Alan Turing – mysliaci stroj kacírskej teórie

Šifry a šifrovanie

Kultúrne dejiny ľudstva už dlho poznajú rôzne spôsoby utajovania. Šifrované správy rozhodovali o osude štátov i jednotlivcov. Tajné šifry prinášali i odnášali veľké finančné čiastky. Z kryptografie sa stala solídna veda s počítačovým vybavením a matematickým softvérom, v ktorom hrajú dôležitú úlohu aj vlastnosti prvočísiel.

Jedným z vynikajúcich matematikov, ktorý prispel k tvorbe šifrovacieho prístroja AGNES, bol **Alan Mathison Turing** (1912 – 1954), priekopník elektronických samočinných počítačov, algoritmizácie a umelej inteligencie.

Cesta životom

Mal veľmi vzdelaných rodičov, ktorí sa zosobášili v Indii. Narodil sa 23. júna 1912 v Londýne. Školu navštevoval v Sherborne (od roku 1926). Potom študoval matematiku na univerzite v Cambridge (od roku 1931). Bol kritizovaný za svoj rukopis, zápasil s angličtinou, z chémie si robil vlastné experimenty, mal svoj myšlienkový svet, v ktorom mali svoje miesto aj teória relativity a kvantová mechanika. V roku 1934 promoval, stal sa členom Kráľovského kolégia (1935) a obhajoval dizertačnú prácu na tému Základná limitná veta pravdepodobnosti. V rokoch 1936 – 1938 študoval na univerzite v Princetone (doktorát u A. Churcha). Počas 2. svetovej vojny bol aj dôstojníkom pre dekódovanie. Od roku 1945 pracoval v národnom fyzikálnom laboratóriu. Neskôr (v roku 1948) prešiel na univerzitu do Manchesteru. V roku 1951 sa stal členom Londýnskej kráľovskej spoločnosti. V roku 1952 bol uväznený za násilné protesty proti obmedzeniam britských homosexuálov. Nečakaná smrť prišla 7. júna 1954 vo Wilmslowe. Vyšetrovanie určilo za príčinu smrti samovraždu otrávením sa kyanidom. Jeho matka tvrdila, že to bola nehoda.



Myšlienky odborných prác

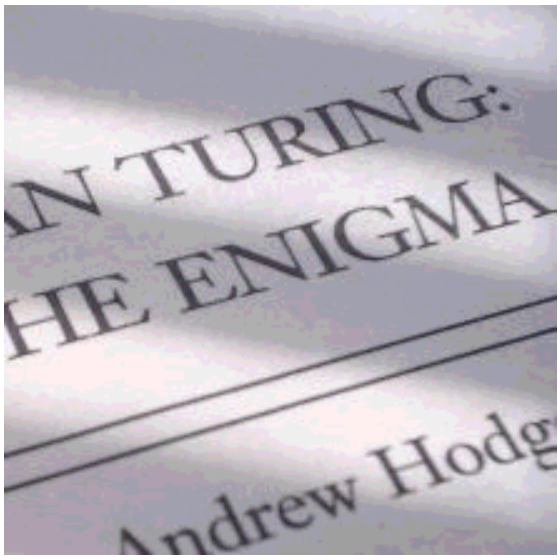
Turing venoval pozornosť matematickej logike a teórii rekurzívnych funkcií. V práci *On Computable Numbers – O vypočítateľných číslach* vypracoval teóriu algoritmov. Súčasne (1936) s E. S. Postom publikoval Turing teóriu abstraktného počítača, v ktorej vysvetlil funkčné procesy počítačového automatu. V roku 1947 zverejnil prácu *Mysliaci stroj – kacírska teória*, v ktorej uvažoval o učiacom sa stroji

a umelej inteligencii. V roku 1950 sa zaoberal biologickými javmi a ich vysvetlením matematickým a algoritmickým popisom.

Turingov stroj

Je to zariadenie, ktoré obsahuje hlavicu a pásku. Hlavica je mechanizmus, ktorý v každom okamihu ukazuje na jedno okienko pásky. Stroj má možnosť posunu o jedno okienko doľava a doprava. V okienkach môžu byť zapísané symboly konečnej abecedy. Páska prechádza čítacou hlavicou, ktorá priradí riadiacej jednotke pre každý okamih jeden z možných stavov. Jednotka obsahuje program, ktorý určuje podľa konkrétneho stavu nový stav. Takto bol opísaný model abstraktného programovacieho stroja na spracovanie symbolov.

Význam diela



Alan Mathison Turing prispel k riešeniu problémov efektívne vyčísliteľných funkcií, aproximácií Lieovych grúp i teórie Riemannovej dzeta funkcie. Spresnil intuitívny pojem algoritmu a rozvinul metódy riešenia algoritmizovateľných problémov. Podieľal sa na realizácii prvého anglického počítača a jeho programového vybavenia. Predpokladal, že stroje môžu imitovať myšlienkové procesy, generovať odpovede mimo rámca ohraničenej množiny možností, prejaviť umelú inteligenciu. Presvedčil seba aj ostatných, že principiálna možnosť riešenia ľubovolného algoritmizovateľneho problému je technicky reálna.

Dušan Jedinák