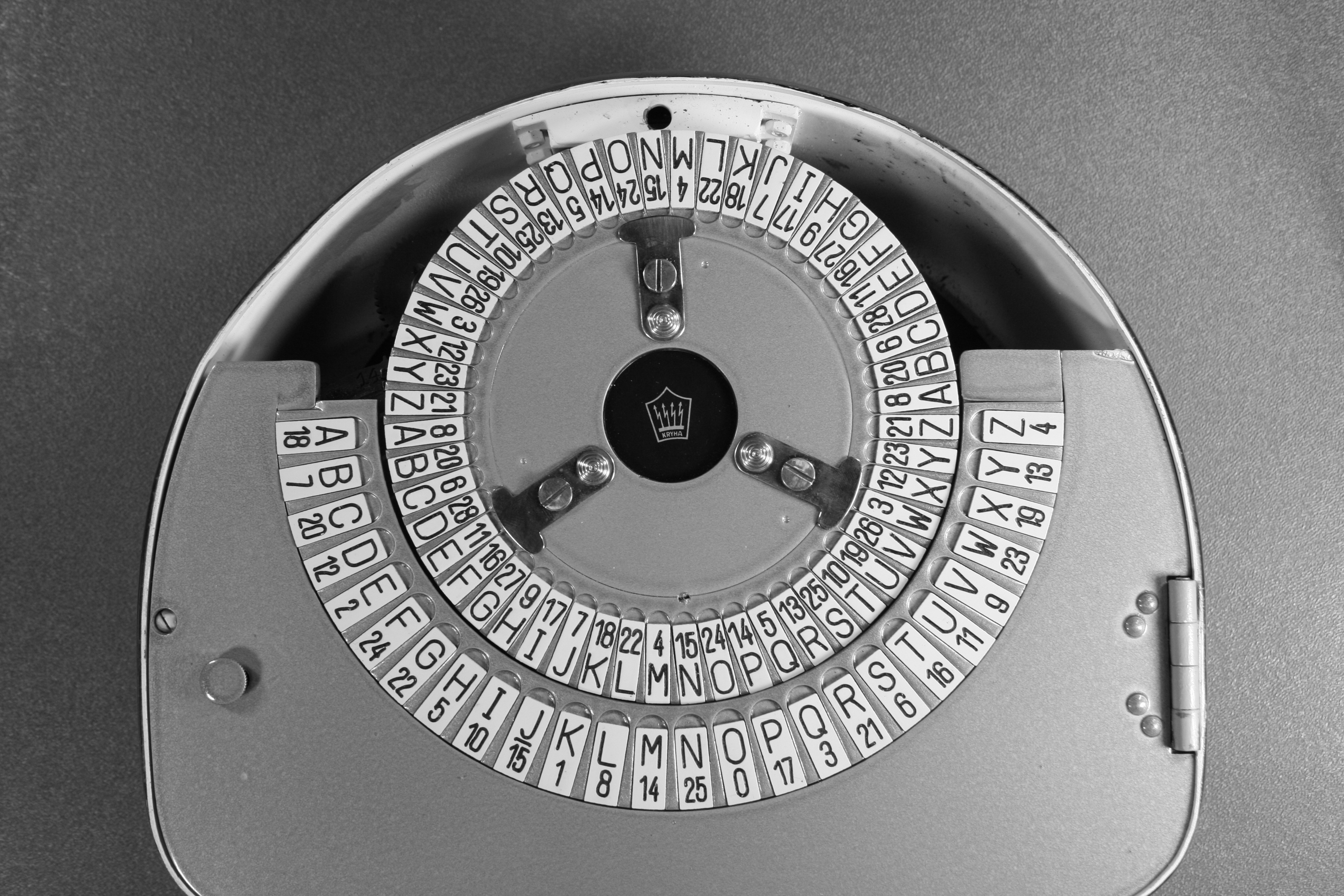
**Глава 2. Электромеханические устройства в шифровании.**

Новым шагом в криптографии стало использование электромеханических машин. Наиболее веской причиной для их использования были мировые войны двадцатого века. В них электромеханические устройства использовались как для шифрования, так и в последствии для дешифрования текстов. Это позволило создавать более сложные шифры и взламывать их.

1. [Шифровальная машина KRYHA](http://kryptography.narod.ru/mashiny.html#kryha)  
   В начале 1920 годов была изобретена KRYHA. Эта машина состояла из двух концентрических колец, на которых написан алфавит. Внутреннее кольцо перемещалось на определенное число мест с помощью рычага, приводившего в действие пружинный двигатель. Тогда каждая буква исходного текста, алфавит которого был написан на внешнем кольце, соответствовала букве на внутреннем кольце, с помощью которого и шифровался исходный текст. Это устройство использовалось в том числе дипломатами Германии во времена Второй мировой войны, которые не знали, что шифр был раскрыт американцами.
2. Шифровальное устройство М-94.   
   Устройство состояло из 25 алюминиевых колец, соединенных стержнем длиной в 12 сантиметров. Каждое кольцо содержало буквы алфавита в произвольном порядке по окружности. Исключением являлось только первое кольцо, начинающееся со слов «ARMY OF THE USA» (армия США).

3. Шифровальная машина Enigma  
В 1923 году было создано электромеханическое устройство под названием Энигма, которое служило для зашифровки и расшифровки текстовой информации. Наибольшее распространение машина получила в нацистской Германии во времена Второй мировой войны. Несмотря на слабость шифра с точки зрения современной криптографии, в средине двадцатого века только стечение благоприятных факторов позволило дешифровать Энигму.

Энигма – роторная машина. Она содержала в себе механическую и электрическую подсистемы. Клавиатура была подсоединена к роторам (набор крутящихся дисков, расположенных вдоль вала и прилегающих к нему), которые при нажатии клавиш сдвигались в сторону (самый правый сдвигался на одну позицию, а при определенных условиях перемещались и другие роторы). Это смещение приводило к разным криптографическим преобразованиям при каждом последующем нажатии на любую из клавиш клавиатуры.

Процесс шифрования протекал электрически. Механические части смещались, контакты замыкались, образовывался меняющийся механический контур. При нажатии на клавиши контур размыкался, цепь, через которую проходил ток, менялась и включал одну из ряда лампочек, которая отображала нужную букву.

Сам по себе метод шифрования был прост – элементарная замена, на за счет нескольких связанных роторов из-за их постоянного движения надежность шифра возрастала.