Криптография: история развития и базовые знания

Петровская Л.А
547-Д9-ЗПИН

Человечество вступает в новую большую игру — и это отнюдь не война за нефтепроводы... Новое всемирное сокровище — это контроль над гигантскими потоками данных, соединяющими целые континенты и цивилизации, связывающими в единое целое коммуникацию миллиардов людей и организаций»

Криптография – это очень серьезная наука. Не исключаю того, что самая сложная математическая дисциплина.

– Евгений Касперский

Криптография как наука

- **Криптогра́фия** (от др.-греч. κρυπτός — скрытый и γράφω — пишу) - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта)

- **Эней Тактик** (IV век до н. э.) - описание «книжного шифра» — метода передачи секретных сообщений с помощью малозаметных пометок рядом с буквами в книге или документе

Терминология

- **Криптоанализ** — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
- Криптография и криптоанализ составляют **криптологию**, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).
- **Криптографическая стойкость** — способность криптографического алгоритма противостоять криптоанализу.
- **Криптографическая атака** — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Криптография в древнем мире

Атбаш

Примеры использования криптографии можно встретить в священных иудейских книгах, в том числе в книге пророка Иеремии (VI век до н. э.), где использовался простой метод шифрования под названием атбаш.

Атбаш — простой шифр подстановки для иврита. Правило шифрования состоит в замене *i*-й буквы алфавита буквой с номером *n* - *i* + 1, где *n* — число букв в алфавите. Пример для латинского алфавита выглядит так:

Исходный текст: **abcdefghijklmnopqrstuvwxyz**
Зашифрованный текст: **ZYXWVUTSRQPONMLKJIHGFEDCBA**

Происхождение слова «атбаш» объясняется принципом замены букв. Слово составлено из букв «алеф», «тав», «бет» и «шин», то есть первой и последней, второй и предпоследней букв еврейского алфавита.

Скитала

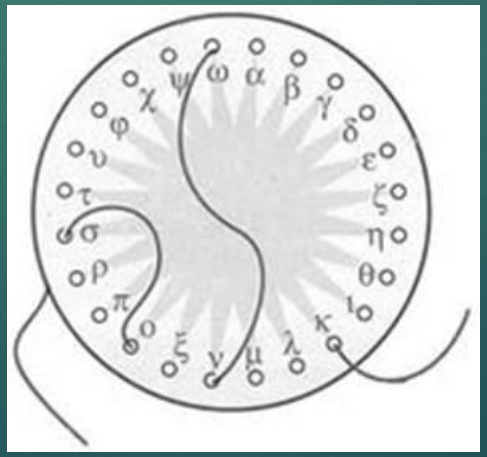
Также является одним из древнейших известных криптографических устройств, известный так же как *шифр Древней Спарты*.

Шифруемый текст писался на пергаментной ленте по длине палочки, после того как длина палочки оказывалась исчерпанной, она поворачивалась и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты. Дешифровка выполнялась с использованием палочки такого же диаметра.

Диск Энея, линейка Энея, книжный шифр

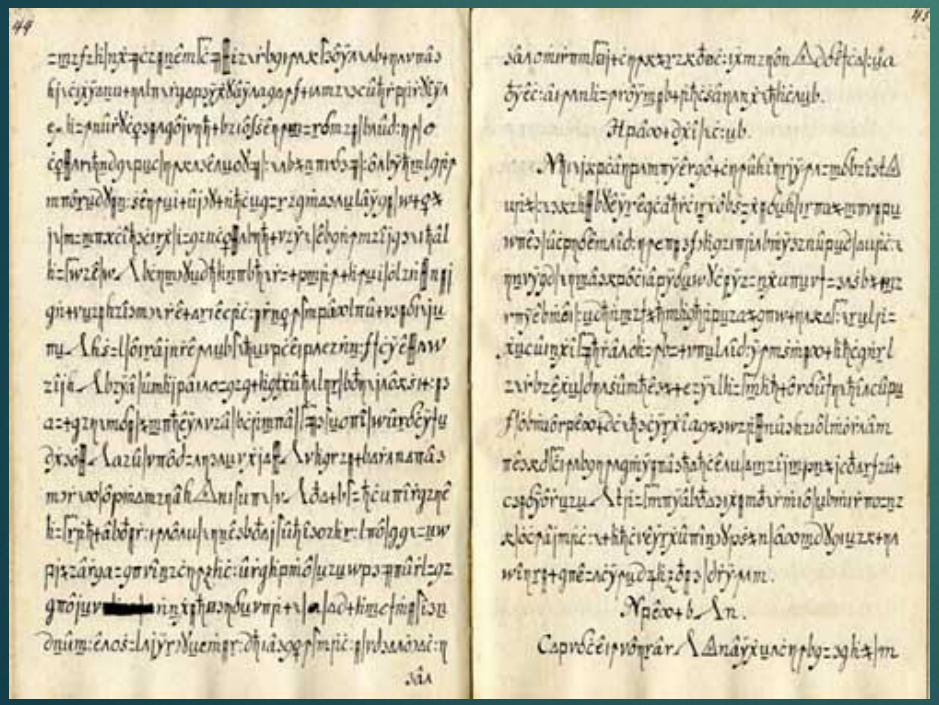
С именем Энея Тактика, полководца IV века до н. э., связывают несколько техник шифрования и тайнописи.

Диск Энея представлял собой диск диаметром 10—15 см с отверстиями по числу букв алфавита. Для записи сообщения нитка протягивалась через отверстия в диске, соответствующим буквам сообщения. При чтении получатель вытягивал нитку, и получал буквы, правда, в обратном порядке. Эней ткже предусмотрел способ быстрого уничтожения сообщения — для этого было достаточно выдернуть нить, закреплённую на катушке в центре диска.



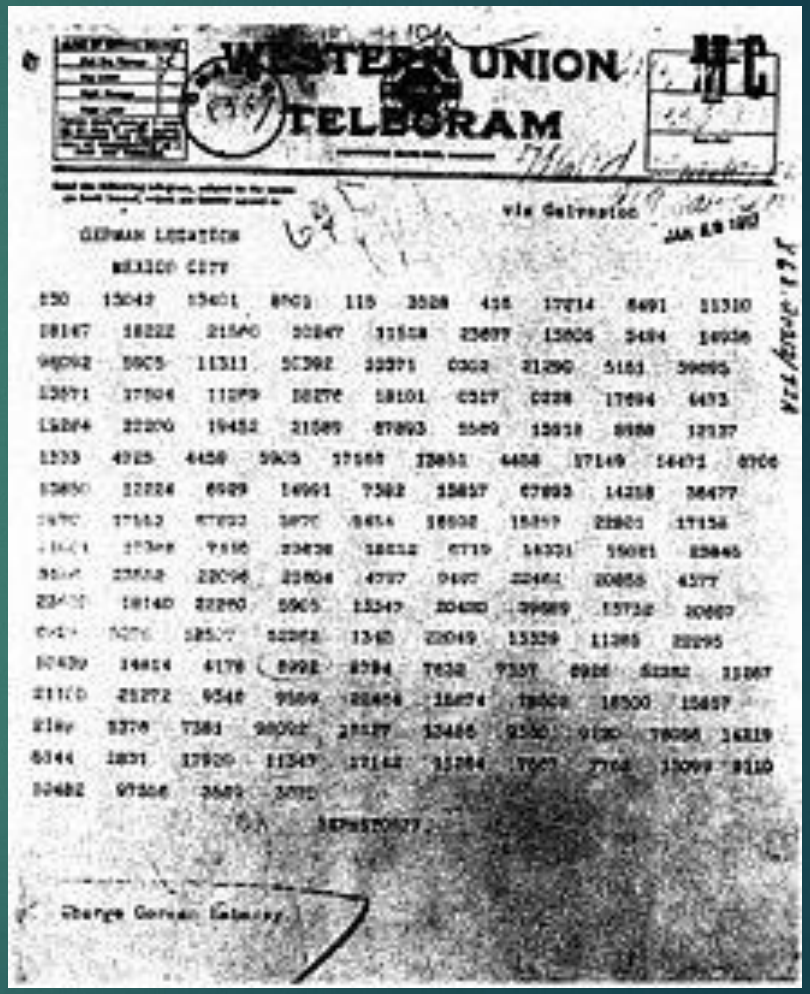
Средние века

Одним из самых известных шифров Средних веков называют **кодекс Copiale** — изящно оформленную рукопись с водяными знаками, не расшифрованную до сих пор. Эпоха Возрождения стала золотым веком криптографии: ее изучением занимался Фрэнсис Бэкон, описавший семь методов скрытого текста.



Первая мировая война

Во время Первой мировой войны криптография стала признанным боевым инструментом. Разгаданные сообщения противников вели к ошеломляющим результатам. Перехват телеграммы немецкого посла Артура Циммермана американскими спецслужбами привел к вступлению США в боевые действия на стороне союзников.



“Фотокопия телеграммы Циммермана”

Вторая мировая война

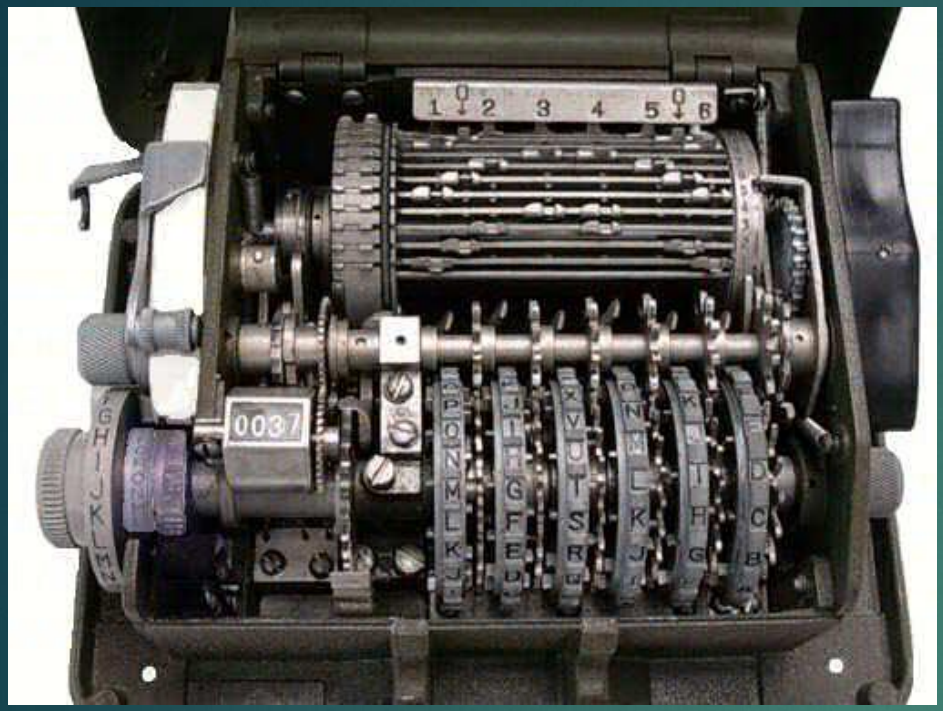
Германия: «Энигма», «Fish»

История самой известной электрической роторной шифровальной машины — «Энигма» — начинается в 1917 году — с патента, полученного голландцем Хьюго Кохом.

В конце 1920-х — начале 1930 годов, несмотря на переданные немецким аристократом Хансом Тило-Шмидтом данные по машине, имевшиеся экземпляры коммерческих вариантов, британская и французская разведка не стали браться за задачу криптоанализа.К тому времени они уже сочли, что шифр является невзламываемым.

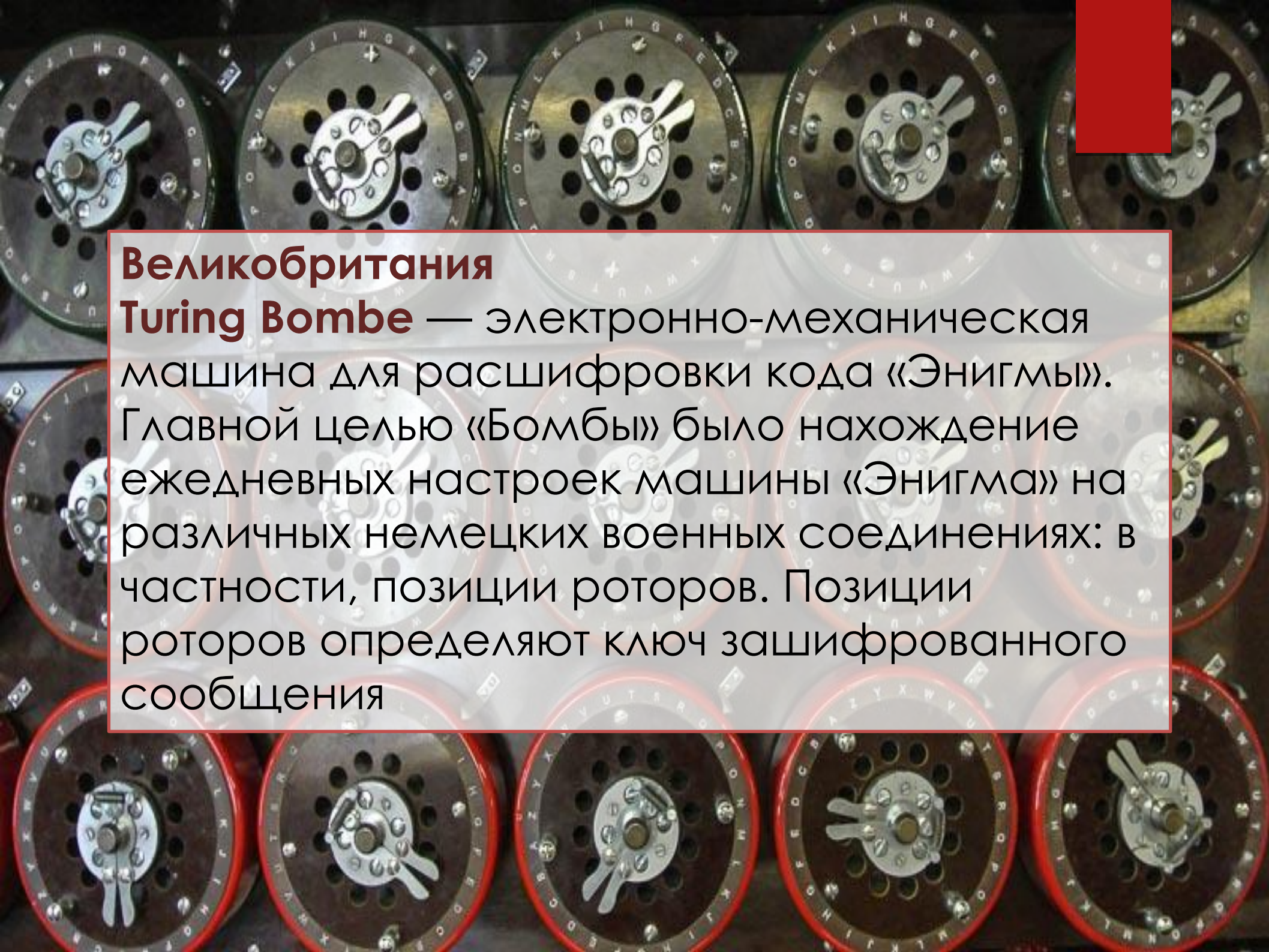
В армии и флоте **СССР** использовались шифры с кодами различной длины — от двух символов (фронт)до пяти (стратегические сообщения).

По ленд-лизу СССР получил несколько **М-209**, которые использовались как основа для создания своих собственных шифровальных машин, хотя об их использовании неизвестно.
Также для связи высших органов управления страной (в том числе Ставки Верховного Главнокомандования) и фронтами **использовалась ВЧ-связь.** Она представляла собой технические средства для предотвращения прослушивания телефонных разговоров, которые модулировали высокочастотный сигнал звуковым сигналом от мембраны микрофона.
Уже во время Второй мировой войны механизм заменили на более сложный, который разбивал сигнал на отрезки по 100—150 мс и три-четыре частотных полосы, после чего специальный шифратор их перемешивал.
На приёмном конце аналогичное устройство производило обратные манипуляции для восстановления речевого сигнала.



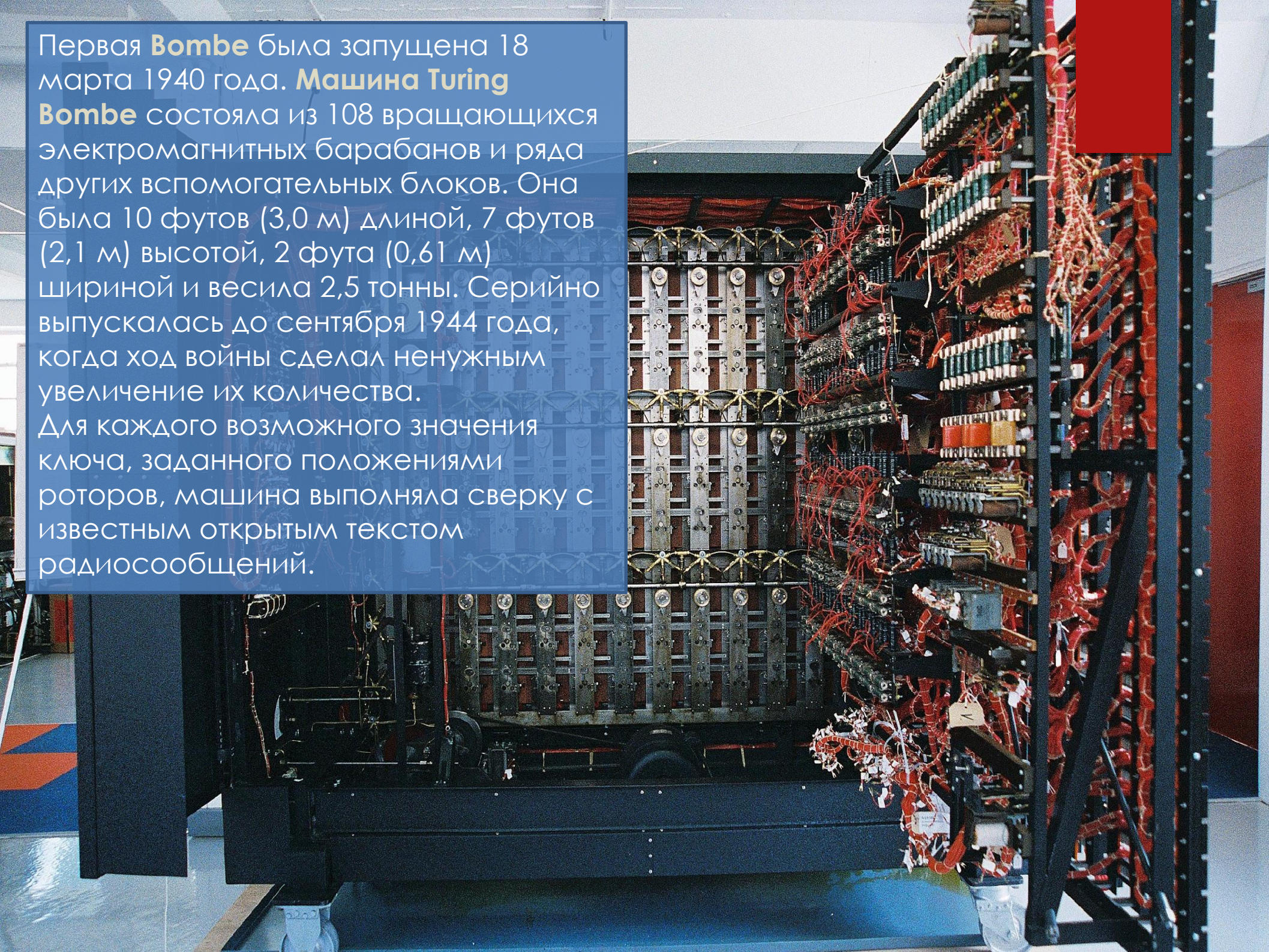
СССР. Шифровальная машина М-209 В армии и флоте СССР использовались шифры с кодами различной длины — от двух символов (фронт) до пяти (стратегические сообщения). Коды менялись часто, хотя иногда и повторялись на другом участке фронта. По ленд-лизу СССР получил несколько М-209, которые использовались как основа для создания своих собственных шифровальных машин, хотя об их использовании неизвестно.

Для отделения ВЧ сигнала от высоковольтного оборудования подстанции в фазный провод ВЛ высокого напряжения монтируется ВЧ заградитель. который ограничивает величину потерь ВЧ сигналов через параллельные контуры.

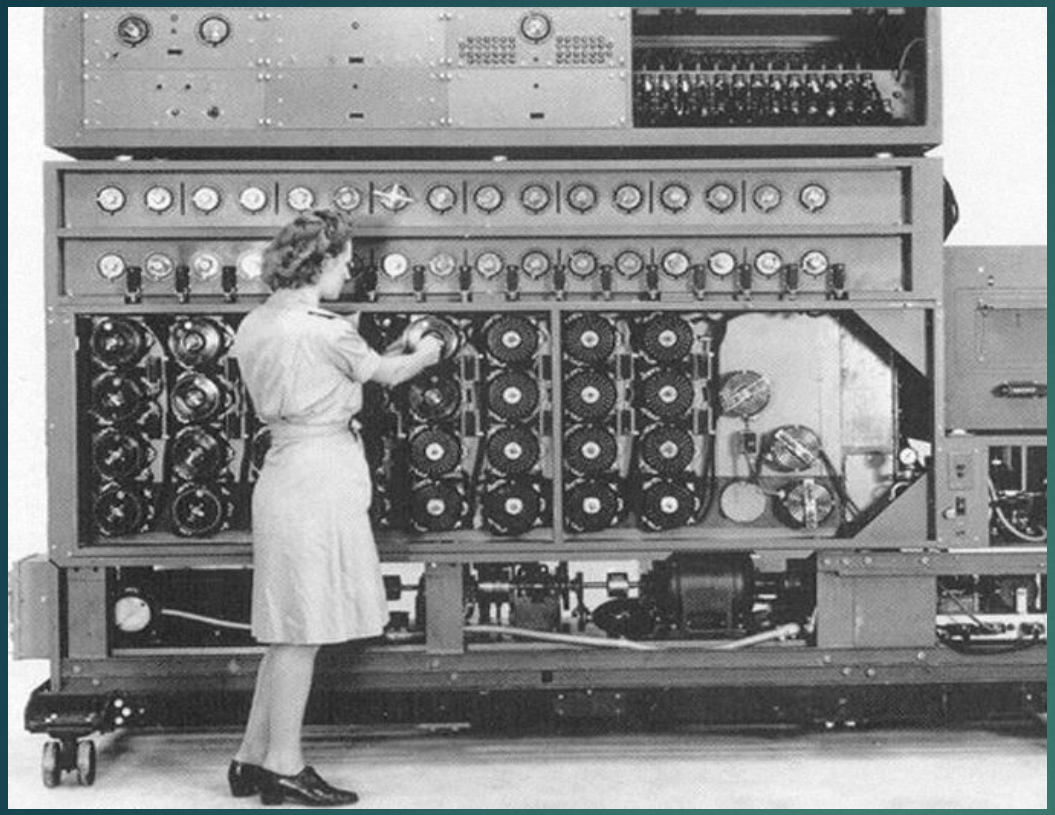


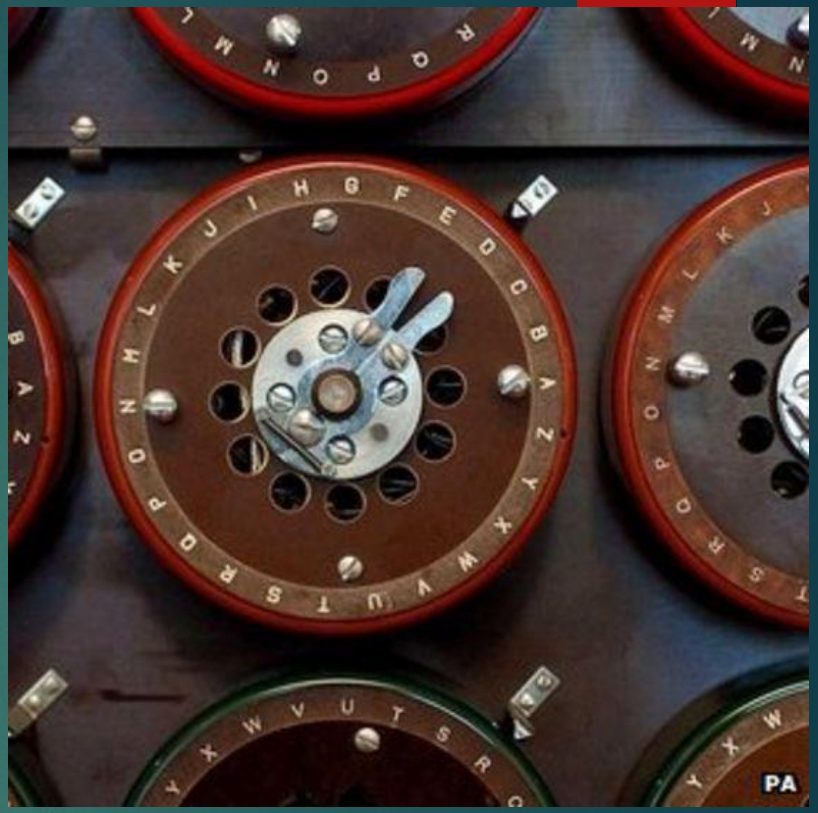
Великобритания

Turing Bombe — электронно-механическая машина для расшифровки кода «Энигмы». Главной целью «Бомбы» было нахождение ежедневных настроек машины «Энигма» на различных немецких военных соединениях: в частности, позиции роторов. Позиции роторов определяют ключ зашифрованного сообщения



Первая **Bombe** была запущена 18 марта 1940 года. **Машина Turing Bombe** состояла из 108 вращающихся электромагнитных барабанов и ряда других вспомогательных блоков. Она была 10 футов (3,0 м) длиной, 7 футов (2,1 м) высотой, 2 фута (0,61 м) шириной и весила 2,5 тонны. Серийно выпускалась до сентября 1944 года, когда ход войны сделал ненужным увеличение их количества.
Для каждого возможного значения ключа, заданного положениями роторов, машина выполняла сверку с известным открытым текстом радиосообщений.





Разработанный под руководством Алана Тьюринга и Джоан Кларк дешифратор. Его использование позволило союзникам расколоть казавшийся монолитным код «Энигмы».

Современные методы использования криптографии

Появление доступного интернета перевело криптографию на новый уровень. Криптографические методы стали широко использоваться частными лицами в электронных коммерческих операциях, телекоммуникациях и многих других средах. Первая получила особенную популярность и привела к появлению новой, не контролируемой государством валюты — биткойна.

Криптография,будет активно развиваться. Одна из ее новых задач – разработка скоростных методов шифрования с высоким уровнем секретности. Эта задача обусловлена появлением новых каналов связи (беспроводные сети, сотовая связь, Интернет), по которым передаются всё большие объемы информации. И как бы ни росли со временем вычислительные возможности у криптографов, достигать оптимальной стойкости криптографических систем при ограниченной скорости шифрования можно будет, лишь применяя при их разработке серьезные математические результаты. Как-никак задача нахождения оптимума – это математическая задача. Так было и тысячу лет назад, так будет и в далеком будущем.

Спасибо за внимание!