифр Цезаря*.

Более сложная система использует случайный ряд символов для нижнего алфавита. Принцип, положенный в основу этой «случайности», имеет много общего с перестановочными шифрами. Например, ниже показан принцип подстановке, основанный на взаимной перестановке во втором (нижнем) алфавите в 13 парах символов, расположенных случайным образом:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	W	M	R	Z	L	N	T	U	A	O	F	C	G	K	S	Y	D	P	H	I	X	B	V	Q	E

Этот принцип случайности использовался и при изготовлении роторов и рефлекторов для Энигмы. Всего за время Второй мировой войны немцами было изготовлено восемь роторов и четыре рефлектора, но одновременно могло использоваться ровно столько, на сколько была рассчитана машина.

Техническую спецификацию на все произведенные роторы и рефлекторы можно найти в [12, 21]. Ниже на рис. 4.5 и 4.6 представлены эти спецификации соответственно на роторы и на рефлекторы.

Достаточно подробная информация об основных особенностях и обстоятельствах патентования, разработки и сферах использования практически всех (или большинства) версий Энигмы содержится в [22].

INPUT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rotor I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
Rotor II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Rotor III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
Rotor IV	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B
Rotor V	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
Rotor VI	J	P	G	V	O	U	M	F	Y	Q	B	E	N	H	Z	R	D	K	A	S	X	L	I	C	T	W
Rotor VII	N	Z	J	H	G	R	C	X	M	Y	S	W	B	O	U	F	A	I	V	L	P	E	K	Q	D	T
Rotor VIII	F	K	Q	H	T	L	X	O	C	B	J	S	P	D	Z	R	A	M	E	W	N	I	U	Y	G	V
Beta rotor	L	E	Y	J	V	C	N	I	X	W	P	B	Q	M	D	R	T	A	K	Z	G	F	U	H	O	S
Gamma rotor	F	S	O	K	A	N	U	E	R	H	M	B	T	I	Y	C	W	L	Q	P	Z	X	V	G	J	D

Рисунок 4.5 Спецификация на роторы Энигмы

reflector B	(AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW)
reflector C	(AF) (BV) (CP) (DJ) (EI) (GO) (HY) (KR) (LZ) (MX) (NW) (TQ) (SU)
reflector B Dünn	(AE) (BN) (CK) (DQ) (FU) (GY) (HW) (IJ) (LO) (MP) (RX) (SZ) (TV)
reflector C Dünn	(AR) (BD) (CO) (EJ) (FN) (GT) (HK) (IV) (LM) (PW) (QZ) (SX) (UY)

Рисунок 4.6 Спецификация на рефлекторы Энигмы

Рассмотрим пример использования приведенных спецификаций.

Пример 4.1. В этом примере мы процедуру только зашифрования одной буквы («G»).

Предположим, что Энигма оснащена роторами I, II, III (см. рис. 4.5). Таким образом, правым ротором (R) является III приведенной спецификации. Предположим также, что каждый ротор находится в своем положении A, когда

выполняется шифрование. Если взять информацию с этой страницы, указав фактическую разводку ротора, это означает, что правый ротор R производит подстановку в соответствии с переставленными буквами исходного алфавита, т. е. буква «G» будет заменена буквой «C»:

```
ABCDEF G HIJKLMNOPQRSTUVWXYZ
BDFHJL C PRTXVZNYEIWGAKMUSQO
```

,

центральный ротор (M) или II заменяет букву «C» на букву «D»:

```
AB C DEFGHIJKLMNOPQRSTUVWXYZ
AJ D KSIRUXBLHWTMCQGZNPYFVOE
```

,

левый ротор (L) или III – соответственно букву «D» на букву «F»:

```
ABC D EFGHIJKLMNOPQRSTUVWXYZ
EKM F LGDQVZNTOWYHXUSPAIBRCJ
```

.

Предположим далее, что используется рефлектор B (спецификация на рис. 4.6 – первая строка):

```
ABCDE F GHIJKLMNOPQRSTUVWXYZ
YRUHQ S LDPXNGOKMIEBFZCWVJAT
```

.

Обратим внимание на то, что рефлектор имеет только 13 соединений, т. е. имеется 13 пар подстановок: A - Y, B - R и т. д. В нашем примере произошла подстановка F -> S.

Ток теперь проходит обратный путь через три ротора в последовательности L-M-R.

Эффект преобразования левого ротора (обратный):

```
ABCDEFGHIJKLMNOPQR S TUVWXYZ
UWYGADFPVZBECKMTHX S LRINQOJ
```

,

соответственно – среднего ротора (обратный):

```
ABCDEFGHIJKLMNOPQR S TUVWXYZ
AJPCZWRLFBDKOTYUQG E NHXMIVS
```

и, наконец, – правого ротора (обратный):

```
ABCD E FGHIJKLMNOPQRSTUVWXYZ
TAGB P CSDQEUFVNZHYIXJWLRKOM
```

После всех (в данном случае – 7) подстановок буква «G» будет зашифрована буквой «P».

Процедура расшифрования шифртекстов предусматривала настройку отражателя, роторов и коммутационной панели машины в соответствии с таблицами (книгами) и использованными при зашифровании паролями. Достаточно подробно информацию об этом можно получить в [23], комментариев к функционалу Энигмы и ее симулятору [24]. Подробное описание кода симулятора на языке Pyton содержится в книге [25].

В начале данного параграфа

4.1.4 Оценка криптостойкости Энигмы

Для получения общего представления об особенностях работы криптоаналитиков над шифрами Энигмы полезно ознакомиться с содержанием материалов в [26].

Как мы неоднократно подчеркивали, преобразование «Энигмы» для каждой буквы может быть определено математически как результат подстановок. Рассмотрим трехроторную модель Энигмы. Положим, что символом B обозначаются операции с использованием коммутационной панели, соответственно символы Re – отражателя, а L, M и R – обозначают действия левых, средних и правых роторов соответственно. Тогда процесс зашифрования символа m с использованием некоторой ключевой информации K формально можно записать в следующем виде:

$$E_K = f\,(m, B, Re, L, M, R). \qquad (4.1)$$

Чтобы оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства Энигмы:

- выбор и порядок роторов,
- разводку (коммутацию) роторов,
- настройку колец на каждом из роторов,
- начальное положение роторов в начале сообщения,
- отражатель,
- настройки коммутационной панели.

Используются различные варианты подсчета всех возможных состояний перечисленных конструктивных модулей машины [27]. К сожалению для немцев, взломщики шифра союзников знали машину, роторы и внутреннюю разводку этих роторов. Поэтому им нужно было учитывать только возможные способы настройки Энигмы. Такая априорная информация о конструктивных особенностях устройства для шифрования (вспомним об основных постулатах О. Керкгоффса [2]) в нашем случае снижает уровень (теоретический) криптостойкости (до практического). Немецкие криптологи полагали, что один ротор может быть подключен 4×10^{26} различными способами. Сочетание трех роторов и отражателя позволяет получить астрономические цифры возможных вариантов подстановок. Для союзников, которые знали конструкции роторов, число различных вариантов существенно уменьшалось.

Рассмотрим пример для трехроторной Энигмы Вермахта с отражателем (по умолчанию – B, см. рис. 4.6) и выбором из 5 роторов. Использовались 10 штекерных кабелей на коммутационной панели (количество кабелей по умолчанию, поставляемых с машиной).

Чтобы выбрать 3 ротора из возможных 5, существует 60 комбинаций (5 x 4 x 3). Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора (26 x 26 x 26). Кольцо на каждом роторе содержит маркировку ротора (что здесь неважно) и выемку, которая влияет на шаг перемещения расположенного левее ротора. Каждое кольцо может быть установлено в любом из 26 положений. Поскольку слева от третьего (наиболее левого) ротора нет ротора, на расчет влияют только кольца самого правого и среднего ротора. Это дает 676 комбинаций колец (26 x 26).

Коммутационная панель обеспечивает самый большой набор возможных настроек. Для первого кабеля одна сторона может иметь любое из 26 положений, а другая сторона - любое из 25 оставшихся положений (одна буква коммутируются с другой). Однако, поскольку комбинация и ее обратная сторона идентичны (AB такая же, как BA), мы должны игнорировать все двойные числа во всех возможных комбинациях для одного кабеля, предоставляя $(26 \times 25) / (1! \times 2^1)$ или 325 уникальных способов коммутаций одним кабелем. Для двух кабелей: есть (26 x 25) комбинаций – для первого кабеля и, поскольку два разъема уже используются, то получается (24 x 23) комбинаций – для второго кабеля. Следуя этой простой логике, получается $(26 \times 25 \times 24 \times 23) / (2! \times 2^2) = 44\,850$ уникальных способов коммутаций с использованием двух кабелей. Для трех кабелей – $(26 \times 25 \times 24 \times 23 \times 22 \times 21) / (3! \times 2^3) = 3\,453\,450$ комбинаций и так далее. Таким образом, с использованием 10 кабелей на коммутационной панели получаются 150 738 274 937 250 различных комбинаций. Формула, где n равно количеству кабелей, равна $26! / (26 - 2n)! \cdot n! \cdot 2^n$. Численно это дает:

60 x 17 576 x 676 x 150 738 274 937 250 = 107 458 687 327 250 619 360 000 или $1{,}07 \times 10^{23}$.

Таким образом, практически рассматриваемая версия Энигмы (три ротора с выбором из 5 роторов, отражатель B и 10 штекерных кабелей для коммутационной панели) может быть настроена на $1{,}07 \times 10^{23}$ различных состояний, что сопоставимо с 77-битным криптографическим ключом.

Добавление четвертого ротора (например, для *Naval Enigma M4*) для повышения его криптостойкости было практически бесполезным: неподвижный четвертый ротор «усложнил машину» только в 26 раз и вместе с тонким отражателем мог рассматриваться как настраиваемый отражатель с 26 положениями. Внедрение общего числа роторов в 8 единиц (на *Kriegsmarine M3*), а затем – на четырехроторной версии (*M4*) было гораздо более эффективным шагом. Они увеличили комбинации роторов с 60 до 336.

Оценим далее практический размер криптографического ключа (или его эквивалент) для четырехроторной версии *Krigsmarine Enigma M4*. Эта машина использует 3 обычных ротора, выбранных из набора из 8. Это, как мы уже отметили, дает 336 комбинаций подключений роторов (8 x 7 x 6). *M4* также имела специальный четвертый ротор, называемый *Beta* или *Gamma* (без кольца), который дает 2 варианта. Они не совместимы с другими роторами и подходят только как четвертый (самый левый) ротор. Четыре ротора могут быть установлены в любом из 456 976 положений (26 x 26 x 26 x 26). Рефлектор не меняется. Четвертый ротор был неподвижным. Версия *M4* была снабжена также 10 кабелями для коммутационной панели.

В сумме это дает: 336 x 2 x 456 976 x 676 x 150 738 274 937 250 = = 31 291 969 749 695 380 357 632 000 или $3{,}1 \times 10^{25}$, *что сопоставимо с 84-битным ключом*.

Проблема криптоанализа шифров Энигмы была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, применяемых в то время). Исчерпывающий поиск всех возможных $1{,}07 \times 10^{23}$ настроек (атака *brute force*) был невозможен в 1940-х годах, а его сопоставимый 77-битный ключ огромен даже для современных электронных систем. Чтобы дать представление о размере этого числа, представим, что у нас есть $1{,}07 \times 10^{23}$ листов бумаги толщиной около 1 мм. Из этих листов можно сложить примерно 70 000 000 стопок бумаги, каждая из которых простирается от Земли до Солнца. Кроме того, $1{,}07 \times 10^{23}$ дюйма равно 288 500 световых лет.

4.2 ПРАКТИЧЕСКОЕ ЗАДАНИЕ

1. Ознакомиться с функционалом хотя бы одного (по согласованию с преподавателем) симулятора Энигмы:
1.1 Симулятор Энигмы M3 (*M3* Enigma Simulator)
https://cryptocellar.org/simula/m3/index.html
1.2 Симулятор Энигмы M4 (*M4* Enigma Simulator)
https://cryptocellar.org/simula/m4/index.html
1.3 Симулятор Энигмы Army/Air Force and the Railway
https://cryptocellar.org/simula/enigma/index.html
1.5 Симулятор Энигмы для Абвера (*Abwehr* Enigma Simulator)
https://cryptocellar.org/simula/abwehr/index.html
1.5 Симулятор Энигмы для Тирпица (*T (Tirpitz)* Enigma Simulator)
https://cryptocellar.org/simula/tirpitz/index.html

Произвести зашифрование сообщения (собственные имя, отчество, фамилия) при 8-10 различных настройках машины-симулятора. Оценить частотные свойства символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста.

2. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (*L*-*M*-*R*) и отражателя *Re* следует выбрать из таблиц на рис. 4.5 и 4.6 в соответствии со своим вариантом, представленным в таблице 4.1. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, *i*) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.

Таблица 4.1

Вариант задания	*L*	*M*	*R*	*Re*	L_i-M_i-R_i
1	I	II	III	B	0-2-2
2	II	III	V	C	1-2-2
3	III	VII	I	B Dunn	1-0-1
4	IV	III	II	C Dunn	0-0-4
5	I	Beta	Gamma	B	3-1-3
6	II	Gamma	IV	C	1-1-1
7	Beta	Gamma	V	B Dunn	0-2-2
8	V	VI	VII	C Dunn	1-2-2
9	VIII	II	IV	B	1-0-1

10	Gamma	III	Beta	C	0-0-4
11	Beta	VIII	I	B Dunn	3-1-3
12	III	Gamma	V	C Dunn	1-1-2
13	VI	IV	II	B	1-2-2
14	II	Beta	VIII	C	0-2-2
15	VII	Gamma	II	B Dunn	1-2-2

.

С помощью разработанного приложения зашифровать сообщение в соответствии с п.1 практического задания, применив не менее 5 вариантов начальных установок роторов.

Оценить криптостойкость вашего варианта машины.

3. Результаты оформить в виде отчета по установленным правилам.

ВОПРОСЫ ДЛЯ КОНТРОЛЯ И САМОКОНТРОЛЯ

1. Дать пояснение к структуре шифровальных машин Энигма.
2. На основе каких шифров строится машина Энигма?
3. Дать пояснение к принципам зашифрования сообщений.
4. Дать характеристику криптостойкости шифровальной машины Энигма.
5. Дать характеристику (с численными оценками) криптостойкости машины-симулятора на основе разработанного приложения.
6. Пояснить основные принципы расшифрования сообщений Энигмы.
7. Ваши предложения по модификации известных аналогов Энигмы?