



АЛАН МЭТИСОН ТЬЮРИНГ

1912-1954

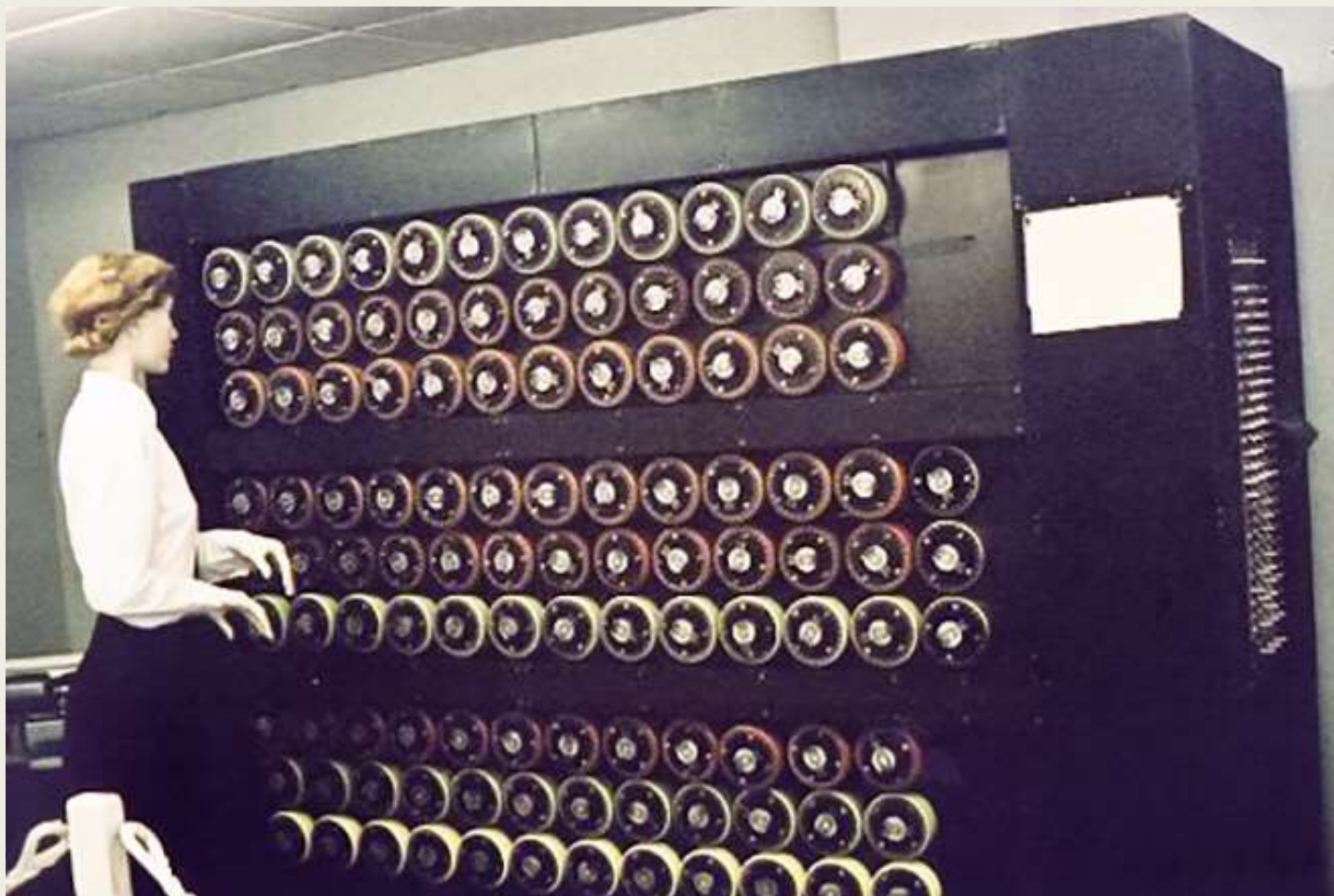
В чем суть разных вкусов и разных пристрастий, если не в том, что наш мозг работает по-разному, и все мы мыслим иначе?" (Алан Тьюринг).

Вкратце:

- Английский математик, логик, криптограф, оказавший существенное влияние на развитие информатики. Кавалер Ордена Британской империи (1945), член Лондонского королевского общества (1951).

- Предложенная им в 1936 году абстрактная вычислительная «Машина Тьюринга», которую можно считать моделью компьютера общего назначения, позволила формализовать понятие алгоритма и до сих пор используется во множестве теоретических и практических исследований.

Машина Тьюринга



- Научные труды А. Тьюринга — общепризнанный вклад в основания информатики (и, в частности, — теории искусственного интеллекта).

Детство и юность:

- Алан Матисон Тьюринг родился в Майда-Вейле, Лондон, 23 июня 1912 года. Школьные учителя признавали необычайные умственные способности Алана, но не придавали им значения. Мальчик посещал престижную школу города Шернборна, где особый интерес проявлял к точным наукам. В биографии ученого содержится ряд интересных фактов. Первый день учебы юноши случайно совпал с началом забастовки, и он был вынужден преодолеть 100 км на велосипеде, чтоб провести ночь в безопасности в отеле, вдали от бунтующей толпы.

Алан Тьюринг появился на свет 23 июня 1912 года в лондонском роддоме в Пэддингтоне. 7 июля его крестили в церкви Святого Спасителя и дали имя Алан Мэтисон Тьюринг.



Университет

В 1931 году Тьюринг поступает в Кембриджский университет.

В университетском Кингз-колледже Алан Тьюринг, бывший в школе самым отстающим учеником, с головой погружается в учебу и науку, самозабвенно изучая математику и квантовую физику.

Однокурсники так же, как и его школьные соученики, считают Тьюринга странным и замкнутым, совершенно далеким от светского университетского сообщества.



Любимый отдых неординарного студента — решение шахматных головоломок и шарад, постановка химических опытов, серьезные занятия греблей и бегом. В это же время, в начале 30-х годов XX столетия, Тьюринг увлекается трудом Джона фон Неймана «Математические основы квантовой механики», которое производит на Алана очень сильное впечатление.

Наука:

В 1936 году вышла работа Тьюринга «О вычислимых числах», в тексте которой Алан ввел понятие универсальной машины (позднее она названа машиной Тьюринга). Машина Тьюринга вычисляла все, что только возможно, концепция современного персонального компьютера базируется на проекте, разработанном Тьюрингом.

- Затем Тьюринг сосредоточился на изучении математики и криптологии на базе Института перспективных исследований в городе Принстоне, штат Нью-Джерси. После защиты докторской диссертации в Принстонском университете в 1938 году молодой ученый вернулся в Кембридж, где устроился на работу на неполный рабочий день в Центр правительственной связи – британскую правительственную организацию, которая работала над взломом шифров.

Криптоанализ

Во время Второй мировой войны Алан Тьюринг принимал активное участие во взломе немецких шифров в Блетчли-парке. Историк и ветеран Блетчли-парка Эйза Бриггс однажды сказал:

Блетчли-парку был нужен исключительный талант, исключительная гениальность, и гениальность Тьюринга была именно такой.

С сентября 1938 года Тьюринг работал на полставки в GCHQ — британской организации, специализировавшейся на взломе шифров. Совместно с ДиллиНоксом он занимался криптоанализом "Энигмы". Вскоре после встречи в Варшаве в июле 1939 года, на которой польское Бюро шифров предоставило Великобритании и Франции подробные сведения о соединениях в роторах "Энигмы" и методе расшифровки сообщений, Тьюринг и Нокс начали свою работу над более основательным способом решения проблемы. Польский метод основывался на недоработках индикаторной процедуры, которые немцы исправили к маю 1940 года. Подход Тьюринга был более общим и основан на методе перебора последовательностей исходного текста, для которого он разработал начальную функциональную спецификацию Bombe.

Машина Тьюринга-Велшмана

В течение нескольких недель после прибытия в Блэтчли-парк Тьюринг написал спецификации к электромеханической машине, которая могла помочь со взломом «Энигмы» более эффективно, чем польская «криптологическая бомба». Машина Тьюринга с улучшениями, предложенными математиком Гордоном Велшманом, стала важнейшим инструментом для расшифровки сообщений «Энигмы». Машина получила название Bombe.

Машина искала возможные настройки, использованные для шифрования сообщений (порядок роторов, положение ротора, соединения коммутационной панели), опираясь на известный открытый текст. Для каждой возможной настройки ротора (у которого было 10^{19} состояний или 10^{22} в модификации, использовавшейся на подводных лодках) машина производила ряд логических предположений, основываясь на открытом тексте (его содержании и структуре). Далее машина определяла противоречие, отбрасывала набор параметров и переходила к следующему. Таким образом, большая часть возможных наборов отсеивалась и для тщательного анализа оставалось всего несколько вариантов.

Вторая мировая война

- Во время Второй мировой войны Тьюринг стал ведущим участником расшифровки шифров немцев. Он работал в Bletchley Park, на станции военного времени GCCS, где совершил пять крупных открытий в сфере криптоанализа, включая разработку электромеханического устройства, используемого в целях расшифровки сигналов шифровальной машины Германии «Enigma».

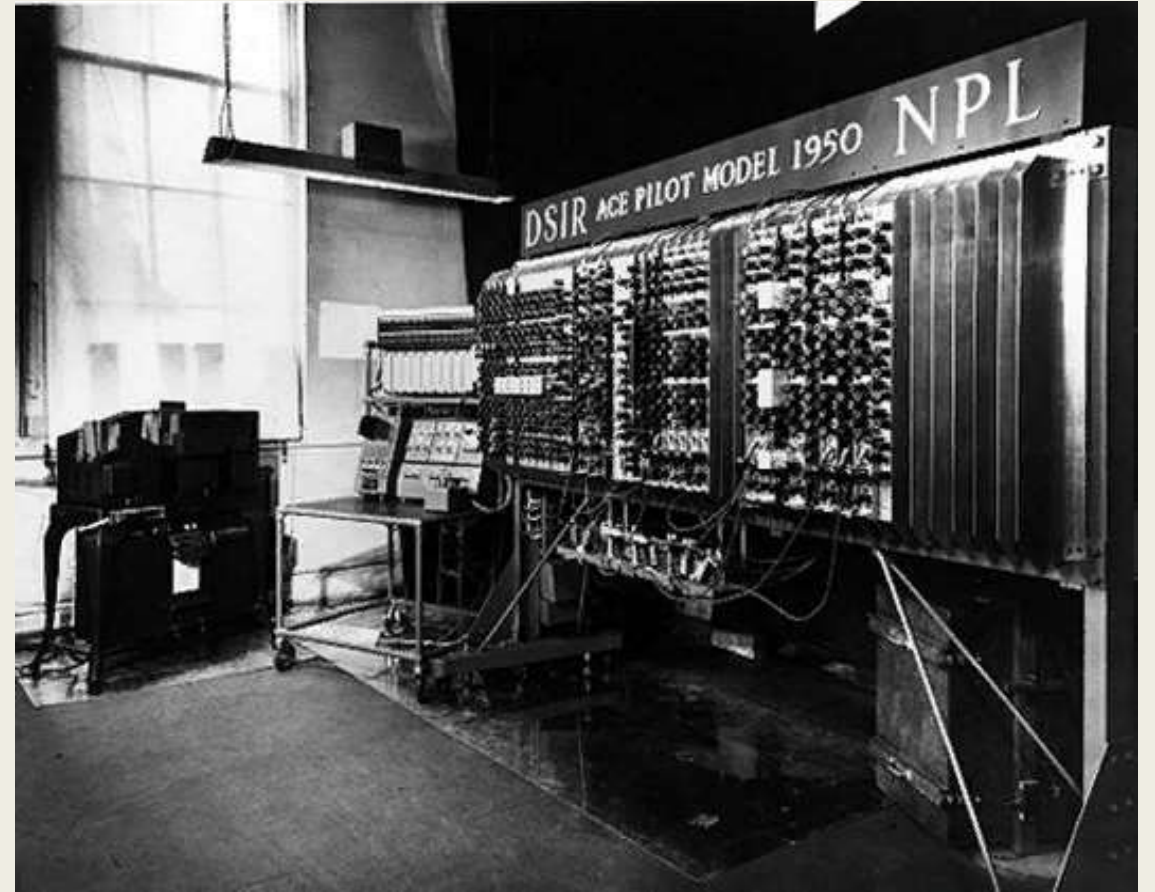
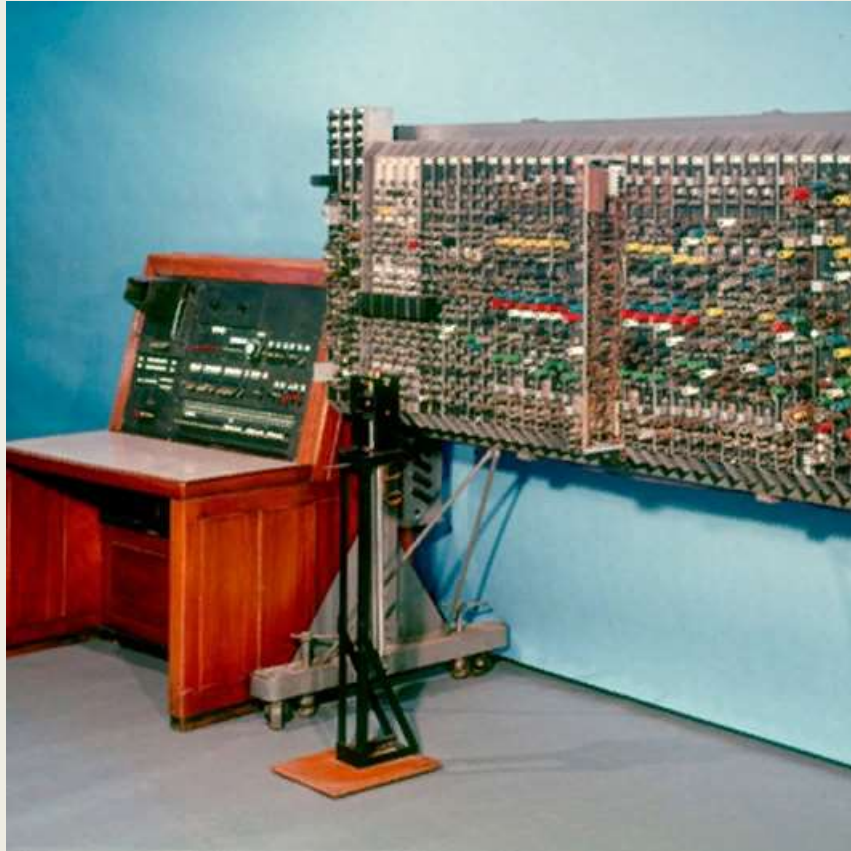
Энигма



Первые образцы Энигмы появились в 20-х годах прошлого столетия. Машина активно использовалась Германией в годы второй Мировой Войны для передачи сообщений между подразделениями и командованием. Хотя устройство механизма было известно, долгое время ее шифр считался не поддающимся взлому. Лучшие лингвисты и математики по всему миру боролись с загадкой Энигмы пока в 1932 году группе польских ученых, основываясь на математических методах и методах обратной обработки, не удалось расшифровать код. Но даже после этого проблема оставалась острой, поскольку устройство машины было усложнено. В 1940 году английский математик Алан Тьюринг построил первый образец другую машины, способной решить задачу расшифровки путем подбора исходного кода.

Ранние компьютеры

С 1945 по 1947 год Тьюринг проживал в Ричмонде и работал над ACE (англ. Automatic Computing Engine) в Национальной физической лаборатории. 19 февраля 1946 года он представил работу, которую можно назвать первым детальным описанием компьютера с хранимой в памяти программой. Незаконченная работа «Первый проект отчёта о EDVAC» (1945) Фон Неймана предшествовала ей, но была намного менее детальна.



- Вклад Тьюринга в процесс взлома кодов этим не ограничивается: Алан также написал две статьи о математических подходах к дешифровке кода, которые считаются стратегически важными активами Кодекса и школы Surpher (позже известной как штаб-квартира правительства)

- Тьюринг умер 7 июня 1954 года. Миссис Кристи (домработница Алана) приготовила хозяину завтрак и поднялась в спальню, чтобы позвать Тьюринга к столу, но обнаружила в постели бездыханное тело ученого, а на прикроватном столике лежало надкушенное яблоко. После посмертной экспертизы выяснилось, что причиной смерти было отравление цианидом.



Кино

На экраны вышел фильм «Игра в имитацию» с Кирой Найтли и Бенедиктом Камбербэтчем в главных ролях. Последний сыграл знаменитого учёного Алана Тьюринга, разгадавшего код «Энигмы» - шифровальной машины, использовавшейся во вторую мировую немцами.

