FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Seminární práce

Alan Turing

Martin Jandík

1. ročník KŘT

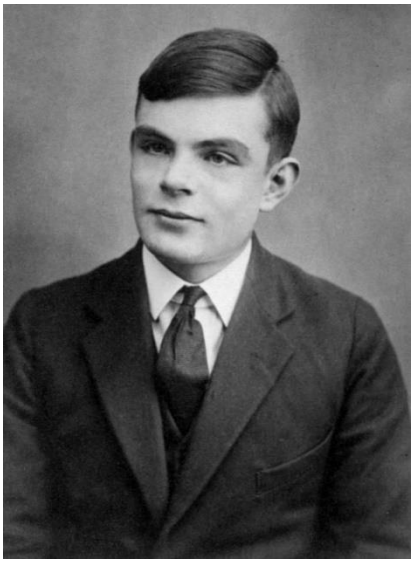
Obsah:

Použité zdroje:

https://en.wikipedia.org

SINGH, S. Kniha kódů a šifer

Alan Mathison Turing (23. června 1912 – 7 června 1954)



Alan Turing se zapsal ke špičkovým vědcům prolomením tajných kódů a systému šifrovacího stroje Enigma a tím tak nepřímo pomohl Spojencům k zásadnímu benefitu v dění 2. světové války. I přes všechen věhlas a obrovský inteligenční potenciál, díky němuž se mohl Alan Turing celý život věnovat průkopnictví moderní informatiky, byl jeho život ukončen velmi brzy a za velmi smutných okolností, kdy přestaly být podstatné jeho pracovní výsledky a na Alana Turinga začalo být pohlíženo pouze a jen z hlediska roviny osobní.

Dospívání

Celým jménem Alan Mathison Turing se narodil v čtvrti Maida Londýně 23. června roku 1912 jako syn manželů Julia a Ethel Turingových. Před narozením syna bydleli Turingovi rodiče v Chatrapuru, ve městě ležícím poblíž Madrasu v jižní Indii. Zde působil Julius Turing, otec Alana, jako úředník. Rodiče si však přáli, aby jejich dítě narodilo na území Anglie. Krátce po narození malého Alana se otec vrátil zpět do Indie. Dalších patnáct měsíců později, odjela také jeho matka. Malý chlapec se tak stal jakýmsi „sirotkem“, kdy rodiče bydleli tisíce kilometrů daleko, zatímco o Alana se starali rodinní přátelé a také chůvy. Počítalo se s tím, že jakmile Alan dospěje do potřebného věku, stane se žákem internátní školy, kde převezmou jeho výchovu. Když bylo Alanu Turingovi 14 let, zapsal se na školu Sherborne School v Dorsetu, kde ho také přijali. Naneštěstí se jeho první školní den konala generální stávka. Preciznost a důslednost byla Turingovi vlastní celý život. Na svoji školní premiéru se rozhodl dostavit do školy včas, a tak jel na kole. Asi by nešlo o nic mimořádného, kdyby ovšem vzdálenost do školy od místa bydliště nebyla 100 km. O tomto neuvěřitelném sportovním výkonu mladého chlapce tehdá dokonce psaly místní noviny.

Počátky vědecké kariéry

Ze začátku byl Turing dost průměrný student. Výjimkou byli přírodní vědy, v nichž se projevoval určitý talent. Nikdo by tehdy z profesorského sboru Sherborne School neřekl, že jejich nenápadný a tichý žák bude hrát klíčovou roli v hodně válečných strategiích 2. světové války. Turing byl studentem spíše držícím se v ústraní, kterého stresoval poměrně přísný školní výchovný dril. Našel však člověka, se kterým si hodně rozuměl, talentovaného nadšence pro přírodní vědy, jako byl on sám, Christophera Morcoma. Za krátký okamžik se z nich stali nerozluční přátelé. Morcom byl nejspíš ještě více talentovaný než Turing, ale bohužel zemřel na tuberkulózu dne 13. února 1930. Pro Alana představovala jeho smrt obrovskou osobní tragédii. Alana Turinga k Christopherovi poutala i láska. Alan Turing byl homosexuál, a ačkoliv svou orientaci moc neskrýval, byl i přesto hodně obezřetný. Po smrti milovaného člověka se začal ještě více snažit o vědeckou činnost a ze všech sil se usiloval o stipendium do Cambridge. Christopher již totiž byl na Cambridge přijat a není pochyb o tom, že by patřil mezi nejlepší studenty této prestižní univerzity. Roku 1931 byl přijat na King‘s College v Cambridgi.

Matematika a logika

V době kdy Turing studoval na Cambridgi, probíhala mezi studenty velmi intenzívní debata o povaze matematiky a logiky. Doteď totiž platilo všeobecné tvrzení, že na jakoukoliv matematickou otázku lze najít odpověď. Nyní však bylo dokázáno, že na všechny matematické otázky, není zcela zřejmá odpověď. Právě kvůli této vědecké diskuzi napsal Turing odbornou stať s názvem „On Computable Numbers“ (O vyčíslitelnosti), publikovanou r. 1937, v níž se přiklání k novému tvrzení, že v matematice nelze vždy zcela jednoznačně určit, co je pravda a co je omyl, neboť matematická logika je složitější a hlubší pojem, než se všeobecně předpokládalo. Turing zde přichází s vizí zkonstruovat

jakýsi pomyslný stroj, který by prováděl matematické operace či algoritmy. To vše vycházelo z Turingova předpokladu, že by se čísla k vynásobení vložila do stroje prostřednictvím papírové pásky podobné děrné pásce. Výsledek násobení by se pak zapsal na jinou pásku.

Předchůdce dnešního počítače

Výše zmíněný stroj, jehož sestavení Turing zvažoval, by samozřejmě neprováděl pouze operace jako je násobení, ale samozřejmě také dělení, umocnění či rozklad na činitele. Ovšem podle jeho původní vize by na každou operaci musel sestrojit unikátní stroj. Z tohoto důvodu posunul Turing svou představu ještě dál a vymyslel stroj, jehož vnitřní chod by se mohl změnit tak, aby vykonával všechny funkce jednotlivých strojů v jednom. Turing tento imaginární stroj označil jako „univerzální Turingův stroj“, protože by byl schopen odpovědět na libovolnou otázku, kterou si jen dokáže vymyslet. Turing se tak stal zakladatelem moderní informatiky. Doba studia na Cambridgi byla pro Turinga velmi šťastným obdobím. Dosáhl velkého akademického úspěchu a překvapivě se pohyboval také ve velmi tolerantním prostředí, protože se jeho zakázaná orientace utajila.

Enigma

Druhá světová válka výrazně ovlivnila životy mnoha lidí – vojáků, civilistů a samozřejmě i nejrůznějších akademiků. Alan Turing byl, i přes svůj nízký věk, natolik uznávanou osobností v oblasti matematiky a logiky, že to nebylo moudré během 2. světové války oslovit právě jeho ke spolupráci s kryptoanalytickým oddělením, aby pomohl svým intelektem k prolomení kódu šifrovacího stroje Enigma.

Enigma – legendární šifrovací stroj, jehož šifra byla dříve jednou prolomena polským studentem statistiky a nadaným matematikem Marianem Rejewskim. To už se však první světová válka chýlila ke konci. Za tu dobu Enigma, jak je běžné u všech zařízení, prošla dalším vývojem a vyšším zabezpečovacím procesem. O dvacet let později se zdála být její funkce díky přidaným kotoučům určených k zašifrování textu neprolomitelná, neboť kódových variací vznikl téměř nevyčíslitelný počet s neuvěřitelným množstvím nul. Alan Turing tenkrát však dokázal něco, co můžeme označit za naprosto geniální tah v dějinách kryptoanalýzy. Zjednodušeně lze říct, že Turing po precizní analýze jednotlivých možných zapojení obvodů Enigmy v kombinaci s nastavením kotoučů, vymyslel možnost prověřovat jednotlivé okruhy na samostatných dešifrovacích strojích, kterým se slangově říká „bomby“. Tyto „bomby“ vlastně představovali předchůdce počítačů, resp. právem je již jako počítače můžeme nazývat. Komplex Turingových počítačů dokázal v té době ve velmi rekordním čase (cca jedna operace za vteřinu) prověřit nejrůznější kombinace uspořádání kotoučů a propojovacích mechanismů. Tyto „bomby“ ověřovaly nastavení kotoučů a odhalovaly klíče, přičemž klapaly jako milion pletacích jehlic. Když šlo všechno dobře, bomba mohla nalézt klíč Enigmy za hodinu. Jakmile se podařilo pro konkrétní zprávu určit nastavení kotoučů, bylo už jednoduché odvodit denní klíč a dešifrovat všechny ostatní zprávy zaslané téhož dne.
Po skončení válečného konfliktu bylo na Turingův převratný proces v dějinách kryptoanalýzy uvaleno informační embargo a až o skoro 30 let později směl být zveřejněn proces kryptoanalýzy prolomení šifrovacího stroje Enigma. Alan Turing se mohl i nadále věnovat své vědecké činnosti, nicméně z pohledu člověka, který již svůj převratný objev učinil a nesmí jej jakkoliv dát do povědomí veřejnosti, byla poválečná léta možná na horším bodě nežli vzestupná kariéra v době cambridgeských studií.

Tragický konec

Po válce se Turing věnoval vývoji prvních počítačů řízených programem, který je uložen v jejich vnitřní paměti. Šlo však jen o zbytky bývalého úspěchu, na nějž bylo uvalena mlčenlivost. A tak se veřejnost více zajímala o Turingův soukromý život. Tolerance Turingovy sexuální identity z dob jeho studií se vytratila. Alanu Turingovi se stal r. 1952 osudný tím, že mu byl vykraden byt. Vědec se tehdy snažil

nezamlčet žádná fakta a důkazy, a tak přiznal při výslechu na policii i svoji homosexuální orientaci. Homosexualita byla v Británii trestný čin až do roku 1994. Tím pádem se Alan Turing stal dle tehdejších britských zákonů pachatelem trestného činu. Soud mu nařídil navštěvovat psychiatra a podstoupit hormonální léčení. Ze všech výzkumných činností byl samozřejmě již talentovaný matematik navždy vyloučen. Hormonální léčba, psychika zbořená ztrátou zaměstnání, které představovalo celý jeho život a obezita. Všechny tyto překážky byli poslední kapkou k ukončení života jednoho z nejtalentovanějších vědců v matematicko – informatické oblasti 20. století. Alan Turing už neměl sílu zvládat neustálé depresivní stavy a silné zdravotní problémy. Dne 7. června 1954 ukončil Alan Turing svůj dvaačtyřicetiletý život. Volbou jeho smrti byl kyanid obsažený v jablku. Vědecký odkaz a přínos v oblasti moderní kryptografie byl u této legendy oceněn až mnoho let později po jeho smrti. Jako cena útechy jeho památky může být snad jen to, že od roku 1966 je udělována tzv. Turingova cena za významný přínos v oblasti informatiky.