

Alan Turing

Introduction

Alan Turing student på King's College, Cambridge deltog i dekryptandet av enigma maskinen. Turing var också väldigt intresserad av Artificiell intelligens(AI). Turing satte upp regler för när en dator är lika smart som en människa.

Turings uppväxt

Alan Turing föddes och växte upp i Maida Vale som är ett distrikt i London. Turings föräldrar kommer från en handels familj i Skottland. Redan i tidig ålder kunde hans föräldrar se att han hade geni drag som han senare använde för att göra ett avtryck på världen.

Utbildning

När Turing blev gammal nog så satte hans föräldrar honom på en dagskola som hette "St Michael's" som låg på "20 Charles Road" när han var 6 år gammal. Hans fröken insåg snart hans talang och det gjorde även många av de andra lärarna. Mellan 1922 och 1926 gick Turing ut på "Hazelhurst Preparatory School" en skola som låg i en by som hette "Frant in Sussex" nu mera kallad "East Sussex". När Turing blev 13 år gammal började han på Sherborne School i en handelsstad som hette "Sherborne". Första dagen på terminen, han bodde då 97 km ifrån skolan och cyklade hela vägen men övernattade på ett värdshus han hade en ostoppar vilja. Men på skolan trots sin naturliga talang inom matte och fysik ämnen fick han ingen större respekt från några av lärarna på skolan vars definition av utbildning var riktad mer åt det klassiska. Hans rektor skrev till Turings föräldrar och skrev: "I hope he will not fall between two stools. If he is to stay at public school, he must aim at becoming educated. If he is to be solely a Scientific Specialist, he is wasting his time at a public school".

Trots detta fortsatte Turing på skolan och visade enastående resultat från dem ämnena han älskade. Han löste avancerade problem utan att ha studerat jämn elementär kalkyl då han bara var 15 år gammal. När Turing fyllde 16 stötte han på Einstein's ifrågasättande av Newton's lagar om rörelse. Inte bara förstod han utan det är möjligt att han lyckades härleda ifrågasättandet från en text där det aldrig gjordes gjordes uttryckligt. På skolan träffade Turing sin första kärlek, en kille som hette Christopher Morcom som senare dog i tuberkulos på grund av infekterad mjölk han hade druckit något år tidigare. Detta fick Turing att må väldigt dåligt men det gjorde bara att han började arbeta hårdare än någonsin inom deras gemensamma ämnen. Turing skrev ett brev till Morcom's mamma:

"I am sure I could not have found anywhere another companion so brilliant and yet so charming and unconceited. I regarded my interest in my work, and in such things as astronomy (to which he introduced me) as something to be shared with him and I think he felt a little the same about me ... I know I must put as much energy if not as much interest into my work as if he were alive, because that is what he would like me to do".

Efter hans studier på Sherborne började han studera på King's College i Cambridge. Där han fick första klass heder inom matematik. När han blev 22 år gammal blev han utvald till en medlem av en forsknings grupp där han bevisade den centrala gränsteorin. 1936 publicerade Turing en rapport "on Computable Numbers, with an Application to the Entscheidungsproblem". Han tog Kurt Gödels resultat och bytte ut hans universella aritmetiska språk med formulär och hypotetiska maskiner som kommer att bli kallade "Turing Machines". Turing kunde då bevis att hans maskin kunde lösa vilken tänkbar matematisk beräkning som helst så länge den var uttryckt i ettor och nollor. Han bevisade även att man inte kunde beräkna algoritmetiskt ifall hans turing machine någonsin kommer att stanna. En idag är turing maskiner en central del i "theory of computing" läran.

Dekryptandet av Enigma

Under andra världskriget hade tyskarna upptäckt att man kunde använda radiosignaler för att snabbt skicka meddelanden på slagfältet. Efter som Tyskarna använde sig av radiosignaler kunde andra länder fånga upp deras signaler. Då behövde Tyskarna ett sätt att koda deras meddelanden(krypta meddelanden). Då utvecklade Tyskarna en Maskin som skulle göra om läsbar text till en obegriplig kod. Denna Maskin kallades För "The Enigma Machine".

Maskinen var byggd som en gammal skrivare men tangenterna var kopplade på ett sätt som gjorde att ett "A" på tangentbordet blev ett V på pappret men tryckte du på ett "A" en gång till så blev det inte längre ett "V" utan kunde istället bli en annan bokstav ur alfabetet. Maskinen funkade så att man tryckte på exempelvis ett "A" då skickades signalen "A" till en rotor som liknade ett kodlås fast större med bokstäver istället för siffror. signalen togs emot av rotorn som kunde vara exempelvis inställd på ett G då ändras våran "A" signal till ett G istället. Men för att göra det mer krångligt så hade rotorn en insida där sladdar kopplade om bokstäverna, så vårat "G" exempelvis var kopplat till ett "R" efter signalen gått igenom rotorn så lämnade rotorn signalen "R". Denna sortens rotor gick signalen igenom 3 gånger. så tillslut kanske signalen var ett "H" när den lämnade rotorerna. Då gick signalen till tangenterna som var omkopplade där med. Och dem gick att koppla på 100 000 000 000 000 olika sätt.

Men efter du tryckt på "A" tangenten en gång så roterade en rotor tex första trycket var den inställd på AAA andra trycket AAB och gav ut en annan slut signal. Detta gjorde att det såg ut som att koden inte följde något speciellt mönster. Eftersom man kunde ha så många olika start inställningar på maskinen. Tex kunde man koppla om alla tangenter till en speciell inställning ändra rotorerna så att dem startade i olika lägen, ändra hur rotorerna var kopplade på insidan. Detta gjorde att antalet olika permutationer låg över 300 000 000 000 000 000 000 inställningar.

Detta ser nästintill omöjligt ut att Knäcka. Men Maskinen hade en stor svaghet, om man tryckte på "A" var det omöjligt att få ett "A" på pappret det gick alltså inte att få samma input som output. Så om det på pappret fanns ett A kunde man veta att på den positionen kan det inte finnas något A. Detta var gamebreaking då man kunde eliminera massa permutationer.

Detta är något otroligt komplicerat och det ligger mycket mer bakom dekryptandet. Men jag tänker gå in på vad turing hade för medvärkan.

Turing placerades i hemlighet på ett Project att knäcka enigma koden.

Turing skapade då en maskin "Bombe" som var en stor maskin med 36 rotorerna som representerade sex trerotor enigmas fast Bomben jobbade baklänges för att hitta rotorernas potentiella grund inställningar och provade all permutationer som rotorerna kunde ha efter en potentiell matchning. Ifall bombe hittade en potentiell match stannade maskinen och så fick man prova på en riktig enigma maskin britterna fått tag på. Det fanns 200 bombe i storbritannien. Turings maskin gjorde så att krigets längde minskades med ca 2 år. Efter kriget tog man sönder alla bombe för att inte avslöja hur dem fungerade.

Efter kriget så blev turing dömd för att vara homosexuell som var förbjudet under den tiden. Han dömdes till fängelse och fick inte fortsätta sina studier. Så turing tog tragiskt sitt liv, han dog 41 år gammal. 50 år senare tog dem tillbaka domen och erkände ett misstag. Det spekuleras om att han tog ett bett ur ett förgiftat äpple och att det var så "Apple" fick sin berömda logga. Men Appel erkände att det inte var av den anledningen men sa att det hade varit en ära om det var så.

Idag ses Alan Turing som Fadern för modern Datorkunskap och datoranvändning

https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

https://en.wikipedia.org/wiki/Alan_Turing#Early_life

Quora articular.

Youtube documentärer och förklaringar kring både enigma maskinen och bomben.