Энигма

Олейников И.А.

Декабрь 2019

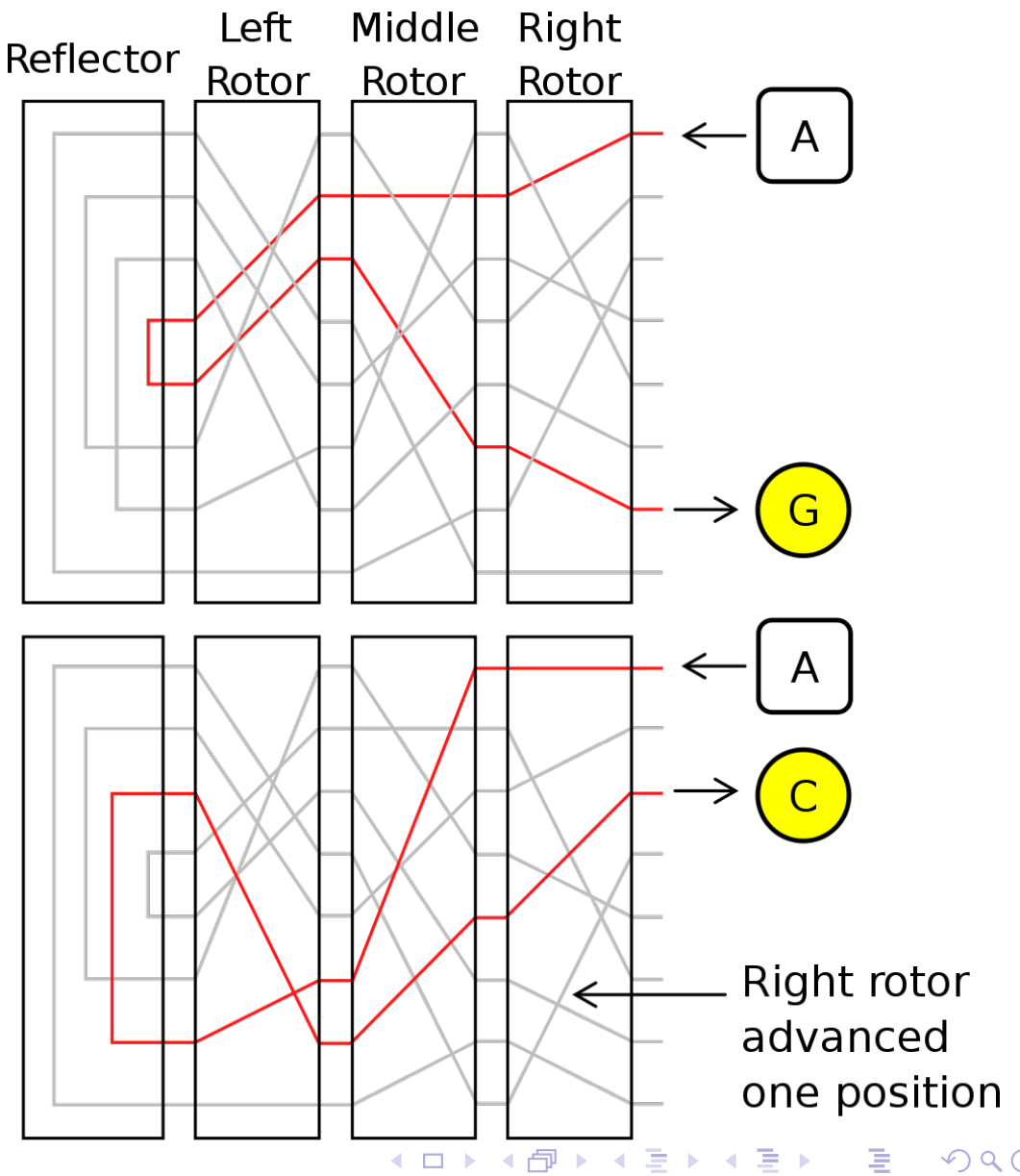
Содержание

Что это такое ?

- Переносная шифровальная машина для зашифровывания и расшифровывания секретных сообщений.
- Целое семейство шифровальных машин, применять которые начали с 20-х годов XX века.
- Было выпущено примерно 100 000 экземпляров.

Как она работает ?

- Цезарь на стероидах
- Роторы
- Рефлектор
- Коммутационная панель
- Лампочки
- Аксессуары



История

или почему больше не значит лучше ?

- Два немца в 1918 получили патент на шифровальную машину.
- Работа над model A, B.
- В 1926 придумали рефлектор: model C -> model D
- В 1928 немецкая армия внедряет свою модель.
- В 1930 появляется Enigma I с коммутационной панелью.
- Enigma II как неудачный эксперимент.

Применение

Бизнес и государство

- Коммерческое использование почтой, государственными структурами и правительственными организациями.
- Вся Европпа, США и Япония.
- Военная служба и армейские модификации.

Взлом

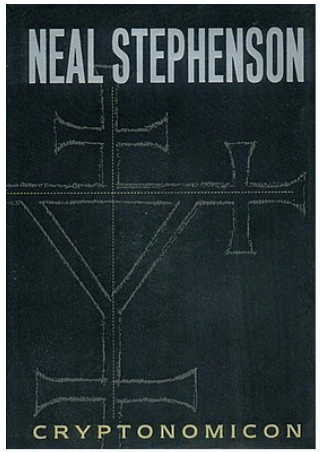
Поляки всех опередили

- Biuro Szyfrów + французская разведка 1933 год
- Bletchley Park и Turing Bombe

В попкультуре

500 000 $ и доставка на дом

- Игра в имитацию, Энигма и U-571
- Энигма и Криптономикон
- ebay, аукционы и блошиный рынок



Ссылки

- Wiki - Энигма
- Wiki - Enigma machine
- Wiki - Bombe
- Habr - Алгоритм Энигмы
- Habr - Энигма — шифрование сообщений в войну