Alan Turing i njegov doprinos kriptoanalizi i računalstvu

Ivanković, Ana-Marija

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ODJEL ZA FIZIKU

ANA-MARIJA IVANKOVIĆ

ALAN TURING I NJEGOV DOPRINOS KRIPTOANALIZI I RAČUNALSTVU

Diplomski rad

Osijek, 2016.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ODJEL ZA FIZIKU

ANA-MARIJA IVANKOVIĆ

ALAN TURING I NJEGOV DOPRINOS KRIPTOANALIZI I RAČUNALSTVU

Diplomski rad

predložen Odjelu za fiziku Sveučilišta J. J. Strossmayera u Osijeku

zbog stjecanja zvanja magistra edukacije fizike i informatike

Osijek, 2016.

Ovaj diplomski rad je izrađen u Osijeku pod vodstvom izv. prof. dr. sc. Darka Dukića u sklopu Sveučilišnog diplomskog studija fizike i informatike na Odjelu za fiziku Sveučilišta Josipa Jurja Strossmayera u Osijeku.

SADRŽAJ

Sveučilište J. J. Strossmayera u Osijeku
Odjel za fiziku

Diplomski rad

ALAN TURING I NJEGOV DOPRINOS KRIPTOANALIZI I RAČUNALSTVU

ANA-MARIJA IVANKOVIĆ

Sažetak

Predmet izučavanja ovog diplomskog rada je životni put i doprinos kriptoanalizi i računalstvu znamenitog britanskog matematičara, kriptografa, logičara i vizionara, te čovjeka osebujnog karaktera i uma, Alana Mathisona Turinga. Nakon uvoda, upoznat ćemo se s Turingovim djetinjstvom, školovanjem i profesionalnom karijerom, kao i kontroverzama vezanim uz njegovu smrt. Zatim će se detaljnije ukazati na njegove najvažnije doprinose u području kriptoanalize i računalstva. Pri tome će se posebno istaknuti Turingova uloga u pobjedi Saveznika u Drugom svjetskom ratu. Na kraju će se pokušati odgovoriti kako se prema Turingu i njegovom radu odnosi suvremeno društvo. Alan M. Turing je po mnogočemu bio ispred svog vremena pa tek počinjemo biti svjesni njegove važnosti za svijet u kojem danas živimo.

(40 stranica, 17 slika, 1 tablica, 18 literaturnih navoda)

Rad je pohranjen u knjižnici Odjela za fiziku

Ključne riječi: Alan M. Turing/kriptoanaliza/računalstvo/Turingov stroj

Mentor: izv. prof. dr. sc. Darko Dukić

Ocjenjivači: izv. prof. dr. sc. Branko Vuković, izv. prof. dr. sc. Ramir Ristić

Rad prihvaćen: 11. srpnja 2016.

J. J. Strossmayer University in Osijek
Department of Physics

Master Thesis

ALAN TURING AND HIS CONTRIBUTION TO CRYPTANALYSIS AND COMPUTING

ANA-MARIJA IVANKOVIĆ

Abstract

The case study of this thesis is Alan Mathison Turing's life and contribution to cryptanalysis and computing. Alan Turing was famous British mathematician, cryptographer, logician and visionary, and a person of a distinctive character and mind. After the introduction, we will explore Turing's childhood, education, and professional career, as well as the controversies related to his death. In the next section, his most important contributions in the field of cryptanalysis and computing will be discussed in detail. Thereby, a particular emphasis will be put on Turing's role in the Allied victory in World War II. In the end, an attempt will be made to answer how the modern society refers to Turing and his work. Alan M. Turing was in many ways ahead of his time, and we are just starting to realise his importance for the world we live in today.

(40 pages, 17 images, 1 table, 18 references)

Thesis deposited in Department of Physics library

Keywords: Alan M. Turing/cryptanalysis/computing/Turing machine

Supervisor: Darko Dukić, PhD, Associate Professor

Reviewers: Branko Vuković, PhD, Associate Professor, Ramir Ristić, PhD, Associate Professor

Thesis accepted: July 11, 2016

1. UVOD

„*Ponekad ljudi o kojima nitko nema posebno mišljenje učine stvari koje nitko nije mogao zamisliti.*“[1]

Razni oblici komunikacije sveprisutni su kroz tisućljeća ljudske civilizacije, a potreba za sigurnim komunikacijama vezana je ponajprije uz ratove. Veliki sukobi, poput Prvog i Drugog svjetskog rata, tu su potrebu podigli na najvišu razinu. Svaka komunikacija se sastoji od niza uređenih podataka – informacija, koje imaju ključnu ulogu u razvitku društva znanja i kritičkog načina razmišljanja. Shodno tome, kao posebna grana matematičke statistike i teorije vjerojatnosti nastala je teorija informacije. Teorija informacije se, između ostalog, bavi proučavanjem informacije, komunikacijskog sustava, prijenosom podataka, kompresijom podataka i kriptografijom.

Kriptografija je znanstvena disciplina kojoj je najvažniji zadatak pretvaranje jasnog i razumljivog sadržaja u sadržaj koji je razumljiv samo onima kojima je upućen, a njezini su temeljni pojmovi: ključ, šifriranje i dešifriranje. Ključ je podatak kojim se uz pomoć poznatog algoritma dolazi do prvotne poruke i obrnuto. Šifriranjem se poruka pretvara u nerazumljiv oblik svima, osim onima kojima je upućena, a dešifriranjem se nerazumljiva poruka pretvara u razumljivu. Kriptoanaliza se bavi proučavanjem kriptografskih sustava s ciljem njihovog razumijevanja kako bi se otkrio šifrirani sadržaj.

Glavnu ulogu u kriptiranoj komunikaciji između njemačkih vojnih jedinica u Drugom svjetskom ratu je imao stroj kojeg je 1919. godine patentirao i konstruirao njemački inženjer Arthur Scherbius (1878.–1929.), a nazvao ga je Enigma. O važnosti i složenosti ovog stroja bit će riječi kasnije u radu, ali treba napomenuti da ga je 1926. godine njemačka mornarica počela koristiti kao sustav zaštite informacija, a uz nekoliko izmjena i njemačka kopnena vojska te zrakoplovstvo. Nacistički vođa Adolf Hitler je bio uvjeren da je ovaj stroj nemoguće „iznenaditi“, a time i pročitati tajne poruke koje su se preko njega slale. Zahvaljujući suradnji francuskih i poljskih obavještajnih agenata, koji su se domogli postavki uređaja Enigme, talentirani poljski matematičar Marian Rejewski (1905.–1980.), primjenom raznih matematičkih metoda, osmišljava način kako dešifrirati Enigmu i pomoći poljskoj obavještajnoj službi u

[1] Citat iz filma „Igra oponašanja“ (eng. *The Imitation Game*), redatelja Mortena Tylduma iz 2014. godine koji je rađen prema knjizi Andrewa Hodgesa „Alan Turing: The Enigma“ iz 1983. godine.

praćenju njemačke vojne komunikacije. No, njegov uspjeh nije potrajao dovoljno dugo jer su Nijemci ponovno izmijenili uređaj i povećali broj mogućih kombinacija. Poljaci su shvatili koliko je situacija vrlo ozbiljna i složena te su rezultate svog rada, uključujući planove i nacrte Rejewskog, proslijedili britanskim i francuskim saveznicima.

Drugi svjetski rat je počeo te svjesni opasnosti koja se sprema, Britanci osnivaju poseban ured nazvan Vladina škola za kodove i šifre (eng. *Government Code and Cypher School*) sa sjedištem u Bletchley Parku, sjeveroistočno od Londona. Tu su okupili grupu talentiranih znanstvenika i stručnjaka među kojima je bio i Alan Mathison Turing. On je u proljeće 1940. godine, koristeći suvremene matematičke metode, otkrio proceduru dešifriranja poruka uz pomoć kopija stroja Enigme, bez poznavanja dnevnog ključa. Usavršavanjem poljske verzije uređaja za dešifriranje Enigme, naziva Bomba, uspostavlja koncept algoritma i matematički model računala poznatijeg kao Turingov stroj.

Postavši uspješan u području kriptoanalize, Turing provodi više vremena u radu sa strojevima, ali i počinje postavljati brojna pitanja vezana uz povezanost strojeva i čovjeka. Mogu li strojevi s ljudima komunicirati ljudskim jezikom? Mogu li strojevi imati uvjerenja i slobodnu volju? Mogu li strojevi pogriješiti? Mogu li strojevi osjećati? Mogu li strojevi biti „začarani“ idejama, ljudima, drugim strojevima? Mogu li se strojevi zaljubiti te koje bi bile odgovarajuće društvene norme za zaljubljene strojeve? Mogu li se strojevi naljutiti i patiti? Mogu li ljutiti strojevi, pokazati svoje zatomljene osjećaje odlaskom iz kuće i otrčati maratonsku utrku?[2] Brojna od ovih pitanja povezana su i s njegovim unutarnjim stanjem svijesti, ali za njega su predstavljala i temeljna znanstvena pitanja vezana uz razvoj umjetne inteligencije. Alan M. Turing, kako je navedeno u prvoj rečenici ovog uvodnog dijela, zaista je bio čovjek o kojem se dugo vremena malo znalo i o kome nitko nije imao nekakvo posebno mišljenje, no učinio je nezamislive stvari. Svijet i ljudi, koje je toliko mnogo zadužio, na kraju će ga odvesti u smrt. Privatni i profesionalni život ove jedinstvene osobe bit će ukratko prezentirani u sljedećem poglavlju, a nakon toga će se izdvojiti najvažniji doprinosi Alana M. Turinga kriptoanalizi i računalstvu.

[2] Pitanja nastala po uzoru na predgovor knjige: Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. xi-xii.

2. ŽIVOTOPIS ALANA M. TURINGA

U ovom dijelu upoznat ćemo se s djetinjstvom, školovanjem, prvim doticajem sa znanošću te profesionalnom karijerom Alana M. Turinga. Nakon toga će se izdvojiti neke od kontroverzi vezane uz Turingovu smrt.

2.1. DJETINJSTVO

Prezime „Turing" je normanskog porijekla, no kako se početkom 14. stoljeća obitelj naselila u Aberdeenshire u Škotskoj, te tamo ostala i do danas, može se smatrati i da je škotskog porijekla. Posljednje slovo prezimena, *g*, je nadodano od strane Sir Williama Turinga iz Aberdeenshirea za vrijeme vladavine škotskog kralja Jamesa VI., odnosno engleskog kralja Jamesa I.[3] „Sreća prati hrabre" bilo je geslo obitelji Turing, no koliko god su se trudili biti hrabri, nikada nisu bili dovoljno sretni. Mnogi stariji članovi obitelji su umrli bez muških nasljednika pa je početkom 20. stoljeća obiteljska loza Turinga bila jako mala.

Alanov djed, John Robert Turing (1723.–1828.) je diplomirao matematiku 1848. godine kao jedanaesti u klasi studenata na Trinity Collegeu, sveučilišta Cambridge, no ubrzo se prestaje baviti matematikom zbog zvanja svećenika. Ženi se devetnaestogodišnjom Fanny Boyd s kojom će dobiti desetero djece.[4]

Julius Mathison Turing (1873.–1947.), Alanov otac, unatoč tome što nije naslijedio matematičke sposobnosti, bio je darovit student književnosti i povijesti, i kao takav je dobio stipendiju za Corpus Christi College na sveučilištu Oxford, gdje je i diplomirao 1894. godine. Poslije diplome je postao civilni dužnosnik u Indiji. Nakon desetljeća obavljanja dužnosti, u travnju 1907. godine se odlučuje vratiti u Englesku kako bi, između ostalog, pronašao suprugu i oženio se. Pri ukrcaju na brod kojim se vraćao u Englesku upoznao je Alanovu majku Ethel Saru Stoney.[5]

[3] Cooper, S. B., Van Leeuwen, J. (ur.): Alan Turing: His Work and Impact. Amsterdam: Elsevier, 2013., str. 5.
[4] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 4.
[5] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 5-7.

Slika 1. Julius Mathison Turing oko 1907. godine

Izvor: Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983. (list of plates)

Alanova majka, Ethel Sara (1881.–1976.), poticala je iz dobrostojeće obitelji Stoney, u kojoj su bili vrsni znanstvenici i matematičari. Stoneyevi su bili englesko–irska obitelj, porijeklom iz Yorkshirea. Sa sedamnaest godina su ju upisali u Cheltenham Ladies College kako bi se riješila nepravilnog, provincijskog izgovora koji nije priličio mladim damama, no ona tamo nije bila ni približno sretna jer je trpjela podcjenjivanja od strane potomaka engleskog nižeg plemstva. Na vlastiti zahtjev je poslije šest mjeseci odlučila otići studirati glazbu i umjetnost u Pariz na sveučilište Sorbonne. No, ni to nije dugo potrajalo jer zaključuje kako je francuski snobizam ravan onome u Engleskoj te se zajedno sa sestrom vraća roditeljima u Indiju.[6] Njezini rođaci su imali više sreće ili strpljenja kada je školovanje bilo u pitanju te je tako 1891. godine Sarin daljnji rođak, irski fizičar George Johnstone Stoney (1826.–1911.), teoretski otkrio i dao ime atomskoj čestici, danas poznatijoj pod imenom elektron. Sarin otac, Edward Waller Stoney (1844.–1931.), je bio glavni inženjer željeznice u Madrasu u Indiji. Troje iz obitelji Stoney su postali članovima britanskog Kraljevskog društva.[7]

[6] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 7.
[7] Cooper, S. B., Van Leeuwen, J. (ur.): Alan Turing: His Work and Impact. Amsterdam: Elsevier, 2013., str. 5.

Alanovi roditelji su se vjenčali 1907. godine u Dublinu u Irskoj, a u siječnju 1908. godine su se vratili natrag u Indiju. Očev prvi dopust obitelj Turing koristi za povratak u Englesku pa je Alan rođen u Londonu 23. lipnja 1912. godine. Zbog obveza, Alanov otac se ubrzo morao vratiti u Indiju, a Alanova majka je kratko ostala s Alanom i njegovim starijim bratom Johnom.[8]

Kako su se bojali da će indijske vrućine naštetiti zdravlju djece, roditelji su odlučili ostaviti Alana i njegovog brata umirovljenom pukovniku Wardu i njegovoj ženi na čuvanje. Oni su živjeli u malom priobalnom gradiću St. Leonards–on–Sea, blizu Hastingsa, na jugoistoku Engleske. Osim Wardovih, za Alana i brata se brinula i dadilja Thompson, koja je bila njihova prva učiteljica. Dadilja je Alana opisala kao dječaka s vrlo neobičnim osobinama. U sjećanje joj se snažno urezalo Alanovo poštenje i inteligencija, koji su bili vrlo izraženi za dječaka njegovih godina. Igrajući se s njim, ponekad je pokušala namjestiti Alanu pobjedu u igri, no on je uvijek odbijao kršiti pravila na takav način.[9]

Slika 2. Alan Turing kao petogodišnjak

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 3.

[8] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 7-9.
[9] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 9-13.

Alanova majka je provela nekoliko mjeseci tijekom 1915. godine s djecom, no u jesen se vratila u Indiju. U proljeće 1916. godine cijela je obitelj ponovno zajedno u Engleskoj. Budući da je prijetila opasnost od njemačkih podmornica, roditelji su odlučili kako se neće izložiti opasnosti zajedničkog putovanja. Stoga se otac sam vratio, dok je majka sljedeće tri godine provela s djecom.[10]

Odlazak u crkvu je bila omiljena razonoda gospođe Turing pa je sa sobom vodila i Alana, no njemu nikako nije odgovarao snažan miris tamjana. Majka je s Alanom odlazila i na satove slikanja gdje je zabavljao studentice umjetnosti. Bio je veselo i društveno dijete.[11]

Alan nije imao urođen osjećaj za lijevo i desno te je zbog toga na palcu lijeve ruke napravio crvenu točku i nazvao ju „poznatom točkom". Govorio je da bi kada odraste htio postati liječnikom, što je za njegove roditelje predstavljalo iznimno zadovoljstvo. Stoga ga je majka, u ljeto 1918. godine, poslala na privatne sate latinskog jezika u školu St. Michael u Hastingsu. No, njega latinski jezik nije zanimao, a učenje mu je dodatno otežavao loš rukopis i nemarnost. Ravnateljica te škole nije uočila dječakov jezični talent, već matematički.[12]

Poslije tri godine izbivanja, u veljači 1919. godine, Alanov otac Julius se vratio kući. Nije mu bilo nimalo lako ponovno uspostaviti autoritet nad Alanom. Tijekom ljetnih praznika, Julius je svoju obitelj odveo na daleki sjeverozapad Škotske. Tijekom jednog od izleta, Alan je na temelju putanje leta pčela i mjesta njihovog presijecanja odredio položaj pčelinjeg gnijezda, što je izazvalo oduševljenje kod ostalih članova obitelji. Kada su u prosincu 1919. godine roditelji ponovno otišli u Indiju, Alan se vratio u dom obitelji pukovnika Warda. Nakon gotovo dvije godine majka opet dolazi u Englesku i zaključuje da je Alan, od veselog, razigranog i druželjubivog dječaka, postao povučen, nedruštven i zamišljen. S njim je provela ljetne praznike u Bretanji (Francuska), a zatim ga je pripremala za školu Hazelhurst u Sussexu.[13]

[10] Davis, M.: Na logički pogon: Podrijetlo ideje računala. Zagreb: Naklada Jesenski i Turk, 2003., str. 165.
[11] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 10-11.
[12] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 11.
[13] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 14.

Slika 3. Alan i majka na stijenama St. Lunairea u Bretanji, 1921. godine

Izvor: Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983. (list of plates)

2.2. ŠKOLOVANJE

Alan M. Turing je 1922. godine započeo školovanje u osnovnoj školi Hazelhurst, u koju je išao i njegov stariji brat John. Tu je školu pohađalo 36 dječaka starih između devet i trinaest godina. Alanu se škola nije svidjela, budući da je smatrao da odvraća pažnju od stvari koje su se njemu činile važnima. Sljedeće ljeto je proveo zajedno s bratom i roditeljima u Škotskoj, no ujesen su se majka i otac ponovno vratili u Indiju. Njihov odlazak je Alan teško podnio.[14]

Krajem 1922. godine, Alan je dobio na poklon knjigu Edwina Tenneyja Brewstera „Prirodna čuda koje svako dijete treba znati“ (eng. *Natural Wonders Every Child Should Know*). Alan je kasnije rekao majci kako je ova knjiga bila prva koja mu je otvorila oči prema znanosti te je imala veliki utjecaj na njega. Knjiga je bila vođena idejom da se prirodne pojave mogu opisati znanstvenim dokazima, a ne religioznim pozivanjem na svemoguću silu.[15]

[14] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 14-15.
[15] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 16.

U proljeće 1926. godine Alan polaže prijemni ispit te se upisuje u javnu školu Sherborne koja se nalazila u Dorsetu. Ova škola je bila značajna za nastavak njegovog formalnog obrazovanja. U britanskim javnim školama, koje su u to vrijeme prvenstveno bile namijenjene dječacima, naglasak se stavljao na sportske aktivnosti, posebno na nogomet i kriket, te na klasične predmete, poput grčkog i latinskog jezika i kulture. Školska pravila su regulirali stariji dječaci, nerijetko fizičkim nasiljem nad mlađim kolegama. U takvom okruženju, bez ikakvog ženskog utjecaja, događala su se i intenzivna muška prijateljstva koja su ponekad rezultirala homoseksualnim odnosima.[16]

Osim upisa mlađeg sina u javnu školu, obitelj Turing je u to vrijeme doživjela još jednu veliku promjenu. Alanov otac je nakon 20 godina službe, nezadovoljan svojim položajem, podnio ostavku na mjestu civilnog dužnosnika u Indiji te se sa suprugom vratio u Europu. Kako bi izbjegli plaćanje poreza u Engleskoj, smještaju se u gradu Dinard u Bretanji, na sjeverozapadu Francuske.[17]

Alan je u Sherborneu i dalje neuredno pisao te je pokazivao vrlo slab interes za engleskim i latinskim jezikom. Nasuprot tim predmetima, volio je prirodne znanosti. U četrnaestoj godini je sam utvrdio postupak za izdvajanje joda iz morske trave koju je prikupio na plaži ispred svog novog doma u Dinardu. Profesor kemije je bio oduševljen znanjima do kojih je sam došao, dok je njegov kolega zaključio kako Alan jako brzo usvaja nove pojmove i ima odlike genijalca. U petnaestoj godini je u rješavanju složenijih matematičkih problema bio na puno višoj razini od drugih učenika. Tih se godina razvilo i njegovo intenzivno prijateljstvo s Christopherom Morcomom. Kada je zbog tuberkuloze 1930. godine Morcom umro, bio je to veliki gubitak za Alana.[18]

U prosincu 1930. godine Alan je pokušao izboriti stipendiju za Trinity College, ali ju unatoč odlučnosti i zalaganju nije dobio. Međutim, uspijeva se izboriti za stipendiju King's Collegea, na sveučilištu Cambridge, pa u listopadu 1931. godine započinje preddiplomski studij matematike, kojeg je završio 1934. godine. Sveučilišni počeci su za Alana bili teški. Kako je bio povučen,

[16] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 7.
[17] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 6.
[18] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 8-12.

nije uspijevao uspostaviti društvene odnose. Tome je vjerojatno pridonosilo i to što je tijekom razgovora često zamuckivao i pričao u bujicama riječi. Tijekom studija se bavio veslanjem i trčanjem na duge staze.[19]

U znanstvenom smislu, King's College je pružio Alanu brojne mogućnosti. Na njega su posebno značajno utjecali matematičar Godfrey Harold Hardy (1877.–1947.) i astrofizičar Arthur Stanley Eddington (1882.–1944.). Pozornost profesora je uspio privući svojim dokazom centralnog graničnog teorema. No, ispostavilo se da je do istoga, što Turingu nije bilo poznato, godinama ranije došao finski matematičar Jarl Waldemar Lindeberg (1876.–1932.).[20]

Slika 4. Prolaz u obliku luka na King's Collegeu, 1925. godine

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 15.

[19] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 13-16.

[20] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 18-19.

Nakon završetka studija, u ožujku 1935. godine, postao je član znanstvenog društva na King's Collegeu. Iz tog je vremena poznat njegov interes za jednim od 23 poznata problema njemačkog matematičara Davida Hilberta (1862.–1943.). „Problem odluke“ (njem. *Entscheidungsproblem*) bavi se pitanjem mogućnosti da se za bilo koju pravilno konstruiranu matematičku tvrdnju algoritamski utvrdi je li ispravna. Alan M. Turing je u svom radu „Izračunljivi brojevi s primjenom na problem odluke“ (eng. *On Computable Numbers, with an Application to the Entscheidungsproblem*), koji je publiciran 1936. godine, pokazao da to nije moguće. Neovisno o njemu, do istog je zaključka došao i američki matematičar i logičar Alonzo Church (1903.–1995.) pa je po njima nazvana poznata Church–Turingova teza. Poslije objavljivanja rada, Alan odlazi na postdiplomski studij na američko sveučilište Princeton, gdje mu mentor postaje upravo Alonzo Church. Na tom je sveučilištu doktorirao u lipnju 1938. godine obranivši disertaciju pod naslovom „Sustav logike temeljen na ordinalnim brojevima“ (eng. *Systems of Logic Based on Ordinals*).[21]

Slika 5. Henry Burchard Fine Hall na sveučilištu Princeton, zgrada Odsjeka za matematiku

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 37.

[21] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 35-37.

Mađarsko–američki matematičar John von Neumann (1903.–1957.) je uočio Alanov potencijal te mu je čak ponudio posao asistenta, no Turing ga je odbio i 1938. godine se vratio natrag na sveučilište Cambridge.[22]

2.3. PROFESIONALNA KARIJERA

Dan nakon što je Velika Britanija objavila rat Njemačkoj, Alan M. Turing se 4. rujna 1939. godine prijavio u Bletchley Park, u kojem je osnovan poseban ured čiji je glavni zadatak bio dešifriranje neprijateljskih vojnih poruka. Bletchley Park je viktorijansko imanje smješteno na željezničkim čvorištima između sveučilišta Oxford i Cambridge. U početku se tu okupila mala skupina matematičara i sveučilišnih profesora, no do kraja rata se njihov broj značajno povećao.[23]

Slika 6. Zgrada Vladinog ureda u Bletchley Parku

Izvor: Lavington, S. (ur.): Alan Turing and His Contemporaries: Building the World's First Computers. Swindon: British Informatics Society Limited, 2012., str. 2.

[22] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 38.

[23] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 47-48.

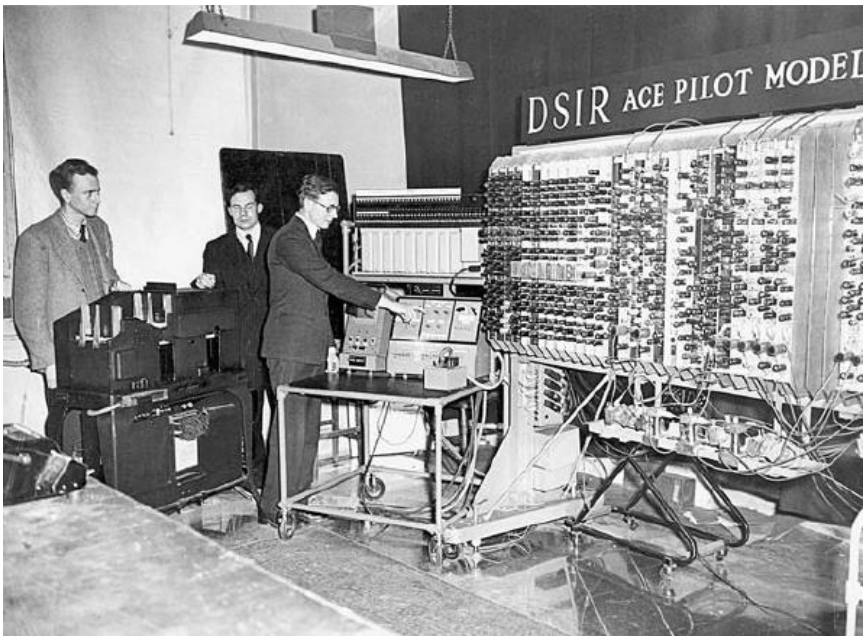
Alan Turing je uložio veliki trud kako bi probio sustav šifriranja koji je koristila njemačka vojska, na taj način razvijajući kriptoanalizu. Uspio je u svom naumu te je osmislio i izradio stroj koji je dešifrirao poruke poslane preko Enigme. Izradom tog stroja značajno je pomogao konačnoj pobjedi Saveznika u Drugom svjetskom ratu.

Turing je tijekom rata sudjelovao i u drugim projektima. U jesen 1943. godine prijavio se u Hanslope Park kako bi radio na dizajnu glasovnog uređaja za šifriranje nazvanog Delilah. Pri tome je surađivao s matematičarom Robinom Oliverom Gandyjem (1919.–1995.) i inženjerom Donaldom Bayleyjem. U ožujku 1944. godine, Turing i njegov tim su pomoću glasovnog uređaja Delilah uspješno šifrirali i dešifrirali Churchillov govor zapisan na traci.[24] No, ovaj glasovni uređaj se pojavio prekasno te se nije koristio za vrijeme Drugog svjetskog rata. Rad na takvom uređaju Turingu je proširilo iskustvo u radu s elektroničkim uređajima, a ono će mu biti od velike pomoći u njegovom kasnijem radu s računalima.

Zbog velikog doprinosa u ratu protiv Njemačke, Turing je 1945. godine nagrađen ordenom Britanskog Carstva, no za razliku od drugih ratnih heroja, nije smio ništa govoriti o poslu kojeg je obavljao. On sam nije pridavao veliko značenje ovakvom priznanju te je medalja koju je dobio pronašla svoje mjesto u ladici.[25]

U listopadu 1945. godine Turing odlazi u Nacionalni fizikalni laboratorij (eng. *National Physical Laboratory*) u Londonu, gdje započinje rad s računalima. Cilj mu je bio uz pomoć inženjera Nacionalnog fizikalnog laboratorija napraviti naprednij stroj od američkog ENIAC-a. Tako je osmišljen ACE (eng. *Automatic Computing Engine*), čiji je dizajn bio vrlo ambiciozan. Turing je bio usmjeren na kreiranje programa koji se sastoje od osnovnih operacija kao što su aritmetičko i logičko uspoređivanje. Binarnu aritmetiku (1 za uključeno, a 0 za isključeno stanje) je smatrao prirodnom za opisivanje stanja stroja.[26]

[24] Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983., str. 360.
[25] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 61.
[26] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 68-69.



Slika 7. ACE Pilot računalo i tri programera

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 72.

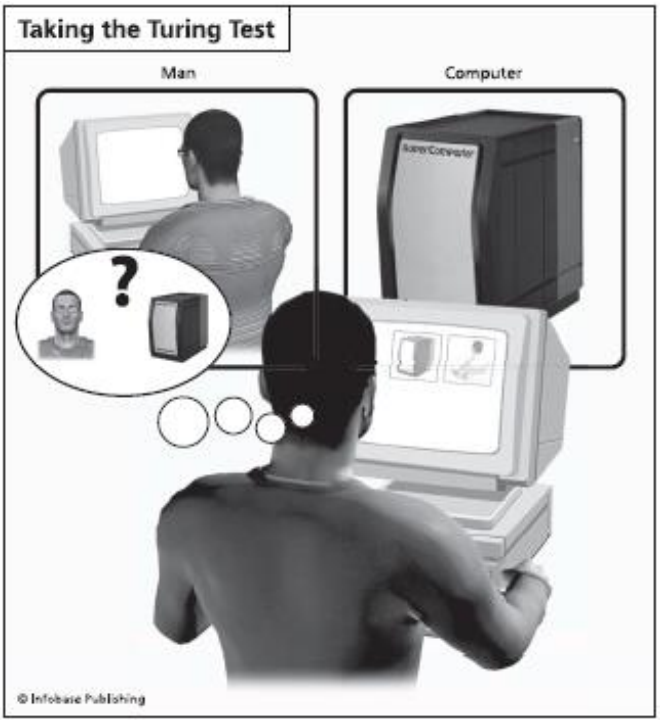
Alan M. Turing je dizajnirao i prvi „strojni jezik" – skup jednostavnijih programskih zapovijedi za aritmetičke i logičke operacije koje su potrebne za izvođenje programa i uspješan prijenos podataka između procesorske jedinice i radne memorije. Usprkos ostvarenim rezultatima, Turing je postao nezadovoljan radom u Nacionalnom fizikalnom laboratoriju. Tome je vjerojatno pridonijelo kašnjenje projekta, ali i to što nije bio timski igrač. Stoga 1947. godine napušta dotadašnji posao i vraća se na Cambridge, gdje uzima slobodnu studijsku godinu. U svibnju sljedeće godine prihvaća poziv da se priključi inovativnom računalnom projektu na sveučilištu Manchester. Stigavši pred kraj projekta, nije mogao puno toga oblikovati i izmijeniti, no napisao je programe koji su imali praktičnu primjenu. Također se bavio računalnim simulacijama.[27]

S vremenom je počeo gubiti zanimanje za praktičnu gradnju strojeva te je postao zaokupljen mislima o stvaranju elektroničkog mozga. To će ga dovesti do novog područja djelovanja – umjetne inteligencije. Šahovska igra, u kojoj je uživao, ali nije bio osobito dobar igrač, motivirat će ga za izradu testa strojne inteligencije. Naime, 1950. godine je napisao detaljan opis programa za igranje šaha, unatoč tome što nije postojalo računalo koje bi ga moglo pokrenuti. Nakon dvije

[27] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 69-72.

godine, isprobao ga je zajedno s prijateljem, računalnim znanstvenikom Alickom Glenniem (1925.–2003.). Turing je „glumio“ stroj i u igri izašao kao gubitnik.[28]

U svom radu iz 1950. godine, naslova „Strojevi za računanje i inteligencija“ (eng. *Computing Machinery and Intelligence*), istaknuo je da ukoliko ne bismo mogli, tijekom pismene komunikacije, razlikovati stroj od čovjeka, tada bismo mogli zaključiti da stroj razmišlja i zbog toga posjeduje inteligenciju. Ovo je razmišljanje pretvorio u pokus koji je kasnije postao poznat kao „Turingov test“. Glavna ideja je bila u tome da netko tko se dopisuje putem monitora s nepoznatim entitetom (osobom ili strojem), točno identificira karakter tog entiteta (osobe ili stroja). Izvorni „Turingov test“ je od osobe tražio da pogodi je li nepoznati sudionik s kojim komunicira muškarac ili žena, a najrelevantniji oblik testa je za potrebe istraživanja umjetne inteligencije od osobe tražio da pogodi koji je od dvaju nepoznatih sudionika osoba, a koji je računalni program.[29]



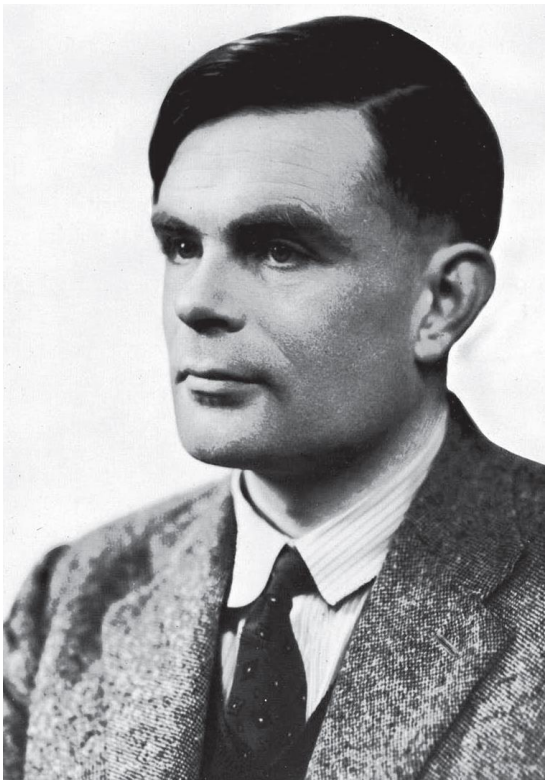
Slika 8. Osoba nastoji odrediti koji je od dvaju sudionika čovjek, a koji je stroj – računalo

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 84.

[28] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 82.

[29] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 84-85.

Zbog svojih iznimnih doprinosa, Turing je u ožujku 1951. godine izabran za člana britanskog Kraljevskog društva.



Slika 9: Alan Turing u vrijeme izbora za člana britanskog Kraljevskog društva, 1951. godine

Izvor: Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983. (list of plates)

U svom radu „Kemijska osnova morfogeneze“ (eng. *Chemical Basis for Morphogenesis*), iz 1952. godine, matematički objašnjava razvoj obrazaca i uzoraka u organizmima. Njegov glavni interes u području matematičke biologije bilo je dokazati postojanje Fibonaccijevih brojeva u strukturi biljaka.[30] Eksperimentalni dokaz tvrdnji iskazanih u tom radu uslijedit će tek 60 godina nakon njegove smrti. Turingovo zanimanje za matematičku biologiju ubrzo se prekinulo, a život mu se u vrlo kratkom razdoblju znatno promijenio.

2.4. KONTROVERZE VEZANE UZ SMRT ALANA M. TURINGA

U siječnju 1952. godine, Alan M. Turing, započinje vezu s devetnaestogodišnjim Arnoldom Murrayjem, a istog tog mjeseca policiji prijavljuje provalu u stan, nakon što mu je Arnold rekao

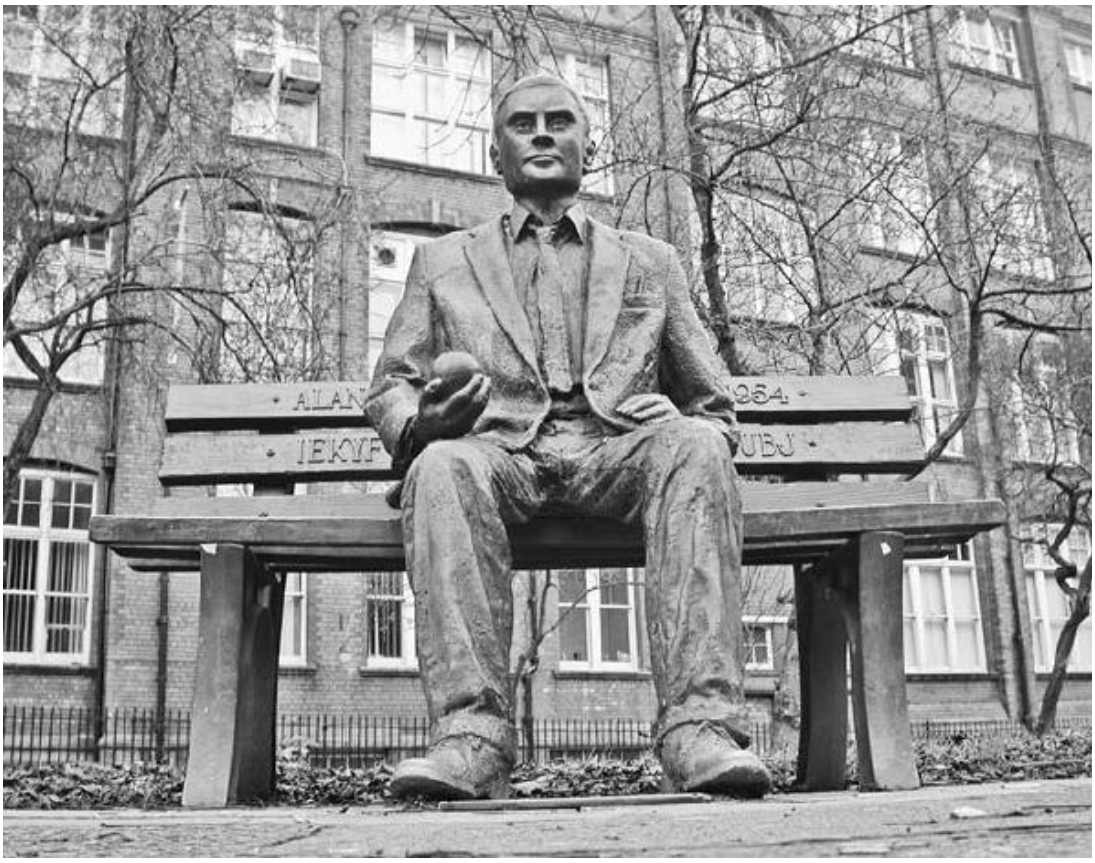
[30] Fibonaccijevi brojevi predstavljaju niz brojeva u kojem je svaki od brojeva jednak zbroju prethodna dva broja u nizu, a niz započinje ovim brojevima: 0, 1, 1, 2, 3, 5, 8, 13…

kako pretpostavlja da je provalu izvršio jedan od njegovih poznanika. Policijski inspektori su bili vrlo radoznali na ispitivanju te su, osim prijavljenog zločina, doznali i kakva je povezanost između njih dvojice.[31]

Turing svoju homoseksualnost nikada nije skrivao. No, u to je vrijeme na snazi bio zakon iz 1885. godine., koji je homoseksualnost smatrao kaznenim djelom te su Turing i Murray, prema članku 11 tog zakona, uhićeni i osuđeni. Kazna za Turinga je bila odlazak u zatvor na dvije godine ili kemijska kastracija, dok je Murray dobio uvjetnu kaznu zatvora. Turing je izabrao kemijsku kastraciju, koja se sastojala od niza hormonskih injekcija.[32] One su ga učinile impotentnim i uzrokovale pojavu ginekomastije na njegovom tijelu. Osim toga, Turing više nije mogao obavljati bilo kakav tajni posao koji je povezan s kriptografijom i kriptoanalizom, a također mu je zabranjen i ulazak u SAD.

Alan M. Turing je umro 7. lipnja 1954. godine. Idući je dan njegovo mrtvo tijelo pronašla kućna pomoćnica i obavijestila policiju. Prema izvješću mrtvozornika, Turing je počinio samoubojstvo trovanjem cijanidom. Policajci su uz uzglavlje kreveta pronašli napola pojedenu jabuku, ali unatoč tome što ju nisu testirali na otrov, zaključili su da je preko nje cijanid ušao u njegov organizam. Pravih dokaza o samoubojstvu nije bilo (npr. nije pronađena oproštajna poruka), niti je Turingov um bio poremećen, kao što je to mrtvozornik tvrdio. Mnogi njegovi suradnici vjeruju kako je njegova smrt bila samo nesretni slučaj, odnosno posljedica udisanja pare cijanida iz pokusa kojeg je radio u svom malom kućnom laboratoriju. Neki ne isključuju ni ubojstvo izvršeno od strane britanskih tajnih službi, s obzirom da je Turing toliko mnogo znao o kriptografiji i kriptoanalizi u vrijeme kada su homoseksualci smatrani prijetnjom nacionalnoj sigurnosti. Oni maštovitiji smatraju kako je pronađena jabuka bila odglumljena scena iz animiranog filma Walta Disneyja „Snjeguljica i sedam patuljaka“, koja je između ostalih bila njegova omiljena bajka.[33]

[31] Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 96-97.
[32] Wikipedia: Alan Turing. URL: https://en.wikipedia.org/wiki/Alan_Turing (06.04.2016.)
[33] Wikipedia: Alan Turing. URL: https://en.wikipedia.org/wiki/Alan_Turing (06.04.2016.)



Slika 10. Kip Alana Turinga s jabukom u ruci na Alan Turing Memorialu u Manchesteru

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 110.

Uz sve teorije i pretpostavke, svijet je tog lipanjskog dana 1954. godine ostao bez velikog čovjeka i znanstvenika, čiji će rad još dugo vremena, nakon njegove smrti, ostati nepoznat široj javnosti. Pitanje je koliko je još toga Alan M. Turing mogao pružiti i kojim bi smjerom krenuo razvoj svih područja u kojima je pokazivao interes. Priznanja i isprike koja je tijekom posljednjih godina posthumno primio dokaz su da njegov genij neće biti zaboravljen.

3. TURINGOV DOPRINOS KRIPTOANALIZI

Vojni stručnjaci su shvaćali važnost informacije te su ju na razne načine pokušavali zaštiti. U Drugom svjetskom ratu njemačka vojska je s tom svrhom koristila uređaj koji se zvao Enigma. Nakon početka rata, Saveznici su usmjerili velike napore kako bi probili kriptografsku zaštitu njemačkih komunikacijskih strojeva.

Slika 11. Enigma s tri rotora

Izvor: Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 222.

Elektromehanički uređaj Enigma pomalo je nalikovao na pisaći stroj. Sastojao se od tipkovnice s 26 tipki označenih slovima, zaslona s 26 žarulja na kojem se prikazivao šifrirani izlaz, električne prespojne ploče i rotora. Većina modela Enigme imala je tri rotora, a oni su bili postavljeni na način da „izlaz“ iz jednoga predstavlja „ulaz“ drugome (početkom Drugog svjetskog rata stroj je imao tri rotora, a 1942. godine mornarički strojevi su počeli koristiti četiri rotora). Izlaz trećeg

rotora je bio spojen s reflektorom, statičnim mehaničkim diskom sličnim rotoru, koji samo s jedne strane ima međusobno prespojene električne kontakte. Zadaća reflektora je bila da drugim putem šalje električni signal kroz rotore. Uređaj se napajao putem ugrađene baterije.[34]

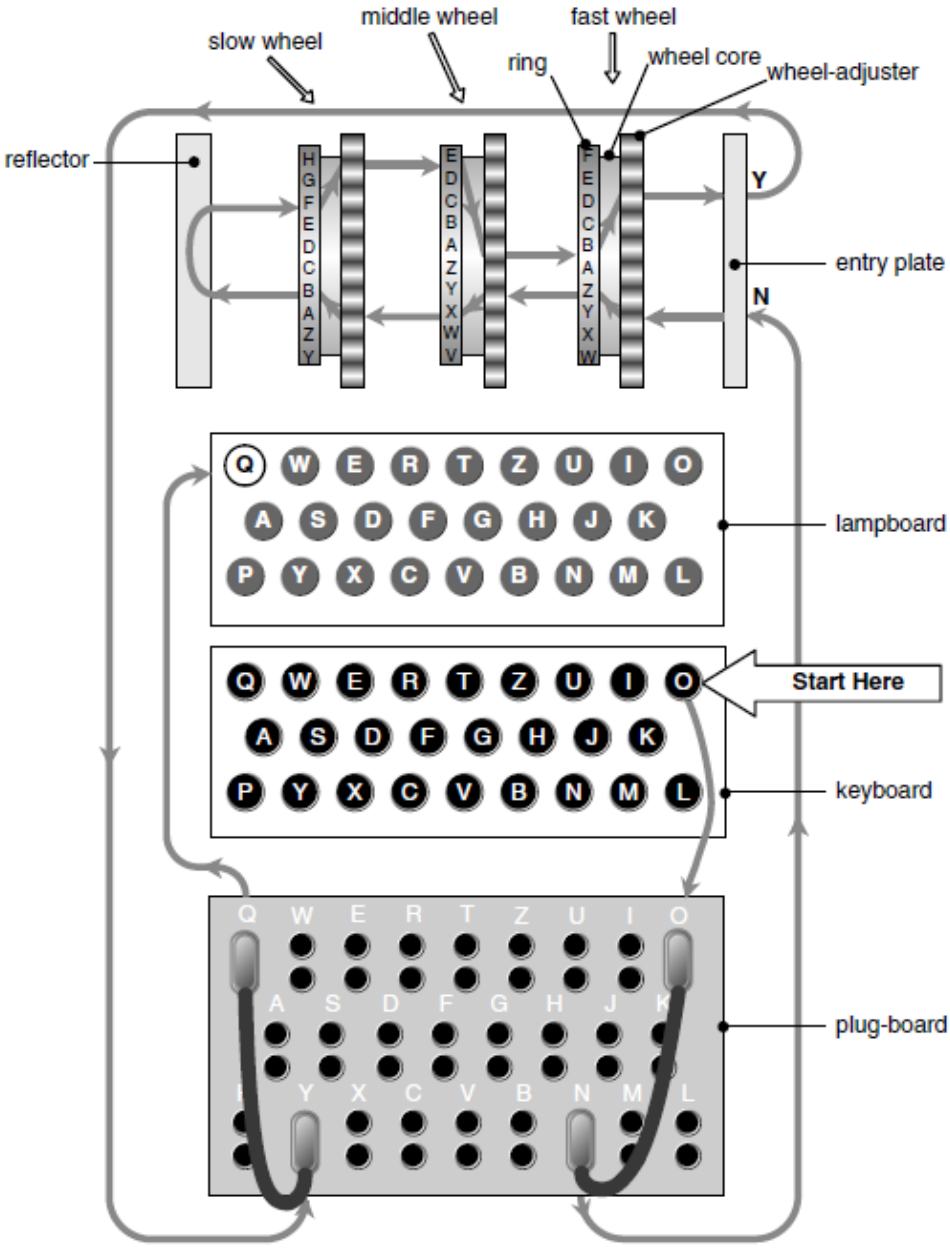
Uloga rotora je bila da slova teksta poznatog svima pretvori u određena slova šifriranog teksta. Jezgra svakog rotora sadržavala je labirint od 26 izoliranih žica, od kojih je svaka bila pridružena jednom od 26 kontakata s desne strane rotora i jednom od 26 kontakata s lijeve strane rotora. Svaki rotor bio je ožičen na drukčiji način.

Ukoliko bi pošiljatelj par puta uzastopno pritisnuo slovo O, povezanost između slova i zaslona sa žaruljama bi se svaki put promijenila te bi za rezultat dala neprekidni niz različito osvijetljenih slova, npr. Q, M, P, W, A, J, Y, R. Međutim, samo slovo O se ne bi nikada pojavilo u tom neprekidnom nizu te se zbog uloge reflektora nijedno slovo, pa tako ni slovo O, šifriranjem nikada ne bi moglo preslikati u samo sebe.[35]

Ponavljanje postavki za šifriranje se izbjegavalo na način da kada se prvi rotor okrenuo za jedan kontakt i napravio puni krug, tek tada je mehanička poluga počela okretati sljedeći rotor čime bi se stvorila zamjenska šifra.[36] Zamjena slova je bila reverzibilna. Npr. ukoliko je O proizvelo Q, tada je i Q proizvelo O, u istim mehaničkim postavkama uređaja. Ovo je bio glavni princip rada Enigme.[37]

Slika 12 prikazuje princip rada Enigme. Ukoliko pritisnemo slovo O na tipkovnici, električna struja će poteći kroz žicu vodeći sve do slova O na električnoj prespojnoj ploči. Zatim će preko električne prespojne ploče doći do slova N, a kroz rotore će proći u suprotnom smjeru, pritom izlazeći kroz rotor na slovu Y, presijecajući električnu prespojnu ploču na slovu Q te će na zaslonu sa žaruljama osvijetliti slovo Q.

[34] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)
[35] Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 220-222.
[36] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)
[37] Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 224.



Slika 12. Shema toka električne struje kroz Enigmu

Izvor: Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 223.

Prije nego je započeo zapisivati poruku pomoću tipkovnice, pošiljatelj je mogao napraviti brojne izmjene u postavkama stroja. Osim toga i primatelj je na svom stroju mogao napraviti izmjene s ciljem dekodiranja poruke. Bilo je moguće učiniti sljedeće:[38]

[38] Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 224–225.

1) Pošiljatelj je mogao napraviti izmjene na prespojnoj ploči izvlačeći električne vodiče iz jednih utičnica i uključujući ih u druge.
2) Pošiljatelj je mogao izmijeniti položaje rotora unutar stroja zaokrenuvši ih ručno.
3) Pošiljatelj je mogao izvaditi dva ili više rotora i zamijeniti im mjesta. Npr. mogao je zamijeniti lijevo i desno položeni rotor, a netaknut ostaviti središnji rotor (svaki je rotor unutar stroja bio različito ožičen). Od prosinca 1938. godine, postojalo je ukupno pet rotora numeriranih od I do V, a unutar stroja su se mogla nalaziti bilo koja tri. Npr. mogli su se koristiti rotori I, II i IV te biti posloženi ovim redom IV/I/II. No, od 1940. godine strojevi korišteni u njemačkoj mornarici su bili opremljeni dodatnim rotorima te je pošiljatelj mogao izabrati bilo koja tri od ukupno osam rotora, numeriranih od I do VIII.

Svaki rotor (I–V) je imao usjeke na različitim mjestima te je svako njihovo mijenjanje ili preslagivanje utjecalo na izmjenu okretaja. Mornarički rotori (VI–VIII) su se neznatno razlikovali, jer su imali usjeke na istim mjestima kao i susjedni rotori, ali su osim njih na istim mjestima imali i dva dodatna usjeka. Dodatni usjek je rezultirao time da je tijekom jednog punog okretaja dvostruko usječen rotor uzrokovao dvostruko pomicanje susjednog rotora.[39]

U slučaju Enigme s tri ožičena rotora, koji su imali 26 kontakata, bilo je 26^3= 17 576 mogućih kombinacija. Takav broj kombinacija nije garantirao veliku sigurnost prijenosa podataka, odnosno postojala je realna mogućnost da se u relativno kratkom vremenu pronađu ispravne postavke rotora. Stoga se broj mogućih postavki, a time i sigurnost, povećavala pomoću izmjenjivih rotora i prespojne ploče. Mehanički sustav rotora je bio jednak, no različiti su im bili električni spojni putovi pa se sa zamjenom rotora mijenjao i sam način šifriranja. Tri rotora mogla su se postaviti na 6 različitih načina, budući da je broj mogućih permutacija 3! = 6. Dakle, broj početnih postavki zamjenom rotora povećavao se 6 puta. Prespojna ploča davala je značajno veći doprinos sigurnosti. Ona je obavljala promjenu električnih putova između tipkovnice i rotora i omogućila je početnu zamjenu slova prije šifriranja. Prespojna ploča se sastojala od 26 priključaka od kojih je svaki prespojni kabel zauzimao dva. Prema tome, moglo se koristiti najviše 13 kabela i izabrati $\binom{26}{2p}$ različitih kombinacija utičnica, gdje p označava broj kabela.[40]

[39] Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer Age. New York: Oxford University Press, 2004., str. 226.

[40] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

Kada se priključi jedan kraj prvog kabela ostaje $2p - 1$ slobodnih priključaka. Nakon spajanja jednog kraja drugog kabela ostaje $2p - 3$ slobodnih priključaka. Iz toga proizlazi da broj načina na koji se p kabela može priključiti na $2p$ priključka iznosi:

$$(2p - 1)\cdot(2p - 3)\cdot(2p - 5)\cdot\ldots\cdot 1.$$

Kombiniranjem izmjenjivih rotora s prespojnom pločom, broj različitih spojnih veza koje je pošiljatelj, odnosno primatelj mogao odabrati iznosi:[41]

$$\frac{26!}{(26-2p)!\,p!\,2^p}.$$

U sljedećoj tablici naveden je broj mogućih kombinacija u ovisnosti o broju korištenih spojnih kabela p.

Broj kabela (*p*)	**Broj kombinacija**
0	1
1	325
2	44 850
3	3 453 450
4	164 038 875
5	5 019 589 575
6	100 391 791 500
7	1 305 093 289 500
8	10 767 019 638 375
9	53 835 098 191 875
10	150 738 274 937 250
11	205 552 193 096 250
12	102 776 096 548 125
13	7 905 853 580 625

Tablica 1. Broj mogućih kombinacija, ovisno o broju korištenih spojnih kabela (p)

Izvor: Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

[41] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

Zbrajanjem svih tih kombinacija dobiva se da postoji ukupno 532985208200576 mogućih postavki spojne ploče. Uzmu li se u obzir načini spajanja i ožičenja triju rotora, kao i sve mogućnosti spajanja reflektora, maksimalan broj različitih postavki Enigme iznosi otprilike $3 \cdot 10^{114}$. Stoga su tvorci Enigme bili uvjereni da je njezino dešifriranje nemoguće.[42]

Pošiljatelj i primatelj raspolagali su s tablicama postavki stroja. Na taj se način osiguravalo da njihovi uređaji budu podešeni na isti način. Skupina korisnika Enigme koja je radila s jednakim tablicama nazivala se mreža. Tablice postavki su vrijedile jedan mjesec te su propisivale na koji način u svakom od dana treba postaviti stroj. U tablici su bili opisani dnevni redoslijed rotora, spojevi na prespojnoj ploči i položaj prstena na rotoru. Osim što su se smatrali osnovnim postavkama, bili su i sastavni dijelovi dnevnog ključa. Glavni razlog dnevnog mijenjanja osnovnih postavki bio je smanjenje broja poruka šifriranih na isti način. Nijemci su bili svjesni da će im sigurnost biti ugrožena ukoliko previše poruka bude šifrirano uz iste postavke te su do kraja Drugog svjetskog rata neke mreže mijenjale osnovne postavke ne na dnevnoj bazi, već svakih osam sati.[43]

Prvi koji su se ozbiljno posvetili dešifriranju Enigme bili su Poljaci, točnije Marian Rejewski. On je provodio većinu svog vremena u analiziranju materijala prikupljenih od strane francuskih obavještajaca. Naime, jedan francuski tajni agent je stupio u kontakt s bratom dužnosnika njemačke vojske koji mu je za naknadu od nekoliko tisuća njemačkih maraka dopustio fotografirati dokumente vezane uz novi sustav šifriranja. U tim dokumentima su bile sadržane upute o korištenju novog sustava (Enigme). Pročitavši te dokumente, Francuzi su shvatili kako se bez poznavanja određenog ključa Enigma ne može dešifrirati te se nisu ni trudili napraviti repliku stroja.[44]

No, Marian Rejewski pročitao je te dokumente i shvatio kako je ponavljanje najveća opasnost za sigurnost stroja. Ponavljanje je bilo najočitije prilikom šifriranja ključa poruke, jer se na početku svake poruke ključ ponavljao dvaput. Primjerice, ukoliko je ključ A B C zapisan kao A B C A B C i šifriran u F O E S C G, slova F i S su bila rezultat šifriranja istog slova A, kao i parovi O i C

[42] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

[43] Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer. New York: Oxford University Press, 2004., str. 227-228.

[44] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html. (29.02.2016.)

od slova B te E i G od slova C. U svakoj je poruci Rejewski počeo uočavati vezu između parova slova. Shvatio je da se sa slovima mogu napraviti lanci, npr. A→F→W→A, B→Q→Z→K→V→E→I→B, C→H→G→O→Y→P→C i J→M→X→S→T→N→U→J.

Rejewski je otkrio kako dužina lanaca ovisi isključivo o postavkama rotora. Ukoliko bismo pomnožili broj mogućih permutacija rotora (6) s brojem mogućih spojnih kombinacija (17 576), za rezultat bismo dobili ukupan broj mogućih postavki rotora (105 456). Dobiveni broj je bio i dalje velik, no ipak je bio nekoliko milijardi puta manji od broja mogućih dnevnih ključeva.[45]

Budući da je na raspolaganju imao repliku stroja Enigme, Rejewski je izradio bazu podataka koja se sastojala od svih mogućih postavki rotora i njihovih pripadajućih duljina lanaca. Pomoću baze podataka je uspio otkriti postavke rotora. Prespojna ploča nije imala nikakvog utjecaja, jer je iz nje izvadio sve kablove, te je problem za pronalazak ispravne postavke rotora sveo na supstitucijsku šifru. Osmislio je mehanički uređaj kojeg je nazvao Bomba (vjerojatno jer su njezini rotirajući mehanički dijelovi stvarali buku). Napravio je šest ovakvih strojeva, od kojih je svaki predstavljao jednu permutaciju poretka rotora. Ovi strojevi su automatski tražili ispravne postavke rotora te su velikom brzinom provjeravali jednu od 17 576 mogućih spojnih kombinacija.[46]

Nijemci su 1939. godine odlučili povećati sigurnost Enigme dodavanjem novih rotora, čime se povećavao broj mogućih kombinacija. Također su prestali na početku svake poruke ključ ponavljati dvaput. U takvim okolnostima, Poljaci su postali svjesni ozbiljnosti situacije te su svoje rezultate u dešifriranju Enigme odlučili podijeliti s Britancima. Nekoliko tjedana kasnije je počeo Drugi svjetski rat.

Britanci su osnovali poseban ured koji se zvao Vladina škola za kodove i šifre (eng. *Government Code and Cypher School*). Sjedište ureda, kako je već navedeno, bilo je u Bletchley Parku. Nakon osnivanja ureda, za rad u području kriptografije prijavilo se mnogo sveučilišnih profesora i znanstvenika, među kojima je bio i Turing. Ubrzo su ovladali poljskim tehnikama dešifriranja, ali su se suočili i s problemom povećanja broja rotora.

[45] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

[46] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

Osim sveučilišnih profesora u uredu se našao i znatan broj žena volonterki. Neke od njih su bile i vrsne matematičarke, među kojima se posebno isticala Joan Elisabeth Lowther Clarke (1917.–1996.), koja je svojim matematičkim vještinama zadivila Turinga. Osim što su bili suradnici u projektu dešifriranja Enigme, postali su i vrlo dobri prijatelji te se Turing početkom 1941. godine odlučio zaručiti za nju. No, zaruke nisu dugo potrajale, jer joj je Alan priznao svoje homoseksualne sklonosti. Clarke nije bila pretjerano iznenađena, jer je jednim dijelom to i predosjećala, te su i dalje ostali u jako dobrim prijateljskim odnosima.

Posao dešifriranja u početku je bio dosta olakšan, budući da su njemački operateri za ključ često odabirali tri uzastopna slova s tipkovnice Enigme, a britanski kriptoanalitičari su otkrili kako se nijedno slovo šifriranjem ne može preslikati u isto to slovo. Turing je shvatio kako pogreška koju su Nijemci činili u obliku ponavljanja ključa na početku svake poruke neće dugo potrajati te je počeo razvijati novu strategiju „napada“ na Enigmu. Njegov uređaj za dešifriranje pretraživao je sve kombinacije postavki rotora kako bi otkrio ispravnu postavku. Usavršavajući poljski uređaj za dešifriranje Enigme, zanemario je sve rezultate između pretpostavljenog i šifriranog slova, osim onih koji omogućavaju zatvaranje strujnog kruga između njih. U nastojanju da što efikasnije probije kod Enigme, Turing i njegovi suradnici fokusirali su se na tri metode napada: metodu dvostrukog ključa, metodu direktne analize rezultata šifriranja i metodu napada temeljenu na pretpostavljenom tekstu.[47]

Britanski analitičari često su mogli pretpostaviti kako glasi dio poruke koju su njemačke jedinice razmjenjivale preko Enigme. Kako bi na temelju te spoznaje dešifrirali poruku, morali su takav tekst točno locirati u šifriranoj poruci. Neka se pretpostavi da se pretpostavljeni tekst „Wettervorhersagebiskaya“, koji su Nijemci često koristili, pa tako i prilikom iskrcavanja Saveznika u Normandiji, želi ispravno smjestiti u šifrirani niz:[48]

QFZWRWIVTYRESXBFOGKUHQBAISE

[47] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

[48] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

Sljedeće lociranje nije ispravno, budući da ne smije biti podudaranja, a pretpostavljeni i šifrirani tekst preklapaju se u slovu S.

QFZ	WRW	IVT	YRE	**S**XB	FOG	KUH	QB
WET	TER	VOR	HER	**S**AG	EBI	SKA	YA

Nakon pomicanja šifriranog teksta za jednu poziciju ulijevo, dobiva se preklapanje na tri mjesta (slova V, E i A), što znači da ni ta lokacija nije korektna.

FZW	RWI	**V**TY	R**E**S	XBF	OGK	UHQ	B**A**
WET	TER	**V**OR	H**E**R	SAG	EBI	SKA	Y**A**

Daljnje pomicanje šifriranog teksta ulijevo rezultira jednim preklapanjem u slovu R.

ZWR	WIV	TY**R**	ESX	BFO	GKU	HQB	AI
WET	TER	VO**R**	HER	SAG	EBI	SKA	YA

Sljedeće preklapanje dovodi do tri preklapanja (slova W, G i A).

WRW	IVT	YRE	SXB	FO**G**	KUH	QB**A**	IS
WET	TER	VOR	HER	SA**G**	EBI	SK**A**	YA

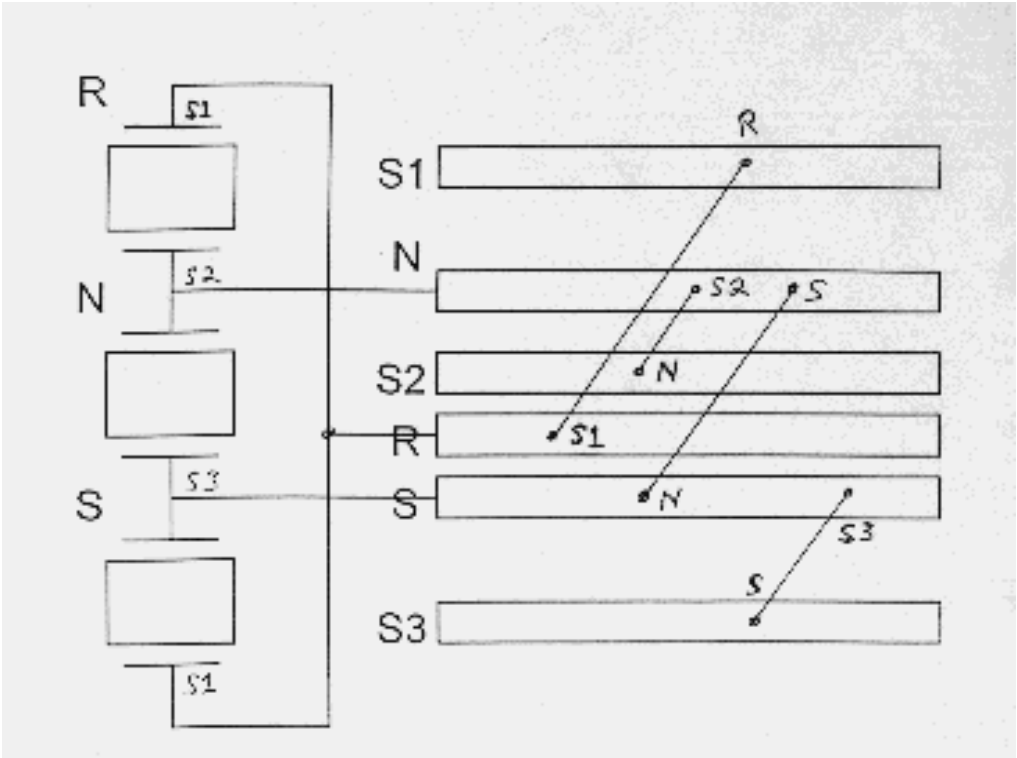
U petom pokušaju dolazi se do pozicije u kojoj se niti jedno slovo iz pretpostavljenog i šifriranog teksta ne preklapaju.

RWI	VTY	RES	XBF	OGK	UHQ	BAI	SE
WET	TER	VOR	HER	SAG	EBI	SKA	YA

Sada je potrebno utvrditi postoji li transformacija koja pretpostavljeni tekst preslikava u šifrirani te na koji način. Za utvrđivanje postojanja transformacije koristit će se sljedeća tablica.

123	456	789	012	345	678	901	23
RWI	VTY	RES	XBF	OGK	UHQ	BAI	SE
WET	TER	VOR	HER	SAG	EBI	SKA	YA

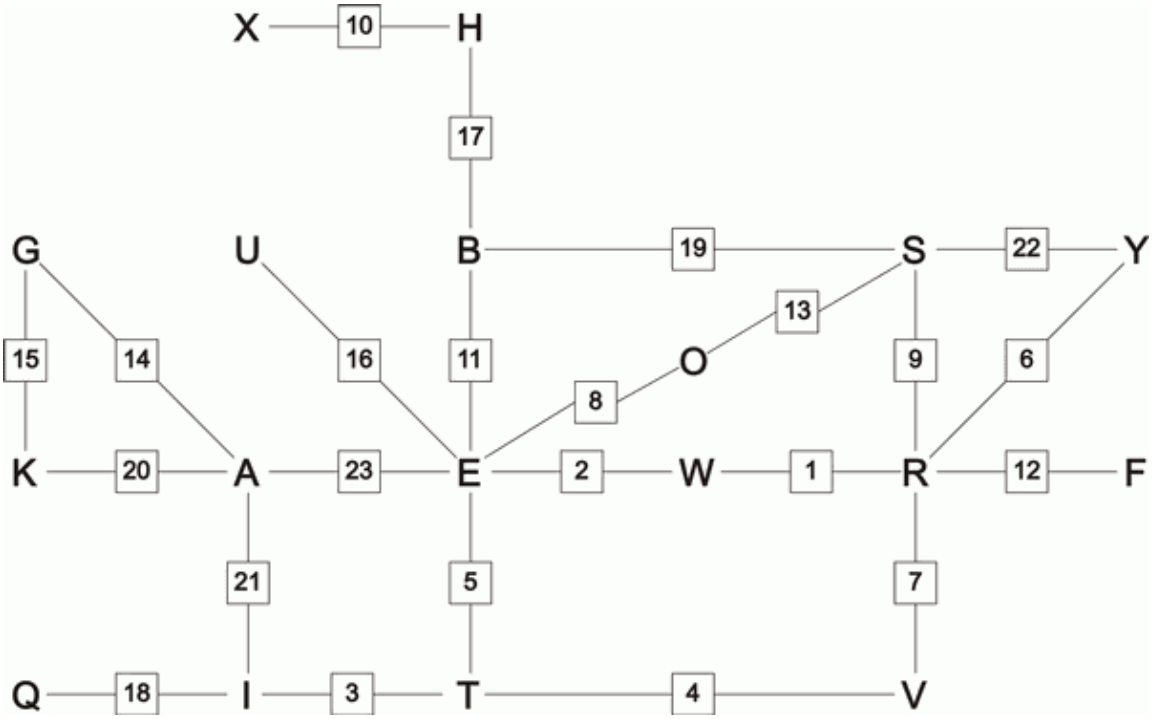
Pri tome je potrebno uzeti u obzir spoznaje o radu prespojne ploče do kojih je prvi došao Gordon Welchman (1906.–1985.). On je otkrio da ukoliko bi neki spoj jedno slovo zamijenio drugim, tada bi istovremeno to drugo slovo zamijenio prvim (npr. ako se slovo A zamijeni slovom B, slovo B se zamijeni slovom A). Turing je s oduševljenjem prihvatio Welchmanovo otkriće. Sljedeća slika prikazuje shemu Welchmanove dijagonalne ploče.



Slika 13. Prikaz dijagonalne ploče Gordona Welchmana

Izvor: Cooper, S. B., Van Leeuwen, J. (ur.): Alan Turing: His Work and Impact. Amsterdam: Elsevier, 2013., str. 431.

Uz pomoć prethodne tablice i svojstva prespojne ploče o uzajamnom preslikavanju slova može se odrediti dijagram veza između slova. U položaju 1, Enigma će slovo R preslikati u slovo W, no na isti način će i slovo W preslikati u slovo R. U položaju 2 će se slovo W preslikati u E, no također će se E preslikati u W. Kada se na taj način povežu svi parovi slova, dobiva se dijagram veza koji je prikazan slikom 14.



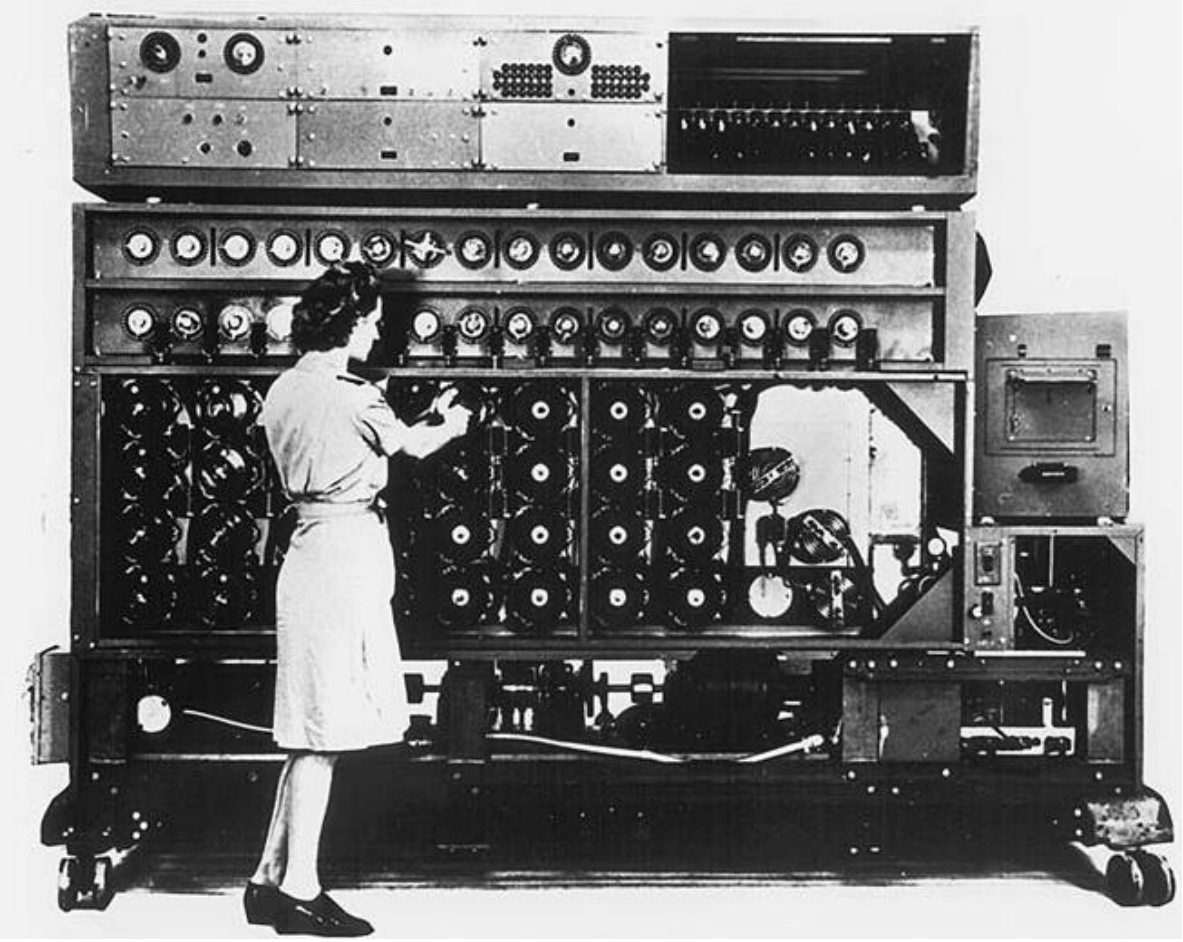
Slika 14. Dijagram veza između parova slova

Izvor: Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html. (29.02.2016.)

Svaka se transformacija sastoji od transformacija na prespojnoj ploči, transformacija reflektora i rotora, te još jedne transformacije na prespojnoj ploči. Neka se pretpostavi da su u gornjem primjeru prespojena slova E i K. U tom će slučaju slovo K postati ulaz rotoru na položaju 23, koji će ga pretvoriti u neko drugo slovo, koje se može označiti s X1. Kako je već uočeno da se slovo E transformira u slovo A na položaju 23, slovo A mora biti prespojeno sa slovom X1, dok će slovo X1 postati ulaz rotoru na položaju 21, transformirajući ga u slovo, koje se može označiti s X2. Na položaju 21 slovo A se pretvara u slovo I te se zaključuje da slovo X2 treba biti prespojeno sa slovom I. Ulaz u rotor na položaju 3 će biti slovo X2 koje će se pretvoriti u slovo X3. Stvarni izlaz je slovo T, a na prespojnoj će ploči biti zamijenjena slova T i X3. Ulaz u rotor na položaju 5 će biti slovo X3, a izlaz će biti neko slovo X4 koje je prespojeno sa slovom E. Pretpostavka je bila da su prespojena slova E i K te ukoliko bi se za izlaz ovakve kružne provjere dobilo neko drugo slovo, pretpostavka bi se pokazala netočnom.[49]

[49] Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)

Točnost pretpostavke o postavci prespojne ploče osiguravala se zadovoljavanjem ovakve kružne provjere, a to je upravo bila temeljna ideja Turingovog „napada“ na Enigmu. Obavještajna operacija dešifriranja Enigme se zvala Ultra, no mnogi kriptoanalitičari koji su pomogli u dešifriranju i dugo godina nakon rata nisu dobili zaslužena priznanja. Procjenjuje se da je dešifriranje Enigme skratilo trajanje rata za dvije godine i spasilo nekoliko milijuna ljudskih života, no rad u Bletchley Parku ostao je dobro čuvanom tajnom gotovo 50 godina.



Slika 15. Žena volonterka koja radi na stroju za dešifriranje Enigme (uređaj pretražuje sve moguće kombinacije postavki rotora tražeći ispravnu)

Izvor: Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011., str. 51.

4. TURINGOV DOPRINOS RAČUNALSTVU

U svom radu „Izračunljivi brojevi s primjenom na problem odluke“ (eng. *On Computable Numbers, with an Application to the Entscheidungsproblem*) Turing je pokazao kako ne postoji algoritam koji će omogućiti rješavanje svih matematičkih problema. Postupak izračunavanja Turing je sveo na minimum. Prilikom računanja, osoba slijedi nekakva određena pravila (algoritam). Prema Turingu, takvu osobu može se ograničiti na izvođenje jednostavnih računalnih radnji, bez dodatnih i nebitnih detalja, a da se konačni rezultat računanja ne promijeni. Osoba dok računa ima sljedeća ograničenja: gotovo u svakoj fazi računanja obraća pažnju na mali broj simbola, a postupci koje izvodi u nekoj fazi ovise o tome na koje je simbole usmjerena pažnja, ali i kakvo je stanje uma osobe koja vrši izračun. Analiza postupka izračunavanja ga je dovela do sljedećih zaključaka: računanje se vrši zapisivanjem simbola u kvadrate na označenoj papirnatoj vrpci; osoba je prilikom računanja usmjerena na simbol koji je zapisan u jednom kvadratu vrpce; u sljedećem koraku, osoba ispisuje simbol u onaj kvadrat na koji je obraćala pažnju te tu pažnju usmjerava na sljedeći prvi kvadrat koji se nalazi na lijevoj ili desnoj strani. Iz navedenog proizlazi kako osobu može zamijeniti stroj koji će izvršavati iste jednostavne operacije.[50] Stroj na kojem se mogu obaviti izračuni zadataka pomoću algoritamskih postupaka naziva se Turingov stroj.

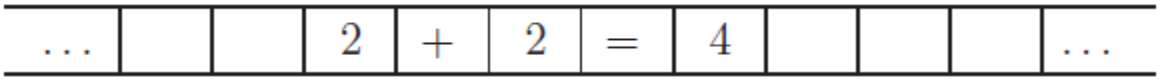
Turingov stroj, kojeg je Alan nazvao automatskim strojem za računanje, predstavlja apstraktni, konceptualni model izračunavanja. Turingov stroj se sastoji od glave za čitanje ili pisanje, memorijske vrpce koja je beskonačna u oba smjera te je ujedno i vanjski medij za pohranu (tvrdi disk)[51] i kontrolne jedinice. Vrpca je podijeljena u kvadrate (polja), a svaki od tih kvadrata može biti prazan ili sadržavati jedan simbol (0 ili 1 ili bilo koji drugi simbol koji mora imati konačan broj). Kada se počne raditi sa strojem, na vrpci se nalazi zapis kojeg možemo usporediti s programskim ulaznim podacima. Glava za čitanje ili pisanje se pomiče po vrpci za jedno mjesto naprijed ili nazad, odnosno lijevo ili desno dok se ne zaustavi kako bi pročitala podatke s vrpce i zapisala nove.[52] Kontrolna jedinica vrši operacije zapisivanja na vrpcu, pomicanja glave za čitanje ili pisanje i promjene stanja, a ovisi o memoriji i simbolu koji se nalazi ispod glave za

[50] Davis, M.: Na logički pogon: Podrijetlo ideje računala. Zagreb: Naklada Jesenski i Turk, 2003., str. 172–176.

[51] Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)

[52] Copeland, B. J.: Alan Turing's Electronic Brain: The Struggle to Build the ACE, the World's Fastest Computer. New York: Oxford University Press, 2005., str. 107.

čitanje i pisanje.[53] Turingov stroj se sastoji od proizvoljnih, ali konačno mnogih stanja koja predstavljaju radnu memoriju, a njihovu ulogu i brojnost treba se odrediti prilikom „sastavljanja“ stroja. Pristupačnost radne memorije očituje se u tome što iz svakog stanja može prijeći u svako drugo stanje ili ostati na mjestu.[54]



Slika 16. Primjer vrpce Turingovog stroja

Izvor: Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf. (30.05.2016.)

Prijelaz iz svakog stanja ili ostanak na mjestu je određen pravilima. Ukoliko je u svakom trenutku rad Turingovog stroja određen pravilima, tada govorimo o deterministočkom Turingovom stroju.[55]

Deterministički Turingov stroj (M) je u pravilu uređena sedmorka (Q, S, T, b, q_0, F, δ), gdje je:[56]

- Q – konačan skup stanja; $Q = \{q_0, q_1, \ldots, q_N\}$
- S – abeceda vrpce, odnosno konačan skup simbola s kojima stroj obavlja rad
- T – ulazna abeceda, odnosno konačan skup simbola koji se mogu naći na vrpci prije nego što stroj počne obavljati rad; $T \subsetneq S$
- b – oznaka da je polje prazno („prazan“ simbol); $b \in S \setminus T$
- q_0– početno stanje rada stroja; $q_0 \in Q$
- F – skup završnih stanja; $F \subseteq Q$
- δ – funkcija prijelaza; $\delta : Q \times S \rightarrow Q \times S \times \{S, L, D\}$, S označava ostanak na mjestu, L označava pomak u lijevu stranu, a D označava pomak u desnu stranu

[53] Manger, R.: Dio III: Turingovi strojevi. URL: http://web.studenti.math.pmf.unizg.hr/~manger/tr/TR-III.pdf (30.05.2016.)

[54] Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)

[55] Brcković, Ž.: Teorija izračunljivosti i neodlučivost logike prvog reda. Diplomski rad. URL: http://darhiv.ffzg.unizg.hr/4515/1/Teorija%20izracunljivosti%20i%20neodlucivost%20logike%20prvog%20reda%20-%20Zeljko%20Brckovic.pdf (29.02.2016.)

[56] Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)

Iz definicije funkcije prijelaza δ uočava se da se Turingov stroj na nekom mjestu na vrpci nalazi u stanju $q \in Q$, odakle je pročitao simbol $s \in S$. Zatim, u ovisnosti o ta dva parametra, prelazi u novo stanje $q' \in Q$, vrši zapis novog simbola $s' \in S$ na vrpcu (na isti položaj na kojem se nalazi) i obavlja pomak iz skupa $\{S, L, D\}$, odnosno ostaje na mjestu ili se pomiče u lijevu ili u desnu stranu. Uređenom petorkom (q, s, q', s', m), pri čemu su $q, q' \in Q$; $s, s' \in S$; $m \in \{S, L, D\}$ se može opisati jedan korak kojeg obavi Turingov stroj, a tom istom petorkom možemo opisati jedno pridruživanje funkcije prijelaza $\delta : (q, s) \xrightarrow{\delta} (q', s', m)$, pri čemu su $q, q' \in Q$; $s, s' \in S$; $m \in \{S, L, D\}$. Stroj se zaustavlja kada funkcija prijelaza δ izvrši preslikavanje, odnosno kada stroj dođe u završno stanje i napravi pomak S (ostanak na mjestu):[57]

$$(q_i, x) \xrightarrow{\delta} (q_p, y, S), \text{ pri čemu su } x, y \in S;\ q_i \in Q;\ q_p \in F$$

U sljedećem primjeru pokazat će se kako se pomoću Turingovog stroja na praznu vrpcu mogu zapisati sljedeći simboli: „2X – X = X“:[58]

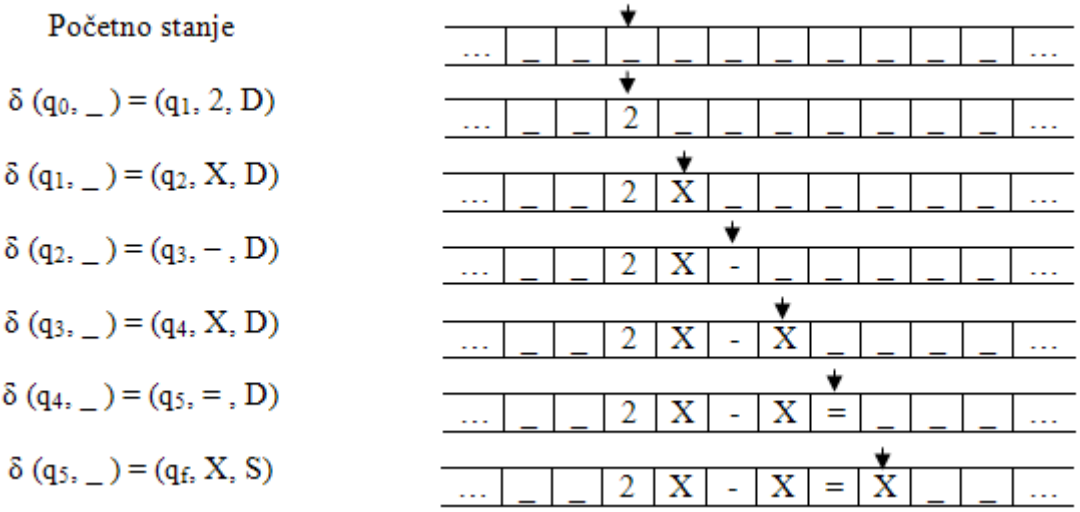
Poznato je da je vrpca prazna. Stoga se može preskočiti određivanje početnog položaja glave za čitanje ili pisanje te je odmah moguće napisati rješenje u skladu s gore navedenom definicijom deterministočkog stroja:

$Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_f\}$
$S = \{ \_ , 2, X, – , = \}$
$T = \varnothing$
$b = \_$
$q_0 = q_0$
$F = \{q_f\}$

Funkcija prijelaza δ definirat će se tako da se popišu sva stanja u koja stroj može doći i svi simboli koje može pročitati (na desnoj je strani prikazano stanje vrpce nakon svakog koraka):

[57] Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)

[58] Primjer te funkcijski, tablični i grafički zapis nastali prema: Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)

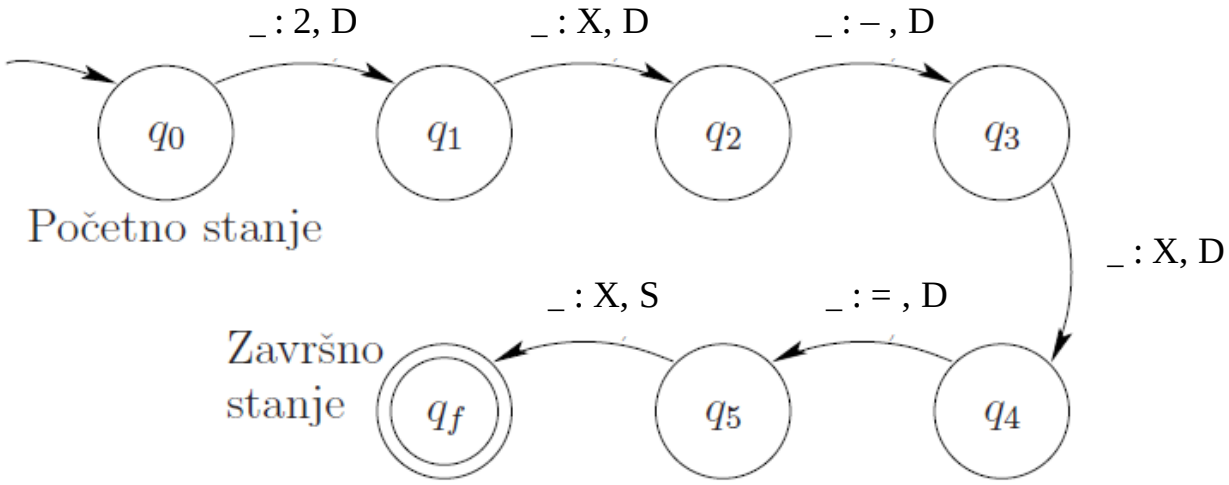


Općenito, nije slučaj da vrpca bude prazna i da funkcije prijelaza δ budu oblika $\delta\ (q, \_\ ) = \ldots$, no u ovom primjeru je to tako te nam stanja služe da upamtimo koji idući simbol treba zapisati.

Isti Turingov stroj može biti zapisan i tablično:

$Q \times S$	q_0	q_1	q_2	q_3	q_4	q_5
_	q_1, 2, D	q_2, X, D	q_3, – , D	q_4, X, D	q_5, = , D	q_f, X, S

Za prikaz se može koristiti i sljedeći zapis:



Stanja stroja su predstavljena čvorovima, pri čemu se završno stanje označava dvostrukom kružnicom. Pomoću strjelica se mogu utvrditi prijelazi između pojedinih stanja, a pomoću zapisa

iznad strjelica saznaje se koji je simbol trenutno prikazan na vrpci, kao i upute koje su potrebne za pisanje novog simbola i pomicanje glave za čitanje ili pisanje.[59]

Osim opisanog Turingovog stroja, postoje i drugi, a jedan od njih je i univerzalni Turingov stroj. Prvotna ideja ovakvog stroja je bila da se ne mora za svaki problem konstruirati nekakav poseban stroj kako bismo ga bili u stanju riješiti. Naime, bio bi dovoljan samo jedan univerzalni Turingov stroj koji bi se mogao programirati za rješavanje različitih problema. Univerzalni Turingov stroj bi za argumente x_1, x_2 računao vrijednost koju bi izračunao Turingov stroj kada bi imao kodni broj x_1 i argument x_2.[60]

[59] Brcković, Ž.: Teorija izračunljivosti i neodlučivost logike prvog reda. Diplomski rad. URL: http://darhiv.ffzg.unizg.hr/4515/1/Teorija%20izracunljivosti%20i%20neodlucivost%20logike%20prvog%20reda%20-%20Zeljko%20Brckovic.pdf (29.02.2016.)

[60] Brcković, Ž.: Teorija izračunljivosti i neodlučivost logike prvog reda. Diplomski rad. URL: http://darhiv.ffzg.unizg.hr/4515/1/Teorija%20izracunljivosti%20i%20neodlucivost%20logike%20prvog%20reda%20-%20Zeljko%20Brckovic.pdf (29.02.2016.)

5. ALAN M. TURING I SUVREMENO DRUŠTVO

Unatoč brojnim profesionalnim uspjesima, Turing je ipak bio izopćen iz društva. Njegov rad na uređajima za dešifriranje ostao je nepoznat dugo vremena. Turingova homoseksualnost, koja se nikako nije uklapala u krute norme tradicionalnog britanskog društva, dodatno je utjecala na zanemarivanje njegovih doprinosa. Više od pola stoljeća nakon njegove smrti, 10. rujna 2009. godine, donekle je ispravljena nepravda koja mu učinjena od strane britanskih vlasti u vidu isprike tadašnjeg britanskog premijera Gordona Browna. Premijer je tada napisao kako je Turing bio izvrstan matematičar te da bi bez njegovih doprinosa povijest Drugog svjetskog rata bila znatno drugačija. Tada je istakao da je zahvalan svim onim ljudima, a naročito Alanu Turingu, čija je borba protiv fašizma bila toliko jaka da su strahote holokausta i totalnog rata postale dijelom europske povijesti, a ne europske budućnosti. U ime britanske vlade i svih onih ljudi koji žive slobodno zahvaljujući Turingovim doprinosima, iskazao je iskreno žaljenje i istaknuo kako je Alan zaslužio puno bolji život, nego što ga je imao.[61]

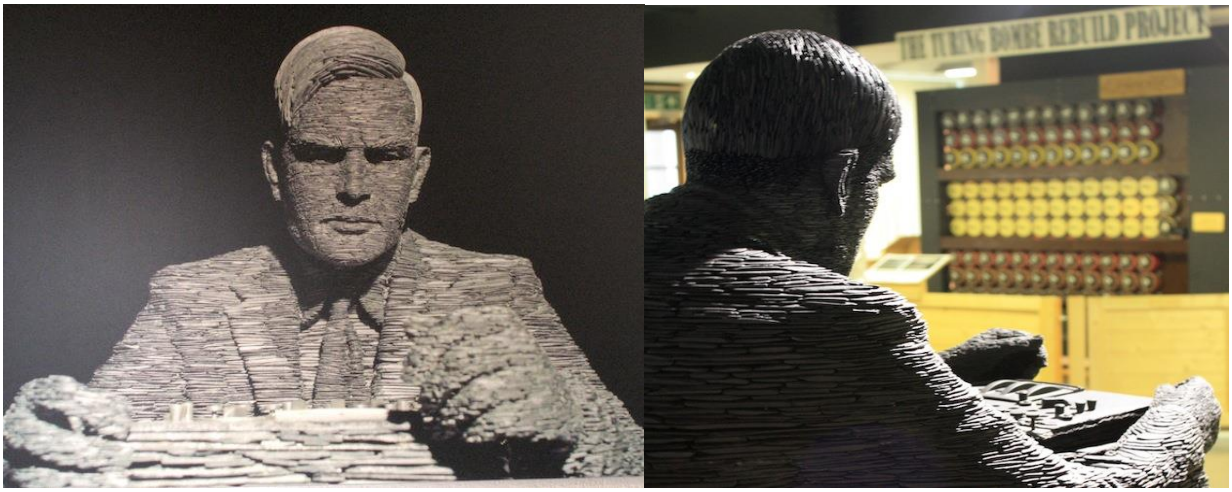
Pet godina nakon isprike premijera, kraljica Elizabeta II. je potpisala ispriku u ime kraljevske obitelji te Turingu dala kraljevski oprost. Stota godišnjica Turingovog rođenja, 2012. godina, bila je proglašena njegovom godinom te su se diljem svijeta održavali brojni programi u čast Alanovih postignuća. Iste te godine je ispred Turingovog memorijalnog centra u Manchesteru prošao olimpijski plamen (London je bio domaćin Ljetnih olimpijskih igara), a gradski vijećnici utemeljili su nagradu Alan Turing za pojedince i skupine koji su se istakli u borbi protiv homofobije u Manchesteru.

Krajem 1980.-tih godina Turingov život i djelo bili su prikazani na kazališnim daskama u drami „Razbijanje koda“ (eng. *Breaking the Code*), redatelja Hugha Whitemorea, a deset godina kasnije i u istoimenoj televizijskoj seriji. Alana Turinga je oba puta utjelovio glumac Derek Jacobi. Osim toga, Turingovim životom i djelom bavilo se nekoliko filmova, među kojima je najpoznatiji „Igra oponašanja“ (eng. *The Imitation Game*), iz 2014. godine, kojeg je režirao Morten Tyldum. Film je snimljen prema knjizi Andrewa Hodgesa „Alan Turing: The Enigma“, a fokusirao se na Turingov život i njegovo djelovanje u Drugom svjetskom ratu. Turinga je u tom filmu utjelovio glumac Benedict Cumberbatch. Film je bio nominiran za nagradu Oscar u nekoliko kategorija, a osvojio ga je za najbolji adaptirani scenarij.

[61] Brown, G.: I'm proud to say sorry to a real war hero. URL: http://www.telegraph.co.uk/news/politics/gordon-brown/6170112/Gordon-Brown-Im-proud-to-say-sorry-to-a-real-war-hero.html (29. 02. 2016.)

Turingu su svojim pjesmama odali počast i brojni glazbenici, a najpoznatiji među njima su svakako britanski elektronski duo Pet Shop Boys, koji su to učinili 2014. godine.

U Bletchley Parku je postavljena Turingova skulptura, a zgrada u kojoj su tijekom Drugog svjetskog rata djelovali kriptoanalitičari postala je muzej.



Slika 17. Skulptura Alana Turinga u Bletchley Parku

Izvor: Ambruš–Kiš, M.: Stotinu godina Alana Turinga. URL: http://www.velikabritanija.net/2012/06/23/alan-turing-100-godina/ (29.02.2016.)

6. ZAKLJUČAK

Alan Turing ostavio je značajan trag u raznim područjima, kao što su kriptoanaliza, računalstvo, umjetna inteligencija, matematika i biologija. Dugo je vremena nakon Turingove tragične smrti njegov rad bio nepoznat široj javnosti, na što je utjecalo više čimbenika. Život i djelo Alana Turinga još uvijek nisu u potpunosti istraženi, iako je posljednjih dva desetljeća mnogo toga učinjeno na njihovom rasvjetljavanju. Najvažnije godine života Turing je posvetio razbijanju neprijateljskih vojnih šifri, čime je zadužio cijeli slobodarski svijet. Nažalost, tek više od pedeset godina nakon smrti njegovo je djelovanje tijekom Drugog svjetskog rata objektivno sagledano i valorizirano.

Osim doprinosa Alana Turinga u području kriptoanalize, u ovom je radu istraženo i njegovo zanimanje za računalstvo, s naglaskom na ono što danas nazivamo Turingovim strojem. Iako je u pitanju jednostavan apstraktan uređaj namijenjen modeliranju procesa koji se odvijaju unutar računala, Turingov stroj smatra se jednim od prvih koraka u razvoju računalstva. Zbog toga, ali i drugih doprinosa, Turinga se često naziva ocem modernog računalstva. Turing je živio u vremenu kada je računalstvo bilo u povojima, ali on je bio veliki vizionar, svjestan važnosti koju će informacijska tehnologija i umjetna inteligencija imati u budućnosti. U tom je smislu poznat njegov test za provjeru umjetne inteligencije čiji je zadatak utvrditi je li neki stroj zaista inteligentan, odnosno može li čovjeka ostaviti u uvjerenju da komunicira s drugim ljudskim bićem.

Turing je po mnogočemu bio ispred svog vremena. Stoga ne iznenađuje da tek počinjemo biti svjesni njegove važnosti za svijet u kojem živimo. Uzimajući u obzir sve ono što se vezuje s ovim genijalnim britanskim matematičarom, kriptografom, logičarom i vizionarom, nećemo pogriješiti ako zaključimo da će lik i djelo Alana M. Turinga još dugo privlačiti pozornost ne samo znanstvenika, već i običnih ljudi koji u njegovom privatnom životu i svestranoj profesionalnoj karijeri pronalaze brojne zanimljivosti, ali i trajnu inspiraciju.

7. LITERATURA

- Ambruš–Kiš, M.: Stotinu godina Alana Turinga. URL: http://www.velikabritanija.net/2012/06/23/alan-turing-100-godina/ (29.02.2016.)
- Brcković, Ž.: Teorija izračunljivosti i neodlučivost logike prvog reda. Diplomski rad. URL: http://darhiv.ffzg.unizg.hr/4515/1/Teorija%20izracunljivosti%20i%20neodlucivost%20logike%20prvog%20reda%20-%20Zeljko%20Brckovic.pdf (29.02.2016.)
- Britannica: Alan M. Turing: Biography. URL: http://www.britannica.com/biography/Alan-Turing (29.02.2016.)
- Brown, G.: I'm proud to say sorry to a real war hero. URL: http://www.telegraph.co.uk/news/politics/gordon-brown/6170112/Gordon-Brown-Im-proud-to-say-sorry-to-a-real-war-hero.html (29.02.2016.)
- Cooper, S. B., Van Leeuwen, J. (ur.): Alan Turing: His Work and Impact. Amsterdam: Elsevier, 2013.
- Copeland, B. J.: Alan Turing's Electronic Brain: The Struggle to Build the ACE, the World's Fastest Computer. New York: Oxford University Press, 2005.
- Copeland, B. J. (ur.): The Essential Turing: The Ideas That Gave Birth to the Computer. New York: Oxford University Press, 2004.
- Čavrak, H.: Enigma. Hrvatski matematički elektronski časopis. URL: http://e.math.hr/enigma/index.html (29.02.2016.)
- Davis, M.: Na logički pogon: Podrijetlo ideje računala. Zagreb: Naklada Jesenski i Turk, 2003.
- Henderson, H.: Alan Turing: Computing Genius and Wartime Code Breaker. New York: Chelsea House, 2011.
- Hodges, A.: Alan Turing: The Enigma. Princeton: Princeton University Press, 1983.
- Lavington, S. (ur.): Alan Turing and His Contemporaries: Building the World's First Computers. Swindon: British Informatics Society Limited, 2012.
- Leavitt, D.: The Man Who Knew Too Much: Alan Turing and the Invention of the Computer. New York: Atlas Books, 2006.
- Manger, R.: Dio III: Turingovi strojevi. URL: http://web.studenti.math.pmf.unizg.hr/~manger/tr/TR-III.pdf (30.05.2016.)

- Šego, V.: Turingovi strojevi. URL: https://web.math.pmf.unizg.hr/nastava/gr/materijali/v06/turingov_stroj-vjezbe.pdf (30.05.2016.)
- Teuscher, C.: Alan Turing: Life and Legacy of a Great Thinker. Berlin: Springer – Verlag, 2004.
- Turing, S.: Alan M. Turing. New York: Cambridge University Press, 2012.
- Wikipedia: Alan Turing. URL: https://en.wikipedia.org/wiki/Alan_Turing (06.04.2016.)

KRATAK ŽIVOTOPIS

Autorica ovog diplomskog rada, Ana–Marija Ivanković, rođena je u Osijeku 1. veljače 1991. godine. U prvi razred Osnovne škole Vladimira Becića u Osijeku krenula je 1997. godine, a 2005. godine se upisuje u Medicinsku školu Osijek, smjer fizioterapeutski tehničar. Po završetku srednje škole, 2009. godine započinje studij na Odjelu za fiziku Sveučilišta Josipa Jurja Strossmayera u Osijeku. U slobodno vrijeme voli čitati autobiografije rock glazbenika, a ubrzo se namjerava upisati u školu stranih jezika kako bi naučila njemački i portugalski jezik.