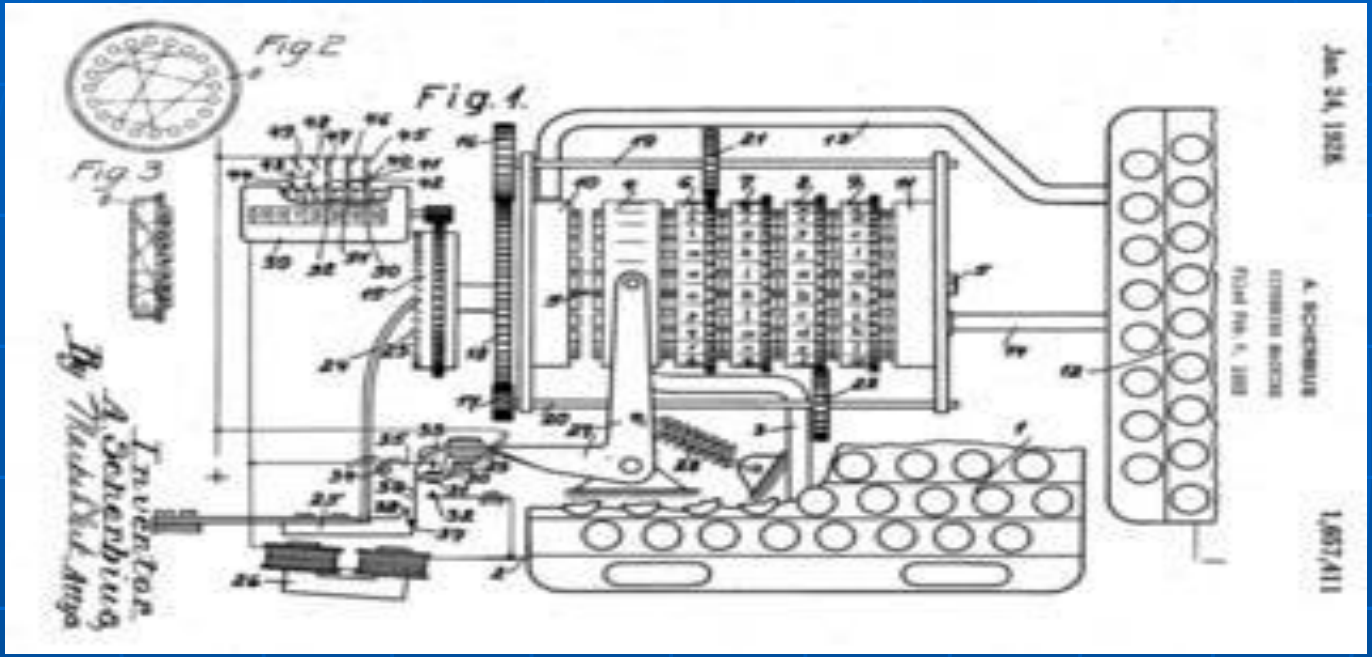
Enigma

Немного истории

- Первая версия была разработана в 1918 г.
- Стала известной в основном из-за того, что использовалась вермахтом во время BoB

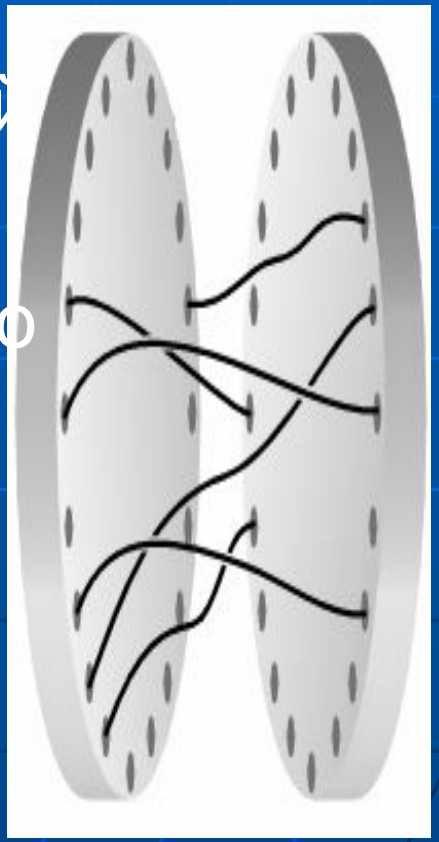
Устройство



Основную работу выполняют роторы и рефлектор

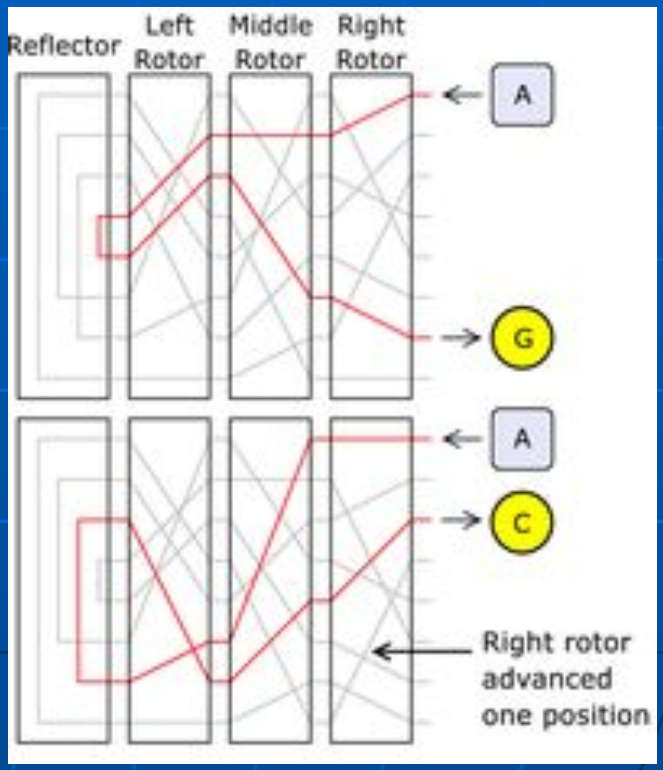
Что такое ротор

- Ротор – диск, имеющий с каждой стороны 26 контактов
- Внутри ротора контакты попарно соединены
- Контакты соседних роторов касаются друг друга, создавая тем самым электрическую цепь



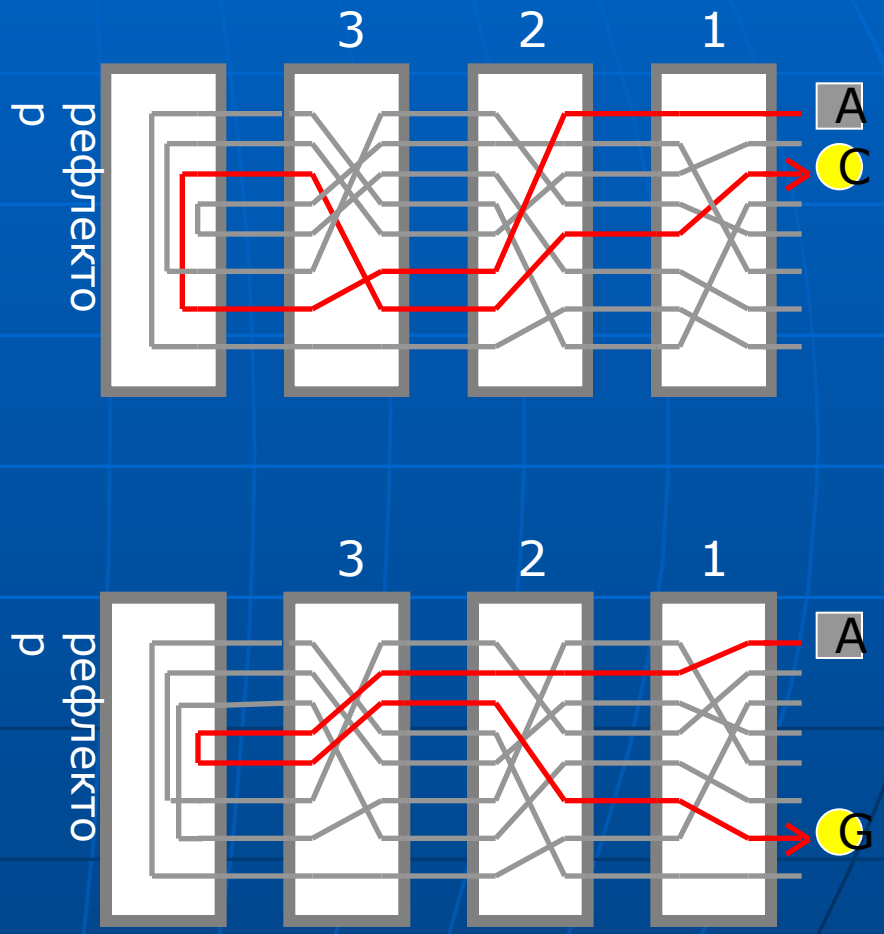
Принцип работы

- Зашифрованная 1-м ротором буква шифруется 2-м ротором, далее – 3-м, затем проходит через рефлектор, шифруется снова 3-м, затем 2-м и 1-м.
- Когда буква зашифрована, роторы поворачиваются по некоторому алгоритму. В результате, одна и та же буква шифруется разными символами.
- Благодаря рефлектору, шифрование и расшифрование выполняются одинаково.



Пример

- На вход поступает ‘A’.
- После прохода через все роторы ‘A’ кодируется в ‘C’.
- 1-й ротор поворачивается на одну позицию вниз.
- На вход поступает ‘A’.
- Теперь ‘A’ кодируется уже по-другому – на выходе получается ‘G’.



Ключ шифра

- Используемые роторы
- Начальное положение роторов
- Правила движения роторов

Особенности шифра

- Симметричность
- Две идущие подряд одинаковые буквы шифруются разными буквами
- Буква не может быть зашифрована самой собой
- Смена алфавитов периодическая:
  $T = P^N$, P – число букв в алфавите,
  N – число роторов.

Спасибо!