**Лекция 4. Роторные и электронные шифраторы. Обзор известных шифровальных машин. Шифровальная машина Энигма. Расшифрование шифр «Энигмы».**

4.1. Вид шифраторов

4.2. Шифровальная машина Энигма

4.2.1. Описание

4.2.1.1. Роторы

4.2.1.2. Ступенчатое движение роторов

4.2.1.3. Входное колесо

4.2.1.4. Рефлектор

4.2.1.5. Коммутационная панель

4.2.1.6. Аксессуары

4.2.1.7. Математическое описание

 4.2.2. Процедуры для использования «Энигмы»

 4.2.2.1. Индикаторы

 4.2.2.2. Аббревиатуры и директивы

 4.2.3. Расшифрование шифр «Энигмы». Криптоанализ «Энигма»

 4.2.4. Клоны «Энигмы»

**Шифратор** — в криптографии устройство для автоматического шифрования. Электромеханические шифраторы появляются в начале 1920-х годов в США и Европе и широко используются вплоть до 1980-х годов, когда распространение получают шифры, предназначенные для использования с вычислительной техникой.

Известные шифраторы:

* [**Машина Лоренца**](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%9B%D0%BE%D1%80%D0%B5%D0%BD%D1%86%D0%B0)**;**
* [**Энигма**](https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0)**;**
* [**M-94**](https://ru.wikipedia.org/w/index.php?title=M-94&action=edit&redlink=1)**,**[**M-209**](https://ru.wikipedia.org/wiki/M-209) (шифраторы «Хагелина», В-21 (1926 год для Швицкую армию ), В-211 (1932 год для Французскую армию), С-35 и С-36 (1934 году Французский генеральный штаб Хагелина попросили создать «карманную» шифрмашину), С-38 (1939 году принят на вооружение шведской армии), С-52 и СХ-52 ( усовершенствованная модель и наиболее успешных механических шифромашин Хагелин);
* [**Фиалка М-125**](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B0%D0%BB%D0%BA%D0%B0_%D0%9C-125)**.**

Также под шифратором может пониматься программное обеспечение, используемое для совершения аналогичной операции.

Электронные шифраторы можно делит на три вида:

* Программные;
* Программно-аппаратные;
* Аппаратные.

**Аппаратное шифрование** — процесс [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), производимый при помощи специализированных вычислительных устройств.

**Шифровальная машина Энигма.**

«**Эни́гма**» (от [др.-греч.](https://ru.wikipedia.org/wiki/%D0%94%D1%80%D0%B5%D0%B2%D0%BD%D0%B5%D0%B3%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) αἴνιγμα — загадка) — переносная [шифровальная машина](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%B0%D1%82%D0%BE%D1%80_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29), использовавшаяся для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и расшифрования секретных сообщений. Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с [20-х годов](https://ru.wikipedia.org/wiki/1920-%D0%B5) [XX века](https://ru.wikipedia.org/wiki/XX_%D0%B2%D0%B5%D0%BA).

«Энигма» использовалась в коммерческих целях, а также в военных и государственных службах во многих странах мира, но наибольшее распространение получила в [нацистской Германии](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B5%D1%82%D0%B8%D0%B9_%D1%80%D0%B5%D0%B9%D1%85) во время [Второй мировой войны](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0). Именно германская военная модель чаще всего является предметом дискуссий.

Впервые шифр «Энигмы» удалось расшифровать в польском [Бюро шифров](https://ru.wikipedia.org/wiki/%D0%91%D1%8E%D1%80%D0%BE_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2) в декабре [1932 года](https://ru.wikipedia.org/wiki/1932_%D0%B3%D0%BE%D0%B4). Трое сотрудников разведки, [Мариан Реевский](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD_%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9%22%20%5Co%20%22%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD%20%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9), [Ежи Рожицкий](https://ru.wikipedia.org/wiki/%D0%95%D0%B6%D0%B8_%D0%A0%D0%BE%D0%B6%D0%B8%D1%86%D0%BA%D0%B8%D0%B9) и [Генрих Зыгальский](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D1%80%D0%B8%D1%85_%D0%97%D1%8B%D0%B3%D0%B0%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9) с помощью данных французской разведки, [математической теории](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D1%82%D0%B0%D1%8F_%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0) и методов [обратной разработки](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D0%B0%D1%8F_%D1%80%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0) смогли разработать специальное устройство для расшифровки закодированных сообщений, которое назвали [криптологической бомбой](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B1%D0%BE%D0%BC%D0%B1%D0%B0%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F%20%D0%B1%D0%BE%D0%BC%D0%B1%D0%B0). В результате этого немецкие инженеры усложнили устройство «Энигмы» и в [1938 году](https://ru.wikipedia.org/wiki/1938_%D0%B3%D0%BE%D0%B4) выпустили обновленную версию, для расшифровки которой требовалось построить более сложные механизмы.

Во время Второй мировой войны в Англии для расшифровки сообщений, зашифрованных с помощью «Энигмы», была создана машина с кодовым названием «[Turing Bombe](https://ru.wikipedia.org/wiki/Turing_Bombe%22%20%5Co%20%22Turing%20Bombe)», оказавшая значительную помощь Антигитлеровской коалиции в войне. Вся информация, полученная [криптоанализом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7) с её помощью, имела кодовое название «*[Ultra](https://ru.wikipedia.org/wiki/Ultra_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%29%22%20%5Co%20%22Ultra%20%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%29)*». Утверждалось, что это достижение явилось решающим фактором в победе союзников.

Несмотря на то, что с точки зрения современной криптографии шифр «Энигмы» был слаб, на практике только сочетание этого фактора с другими (такими как ошибки операторов, процедурные изъяны, заведомо известный текст сообщений (например, при передаче метеосводок), захваты экземпляров «Энигмы» и шифровальных книг) позволили взломщикам шифров разгадывать шифры «Энигмы» и читать сообщения.

Было выпущено, по приблизительным оценкам, около 100 000 экземпляров шифровальных машин «Энигма».

**Описание.**



*Рисунок 1.* [*Электрическая схема*](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%85%D0%B5%D0%BC%D0%B0)*Энигмы, показывающая, куда течёт ток, когда буква «A» шифруется буквой «D»*



*Рисунок 2. Шифрующее действие Энигмы показано для двух последовательно нажатых клавиш — ток течёт через роторы, «отражается» от рефлектора, затем снова через роторы.
Замечание: Серыми линиями показаны другие возможные электрические цепи внутри каждого ротора. Буква****A*** *шифруется по-разному при последовательных нажатиях одной клавиши, сначала в****G****, затем в****C****. Сигнал пошёл по другому маршруту за счёт поворота ротора.*

Как и другие роторные машины, «Энигма» состояла из комбинации механических и электрических подсистем. **Механическая часть** включала в себя [**клавиатуру**](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D0%B2%D0%B8%D0%B0%D1%82%D1%83%D1%80%D0%B0), набор вращающихся дисков — **роторов**, — которые были расположены вдоль вала и прилегали 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).

Конкретный механизм работы 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](https://ru.wikipedia.org/w/index.php?title=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%BF%D1%80%D0%B5%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F&action=edit&redlink=1) при каждом следующем нажатии на клавишу на клавиатуре.

**Механические части двигались**, замыкая контакты и образуя меняющийся электрический контур (то есть, фактически, сам процесс шифрования букв реализовывался электрически). При нажатии на клавишу клавиатуры контур замыкался, ток проходил через различные цепи и в результате включал одну из набора лампочек, и отображавшую искомую букву кода. (Например: при шифровке сообщения, начинающегося с ANX…, оператор вначале нажимал на клавишу **A** — загоралась лампочка **Z** — то есть Z и становилась первой буквой криптограммы. Далее оператор нажимал N и продолжал [шифрование](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) таким же образом далее).

Для объяснения принципа работы машины приведена диаграмма рисунок 1. Диаграмма упрощена: на самом деле механизм состоял из 26 лампочек, клавиш, разъёмов и [электрических схем](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%85%D0%B5%D0%BC%D0%B0) внутри роторов. Ток шёл от [источника питания](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA_%D0%BF%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) (часто это была батарея) (1) через переключатель (2) в коммутационную панель (3). Коммутационная панель позволяла перекоммутировать соединения между клавиатурой (2) и неподвижным входным колесом (4). Далее ток проходил через разъём (3), в данном примере неиспользуемый, входное колесо (4) и схему соединений трёх (в армейской модели) или четырёх (в военно-морской модели) роторов (5) и входил в рефлектор (6). Рефлектор возвращал ток обратно, через роторы и входное колесо, но уже по другому пути, далее через разъём «S», соединённый с разъёмом «D», через другой переключатель (9), и зажигалась лампочка.

Таким образом, постоянное изменение [электрической цепи](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%86%D0%B5%D0%BF%D1%8C), через которую шёл ток вследствие вращения роторов, позволяло реализовать [многоалфавитный шифр подстановки](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B8%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80), что давало высокую, для того времени, устойчивость [шифра](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80).

### **Роторы.**

|  |  |
| --- | --- |
| https://upload.wikimedia.org/wikipedia/commons/thumb/0/05/Enigma-rotor-flat-contacts.jpg/220px-Enigma-rotor-flat-contacts.jpg*Рисунок 3. Левая сторона ротора Энигмы, видны плоские электрические контакты.* | https://upload.wikimedia.org/wikipedia/commons/thumb/f/fe/Enigma-rotor-pin-contacts.jpg/220px-Enigma-rotor-pin-contacts.jpg*Рисунок 4. Правая сторона ротора, видны штыревые контакты. Римская V идентифицирует электропроводку ротора.* |

Роторы — сердце «Энигмы». Каждый ротор представлял собой диск примерно 10 см в диаметре, сделанный из [эбонита](https://ru.wikipedia.org/wiki/%D0%AD%D0%B1%D0%BE%D0%BD%D0%B8%D1%82) или [бакелита](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%BA%D0%B5%D0%BB%D0%B8%D1%82), с пружинными штыревыми контактами на правой стороне ротора, расположенными по окружности. На левой стороне находилось соответствующее количество плоских электрических контактов. Штыревые и плоские контакты соответствовали буквам в алфавите (обычно это были 26 букв от A до Z). При соприкосновении контакты соседних роторов замыкали электрическую цепь. Внутри ротора каждый штыревой контакт был соединён с одним из плоских. Порядок соединения был различным для каждого ротора.



*Рисунок 5. Три ротора и шпиндель, к которому они крепятся.*

Сам по себе ротор производил очень простой тип шифрования: элементарный [шифр замены](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B). Например, контакт, отвечающий за букву E, мог быть соединён с контактом буквы T на другой стороне ротора. Но при использовании нескольких роторов в связке (обычно трёх или четырёх) за счёт их постоянного движения получается более надёжный шифр.

|  |  |  |
| --- | --- | --- |
| **Ротор в разобранном виде** |  | **Три последовательно соединённых ротора** |
| Enigma rotor exploded view.png | 1. кольцо с выемками
2. маркирующая точка для контакта «A»
3. алфавитное кольцо
4. залужённые контакты
5. электропроводка
6. штыревые контакты
7. пружинный рычаг для настройки кольца
8. втулка
9. пальцевое кольцо
10. храповое колесо
 | Enigma rotor set.png |

*Рисунок 6.*

Военные модели «Энигмы» выпускались с различным количеством роторов. Первая модель содержала только три. В более поздних моделях была возможность выбора из пяти (1934 г.), семи (1938 г.) или восьми (1939 г.) роторов. Роторы отмечались римскими цифрами I, …, VIII. До 1938 года германская армия использовала только три из пяти доступных роторов.

Четырёхроторная военно-морская модель «Энигмы», «*Kriegsmarine M4*» имела один дополнительный ротор, хотя была такого же размера, что и трёхроторная, за счёт более тонкого рефлектора. Существовало два типа этого ротора: «Бета» и «Гамма». В процессе шифрования он не двигался, но мог быть установлен вручную на любую из 26 различных позиций.

### **Ступенчатое движение роторов**



*Рисунок 7.*

Ступенчатое движение роторов «Энигмы». Все три собачки (обозначены зелёным) двигаются одновременно. Для первого ротора (1), [храповик](https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%B0%D0%BF%D0%BE%D0%B2%D0%B8%D0%BA) (красный) всегда зацеплен, и он поворачивается при каждом нажатии клавиши. В данном случае выемка на первом роторе позволяет собачке зацепить и второй ротор (2), он повернётся при следующем нажатии клавиши. Третий ротор (3) не зацеплен, так как собачка третьего ротора не попала в выемку второго, собачка будет просто скользить по поверхности диска.

Каждый ротор был прикреплён к шестерёнке с 26 зубцами ([храповику](https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%B0%D0%BF%D0%BE%D0%B2%D0%BE%D0%B9_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%B7%D0%BC)), а группа собачек зацепляла зубцы шестерёнок. Собачки выдвигались вперёд одновременно с нажатием клавиши на машине. Если собачка цепляла зубец шестерёнки, то ротор поворачивался на один шаг.

В армейской модели «Энигмы» каждый ротор был прикреплён к регулируемому кольцу с выемками. Пять базовых роторов (I—V) имели по одной выемке, тогда как в военно-морской модели (VI—VIII) — по две. В определённый момент выемка попадала напротив собачки, позволяя ей зацепить [храповик](https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%B0%D0%BF%D0%BE%D0%B2%D0%B8%D0%BA) следующего ротора при последующем нажатии клавиши. Когда же собачка не попадала в выемку, она просто проскальзывала по поверхности кольца, не цепляя шестерёнку. В системе с одной выемкой второй ротор продвигался вперёд на одну позицию за то же время, что первый — на 26. Аналогично, третий ротор продвигался на один шаг за то же время, за которое второй делал 26 шагов. Особенностью машины было то, что второй ротор также поворачивался, если поворачивался третий. Это означает, что второй ротор мог повернуться дважды при двух последовательных нажатиях клавиш — так называемое «двухшаговое движение», — что приводило к уменьшению периода обращения.

Двухшаговое движение отличает функционирование роторов от нормального [одометра](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BE%D0%BC%D0%B5%D1%82%D1%80). Двойной шаг реализовывался следующим образом: первый ротор поворачивался, заставляя второй также повернуться на один шаг. И, если второй ротор продвинулся в нужную позицию, то третья собачка зацепляла третью шестерёнку. На следующем шаге эта собачка толкала шестерёнку и продвигала её, а также продвигала и второй ротор.

С тремя дисками и только с одной выемкой в первом и втором диске, машина имела период 26×25×26 = 16 900. Как правило, сообщения не превышали пары сотен символов, и, следовательно, не было риска повтора позиции роторов при написании одного сообщения.

При нажатии клавиши роторы поворачивались до замыкания электрической цепи.



*Рисунок 8.*

Роторы «Энигмы» в собранном состоянии. Три подвижных ротора помещены между двумя неподвижными деталями: входное кольцо и рефлектор (помечен «B» слева).

### **Входное колесо**

Входное колесо ([нем.](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Eintrittswalze*), или входной [статор](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%BE%D1%80), соединяло коммутационную панель или (в случае её отсутствия) клавиатуру и ламповую панель с роторами. Несмотря на то, что фиксированное соединение проводов играло сравнительно небольшую роль с точки зрения безопасности, именно это оказалось некоторым препятствием в работе польского [криптоаналитика](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7) [Мариана Реевского](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9%2C_%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD%22%20%5Co%20%22%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9%2C%20%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD), когда он пытался определить способ соединения проводов внутри роторов. Коммерческая модель «Энигмы» соединяла буквы в порядке их следования на клавиатуре: Q→A, W→B, E→C и так далее. Однако военная модель соединяла их в прямом алфавитном порядке: A→A, B→B, C→C и т. д. Только интуитивная догадка Реевского позволила ему изменить расчёты и решить [уравнения](https://ru.wikipedia.org/wiki/%D0%A3%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5).

### **Рефлектор**

За исключением ранних моделей «A» и «B», за последним ротором следовал *рефлектор* ([нем.](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Umkehrwalze*), запатентованная деталь, отличавшая семейство «Энигмы» от других роторных машин, разработанных в то время. Рефлектор соединял контакты последнего ротора попарно, коммутируя ток через роторы в обратном направлении, но по другому маршруту. Наличие рефлектора гарантировало, что преобразование, осуществляемое «Энигмой», есть [инволюция](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B2%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D1%8F_%28%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%29), то есть расшифрование представляет собой то же самое, что и [шифрование](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Однако наличие рефлектора делает невозможным шифрование какой-либо буквы через саму себя. Это было серьёзным концептуальным недостатком, впоследствии пригодившимся дешифровщикам.

В коммерческой модели «Энигма-C» рефлектор мог быть расположен в двух различных позициях, а в модели D — в 26 возможных позициях, но при этом был неподвижен в процессе шифрования. В модели, применявшейся в [абвере](https://ru.wikipedia.org/wiki/%D0%90%D0%B1%D0%B2%D0%B5%D1%80%22%20%5Co%20%22%D0%90%D0%B1%D0%B2%D0%B5%D1%80), рефлектор двигался во время шифрования, как и остальные диски.

В армейской и авиационной моделях «Энигмы» рефлектор был установлен, но не вращался. Он существовал в четырёх разновидностях. Первая разновидность была помечена буквой A. Следующая, *Umkehrwalze B*, была выпущена 1 ноября 1937 года. Третья, *Umkehrwalze C*, появилась в 1941 году. Четвёртая, *Umkehrwalze D*, впервые появившаяся 2 января 1944 года, позволяла оператору «Энигмы» управлять настройкой коммутации внутри рефлектора.

### **Коммутационная панель**



*Рисунок 9. Коммутационная панель в передней части машины. Могло использоваться до 13 соединений. На фотографии переключены две пары букв (S—O и J—A)*.

**Коммутационная панель** ([нем.](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Steckerbrett*) позволяет оператору варьировать соединения проводов. Впервые она появилась в немецких армейских версиях в [1930 году](https://ru.wikipedia.org/wiki/1930_%D0%B3%D0%BE%D0%B4) и вскоре успешно использовалась и в военно-морских версиях. Коммутационная панель внесла огромный вклад в усложнение шифрования машины, даже больший, чем введение дополнительного ротора. С «Энигмой» без коммутационной панели можно справиться практически вручную, однако после добавления коммутационной панели взломщики были вынуждены конструировать специальные машины.

Кабель, помещённый на коммутационную панель, соединял буквы попарно, например, «E» и «Q» могли быть соединены в пару. Эффект состоял в перестановке этих букв до и после прохождения сигнала через роторы. Например, когда оператор нажимал «E», сигнал направлялся в «Q», и только после этого уже во входной ротор. Обычно, «Энигма» поставлялась с шестью кабелями.

Каждая буква на коммутационной панели имела два гнезда. Вставка штепселя разъединяла верхнее гнездо (от клавиатуры) и нижнее гнездо (к входному ротору) этой буквы. Штепсель на другом конце кабеля вставлялся в гнезда другой буквы, переключая тем самым соединения этих двух букв.

### **Аксессуары**

Удобной деталью, использовавшейся на «Энигме» модели «M4», был так называемый «Schreibmax», маленькое печатающее устройство, которое могло печатать все 26 букв на небольшом листе бумаги. В связи с этим, не было необходимости в дополнительном операторе, следящем за лампочками и записывающем буквы. Печатное устройство устанавливалось поверх «Энигмы» и было соединено с панелью лампочек. Чтобы установить печатающее устройство, необходимо было убрать крышечки от ламп и все лампочки. Кроме того, это нововведение повышало безопасность: теперь офицеру-связисту не обязательно было видеть незашифрованный текст. Печатающее устройство было установлено в каюте командира подводной лодки, а офицер-связист только вводил зашифрованный текст, не получая доступа к секретной информации.

Другим аксессуаром была отдельная удалённая панель с лампочками. В варианте с дополнительной панелью деревянный корпус «Энигмы» был более широким. Существовала модель панели с лампочками, которая могла быть впоследствии подключена, но это требовало, как и в случае с печатающим устройством «Schreibmax», замены заводской панели с лампочками. Удалённая панель позволяла человеку прочитать расшифрованный текст без участия оператора.

В 1944 году военно-воздушные силы ввели дополнительный переключатель коммутационной панели, названный «Uhr» (часы). Это была небольшая коробка, содержащая переключатель с 40 позициями. Он заменял стандартные штепсели. После соединения штепселей, как определялось в списке кодов на каждый день, оператор мог поменять переключатель в одной из этих 40 позиций. Каждая позиция приводила к различной комбинации телеграфирования штепселя. Большинство из этих соединений штепселей, в отличие от стандартных штепселей, были непарными.

### **Математическое описание**

Преобразование «Энигмы» для каждой буквы может быть определено математически как результат [перестановок](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0). Рассмотрим трёхроторную армейскую модель. Положим, что «P» обозначает коммутационную панель, «U» обозначает отражатель, а «L», «M», «R» обозначают действия левых, средних и правых роторов соответственно. Тогда [шифрование](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) «E» может быть выражено как:

*{\displaystyle E=PRMLUL^{-1}M^{-1}R^{-1}P^{-1}}E = PRMLUL-1M-1R-1P-1 (1)*

После каждого нажатия клавиш ротор движется, изменяя трансформацию. Например, если правый ротор «R» проворачивается на i позиций, происходит трансформация {\displaystyle \rho ^{i}R\rho ^{-i}} $ρ^{i}Rρ^{-i}$, где ρ — циклическая перестановка, проходящая от «A» к «B», от «B» к «C», и так далее. Таким же образом, средний и левый ротор могут быть обозначены как j и k вращений «M» и «L». Функция шифрования в этом случае может быть отображена следующим образом:

$E=P(ρ^{i}Rρ^{-i})(ρ^{i}Mρ^{-i})(ρ^{i}Lρ^{-i})U(ρ^{i}L^{-1}ρ^{-i})(ρ^{i}M^{-1}ρ^{-i})(ρ^{i}R^{-1}ρ^{-i})P^{-1}$ (2)

**Процедуры для использования «Энигмы»**

В германских вооружённых силах средства связи были разделены на разные сети, причём у каждой были собственные настройки кодирования для машин «Энигмы». В английском центре дешифровки [Блетчли-Парк](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D0%B8-%D0%9F%D0%B0%D1%80%D0%BA%22%20%5Co%20%22%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D0%B8-%D0%9F%D0%B0%D1%80%D0%BA) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) [*Bletchley Park*](https://en.wikipedia.org/wiki/Bletchley_Park)) эти коммуникационные сети именовались ключами и им были присвоены кодовые имена, такие как Red, Chaffinch или Shark. Каждой единице, работающей в сети, на новый промежуток времени назначались новые настройки. Чтобы сообщение было правильно зашифровано и расшифровано, машины отправителя и получателя должны были быть одинаково настроены, конкретно идентичными должны были быть: выбор роторов, начальные позиции роторов и соединения коммутационной панели. Эти настройки оговаривались заранее и записывались в специальных шифровальных книгах.

Первоначальное состояние шифровального ключа «Энигмы» включает следующие параметры.

* Первоначальные позиции роторов: выбранные оператором, различные для каждого сообщения.
* Настройка колец: позиция алфавитного кольца, совпадающая с роторной схемой.
* Настройки штепселей: соединения штепселей на коммутационной панели.

«Энигма» была разработана таким образом, чтобы безопасность сохранялась даже в тех случаях, когда [шпиону](https://ru.wikipedia.org/wiki/%D0%A8%D0%BF%D0%B8%D0%BE%D0%BD%D0%B0%D0%B6) известны роторные схемы, хотя на практике настройки хранятся в секрете. С неизвестной схемой общее количество возможных конфигураций может быть порядка 10114 (около 380 бит), с известной схемой соединений и других операционных настроек этот показатель снижается до 1023 (76 бит). Пользователи «Энигмы» были уверены в её безопасности из-за большого количества возможных вариантов. Нереальным было даже начать подбирать возможную конфигурацию.

### **Индикаторы**

Большинство ключей хранилось лишь определённый период времени, обычно сутки. Однако для каждого нового сообщения задавались новые начальные позиции роторов. Это обуславливалось тем, что если число сообщений, посланных с идентичными настройками, будет велико, то [криптоаналитик](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7), досконально изучивший несколько сообщений, может подобрать шифр к сообщениям, используя частотный анализ. Подобная идея используется в принципе «инициализационного вектора» в современном шифровании. Эти начальные позиции отправлялись вместе с криптограммой, перед зашифрованным текстом. Такой принцип именовался «индикаторная процедура». И именно слабость подобных индикационных процедур привела к первым успешным случаям взлома кода «Энигмы».

Одни из ранних индикационных процедур использовались польскими криптоаналитиками для взлома кода. Процедура заключалась в том, что оператор настраивал машину в соответствии со списком настроек, которые содержат главные первоначальные стартовые позиции роторов. Допустим, главное ключевое слово — AOH. Оператор вращал роторы вручную до тех пор, пока слово AOH не читалось в роторных окошках. После этого оператор выбирал свой собственный ключ для нового сообщения. Допустим, оператор выбрал слово EIN. Это слово становилось ключевым для данного сообщения. Далее оператор ещё один раз вводил слово EIN в машину для избежания ошибок при передаче. В результате, после двойного ввода слова EIN в криптограмме отображалось слово XHTLOA, которое предшествовало телу основного сообщения. И наконец, оператор снова поворачивал роторы в соответствии с выбранным ключом, в данном примере EIN, и вводил далее уже основной текст сообщения.

При получении данного шифрованного сообщения вся операция выполнялась в обратном порядке. Оператор-получатель вводил в машину начальные настройки (ключевое слово AOH) и вводил первые шесть букв полученного сообщения (XHTLOA). В приведённом примере отображалось слово EINEIN, то есть оператор-получатель понимал, что ключевое слово — EIN. После этого он устанавливал роторы на позицию EIN, и вводил оставшуюся часть зашифрованного сообщения, на выходе получая чистый дешифрованный текст.

В этом методе было два недостатка. Во-первых, использование главных ключевых настроек. Впоследствии это было изменено тем, что оператор выбирал собственные начальные позиции для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) индикатора и отправлял начальные позиции в незашифрованном виде. Вторая проблема состояла в повторяемости выбранного оператором-шифровщиком слова-индикатора, которая была существенной трещиной в безопасности. Ключ сообщения шифровался дважды, в результате чего прослеживалось закономерное сходство между первым и четвёртым, вторым и пятым, третьим и шестым символами. Этот недостаток позволил польским дешифровщикам взломать код «Энигмы» уже в 1932 году. Однако, начиная с 1940 года, немцы изменили процедуры для повышения безопасности.

Во время [Второй мировой войны](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0) немецкие операторы использовали шифровальную книгу только для установки роторов и настройки колец. Для каждого сообщения оператор выбирал случайную стартовую позицию, к примеру, WZA, и случайный ключ сообщения, допустим, SXT. Далее оператор устанавливал роторы в стартовую позицию WZA, и шифровал ключ сообщения SXT. Предположим, что в результате получится UHL. После этого оператор устанавливал слово SXT как начальную позицию роторов и ключ к сообщению. Далее он отправлял стартовую позицию WZA и шифровальный ключ UHL вместе с сообщением. Получатель устанавливал стартовую позицию роторов в соответствии с первой триграммой WZA и расшифровывал вторую триграмму, UHL, для распознания ключа сообщения SXT. Далее получатель использовал этот ключ как стартовую позицию для расшифровки сообщения. Таким образом, каждый раз главный ключ оказывался различным и был ликвидирован недостаток, свойственный процедуре с двойным шифрованием ключа.

### **Аббревиатуры и директивы**

Армейская версия «Энигмы» использовала только 26 букв. Прочие символы заменялись редкими комбинациями букв. Пробел пропускался либо заменялся на «X». Символ «X» в основном использовался для обозначения точки либо конца сообщения. В отдельных подразделениях использовались некоторые особые символы. В шифровках армии запятая заменялась на сочетание «ZZ», а вопросительный знак — на «FRAGE» либо «FRAQ». В шифровках, использовавшихся военно-морскими силами, запятая заменялась на «Y», а вопросительный знак — на комбинацию «UD». Комбинация символов «CH», например, в словах «ACHT» (восемь), «RICHTUNG» (направление) заменялась символом «Q» («AQT», «RIQTUNG»). Два, три или четыре нуля заменялись словами «CENTA», «MILLE» и «MYRIA» соответственно[[28]](https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0#cite_note-autogenerated1-28).

Шифровальщики в армии и [люфтваффе](https://ru.wikipedia.org/wiki/%D0%9B%D1%8E%D1%84%D1%82%D0%B2%D0%B0%D1%84%D1%84%D0%B5) отправляли сообщения группами по пять символов. Военно-морские шифровальщики, использующие, как сказано выше, четырёхроторные машины, отправляли сообщения группами по четыре символа. Часто употребляемые слова и имена очень сильно варьировались. Например, слово «Minensuchboot» (минный тральщик) могло быть написано как «MINENSUCHBOOT», «MINBOOT», «MMMBOOT» или «MMM354». Чтобы осложнить [криптоанализ](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7), отдельные сообщения не содержали более 250 символов. Более длинные сообщения разбивались на части, и каждая часть использовала свой ключ. Кроме того, иногда операторы специально забивали зашифрованные сообщения «мусором» (например, бессвязный набор букв, несвязанные с основным текстом слова́), для усложнения дешифровки перехватов противником.

**Расшифрование шифр «Энигмы». Криптоанализ «Энигмы»**

*Основная статья:****[Криптоанализ «Энигмы»](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%C2%AB%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D1%8B%C2%BB%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%20%5C%C2%AB%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D1%8B%5C%C2%BB)***

В течение всего периода активного применения «Энигм», различные правительственные организации стран Европы предпринимали попытки «взлома» машины с целью защиты от нарастающей угрозы со стороны Германии. «Энигма» была необходима Германии для проведения быстрого и скоординированного наступления против ряда стран в рамках Второй мировой войны. В довоенном периоде наибольших успехов в дешифровке сообщений «Энигмы» достигло польское Бюро шифров и лично [Мариан Реевский](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9%2C_%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD%22%20%5Co%20%22%D0%A0%D0%B5%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9%2C%20%D0%9C%D0%B0%D1%80%D0%B8%D0%B0%D0%BD). Во время Второй мировой войны пальму первенства в деле криптоанализа «Энигмы» взял центр британской разведки «Station X», также известный как [Блетчли-парк](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D0%B8-%D0%BF%D0%B0%D1%80%D0%BA%22%20%5Co%20%22%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D0%B8-%D0%BF%D0%B0%D1%80%D0%BA).

**Клоны «Энигмы»**

«Энигма» внесла существенное влияние в сферу изобретения шифровальных машин вообще и роторных машин в частности:

* «Тайпекс» («Typex») была разработана в [Великобритании](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) по чертежам «Энигмы» — она даже содержит детали, изъятые из «Энигмы».
* «GREEN» — [японский](https://ru.wikipedia.org/wiki/%D0%AF%D0%BF%D0%BE%D0%BD%D0%B8%D1%8F) клон «Энигмы», малоиспользуемая машина, содержащая четыре ротора, расположенных вертикально.
* В [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90) [криптоаналитик](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%22%20%5Co%20%22%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7) [Уильям Фридман](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B8%D0%B4%D0%BC%D0%B0%D0%BD%2C_%D0%A3%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC_%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D0%B8%D0%BA) изобрёл «M-325», шифровальную машину, подобную «Энигме» в логических операциях, хотя отличную по конструкции.
* Уникальная роторная машина «Cryptograph» была изобретена в 2002 году [голландским](https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D0%BB%D0%BB%D0%B0%D0%BD%D0%B4%D1%86%D1%8B) криптоаналитиком Татьяной ван Варк (Tatjana van Vark). Она базируется на принципе работы «Энигмы», но имеет ряд существенных отличий — например, увеличенное число роторов и наличие «переключателя супершифрования». Татьяна ван Варк не раскрывает деталей устройства машины, обещая это сделать только в том случае, если кто-либо расшифрует закодированное с помощью этой машины послание.

**Пример.**

**Дневной ключ:**

1. **Настроек коммутационной панели (нем. Steckerverbindunden);**

*ABCDEFGHIJKLMNOPQRSTUVWXYZ*

*ABCDEFGHIJKLMNOPQRSTUVWXYZ*

1. **Порядка установки роторов (нем. Walzenlage);**

**I ротор:**

*RSTUVWXYZABCDEFGHIJKLMNOPQ*

**II ротор:**

*GHIJKLMNOPQRSTUVWXYZABCDEF*

**III ротор:**

*WXYZABCDEFGHIJKLMNOPQRSTUV*

1. **Положений колец (нем. Ringstellung);**

Перестановки для каждый роторов и рефлектор.

1. **Начальных установок роторов (нем. Kenngruppen).**

**I, II, III ротор: –** *H, D, X***.**

**Открытий текст:**

*RECOMMENDATIONFORBLOCKCIPHERMODESOFOPERATIONMETHODSANDTECHNIQUES*

**Шифртекст:**

*HMGZSHQHPUJYACUXYOBGNGQRUSWEUNSRNYEPVNGJFXNONSPNQPEZLGEUMCSHOSXZ*