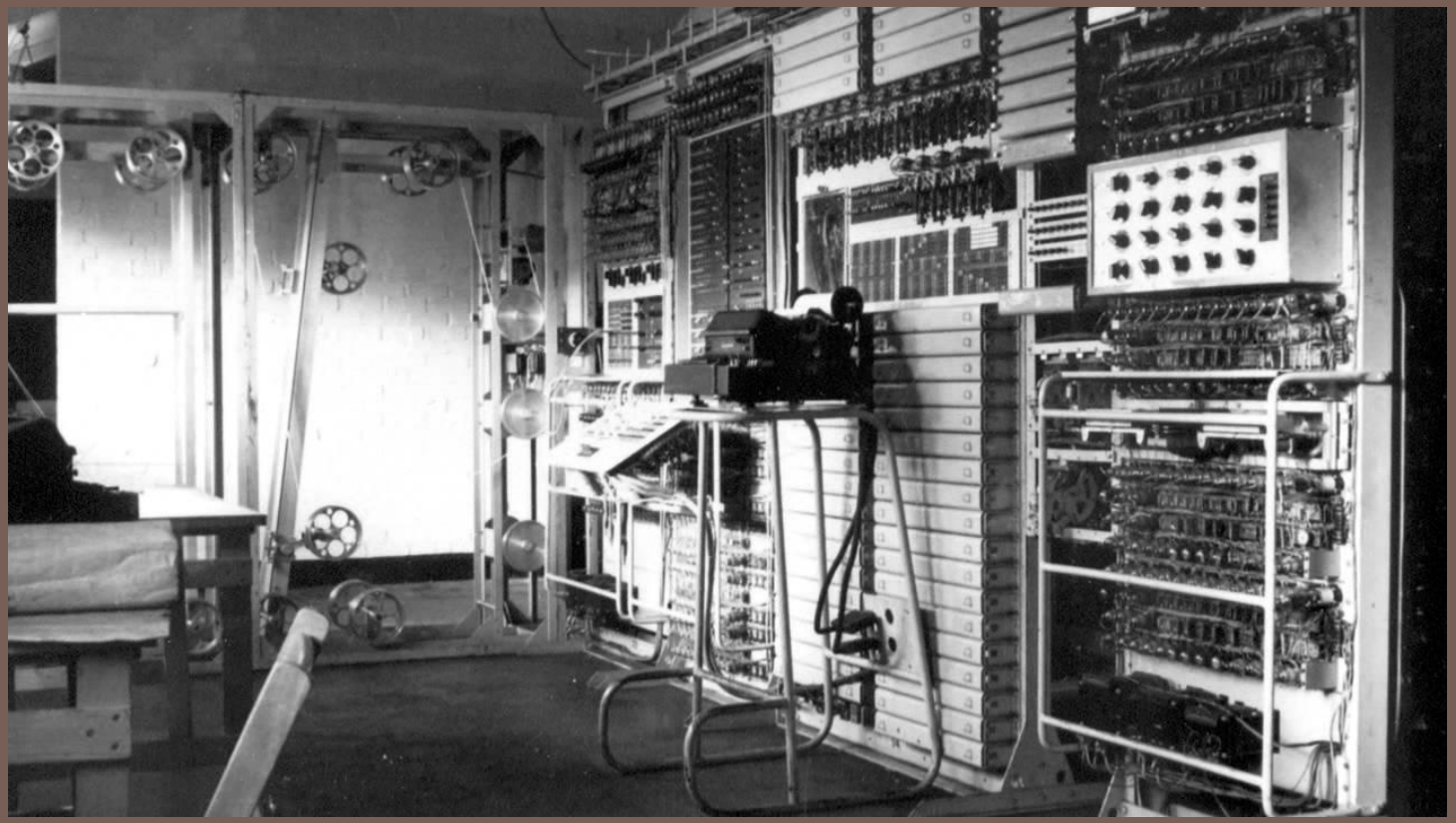
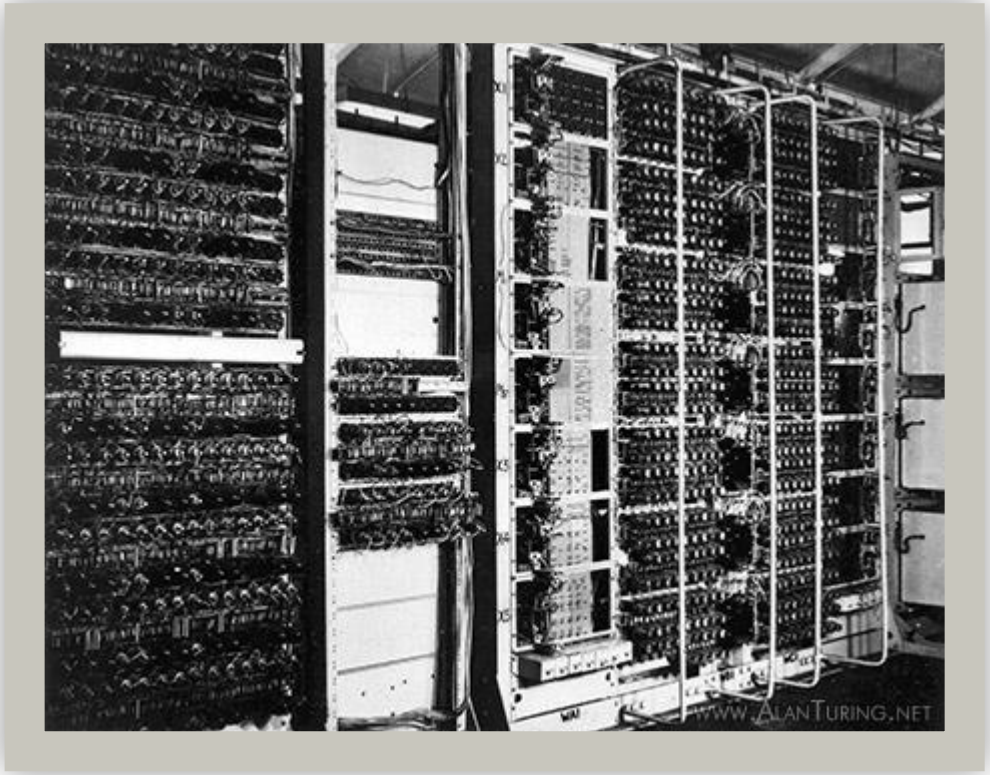
# ПЕРШИЙ ПРОГРАМОВАНИЙ ЕОМ COLOSSUS MARK 2



# Що таке ЕОМ?

**Електронно обчислювальна машина** - комплекс технічних засобів, де основні функціональні елементи (логічні, запам'ятовуючі, індикаційні та ін.) Виконані на електронних елементах, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та



# Війна

7 вересня 1940 для Британії почалася друга світова війна.

Бомбардування Лондона тривало 57 ночей поспіль. До кінця травня 1941 більш 20000 мирних жителів були вбиті в результаті бомбардувань.

# Шифр

У 1940 британська служба радіоперехоплення стала помічати радіоповідомлення незвичайного виду. Замість звичайного для радіообміну коду Морзе ці повідомлення мали код Бодо, що застосовувався у телетайпі.

**Телетайп** - електромеханічна друкарська машина, використовувана для передачі між двома абонентами текстових повідомлень по найпростішому

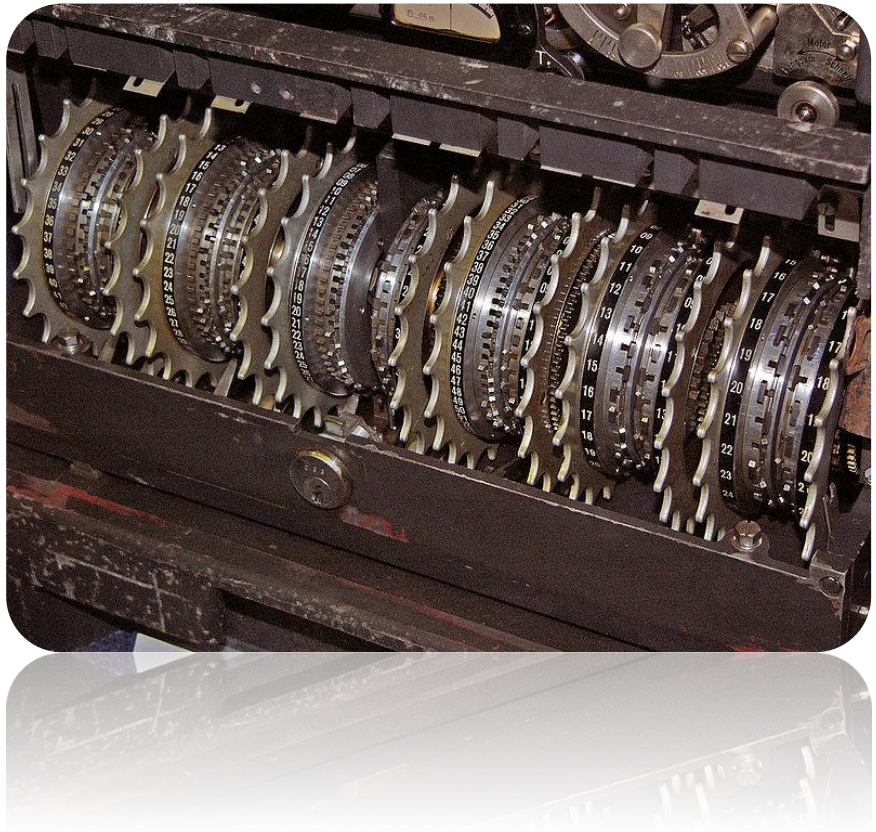
# Блетчлі-парк

Перехоплену радіограму негайно передали в Урядову школу кодів і шифрів (Блетчлі-парк) для детального аналізу. Новий шифр отримав умовну назву «Танні» Для вивчення нового шифру в Блетчлі-парк створили окремий підрозділ, але, незважаючи на це, аналіз просувався

Особняк Блетчли-Парк

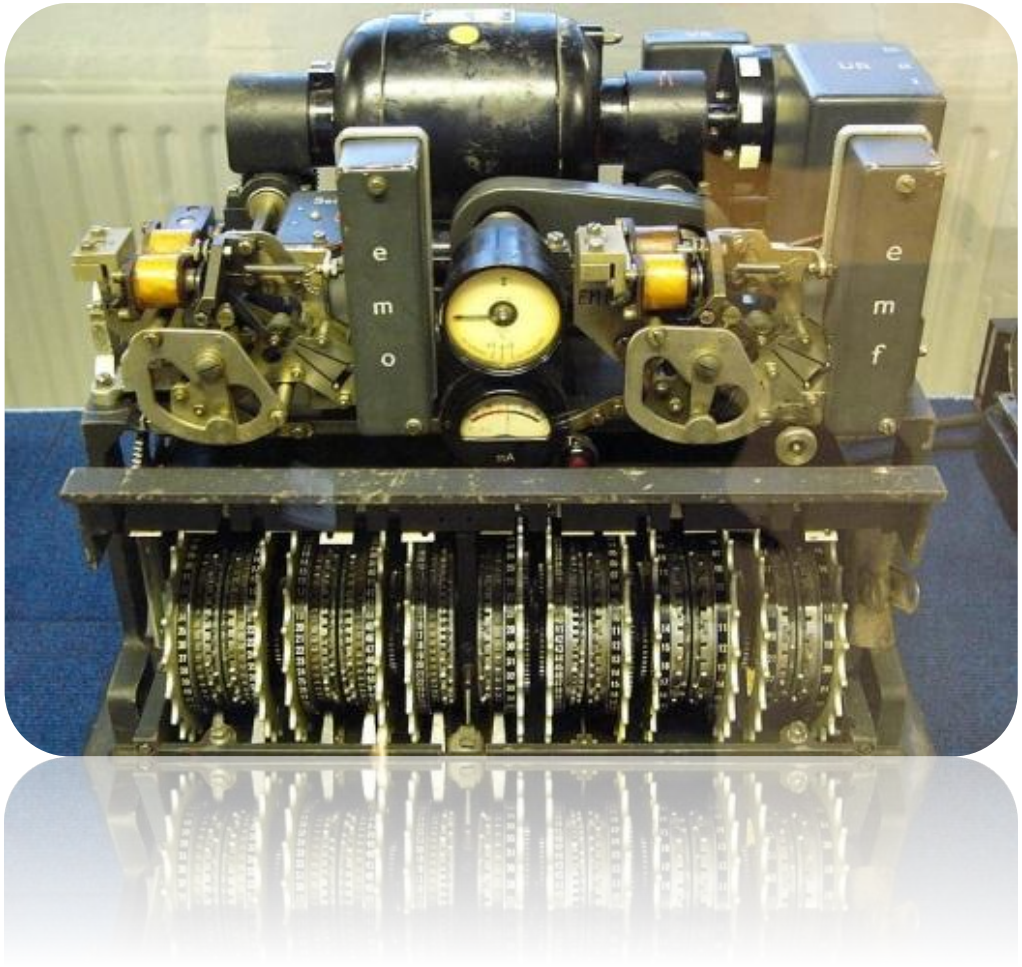
# Помилка

У серпні 1941 року один з німецьких шифрувальників зробив помилку, передавши один за одним два незначно відрізняються радіоповідомлення, зашифрованих за допомогою одного і того ж ключа. Обидві радіограми вдалося перехопити. Це дозволило британцям не тільки розшифрувати текст повідомлення, а й отримати досить довгий уривок шифрувальної послідовності. Стало ясно, що новий німецький пристрій побудований на звичайному принципі шифруючих коліс, але кількість



# Танні (Лоренц)

«**Лоренц**» - німецька шифрувальна машина, що використовувалась під час Другої світової війни для передачі інформації по телетайпу. Британські аналітики називали шифри «Лоренца» і її саму «Танні»



# Початок дешифровки

Отримана інформація дозволяє розшифрувати деякі повідомлення «Танни» вручну, однак це вимагало надто багато часу. Прорив у роботі відбувся завдяки зусиллям Білла Татта, молодого математика з Блетчлі-парку. Татт запропонував використовувати для аналізу методи статистики і побудував статистичну модель «Танні». В результаті йому вдалося з'ясувати, що ключ шифру складається з двох частин. Першою частиною було правило, за яким встановлювалися маленькі механічні наконечники по ободу кожного колеса. Другу частину ключа, названу Колесовим шаблоном, вводив сам оператор для передачі декількох повідомлень (що також було помилкою німецьких шифрувальників)

Білл Татт

# Перші спроби дешифровки

Статистичний аналіз за методом Татта вимагав великого обсягу обчислень, для виконання яких, спільно з інженерами з Dollis Hill, була побудована спеціальна машина, що отримала назву Heath Robinson (по імені героя коміксів, який будував хитромудрі пристрої). Машина мала швидкісне введення з перфострічок і електронні логічні схеми. Її призначенням було обчислення положення дисків «Лоренца». Машина дозволила розшифровувати повідомлення «Танні», але працювала недостатньо швидко (Усього 1000 знаков у секунду) і, крім того, була недостатньо надійною.

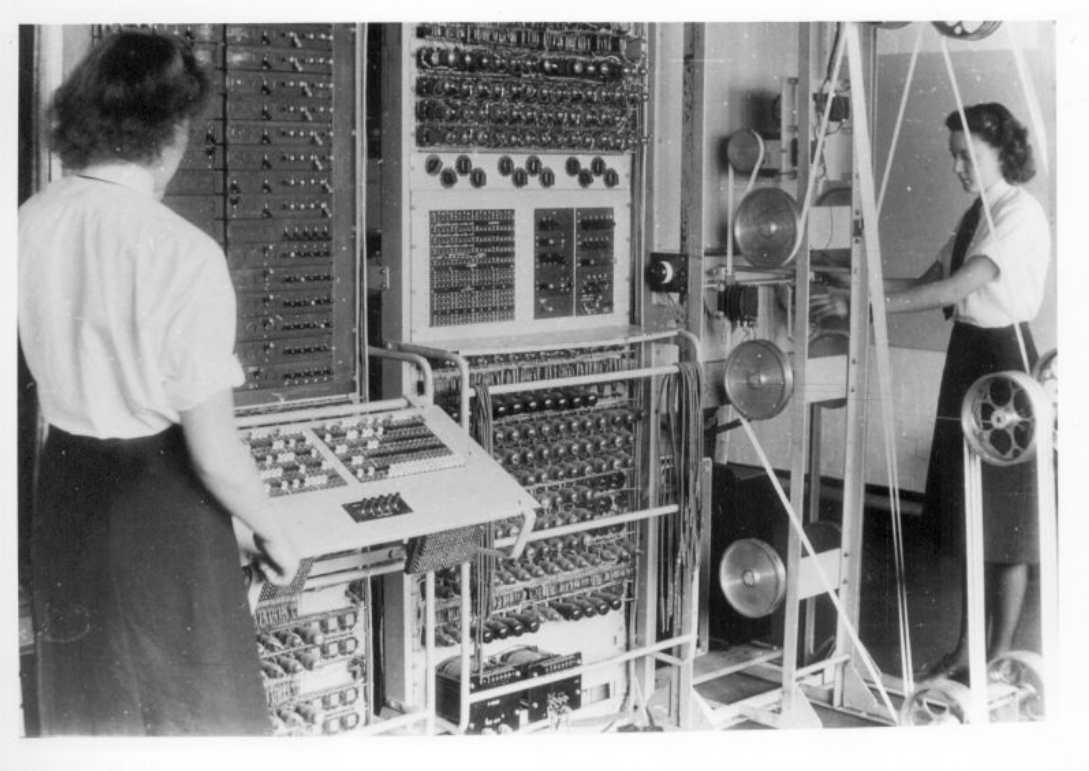
# Початок проекта

Томас Флауерс побачивши недоліки Heath Robinson томас почав проектувати свою ЕОМ. Він вирішив перенести весь процес моделювання роботи шифру на лампові схеми. Завдяки цьому кількість вхідних стрічок скоротилося до однієї, проблема синхронізації зникла, а швидкість зчитування підвищилася до 5000 знаків у секунду. До того ж, у порівнянні з Heath Robinson, нова машина працювала набагато стабільніше. Отримана схема складалася з 1500 електронних ламп і дозволяла розшифровувати повідомлення за

**Томас Гарольд Флауерс -** народився в Лондоні 22 грудня в 1905 році британський інженер. Спеціаліст з вакуумної техніки. Під час Другої світової війни Флауерс керував будівництвом «Колоса»

# Праця Colossus

За допомогою «Colossus» вдалося розшифрувати код, що застосовувався для передачі повідомлень вищих чинів нацистської Німеччини , що внесло значний внесок в перемогу



Colossus у блетчлі-парк

# Colosus Mark II

Влітку 1944 року була представлена нова версія Colossus Mark II, що складаєлася вже з 2500 електронних ламп. Новая модель працювала в 5 разів швидше свого попередника. Відмінною особливістю Mark II була можливість програмування.

Colossus Mark II є першою машиною подібного класу, прообразом сучасних програмованих пристроїв.

На основі схем з електронними лампами був побудований Colossus

# Забуття

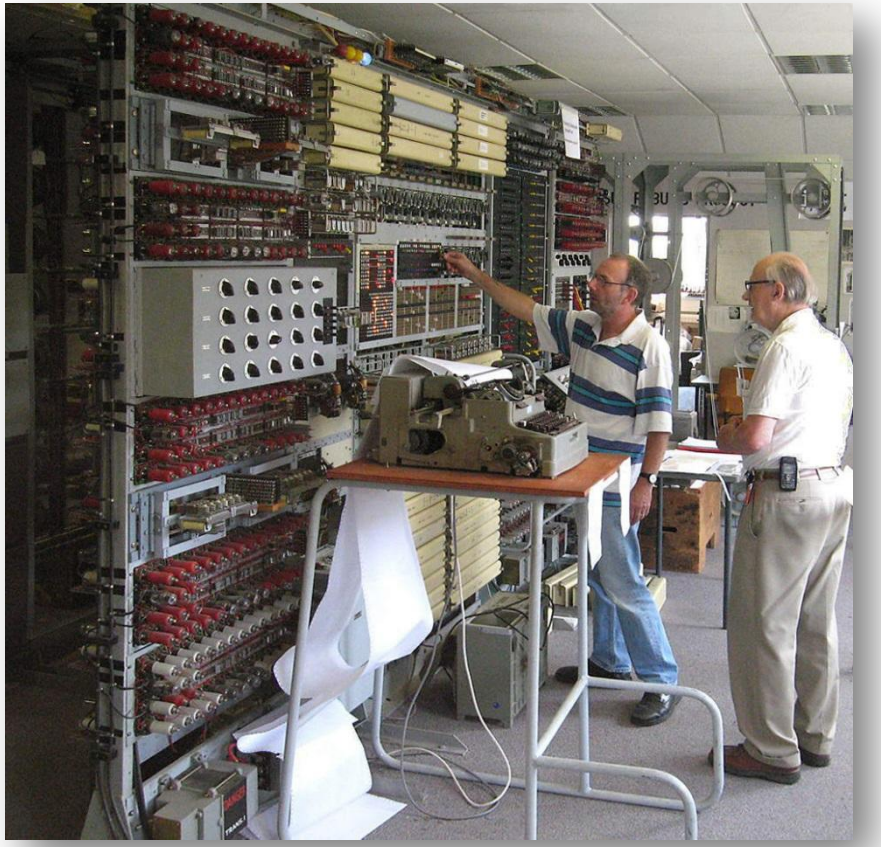
Після закінчення Другої Світової війни необхідність в комп'ютерах класу Colossus відпала через їх вузької специфічною спрямованості. Високий рівень секретності не дозволяв занести Colossus у відкриті джерела з історії обчислювальної техніки аж до жовтня 2000 року (офіційне зняття таємності). Однак, інформація про існування проекту почала просочуватися ще з 1970 року.

Уїнстон Черчілль особисто підписав указ про руйнування машин, однак, деякі комп'ютери Colossus Mark II продовжували діяти для тренувальних або допоміжних завдань до кінця 1950-х. У 1959-1960 рр зруйнували останні екземпляри. У той же час були знищені всі креслення і схеми, використовувані для побудови Colossus.

**Уінстон Черчілль**

# Відродженя

У 1994 група інженерів на чолі з Тоні Сейлом приступила до відновлення Colossus Mark II, використовуючи фотографії, а також записи і розповіді учасників оригінального проекту. Відновлення проходило в блоці F Блетчлі-парку, в кімнаті, де стояв найперший Colossus. Перше відео з працюючим Colossus було записано вже в 1997 році, однак, повністю відновити комп'ютер вдалося тільки в 2008



Тоні Сейл (Праворуч)

# Снова в строю

За словами Тоні Сейла, відновлений Colossus дешифрує повідомлення приблизно з такою ж швидкістю, як ноутбук з процесором Pentium 2 з відповідним ПО, незважаючи на більш ніж півстолітню різницю в поколіннях. Colossus працює так швидко через його вузьку спрямованость у рішенні лише завдань дешифрування певних шифрів.

Завдяки відновленню Colossus в 2007 році відкрився Національний музей комп'ютерів який також знаходиться в


Ноутбук с процессором Pentium 2

# Джерела

fototelegraf.ru

livejournal.com

cryptohistory.ru

postnauka.ru

wikipedia.org

avito.ru