

SZAKDOLGOZAT

Becskeházi Zoltán

Debrecen

2008.

DEBRECENI EGYETEM
INFORMATIKAI KAR

A SZÁMÍTÁSTECHNIKA ÉS AZ
INFORMATIKA FEJLŐDÉSÉNEK
TÖRTÉNETE

Készítette:
Becskeházi Zoltán
informatika tanár szak
levelező tagozat

Témavezető:
Dr. Papp Zoltán
egyetemi adjunktus

Debrecen

2008.

Tartalom

Köszönetnyilvánítás	4
Bevezetés	5
Számrendszerek kialakulása	6
Számszerszámok	7
John Napier és Edmund Gunter	8
Számológépek	9
Blaise Pascal	10
Gottfried Wilhelm Leibniz.....	10
Joseph Marie Jacquard	11
Charles Babbage és Ada Byron	11
George Boole	13
Herman Hollerith	13
Nulladik generáció (jelfogók, relék)	14
Enigma	16
Colossus	20
Alan Turing	22
Neumann János	24
Noam Chomsky	27
Első generáció (elektroncsövek)	29
Második generáció (félvezetők, diódák, tranzistorok)	30
Harmadik generáció (integrált áramkörök).....	30
Negyedik generáció (mikroprocesszor)	31
Ötödik generáció	33
Korai rendszerek	33
Unix története.....	34
A Minix története	35
Fizetős szoftverek	37
Ingyenes szoftverek	38
A Linux története	40
Az internet története.....	44
Xerox PARC	47
Apple története.....	49
A PC és a Windows története	53
Mesterséges élet	56
A jövő.....	59
Összefoglalás	62
Melléklet	62
Irodalomjegyzék	63

Köszönetnyilvánítás

Ezúton mondok köszönetet segítőmnek, Dr. Papp Zoltán egyetemi adjunktusnak a dolgozat elkészítésében nyújtott értékes segítségéért.

Bevezetés

Az első elektronikus számítógépek megjelenésükkor teremnyi méretű, esetenként bizonytalanul működő, aránylag nehezen kezelhető és csak kevesek számára hozzáférhető szerkezetek voltak. Akkor még nem sejtették, hogy egyszer az ember mindennapos segítő eszközévé válhatnak ezeknek a monstrumoknak továbbfejlesztett változatai.

A gyors technikai fejlődés következtében az elmúlt évtizedekben az életünkben fontos szerephez jutott a számítógép és a világhálózat. Ez az előre mutató fejlődés sok esetben megkönnyítette munkánk elvégzését. A feladatvégzés gyorsasága, pontossága és hatékonysága, a számítógépek hálózatba kötése meggyorsította kommunikációnkat. Ügyintézésünk, bevásárlásunk kényelmesebbé, gyorsabbá vált, miközben egyre inkább kiszolgáltatott helyzetbe kerültünk, a gépek és technikák szeszélyeinek következtében. A mindennapi élet során egyre nyilvánvalóbb, hogy mindazokat, akik nem rendelkeznek az informatikai eszközök használatához szükséges készségekkel, azokat a jövő funkcionális analfabétának fogja tekinteni. Ennek elkerülésére fontos folyamatosan képezni a felnövekvő új generációt.

Dolgozatomban azt mutatom be, hogy honnan indult, hogyan fejlődött, és merre tarthat a számítógép és az informatika fejlődése, egészen a kezdetektől fogva. A teljesség igénye nélkül csak azokat a történeti szempontból főbb állomásokat emeltem ki, amelyek véleményem szerint meghatározták a számítástechnika fejlődésének fő irányát, valamint azt, hogy milyen események hatására fejlődött a matematika és a technika. A számítógép megszületése és fejlődése olyan társadalmi eseményekhez, tudományágakhoz köthető, amelyek sokunknak eszébe sem jutna. Például tájékozódás a tengeren és a világban; a csillagászat; a meteorológia; az atombomba és a hidrogénbomba megalkotása; a hidegháborús fenyegetettség; a titkok megőrzése, és azok feltörése. A fejlődés jelentős „mozgatórugója” lehet a kíváncsiság, a háború vagy éppen a félelem.

A fejlődés, mint annyi minden a mai világunkban a rendelkezésre álló pénz mennyiségéhez köthető, de mégsem az egyetlen meghatározó szempont. Ha van cél, elhatározás, akkor anyagi világunkban is tud működni olyan rendszer, amely felveheti a versenyt a profitorientált fejlesztésekkel – lásd LINUX –, melyet szintén be kívánok a munkában mutatni. A téma zárásául a jövőt vázoló és elképzelő gondolatokat és lehetőségeket tárom fel.

Számrendszerek kialakulása

Már az ősi civilizációknál felmerült a sok és a kevés megkülönböztetésén túl a mennyiségek pontosabb meghatározása, azaz meg kellett tanulniuk számolni. Kézenfekvő volt, hogy távoli elődeink kezdetben az ujjukat használták ehhez a művelethez, ami azzal az előnnyel is járt, hogy azok mindig „kéznél voltak”. Az ujjak száma azonban véges, ezért a nagyobb mennyiségek megszámlálásához más módszereket találtak ki. Kavicsok, pálcikák segítségével vagy fonalakra, bőrcsíkokra hurkolt csomókkal tárolták a megszámlált mennyiségről való információt. Európában a rováspálcák voltak a legelterjedtebbek. Természetesen egy idő után a felszaporodott kavicsok, a csomók és a rovások kezelése is meglehetősen nehézkesnek bizonyult, ezért szükségessé vált az átváltásos számábrázolás, egyben a helyi érték bevezetése.

Az egymástól elszigetelt ókori kultúrákban eltérő számrendszerek alakultak ki. Mezopotámiában a sumérok tízes számrendszeren alapuló hatvanas számrendszert használtak, amelynek máig fennmaradt alkalmazása az óra 60 percre és annak 60 másodpercre történő felosztása, vagy a szögeknél a foknak 60 ívpercre, azoknak pedig további 60 ívmásodpercre való osztása.

A nappalnak és az éjszakának 12 órára való felosztása, illetve az év 12 hónapos tagolása tizenkettes számrendszer használatára utal, amelynek eredete egyelőre nincs megnyugtatóan tisztázva, de egyes kutatók állítása szerint időben megelőzte a hatvanas számrendszer kialakulását.

Indiában az ókori hindu matematikusok is tízes számrendszert használtak, de kezdetben még helyi érték nélkül, külön jeleket használva a 10, 20, ... 100, 200, ... 1000, 2000, ... számokra. Feltételezhető, hogy a hinduk a babilóniai népekkel való kereskedelmi kapcsolataik révén ismerkedtek meg a helyiértékrendszerrel.

Mai ismereteink szerint a tízes számrendszer és a helyiértékrendszer összeolvadása Indiában jött létre, kiegészítve a nulla (üres) fogalmával. Európába pedig minden bizonnyal arab közvetítéssel került. Ma arab számokkal számolunk. A római számok közt például nincs nulla, de erre nem is volt kifejezetten szükség, mert a római számok nem használták a helyiértéket: az X jelentése tíz, és nem $[(1*10) + (0*1)]$, mint a 10-é. Ugyanakkor belátható, hogy római számokkal elég nehéz matematikai műveleteket végezni (számolni, kalkulálni). A nulla mint számjegy ezen segít, e tekintetben a legfontosabb számjegy.

A legrégebbi fennmaradt európai kézirat, amelyben hindu-arab számjegyeket találunk, a 976-ból való spanyol *Codex Vigilanus*. A helyiértékes számábrázolás első európai ismertetése a középkor egyik legjelentősebb itáliai matematikusának, *Fibonaccinak (Leonardo da Pisa)* 1202-ben megjelent *Liber Abaci* című könyvében jelent meg. Az ismertetés ellenére nehezen vert gyökeret az új számírási módszer. Az idegenkedés egyik oka az volt, hogy sokkal nehezebben lehetett a római számjegyekkel vezetett üzleti könyveket hamisítani. Többek között ennek köszönhetően a római számírás használata egészen a XVII. századig volt általános, mellette azonban már az arab számok is kezdtek tért hódítani.

Számszerszámok

A mennyiségeknek számokban való raktározása azonban csak a kisebbik problémát oldotta meg, az egyes számolási műveletek elvégzése továbbra is nagy gondot okozott, mivel azt leginkább fejben kellett elvégezni. Szükségessé vált valamilyen „számszerszám” kiagyaltása. Az első számolóeszköz, amelyet több ezer évvel ezelőtt már használtak, az abakusz (*abacus*) volt. Keletkezésének idejét és helyét máig nem sikerült tisztázni, de valószínűleg mezopotámiai eredetű. A szó egyébként *táblácskát* jelent. Az eszköz az egész civilizált világban nagyon gyorsan elterjedt. Az összeadás és a kivonás igen egyszerűen és gyorsan elvégezhető abakusszal, a szorzás és az osztás azonban már körülményesebb. Népszerűsége abban rejlett, hogy mind a négy alapműveletet el lehetett rajta végezni, pontos volt, és használójának még írni-olvasni sem kellett tudni.

A középkorban először Indiában, majd Perzsiában, Kínában és az arab kultúrákban terjedt el az ún. *rácsos módszer*, amely a szorzási művelet elvégzését könnyíti meg. A *gelosia módszernek* is nevezett algoritmus gyakorlatilag egy szorzótáblát képez, amelyben a szorzandó és szorzó számjegyek abszolútértékeit kell csak egymással összeszorozni és ezeket a szorzatokat egy táblázat elemeinek átlóval kettéosztott részébe írni. Az így kapott, megfelelő algoritmus szerint összeadott számok értéke a szorzatot adja eredményül.

A tengeri hajózásban az egyre távolabbi célok biztonságos eléréséhez létfontosságú a pontos helymeghatározás és helyes navigáció, valamint az ezekhez szükséges térképek és táblázatok készítése. Ezek viszont egyre több és bonyolultabb számításokat követeltek, amelyekhez az egyszerű abakusz már nem volt elegendő. Az idegölő és nehezebb számítások megkönnyítésére a matematikusok táblázatokat állítottak össze.

Az 1600-as év vízváltó a tudománytörténetben. *Galileo Galilei* előtt is léteztek természetesen szellemi óriások, azonban ő tette meg azt a hatalmas lépést, amit a

természettudományok matematizálásának nevezünk. Nagy természettudósok addig is kutatták a természet titkait, végeztek méréseket, azonban Galileire volt szükség, hogy ezeket az adatokat matematikai formulákba foglalva megadja a szükséges lökést a természettudományok fejlődésének.

Az európai matematika nem volt lényegesen fejlettebb az arabnál az ezt megelőző időben, amely az európai és kínai eszméken, fogalmakon alapult. Ekkor azonban hirtelen a matematika és a fizika összekapcsolódásának eredményeképpen történik valami Európában, ami elindítja a természettudományokat a Galileitől Newtonig vezető úton. A gyakorlati, empirikus tudásnak és a matematikának ez az összeolvadása lett a „bölcsök köve”, amelynek érintése egy csapásra megváltoztatja a matematikát és a természettudományokat. 1580 körül *Francois Vieta* világrengető felfedezésként bevezeti a matematikában a betűk használatát az ismeretlenek és az általános paraméterek jelölésére. Azt, amit ma algebrának és aritmetikának hívunk, ő *logistica speciosának* illetve *logistica numerosának* nevezett.

John Napier és Edmund Gunter

A bonyolultabb számítások gyorsításában a logaritmus felfedezése jelentett óriási előrelépést, lévén segítségével a szorzást és az osztást összeadásra és kivonásra lehet egyszerűsíteni. A logaritmussal való számolás szépséghibája, hogy számolás előtt szükséges a tényezők logaritmusának a meghatározása, nemkülönben a kapott végeredményt vissza kell alakítani „közönséges” számmá. A szorzás és az osztás művelete lényegesen leegyszerűsödött, viszont ehhez az is kellett, hogy az átalakítások megkönnyítésére logaritmustáblákat állítsanak össze.

Nagy előrelépés volt a logaritmus elvének felismerése 1594-ben, amely *John Napier* nevéhez köthető. Napier életét a politikának, az ország védelmének szentelte, ám közben matematikai problémák megoldásán dolgozott, azon fáradozott, hogy egyszerűsítse a matematikai feladatok elvégzését. A matematikus nevéhez fűződik a logaritmus elvének kidolgozásán túl még a tizedespont használata, és a rácsos módszer gépesítésére kidolgozott „*Napier-pálcák*” számológép, amelyről az 1617-ben kiadott *Rabdologia* című munkájában értekezett. Ez a mechanikus eszköz a szorzás és az összeadás műveletét tudta jelentősen meggyorsítani.

Ám ennek megjelenése már meglehetősen későn volt ahhoz, hogy széleskörűen alkalmazott eszköz legyen, elterjedésének gátját mégis inkább egy zseniális találmány, a *logarléc* megjelenése jelentette.

A logarléc elődjét *Edmund Gunter* londoni tanár találta fel 1620-ban, amely egy favonalzóra rótt logaritmikus skálából állt. Ezzel az eszközzel a szorzás és az osztás művelete a lényegesen egyszerűbb összeadással és kivonással vált helyettesíthetővé. 1630-ban a *William Oughtred* hasonló elv alapján egy körlogarlécet készített, majd nem sokkal később egyesítette találmányát Gunter eszközével. Ezzel létrejött a mai értelemben vett logarléc. Végleges formája 1650 körül alakult ki, ezekben a konstrukciókban már megjelent a léctestben előre-hátra csúsztatható, megfelelő skálabeosztású nyelv is. A négy alapművelet, valamint a hatványozás és a gyökvonás gyors számolását lehetővé tévő eszköz hamar elterjedt, és közel 350 éven át a mérnöki munka szimbólumává vált. A praktikus és idővel egyre több matematikai művelet elvégzésére alkalmassá tett logarléc az elektronikus számológépek elterjedéséig nélkülözhetetlen kelléke volt diáknak, mérnöknek egyaránt.

Számológépek

A logaritmustáblák használata gyorsan tért hódított, kezelésük azonban meglehetősen lassú volt, és nem minden esetben adtak elegendő pontosságot. A biztonságos tengeri hajózáshoz szükséges helymeghatározás, a földmérés és csillagászati számítások pontos számolást igényeltek. Egyre sürgetőbbé vált a kor követelményeinek megfelelő olyan mechanikus számolási segédeszköz megalkotása, amely egyszerre volt könnyen kezelhető, gyors és pontos, és elegendő érvényes számjegyet adott.

A legelső számológépek közül való *Wilhelm Schickard* szerkezete. A Schickard-gép négy alapművelet elvégzésére volt alkalmas, amelyhez a Napier-pálcák elvét használta fel. A szorzási és osztási műveletek során fellépő részeredményeknek tárolására egy külön mechanizmust készített. A gépezet leglényegesebb szerkezeti elemei azok a megfelelően kialakított és egymáshoz illeszkedő tíz- és egyfogú fogaskerekek, amilyenek a napjainkban is jól ismert fordulatszámológát (kilométermutató, villanyóra stb.) működtetik. Az egyeseket számláló 10 fogú kerék mindegyik fogának egy-egy szám felelt meg 0-tól 9-ig. Annak egy teljes körbefordulásával a vele összekapcsolt egyfogú fogaskerék a tízeseket számláló másik 10 fogú fogaskereket mindössze egy foggal tekeri tovább.

Blaise Pascal

Blaise Pascal, az előkelő nemesi családból származó ifjú mindössze 19 éves volt, mikor megunva az apjának végzett fáradságos adószámításokat, Sthickardtól függetlenül 1642-ben megszerkesztett egy fogaskerekekből álló számológépet (*calculator*). Gépe bizonyos értelemben elmaradt Schickard gépétől, hiszen nem tudta automatikusan elvégezni a szorzást és az osztás műveletét, hanem a szorzást ismételt összeadási, az osztást pedig ismételt kivonási műveletek sorozatára vezette vissza.

A gép ma meglehetősen primitívnek tűnik, ám mégis azt kell mondanunk, hogy forradalmi alkotás volt, koncepciójában minden eddigitől új, hiszen megvalósította a magasabb helyiértékre történő átvitelt.

Tehát a mai ismereteink szerint Pascal alkotta meg az első, bizonyíthatóan el is készült és működő számológépet. Az utókor a nyomás egyik mértékegységét, valamint egy programozási nyelvet nevezett el róla.

Gottfried Wilhelm Leibniz

Pascal összeadásra és kivonásra alkalmas készüléke nem hozott üzleti sikert gazdájának, de híre eljutott *Gottfried Wilhelm Leibniz* polihisztor kortársához, aki élénk érdeklődéssel fordult e technikai kérdés felé. Leibniz meglátta a gépi számolásban rejlő lehetőségeket, és késlekedés nélkül hozzálátott Pascal gépének tökéletesítéséhez azzal a céllal, hogy mind a négy alapművelet elvégezhető legyen vele. Valamikor az 1670-as évek legelején készült el számológépével, amelyben sikerrel házasította össze Pascal szerkezeti elemeit saját találmányával, a bordás hengerrel.

A szerkezet alapját képező úgynevezett Leibniz-kerék valójában két részből állt, az egyik az összeadás-kivonás műveletét végezte el, a másik pedig a szorzás-osztás műveletét oly módon, hogy ezeket automatikusan ismételt összeadásra (kivonásra) vezette vissza. A két részegység egymással kapcsolatban volt. Az összeadó gép gyakorlatilag megegyezett a Pascal-géppel. A négy alapműveletes számológépe nyolcjegyű számokkal dolgozott.

Leibniz nevéhez fűződik egyébként a kettes számrendszer bevezetése is, noha annak semmi köze nem volt számológépéhez. Az informatika és számítástechnika fejlődésében alapvető fontosságú felismerését 1679-ben publikálta.

Joseph Marie Jacquard

A XVIII. században már ismert volt a szövőgépeknél használt lyukkártyás vezérlés, amely Jacquard-kártya néven vált világszerte ismertté. *Joseph Marie Jacquard*, olyan automatikus szövőszéket hozott létre, amelynél fából készült, megfelelően kilyuggatott kártyák vezérelték a bonyolult minták szövését. A módszer, amely forradalmasította a textilipart, lyukkártyák sorozatának alkalmazásán alapult. A „program”, amelyet a különböző módon elhelyezkedő lyukak működtettek, lehetővé tette, hogy a szövőhorgok fölemeljék, illetve lehúzzák a nyüst szálait, így szöve különböző mintákat az anyagba.

Charles Babbage és Ada Byron

A XIX. század Angliájában az ipari forradalom sok olyan változást, fejlődést hozott a termelésben és a gazdasági életben, amely újfajta szemléletet, más hozzáállást követelt meg a munkavégzés módszereiben. Watt gőzgépe, Stephenson gőzmozdonya, 1830-ban a Manchester-Liverpool-vasútvonal megnyitása mind azt a törekvést igazolták, hogy az emberi erőt, a kézi munkát gépekkel kívánják helyettesíteni, felváltani.

Ebben a korban élt és alkotott *Charles Babbage* angol matematikus, akinek már 1812-ben jelentek meg tudományos munkái az aritmetikai táblázatok elemeinek gépi eszközökkel történő meghatározására vonatkozóan. Babbage komoly kutatómunkát végzett egy olyan gépnek a létrehozására, amely a bonyolult, ámde ismétlődő matematikai algoritmusok ember általi fáradtságos munkáját képes kiváltani. A logaritmikus táblázatokban hemzsegő hibák készítették arra, hogy nekifogjon egy olyan berendezés megszerkesztésének, amely a logaritmustáblák számolásának lélekölő munkáját pontosan és gyorsan elvégzi.

1822-re el is készült egy működő modellel, amelyet igen nagy sikerrel mutatott be a londoni Királyi Csillagászati Társaságban. Munkájához Babbage az angol kormánytól megbízást és támogatást kapott. A kormány bőkezű volt, Babbage pedig mesterembereket fogadott, és nekilátott a nagy műnek. Babbage szerkezetének a differenciagép (*Difference Engine*) nevet adta, és azon a felismerésen alapult, hogy az egyszerű függvényértékek (hatvány, logaritmus stb.) kiszámítása különbségek összeadására vezethető vissza. A differenciagép gyakorlatilag azon bukott el, hogy Babbage többre törekedett, mint amire kora technológiája képes volt.

1833-ban, amikor a differenciagép fejlesztésével fölhagyott, kezdte meg azt a fejlesztési tevékenységet, amelynek eredményeként az évtized végére megszületett főműve, az analitikus

gép (*Analytical Engine*) ötlete. E gép alapötlete merőben különbözött a korábbi differenciagépétől, mivel már rendelkezett memóriával, és így képes volt számok és a számított eredmények tárolására. Ekkor már meglehetősen világosan látott több olyan elvet, amely a modern számítógépeket jellemzi. Ez már elvileg majdnem egy modern értelemben vett általános célú számítógép volt. Babbage úgy okoskodott, hogy analitikus gépében a lyukkártya elve az utasítások vezérlésére is alkalmazható.

Az analitikus gép működése: A gép automatikus nyomtatási lehetőséggel rendelkezik, bemenetként lyukkártyákat fogad és képes a lyukkártyákon levő utasítások végrehajtására. Azt mondhatjuk, hogy az analitikus gép sok olyan képességgel és egységgel rendelkezett, amellyel a mai számítógépek, így egy *vezérlőművel*, amely a számítógépet működtette. Egy *számológyművel*, amelybe azokat a mennyiségeket visszük be, amelyekkel a műveleteket éppen végezni akarjuk. Egy *szám- és programtároló* egységgel, amelyben a műveletekben szereplő adatok és a műveletek eredményei helyezkedtek el, a tároló mintegy 200 részeredmény tárolására volt alkalmas 1000 oszlopban 50 fogaskerék formájában.

Jóllehet nem sikerült megépítenie egyik gépét sem, az analitikus gépét - melyen haláláig dolgozott - napjaink elektronikus digitális számítógépei őseinek tekinthetjük.

A szerencse azonban nem pártolt el tőle teljesen. Munkásságára felfigyelt a neves angol költő, *Lord Byron* leánya, *Ada Lovelace*. Ez a rendkívüli asszony módszeres alaposággal tanulmányozni kezdte az analitikus gép tervrajzait, hogy annak minden részletét alaposan megismerje. Nem tartott sokáig, hogy meglássa Babbage terveiben a forradalmi újítást, és elkötelezett hívévé vált a számoló csodamasinának. Számos tanulmányt írt és jelentetett meg az analitikus gép természetéről és jelentőségéről, vagyonos embereknél kilincselte támogatásért, egyúttal tartotta a lelket a csüggedésre egyre inkább hajlamossá váló Babbage-ban. Időközben egy programnyelvet is megalkottak a gépéhez, amely az első a számítógépek történetében. Ada Lovelace azonban váratlanul, 36 éves korában elhunyt, és Babbage magára maradt. 1980-ban az Egyesült Államok Védelmi Minisztériuma egy új számítógépes programnyelvet e hölgy iránti tiszteletből ADA névre keresztelt.

A magába forduló, elmagányosodó feltaláló még két évtizedig élt Ada halálát követően, de komoly eredményt nem tudott felmutatni. Találománya túl korán jött, kora sem becsülni, sem kicsiszolni azt nem tudta. Nevét ma mégis tisztelettel emlegetik az egész világon. A mechanikus számológépek kora tulajdonképpen ezzel le is zárult.

George Boole

A kettes számrendszer pontos leírását először Leibniz adta meg 1679-ben, majd közel kétszáz évvel később, 1854-ben teremtette meg hozzá George Boole az algebrát.

Kutatási eredményeit 1848-ban publikálta, majd 1854-ben adta ki nagy művét, amelyben a logikát precíz matematikai formában öntve, axiómákat felállítva lefekteti a formális logika alapjait. Boole munkája mérföldkőnek számít a matematikai logika és a számítógépek történetében, ugyanis később alapjául szolgált az elektromos kapcsolók logikai műveletekhez való alkalmazhatóságának. Olyan matematikai formalizmust alkalmaz, amelyet a számítógépek programozásánál minden feladat megoldáshoz felhasználunk, különösen, ha a számítógép belsejében végbemenő elemi folyamatokat tekintjük. A Boole-féle algebrában jelentek meg legelőször az olyan logikai műveletek, mint az *és*, a *vagy* és a *negáció*. Boole-lal szinte egy időben hasonló következtetésekre jutott August De Morgan is, akinek Boole-hoz hasonlóan sok logikai tételt köszönhetünk.

Boole munkása különösebb visszhang nélkül maradt, mígnem *Claude E. Shannon* amerikai matematikus és villamosmérnök felfigyelt annak előremutató jelentőségére. Shannon az áramkörök és a logika kapcsolatát úgy írta le, hogy ha egy áramkörben a kapcsoló zárt állását IGAZ logikai értéként értelmezzük, a nyitott állását pedig HAMIS-nak, akkor két kapcsoló soros kapcsolásával az ÉS művelet valósul meg. Két kapcsoló párhuzamos kapcsolása pedig a VAGY műveletet eredményezi.

Herman Hollerith

A szövőgépeknél elsőként alkalmazott lyukkártyákban egyre több feltaláló látta meg az automatizálás lehetőségét. Nem volt ez másként *Herman Hollerith* esetében sem, aki 1879-1883 között történetesen az USA Népszámlálási Hivatalának igazgatói tisztét töltötte be. Különösen sok gondot okozott hivatala számára a tízévenkénti népszámlálás adatainak az összegzése, mivel azokat emberi erővel kellett feldolgozniuk. Ez volt az oka annak, hogy Hollerith a korábbi módszerrel szakítva a soron következő népszámlálás adatait már elektromechanikus úton próbálta meg feldolgozni.

A népszámlálási probléma megoldásához kitűnő eszközt talált. Azt javasolta, hogy lyukkártyákra rögzítsék az adatokat, amelyeket a kártyán levő lyukakat érzékelő gépekkel dolgoznának fel. Arra gondolt ugyanis, hogy ha Jacquard eredményesen tudta használni a lyukkártyákat a szövőgépek vezérlésére, akkor miért ne lehetne ezeket a kártyákat

általánosabban, adatok tárolására és valamilyen feldolgozóeszközhöz adatbevitelre felhasználni.

A belügyminisztérium által kiírt pályázatot Hollerith lyukkártyája és feldolgozógépe, az ún. népszámláló gép nyerte el. Hollerith gépének alkalmazásával az 1890-es népszámlálásnál már lyukkártyákat használtak, és a mintegy 63 millió személy és közel 150 ezer körzet adatainak a korábbiaknál jelentősen gyorsabb, és az elemzések, statisztikák szempontjából lényegesen komolyabb feldolgozása óriási sikert aratott.

A későbbi, tökéletesített változatokban Hollerith gépét már író- és számológéppel is összekapcsolták. A feltaláló nemcsak sikeres konstruktőr volt, hanem előrelátó üzletember is. Szabadalmakkal védette le alkotását, egyúttal létrehozta a *Tabulating Machine Company* kereskedelmi társaságot, amely többszöri bővítés után 1924-től az *International Business Machines Corporation*, azaz az *IBM* nevet kezdte viselni. Ez a vállalat ma is a számítástechnikai ipar óriása.

Nulladik generáció (jelfogók, relék)

XX. század elején már széles körben alkalmazták telefonközpontokban és távíró-berendezésekben a *jelfogót*, vagy másik nevén a *relét*, ami lényegében egyenárammal működtetett kétállású kapcsoló. Működésének lényege, hogy a kapcsoló egyik pozíciójában zárja az áramkört, a másikban pedig nyitja, tehát a két pozíció egymással ellentétes hatású. Ezen az elven működik a számítógép is.

A hétköznapi életben számoláskor szinte minden esetben a tízes számrendszert használjuk. Ez a gyakorlat már kicsi korunktól annyira belénk ivódik, hogy az emberek döntő többségében még csak fel sem merül, hogy másként is lehetséges számolni. Az általunk használt 0-tól 9-ig terjedő jelkészlettel bármilyen számot ki tudunk fejezni, ellenben igen bonyolult feladatsor elé állítanánk az elektronikus számítógépeket, ha azok működését is arra alapoznánk. Érthető, hiszen az elektronikus alkatrészekből álló számítógép fizikai tulajdonságaiból adódóan nem tudja közvetlenül értelmezni a számokat. A mai számítógépek a lényegesen egyszerűbb bináris, azaz kettes számrendszer alapján végzik rabszolgamód számolásaikat. Ehhez elegendő az a helyzet, hogy az elektronikus rendszer adott helyén van-e feszültség vagy nincs. Ez analóg megfelelője az 1 és a 0 számoknak.

Az 1930-as évek elején már világszerte nagy erővel folytak a fejlesztések tudományos intézményekben, egyetemeken, magánvállalatok laboratóriumaiban állami támogatásokkal és magántőke bevonásával. A próbálkozások gyakorlatilag egymástól elszigetelten és

függetlenül, egymás eredményeinek ismerete nélkül zajlottak. Ennek oka, hogy a kormányok felismerték a számítástechnika stratégiai jelentőségét, a háború előszele pedig óvatosságra intette a szakembereket és politikusokat egyaránt.

A titkolózásra persze megvolt minden okuk. A nagy teljesítményű számoló- és számítógépeket a lövegek irányzásához szükséges, ám irdatlanul sok számolást igénylő ballisztikai pályák kiszámításánál alkalmazták sikerrel, de fontos szerepet játszottak a rejtjelezési kódok feltörésében is. Éppen ezért nem egy esetben csak évtizedekkel később szerzett tudomást a világ néhány jelentősebb számítógépes fejlesztésről.

Elsőként *Konrad Zuse* német építészmérnök munkásságáról kell szólnunk, aki ha történetesen nem a náci Németországban él és alkot, akkor számítógépeit feltehetően nagyobb sikerre tudta volna vinni. Ettől függetlenül számos olyan szerkezeti elemet talált fel és épített készülékeibe, amellyel mindenkit megelőzött a világon. A Z1 jelölésű számítógépét még egyetemista korában kezdte összerakni, és 1936-ra készült el vele. Ez azonban még mechanikus szerkezet volt. A három évvel későbbi, Z2 modelljébe már 200 jelfogót épített be, amelyet 35 mm-es filmekre lyuggatott program vezérelt. A Z3-as továbbfejlesztett változat 1941-re készült el, amelyet a világ első, teljesen automatikus, kettes számrendszer alapján működő, programvezérelt számítógépének tekintünk. A szerkezet mintegy 2000 jelfogót tartalmazott és 5-10 Hz órajellel működött. Ez a berendezés sajnos 1944-ben egy légitámadás során elpusztult, de 1960-ban Zuse irányításával rekonstruálták az eredeti modellt. Szintúgy Zuse alkotta meg az első számítógépes programnyelvet, amelynek a Plankalkül (plan calculus) nevet adta.

Az amerikai Harvard Egyetem és az IBM közös kutatócsoportot hozott létre, amelyet egy ambiciózus fiatalember, *Howard Hathaway Aiken* irányított. Aiken az egyetem doktoranduszaként kezdett el foglalkozni a számítógépek problematikájával, s e tárgykörben írt elméleti tanulmányával hívta fel magára a figyelmet. Az IBM munkatársaival közösen 1944-re készítették el a Mark I számítógépet. A berendezés leginkább méreteivel nyugözné le mai szemlélőjét. A számítógépek családjában gigantoszaurusznak számító masina hossza tizenhat, magassága pedig két és fél méter volt, tömege pedig meghaladta a négy és fél tonnát. Összesen mintegy 760 000 alkatrészből állt, ebből majdnem három és fél ezer volt a relé, a huzalkötegek hossza pedig elérte a 800 kilométert. A számok tárolására 72 db számláló szolgált, amelyek mindegyike 23 tízes-számrendszerbeli számjegyet és egy előjelet tudott tárolni. Az adatbevitel lyukkártyákkal történt, a vezérlő programot pedig végtelenített lyukszalag tartalmazta. Minden utasítás három részből állt: az első azt tartalmazta, hogy a művelet elvégzéséhez szükséges adat hol található, a második azt, hogy az eredményt hol kell

tárolni, a harmadik pedig, hogy milyen műveletet kell elvégezni. A gép nagyjából négy másodperc alatt végzett el egy szorzást, és csaknem tizenegy másodpercre volt szüksége egy osztás elvégzéséhez.

A Mark I. építésével egy időben zajlott egy másik számítógép kifejlesztése, mégpedig a Bell Telephone Laboratories társaságnál, *George Robert Stibitz* vezetésével. Az 1940-ben elkészült Model 1 számítógép a telefonközpontoknál alkalmazott hagyományos telefonreléket tartalmazott, és alkalmas volt a komplex számokkal való műveletekre is. Újdonságnak számított, hogy a gépbe szabványos távirókéddel vitték be az adatokat, és az eredmények is ebben a formában jelentek meg. A táviróhálózaton keresztül gyakorlatilag az USA egész területéről lehetett kommunikálni a géppel. Az 1940-ben tartott első bemutatón a New Yorkban lévő gép azt a feladatot oldotta meg, amelyet a New Hampshire-i Dartmouth College-ban tápláltak be távirón keresztül.

Enigma

A harmincas évek második felében a náci Németországnak a hatalmi és területszerző törekvései világossá tették Európa nemzetei számára, hogy egy újabb nagy háború kitörése csak idő kérdése. A háborús előkészületek javában folytak, a haditechnika modernizációja mellett az egyéb technikai fejlesztések is komoly szerepet kaptak. Most először jutott olyan fontos szerep egy számítógépnek, hogy jelentős mértékben befolyásolja a történelem alakulását. A dolog érdekessége, hogy minderről nem is olyan régen szerzett tudomást a világ.

Arthur Scherbius német feltaláló 1918-ban *Enigma* néven (görögül rejtély, talány) szabadalmaztatott egy rejtjelező szerkezetet. Különösen háborús viszonyok között viszont a titkosított üzenetek, adatok megfejtése létérdeke a másik hadviselő félnek, ezért mindent megtesz annak érdekében, hogy a kód feltörésével hozzáférjen az előle eltitkolt információkhoz.

Az Enigma egy olyan elektromos-írógép volt, amely ha lenyomtunk egy billentyűt, akkor egy világító táblán megjelent a hozzátartozó kódolt betű. Ugyanannak a billentyűnek az ismételt leütésekor mindig más-más kódolt betűt adott vissza a gép. A nyílt szöveg adott betűjének titkosításához a gépkezelő a billentyűzeten leüti a megfelelő billentyűt. Ez elektromos impulzust küld a központi keverőegységen keresztül, majd egy visszairányító ezt a beérkező jelet küldi vissza, de már más útvonalon, ahonnan a jel kijutva a kijelzőtáblán kigyűjtja a megfelelő kódot.

Nyilvánvaló, hogy a kulcs és az azt tartalmazó kódkönyv nem kerülhet az ellenség kezébe. Az ugyan nagyon is elképzelhető, hogy szerez egy Enigmát, kódkönyv nélkül azonban kénytelen minden lehetséges kulcsot végignézni. Ha egy perc alatt képes megvizsgálni egy-egy beállítást, és éjjel-nappal dolgozik, akkor is csaknem két hétbe telik, mire végez. Ez így elég jó biztonsági szint volna. Ha azonban az ellenség tíz-tizenkét embert állít rá a feladatra, egy nap alatt is eljut a megfejtéshez. Scherbius emiatt úgy határozott, hogy az alapállások számának és ezáltal a lehetséges kulcsoknak a növelésével fokozza találmánya biztonságát.

Először is egyszerűen cserélhető s egyszersmind felcserélhető keverőtárcsákat alkalmazott. A keverőtárcsák beállítása befolyásolja a titkosítást, tehát meghatározó fontosságú a titkosításban és a visszakódolásban.

A másik újítás az volt, hogy egy kapcsolótáblát iktatott a billentyűzet és az első keverő közé, olyasféle dugaszoló táblát, amelyet a régi kézi kapcsolású telefonközpontokban alkalmaztak. E kapcsolótábla lehetővé teszi a feladónak, hogy beiktasson néhány vezetékot, amelyek még az első keverőtárcsába való belépés előtt felcserélnek bizonyos betűket.

1925-ben már futószalagon gyártották a készülékeket, amelyeket a német katonaság a következő évben már rendszerbe is állított, s ezt követően a kormány és olyan állami intézmények is használták, mint például a vasút. Ez már más volt, mint amelyeket Scherbius korábban adott el, másképpen voltak huzalozva a keverőtárcsaik. A kereskedelmi típusú Enigma tulajdonosai tehát nem ismerték teljes egészében a gép kormányzati, illetve katonai változatát. Az ezt követő két évtizedben a német katonaság mintegy harmincezer Enigmát vásárolt. Scherbius találmánya a világ legbiztonságosabb rejtjelezési lehetőségét teremtette meg számukra, és a második világháború kitörésekor addig soha nem tapasztalt titkossági szinten kommunikálhattak. Bár akkoriban úgy vélték, hogy az Enigmának meghatározó szerepe lesz a náci győzelem kivívásában, végül Hitler bukását segítette elő.

A lengyelek, akik közvetlenül veszélyeztetve érezték magukat a németek által, már 1926-ban felfigyeltek arra, hogy a németek egy új rejtjelezési rendszert vezettek be, mégpedig valamiféle gépi titkosírási módszert. A kód feltörésére vonatkozó minden próbálkozásuk hiábavalónak bizonyult, ezért a lengyel katonai titkosszolgálat a matematikusokhoz fordult.

Lengyelországban a korai kutatások az Enigmával kapcsolatban már 1928-ban elkezdődtek, szinte a német hadrendbeállítás után, bár négy évig semmilyen eredményt nem tudtak felmutatni. A Lengyel Kriptológiai Hivatal úgy döntött, hogy felvesz három végzős matematikust a poznani egyetemről. Úgy kezdték, hogy 22 társukkal együtt elvégeztek egy speciális tanfolyamot a kódfeltörésről. A tanfolyam igazi célja az volt, hogy igazi kódtörő zseniket találjanak. *Marian Rejewsky* mutatkozott a leginkább reményteljesnek. Ő a diplomája

megszerzése után még egy év speciális matematikát tanult. 1932. szeptember 1-jén kezdték el a munkát a Kriptológiai Hivatalnál, Varsóban. Rejewsky 1932 októberében egy külön szobát kapott, és megbízást, hogy nézzen körül az Enigma kutatóknál. Kapott egy régi üzleti-célú Enigmát is, a kiinduló típust. Ez a típus, sok dolgot nélkülözött, amit a katonai verzió tudott. Az Enigma titkának megfejtése akkor kezdődött, amikor Rejewsky rájött, hogy felhasználhatja addigi munkájának az eredményeit az Enigma permutációi néhány tulajdonságának elemzésére.

Az Enigma-kód feltöréséhez vezető úton egy honfitársaitól elfordult német férfi, Hans-Thilo Schmidt tette meg az első jelentős lépést. Az Enigma titkának áruba bocsátásával nemcsak pénzhez juthatott, hanem egyszersmind bosszút is állhatott, tönkretehette hazája biztonságos kommunikációját, és megrendíthette a bátyja által irányított szervezetet. 1931-ben érkezett Belgiumba, ahol érintkezésbe lépett egy francia hírszerzővel, és tízezer márkáért átadott neki két fotokópiát. Ezek lényegében az Enigma használati útmutatói voltak, és noha nem tartalmazták a keverőtárcsák huzalozási módjának pontos leírását, olyan utalásokat azonban igen, amelyek a huzalozás kikövetkeztetéséhez használhatóak voltak. Schmidt árulásának köszönhetően a szövetségesek most már meg tudták építeni a német katonai Enigma pontos mását. Ez azonban még kevés volt az Enigmával sifírozott üzenetek megfejtéséhez. A kód ereje nem a gép titkának megőrzésétől függött: a titok (a kulcs) az alapbeállítás volt. Ha egy kriptográfus meg akart fejteni egy elfogott üzenetet, akkor nemcsak egy Enigmára vagy annak pontos másolatára volt szüksége, hanem arra is rá kellett jönnie, hogy a lehetséges kulcsok milliárdjai közül melyiket használták a visszakódoláshoz. A német nyelvű előterjesztés ezt így fogalmazza meg: *„A titkosítási módszer biztonságának értékelésekor feltételeztük, hogy a gép az ellenség rendelkezésére áll.”* A lengyelekkel szemben a franciák még annyi fáradságot sem vettek, hogy megkíséreljék megépíteni az Enigma mását, mert meg voltak győződve, hogy a következő probléma megoldása, azaz egy-egy konkrét Enigma-üzenet kulcsának megtalálása képtelenség. A németek további elővigyázatossági intézkedésként beiktatták azt is, hogy a napi kulccsal együtt minden üzenettel egy-egy új üzenetkulcsot küldtek. Természetesen erről sokáig nem tudtak, illetve azt sem, hogy beállításait hogyan írták át néhány karakterre.

A lengyeleket minden érdekelte, aminek valami köze volt az Enigmához, ezért a franciák egy katonai együttműködési megállapodásnak megfelelően egyszerűen átadták nekik a Schmidt-féle dokumentumok fotókópiáit, és az Enigma kód feltörésének reménytelen feladatát a lengyelekre hagyták. A Schmidt-féle dokumentumok nemcsak a keverőtárcsák belső huzalozására utaltak, hanem részletesen leírták a németek által használt kódkönyvek

felépítését is. Ezen tudás birtokában képesen voltak másolatokat készíteni az Enigmáról, és elolvasni a német üzeneteket. Ugyanakkor rájöttek arra is, hogyan közlik a címzettel az éppen érvényes beállításokat. Rejewski arra az alaptételre építette fel a stratégiáját, hogy az ismétlés a kód gyöngesége. Az Enigma esetében a legnyilvánvalóbb ismétlődés az üzenetkulcs volt, amely sifírozott formában kétszer is ott állt minden üzenet legelején. A németek ezzel a kétszerezéssel küszöbölték ki a rádióinterferencia és a kezelő tévedése által bekövetkező hibákat, azzal viszont nem számoltak, hogy ezzel az egész kódolási eljárás biztonságát veszélyeztetik. A lengyelek a franciákon keresztül még mindig kaptak információkat Schmidttől. A német kém azzal, hogy 1931-ben kiszolgáltatta a franciáknak az Enigma két dokumentációját, nem fejezte be a tevékenységét, még hét évig folytatta. Schmidt minden egyes találkozóra vitt egy vagy több kódkönyvet, amelyek mindegyike egy hónapra szóló napi kulcsot tartalmazott. A kulcsok rengeteg időt és fáradságot takaríthattak volna meg Rejewski számára, azonban ezeket az információkat nem adták át részére. A Kriptológiai Hivatalnál úgy gondolták, hasznosabb, ha Rejewski még békeidőben felkészül a háborús időkben rá váró feladatok segítség nélküli ellátására.

A második világháború kezdetéig a lengyel kódtörők szinte egy az egyben tudták olvasni a német kódokat. A németek az Enigmát 1939-ben továbbfejlesztették, a kód egyszerre zavaros betűk sorává változott, amellyel szemben már a lengyelek tehetetlennek bizonyultak. Az Enigma-kezelők a már meglévők mellé két-két új keverőtárcsát kaptak, miáltal a tárcsák hatvanféle egymásutániséget vehettek föl. A következő hónapban, amikor a németek a kapcsolótábla vezetékeinek számát hatról tízre emelték, tovább romlott a helyzet. A keverőtárcsákba történő jelbevitel előtt már nem tizenkét betű felcserélésével kellett számolni, hanem húszéval. Az elméletileg lehetséges kulcsok száma 159 000 000 000 000 000 000-ra növekedett. Belátható, hogy ezután a németeket még az sem zavarta, ha néhány Enigma az ellenség kezére került. A lengyel oldal megalkotta az Enigma matematikai megoldását, viszont nem volt megfelelő méretű számítási kapacitásuk ahhoz, hogy alkalmazni is tudják. Az addigi kódfejtési eredményeiket viszont átadták a francia és az angol katonai hírszerzésnek. Sokáig azonban ők sem tudtak mit kezdeni a kóddal.

Becslések szerint 1942 végére a németek legkevesebb 30 ezer Enigmát gyártottak le. Valamennyi katonai parancsnokságon, Luftwaffe-támaszponton, hadihajón, tengeralattjárón, kikötőben, nagyobb vasútállomáson, SS-osztagnál és Gestapo-központban volt belőle. A német híradós tisztek igen megbízhatónak tartották, és biztonságosnak hitték ezt a gépezetet. Ami nem meglepő, ha figyelembe vesszük az Enigma által előállítható permutációk irdatlan számát. Az áramkörök folyton változtak, permutációik száma csillagászati volt.

Ezekben az időkben nem voltak még szuperszámítógépek, sőt, egyáltalán nem voltak számítógépek, úgyhogy az ellenségnek a kód megfejtésére irányuló számításait legfeljebb kézi, mechanikus számológépek gyorsíthatták. Látható tehát, hogy csak az volt képes dekódolni az üzeneteket, aki ismerte a tárcsakiválasztást, a tárcsák indulóhelyzetét és a kapcsolótábla-csatlakozásokat. Ezeket pedig a németek igen gyakran változtatták. Fel sem merült bennük, hogy ilyen számadatok mellett esetleg megfejthették a kódot. Pedig így történt.

Colossus

A briteknek kezdetben nem volt birtokukban Enigma, így nem volt sok esély az üzenetek megfejtésére. Ezért az angolok majdnem feladták. Különösen a rotorok huzalozása volt ismeretlen addig, amíg egy 1939. július 25-én egy titkos megbeszélésen a lengyelek át nem nyújtottak egy Enigma replikát a megdöbbsent angoloknak.

A brit kódfejtők főhadiszállását a háború kitörésekor a Londontól 40 mérföldre lévő Bletchley Parkban rendezték be, ahol a legkiválóbb matematikusokat és elméket állították csatasorba. Eredménytelenül. A németek kódjainak visszakódolása olyan hatalmas mennyiségű számolást vett igénybe, hogy a berlini hadvezetés joggal gondolhatta, véges idő alatt képtelenség emberi erővel megfejteni rejtjelezett üzeneteiket. A hadiszerezése azonban az angolok mellé állt. Egy tengeri ütközet során sikerült elfoglalniuk egy súlyosan megrongálódott német tengeralattjárót, ahonnan megszerezték az aktuális kódkönyveket. Ennek és egy kezdetleges számítógépnek a segítségével sikerült visszafejteni a német haditengerészeti egységek közötti üzenetváltásokat.

1940-ben a német légerő porig bombázta Coventryt Angliában, és iszonyú károkat okozott a polgári lakosságnak. Az angolok – Winston Churchill vezetésével – megmenthették volna a várost, mivel előzetesen tudomásuk volt a készülő támadásról. Ehelyett a város és számos emberélet feláldozása mellett döntöttek, sőt még sok más helyen és időben hoztak áldozatot annak érdekében, hogy Hitler és a német katonai főparancsnokság előtt titokban maradjon a „holtbiztosnak” tartott rejtjelrendszer megfejtése. A szövetségesek ismerték az ellenség terveit, parancsait, gyakran előbb tudták, mint a német harctéri parancsnokok.

Alan Turing is itt dolgozott, ő volt az „Univerzális Turing-gép” megalkotója, amely a modern digitális számítógéptechnika koncepcionális elődje. Rájöttek arra, hogy hogyan lehet kiiktatni néhány beállítást, és így drasztikusan lecsökkentették a lehetőségek számát.

A brit titkosszolgálat azonban nem sokáig örülhetett szerencséjének, a németek 1942 februárjában átálltak az Enigma egy még továbbfejlesztett változatára, és az addig alkalmazott kódtörő matematikai módszerek egy csapásra elavultak. Folytatódott a sötétben való tapogatózás, amely temérdek munkával járt ugyan, gyakorlati eredménye azonban nagyon csekélynek bizonyult. A feszített tempójú munka közel egy év után sem hozott átütő sikert. A végtelenségig kígyózó egyenletekkel, függvények és matematikai modellek seregével való küzdelem már-már kilátástalannak látszott, amikor a Bletchley Park-i kriptográfusok stratégiát váltottak. Úgy gondolták, nem elég új matematikai modellek után kutatni, hanem a számolási kapacitást kell növelni, éspedig egy speciálisan erre a célra kifejlesztett számítógéppel. *Alan Turing* matematikus elmélete alapján *Thomas Harold Flowers* postamérnök és *Max Newman* professzor nekiláttak egy ilyen berendezés megalkotásának, amelynek a Colossus fedőnevet adták.

Az idő sürgetett, hisz a háború javában dúlt és még senki sem tudta megmondani, mi lesz a vége. Az 1943 márciusától számított tervezés kezdetétől a kész számítógép 1944 januárjában tartott beüzemeléséig mindössze 10 hónap telt el, de az eredmény minden várakozást felülmúlt. Még abban a hónapban sikerült a Bletchley Park-i kriptográfiai kommunában a Colossus segítségével megfejteni egy német üzenetet, amelynek feltöréséhez korábban hónapokra lett volna szükség. Attól a naptól kezdve a titok többé nem számított titoknak. Az angol hadvezetés nemcsak nyomon tudta követni az ellenséges tengerészeti egységek mozgását, hanem előre tudta azok tervezett hadmozdulatait is. A Harmadik Birodalom tengeralattjáró-flottája teljesen kiszolgáltatott helyzetbe került. A németek számára érthetetlennek tűnt az angolok tájékozottsága, ennek ellenére a németek szentül meg voltak győződve az Enigma feltörhetetlenségében. Inkább hittek abban, hogy a tengerészeti egységek mozgásairól radarok segítségével szerez tudomást az ellenség, nem pedig az üzenetek megfejtése által. Évtizedekkel később derült ki, a Colossus naponta 3000 kódolt üzenetet volt képes megfejteni, közöttük Hitler levélváltásait is. Ez utóbbiakból kiderült, hogy Hitler elhitte a szövetségesek dezinformációit. Történetesen azt, hogy Normandia helyett a Calais-szoroson át indul majd a támadás, és Dél-Angliában állomásozik az átkelésre váró hadsereg. Emiatt Hitler Belgiumban állomásoztatta páncélos divízióit. A normandiai partraszállást követően a szövetségeseknek első dolguk volt Észak-Franciaország telefon- és távíróvezetékeinek a megsemmisítése, arra kényszerítve a németeket, hogy rádiók útján tudjanak csak kommunikálni az egységekkel.

A Colossus megépítéséről csak alig néhány ember tudott, létezésének a pusztta ténye is a lehető leghigorúbb hadititoknak számított. Olyannyira, hogy az ott történetekre csak a múlt

század hetvenes éveiben derült fény, az angol kormány pedig csak 2000 szeptemberében oldotta fel a teljes titkosítást. Csak ekkor kerültek hozzáférhetővé a Colossusra vonatkozó tervrajzok és leírások. Mint utólag kiderült, a háború végéig összesen tíz, fokozatosan fejlesztett Colosszus készült el, de Németország kapitulációját követően Winston Churchill parancsára nyolcat szétszedtek, a maradék kettőt pedig 1960-ban likvidálták. Hasonlóképpen az összes velük kapcsolatos dokumentáció is megsemmisítésre került, mindössze néhány leírást hagytak meg a tudománytörténészek számára. Ez utóbbiak titkosításának feloldására került sor az ezredfordulón.

A Colossusok rászorgáltak a nevükre szobanagyságú méretük miatt, de nem ez az oka annak, hogy a fentiekben kissé részletesebben foglalkoztunk történetükkel. Mivel létezésükről sokáig nem tudtak, egészen a közelmúltig az 1946-ban elkészült ENIAC-ot tartották a világ első elektronikus számítógépének. A Colossus (akárcsak az ENIAC) már nem elektromos jelfogókkal, hanem elektroncsövekkel működött. Az elektroncsövet még 1906-ban találta fel *John Ambrose Fleming*, de kezdetben csak a távközlésben alkalmazták. A Colossus jelentős sikere elsősorban abban mutatkozott meg, hogy megalkotói a kapcsolási mechanizmust elektroncsövekkel oldották meg, amely nagyságrendekkel gyorsabb az elektromos reléknél, ráadásul nem tartalmaznak mozgó alkatrészeket.

Alan Turing

Alan Turing nem épített tényleges berendezéseket, konstrukciói papíron maradtak. Célja a formális logika egy rendkívül mély problémájának vizsgálata volt. Automatái arra voltak jók, hogy segítségükkel leírja, hogyan lehet az alapproblémával megbirkózni. 1936-ban alkotta meg azt a matematikai objektumot, a róla elnevezett automatát vagy gépet, mint olyan „szerkezetet”, amellyel matematikai problémák megoldhatók.

Turing vizsgálatának középpontjában a bináris számjegyekből álló végtelen sorozatok állnak. Arra a kérdésre keresett választ, hogy adott, előírt sorozatokat mely automaták képesek létrehozni. Az általa felállított szabályok értelmében egy automata akkor tud egy ilyen sorozatot megalkotni, ha bemenetként vagy utasításkészletként a szalag egy véges darabja, azaz egy véges számú négyszöget tartalmazó szalag szolgál, és akkor tudja leírni a végtelen sorozatot, ha végtelenítve fut. Más szóval, ha az automata akármeddig működhet, a végtelen sorozat bármely kiválasztott – véges – részét viszonylag rövid idő alatt létre fogja hozni.

A Turing által bizonyított eredmény érdekes volt és váratlan. Azt jelenti, hogy létezik univerzális automata abban az értelemben, hogy ki tud számítani minden olyan sorozatot, amit valamelyik speciális automata ki tud, föltéve, hogy megfelelő bemeneti utasításokat kap. Elég paradoxnak tűnik az eredmény, hiszen elvileg a legkülönbözőbb méretű és bonyolultságú automaták képzelhetőek el. Mindazonáltal Turing bebizonyította, hogy igaz. Lényegében azt mutatta meg, hogy minden speciális automata leírható egy véges utasítássorozattal, és ha ezt betápláljuk az általa definiált univerzális automatába, akkor az ennek hatására a speciális automatát fogja szimulálni.

Neumannt rettenetesen izgatta a dolog, és 1947-ben két fő területre kezdte összpontosítani tevékenységét: egyrészt azt vizsgálta, mennyire bonyolultnak kell egy berendezésnek vagy konstrukciónak lennie ahhoz, hogy képes legyen önmagát reprodukálni. Másrészt annak a problémának akart a végére járni, hogyan kell meghibásodásra képes alkatrészekből egy berendezést optimálisan megszervezni.

Ezek a gondolatok szorosan kötődnek Gödel látványos eredményéhez, amellyel a matematikai logikát egy számításelméleti problémává redukálta. Valójában azt mutatta meg, hogy a logika alapvető fogalmai rekurzívak, ami azzal egyenértékű, hogy ki lehet őket számítani a Turing-féle gépen.

Nem fordulhat elő ellentmondás vagy következetlenség. Visszautasították, hogy *„egy állítást akár igaznak akár hamisnak tekintsenek, hacsak nem létezik olyan eljárás, amellyel ez a dilemma eldönthető”*. A szóban forgó eljárásnak véges sok lépésből kellett állnia, és csak véges sokszor volt szabad felhasználni. A végtelen halmazok esetében elvetette a kizárt harmadik elvét, amely azt mondja ki, ha egy állítás igaz, akkor az ellentétének hamisnak kell lennie. Ezt a törvényt valamennyien jól ismerjük a sík geometriájából, ahol gyakran bizonyítunk állításokat úgy, hogy azt mondjuk *„tegyük föl, hogy az állítás ellenkezője igaz”*, és ebből a föltevésből abszurd következtetésre jutunk.

Ilyen körülmények között lépett színre Neumann 1924-ben. 1927-ben tette közzé híres dolgozatát a matematika ellentmondás-mentességének problémájáról. Érdekes megjegyezni, hogy Neumann ez időben azt sejtette, hogy az analízis egészének konzisztenciáját be lehet bizonyítani. Néhány évvel később, 1930-ban a matematika és a logika másik nagy fiatal kutatója, Kurt Gödel megmutatta, hogy bizonyos logikai struktúrák szükségképpen tartalmaznak olyan állításokat, amelyek igazsága az adott rendszeren belül nem dönthető el. A bizonyítás nagyon egyszerű volt. Tulajdonképpen *„egy olyan igaz tételt alkotott, amelynek formális bizonyítása ellentmondásra vezet”*.

Neumann szerint Gödel volt a logika legnagyobb művelője Arisztotelész óta.

Neumann János

Miért olyan fontosak a számítások az emberiség számára? Első ránézésre úgy tűnhetnék, hogy a számolás az emberi tevékenységnek csupán csekély részét alkotja. A Galilei utáni világban úgy festhet, hogy a matematika az egyik lábával a természettudományok, a másikkal pedig a számolás talaján áll. Éppen ezért az átlagember azt gondolhatná, hogy intellektuális tevékenységének csupán kicsiny részét kell a számításokra vesztegetnie. Az átlagembert azonban továbbra sem érdekli túlságosan, mivel számára úgy tűnik, a számítások tudománya inkább csak a műszaki kérdésekkel van kapcsolatban, és ennél fogva a mindennapok világában meglehetősen érdektelen. Annak, hogy ez még sincs egészen így, az első igazán jó példája valószínűleg a mindennapi időjárás-előrejelzés. Említhetnénk ugyan számos más példát is, amelyek mindegyikéről úgy tűnik, csak áttételesen vagy közvetve befolyásolja az emberek mindennapjait.

A számítógép számos olyan problémát képes megoldani, amely matematikai formulákba önthető, ez mégis meglehetősen steril és aligha kielégítő definíció, hiszen azt sugallja, hogy a tudományos és műszaki alkalmazások az utca emberétől igen távol állnak. Helyesebb ezért, ha felismerjük, hogy az, amivel a számítógép valójában foglalkozik, nem csupán a számok világa, hanem a szó szélesebb értelmében vett információ. Nem kifejezetten a számokkal dolgozik, hanem inkább az információk átalakításával és továbbításával. A tárolt program koncepciójának legnagyobb jelentősége talán éppen ebben rejlik. Mint láttuk, az információt – azaz a valamely problémára jellemző utasításokat – numerikus alakban kódolni és a számítás során aztán a számítógép segítségével tetszés szerint változtatni lehet. Minden bizonnyal innen ered az az ötlet, hogy az információt digitális alakra kell hozni, majd utána tetszés szerint tovább alakítani.

A decimálisról a számok bináris ábrázolására áttérve az aritmetika jelentősen egyszerűsödik ugyan, ezt azonban azon az áron értük el, hogy a szükséges lépések száma jelentősen megnőtt. Elektronikus feldolgozás esetén ez az ár kifejezetten alacsony, viszont elektromechanikus feldolgozásnál lehetetlenül magas. Minthogy egy elektroncsövet tartalmazó áramkör 1945-ben mikroszekundum egymilliomod másodperc - nagyságrendű idő alatt volt képes működni, nem okozott problémát, hogy az ennyi ideig tartó lépésekből ezer darabot kellett végrehajtani. Valóban, ezer mikroszekundum még mindig csak egy milliszekundum - egy másodperc egyezred része. A bináris aritmetika tehát rendkívüli egyszerűsége folytán vált valamennyi modern számítógép csodaszerévé. Az így elérhető előnyök bőséges kárpótlást jelentettek a lépésszám megnövekedéséért.

Neumann a következő véleményen volt: a program igen sokarcú lesz, föl fogja ölelni a műszaki tudományok eredményeit, a formális logikát, a logikai tervezést és programozást, a matematikát és néhány forradalmian új, jelentős alkalmazást. Ez utóbbi az 1948-ban keletkezett numerikus meteorológia lett.

A következőket írta: „*E program célja egy teljesen automatikus, digitális, általános célú elektronikus számológép kifejlesztése és megépítése... Továbbá, bár a gép kifejezetten digitális jellegű, fontos, hogy néhány folytonos változású berendezéssel is föl legyen szerelve, amelyek lényegében alternatív be-, ill. kiviteli egységként működhetnek...*

A gép általános logikai vezérlése a memóriából fog történni... bináris számjegyekkel kódolt utasítások segítségével... Ezek az utasítások olyan rendszert alkotnak, amely a gépnek jelentős rugalmasságot biztosít. Várakozásaink szerint hatékonyan és rendkívül nagy sebességgel lesz képes a problémák igen széles osztályának kezelésére... Ilyen értelemben a gépet minden célra alkalmas eszközzé kívánjuk fejleszteni.

...a csillagok kutatásánál is hasznos lehet. A matematikai statisztikában föltétlenül új megközelítési módra fog lehetőséget nyújtani: a statisztikai kísérletek számszerű kiértékelése útján történő vizsgálatokra...

Mindezeket túl azonban egy ilyen gép ésszerű fölhasználás esetén forradalmasítani fogja számítási módszereinket. Valóban, ez a berendezés minden tárgyilagos vélemény szerint becsülve is tízezerszer (de valószínűleg még ennél is többször) gyorsabb lesz, mint amire a jelenlegi számítási módszerekkel egy asztali szorzógéppel felszerelt ember képes. A ma létező számítási módszereket azonban kifejezetten ezekre a gépekre vagy még ennél is lassúbb (csak az ember közreműködését igénylő) eljárásokra dolgozták ki. A tervezett gép viszont olyan radikálisan meg fogja változtatni a matematikai számítások lehetőségeit, az azokkal kapcsolatos nehézségeket, azok egyes momentumainak lényeges vagy lényegtelen voltát és egész belső rendszerét, oly mértékben föl fogja borítani minden jelenleg alkalmazott eljárás belső egyensúlyát, hogy a régi módszerek hatékonysága el fog törpülni azon újaké mellett, amelyeket ezután kell majd kidolgozni. Ezen eljárások megítélése új kritériumok (matematikai egyszerűség, bonyolultság, elegancia) alapján fog történni.

Ilyen új eljárások kidolgozása egy nagyszabású matematikai és matematikai logikai program végrehajtását jelenti. Ennek bizonyos fázisai már most előre láthatóak, és szükségképpen befolyásolni fogják a megépíteni tervezett gép logikai és vezérlési rendszerét. A munka oroszlánrészét akkor kell majd elvégezni, ha a gép már elkészül és használható lesz. Ekkor magát a gépet kell majd kísérleti eszközként fölhasználni. Várakozásaink szerint a nagy

sebességű számítások jövőbeni fejlődésére döntő hatással lesznek a program jelenlegi szakaszában szerzett tapasztalatok, kidolgozott értékelések és elméleti megfontolások."

A gép alkalmazási területe igen rövid időn belül még a Neumann által ekkor fölvázolt kereteket is kinőtte.

A munkában résztvevők négy csoportra oszlottak, éspedig 1. mérnöki, 2. logikai tervező és programozó, 3. matematikai, 4. meteorológiai csoportokra. Valamennyi területen alapvető jelentőségűt sikerült alkotniuk.

Neumann és munkatársai egy jelentést (*First Draft*) készítettek, amely „*az elektronikus számítógépekkel összefüggő általános logikai megfontolások néhány aspektusával foglalkozó dolgozat közül az első volt.*” Megjelenésük után azonnal elküldték őket az Egyesült Államok Szabadalmi Hivatalának és a Kongresszusi Könyvtárnak egy írásbeli nyilatkozat kíséretében, amelyben azt kérték, hogy az anyagot a nyilvánosság számára tegyék hozzáférhetővé.

A dolgozat a számítástechnika meghatározó jelentőségű dokumentuma, amely sok tekintetben a modern számítógépek alapidokumentumaként értékelhető. Rendkívül részletesen tárgyalta, hogyan lehet egy számítógép működését megszervezni, a gépet megépíteni és programozni. A dolgozatok az ún. Neumann-féle gépet írják le, amelynek struktúrája – csekély módosításokkal mind a mai napig szinte minden modern számítógép számára mintául szolgált.

Nemcsak a tárolt programú számítógépek tervezésének elveit adja meg, de számos rendkívül bonyolult problémát is előre lát, és zseniális javaslatokat tesz megoldásukra.

Minden olyan berendezésnek, amely igényt tart arra, hogy általános célú számítógépnek nevezze, nyilvánvalóan tartalmaznia kell bizonyos egységeket: rendelkeznie kell egy-egy olyan, amelyben az aritmetikai műveletek elvégezhetőek; ahol a számokat lehet tárolni; ahol az adott, megoldandó problémát jellemző utasításrendszert tárolja; amely automatikusan, a megfelelő sorrendben végre tudja hajtani ezeket az utasításokat; és amely a gépet működtető emberrel fenntartja a kapcsolatot. Elvileg kétfajta memóriát vagy tárolóegységet különböztetünk meg: a felhasznált, vagy a számítások során eredményül kapott számok, illetőleg az utasítások tárolására szolgáló egységeket. Ha az utasításokat numerikusan kódolják, és ha a vezérlés valamilyen módon különbséget tud tenni egy utasítás és egy szám között, akkor e két tárolási feladatot egyetlen memóriaegység is elláthatja.

Összegezve tehát úgy tervezték, hogy a gép négy fő részből fog állni: egy aritmetikai egységből, egy memóriából, egy vezérlőegységből és egy be-, ill. kiviteli egységből.

Az aritmetikai egység (központi feldolgozóegység) annak a rendszernek a része volt, amely a gép által eleminek tekintett aritmetikai műveletek végrehajtására készült. Nem volt

rögzített szabály arra nézve, hogy melyek legyenek ezek a műveletek. Az elemi műveletek azonban, bármit választunk is annak, azok, amelyek a gépbe be vannak huzalozva. Minden más műveletet ezekből lehet felépíteni egy megfelelően kialakított utasítássorozat segítségével. Hogy egy szélsőséges példát említsünk, elvileg építhető olyan aritmetikai egység, amely csak az és, a vagy, valamint a nem alapvető műveleteket képes végrehajtani (tulajdonképpen az is elegendő, ha ezek közül csak kettőt), majd a Boole és követői által kidolgozott módon a szokásos aritmetikai műveleteket az említett alapvető logikai műveletekből építik fel, megfelelő sorrendben alkalmazva őket. Nem célszerű persze ezt a megoldást választani, mert túlzottan lassú volna. Kevésbé szélsőséges példa, ha akár a szorzást, akár az osztást, akár mindkettőt elhagyjuk, és csak az összeadást és a kivonást tartjuk meg alapl műveletekként. A szorzás fölépíthető megfelelő sorrendben végrehajtott összeadásokból, az osztás hasonlóképpen.

Noam Chomsky

A második világháború alatt és az azt követő években a kutatási és fejlesztési munkákban forradalmi változások következtek be. A műszaki- és természettudományokban ugrásszerűen megnőtt a magasan képzett szakemberek száma, ráadásul sokkal nagyobb hányaduk kezdett a kutatás és fejlesztés területén dolgozni, mint az azt megelőző időkben. Ez a változás természetesen az új műszaki és tudományos eredmények, velük együtt pedig a tudományos publikációk számának hirtelen növekedésével járt.

Korábban egy szakember viszonylag könnyen figyelemmel kísérhette azt a mintegy 5-6 folyóiratot, ahol tartalmas cikkeket remélhetett. A problémát tovább nehezítette, hogy a publikációk egy része, elsősorban az angolul beszélők számára „szokatlan” nyelven volt írva, mint az orosz, japán vagy akár a magyar.

Az információhoz való hozzáférés igénye hirtelen megnövelte a fordítandó cikkek számát olyannyira, hogy ezt a lényegében egysíkú, majdhogynem mechanikus munkát sem fordítói kapacitással, sem pénzzel nem lehetett győzni.

Ugyanakkor az egyik, éppen abban az időben, az 50-es évek elején kiteljesedő, és az információrobbanáshoz nem kis mértékben hozzájáruló új tudomány, a számítástechnika azt állította, hogy célja a gépies szellemi munka kiváltása. Magától értetődő volt tehát az a törekvés, hogy a fordítást, ezt a gépies szellemi munkát egy számítástechnikai eszköz, a számítógép végezze.

Minthogy azonban a számítógép csak szabatosan megfogalmazott feladat megoldására képes, szükség volt a fordítás, mint feladat formális leírására. Ez volt tehát az a kiváltó társadalmi igény, amely az 50-es években szinte a semmiből egy új tudomány, a matematikai nyelvészet megalkotását eredményezte. Az új tudomány születési évének az 1956-os esztendő tkinthetjük. Ekkor publikálta ugyanis a szakma atyja, és mindmáig egyik legnagyobb egyénisége *Noam Chomsky* munkásságának első eredményeit. A korai és látványos sikerek hatására igen nagy pénzek, dollármilliók áramlottak a szakmába, és ezzel együtt egy sereg kitűnő koponya kapcsolódott be ennek a divatszakmának a művelésébe.

Sajnos a kezdeti lendület – legalábbis ami az új eredményeket illeti – később alábbhagyott, jóllehet az anyagi és személyi feltételek továbbra is kedvezőek voltak. Végül is *Johnson* elnök 1967-ben összehívta a szakma specialistáit, vizsgálnák meg, milyen perspektívája van a természetes nyelvek számítógépes fordításának, várható-e ezen a területen a közeljövőben sikeres áttörés.

A döntés a következő évben született meg: *„Véleményük szerint, a számítástechnika pillanatnyi fejlettsége nem ígér gyors eredményt, a feltételek még nem érettek meg az eredeti célkitűzés megvalósítására.”*

Ennek hatására az elsősorban állami pénzekből csordogáló dollárfolyam csapjait persze azonnal elzárták, és a téma művelői közül sokan más, jövedelmezőbb foglalkozás után néztek, csak a szakma legmegrögzöttebb hívei maradtak. Ezzel a téma a nagy érdeklődéssel kísért gyakorlati tudomány állapotából felemelkedett vagy lesüllyedt (nézőpont kérdése), az elméleti tudományok gyanúsán tiszteletreméltó státusába.

Szerencsére a természetes nyelveknél sokkal egyszerűbbek a mesterséges nyelvek, nevezetesen azok, amelyek nem az emberek közötti kommunikációt, hanem az ember és a számítógép közötti kapcsolatteremtést szolgálják. Fogalmi körük erősen leszűkített, nyelvtani szabályaik egyszerűek, általában nem ismernek kivételt, mondataik egyértelműek.

A matematikai nyelvészet eredményei éppen ezért jóval könnyebben voltak alkalmazhatóak a gépi nyelvek fordításának területén, mind a fordítás elméletének megteremtésére, mind a fordítóprogramok gyakorlati megvalósítására. Így alakult ki azután egy tudomány, a matematikai nyelvészet gyakorlatibb melléktermékeként a számítástechnikai nyelvészet.

A matematikai nyelvészet, vagy ha úgy tetszik számítástechnikai nyelvészet mint tudomány, *Chomsky* 1956-ban megjelent cikkeivel vette kezdetét. Az automata elmélet jó húsz évvel idősebb fiatalabb rokonánál, mégis nagyon szorosan kapcsolódnak egymáshoz.

Első generáció (elektroncsövek)

A gyorsabb megoldásokat keresve a reléket elektroncsövekre cserélték. A bolgár származású *John Vincent Atanasoff* matematikus és *Clifford Edward Berry* villamosmérnök voltak azok, akik elsőként raktak össze elektroncsöves számítógépet 1940-ben az Iowa State College laboratóriumában. Az ABC (Atanasoff Berry Computer) közel 300 elektroncsővel működött, de csak lineáris egyenletek megoldásaira tervezték, és nem volt programozható.

A Colossus 2500 elektroncsövet tartalmazott. Az ma már kétségbevonhatatlan tény, hogy ez volt az első „működőgép”, teljesen elektronikus számítógép, azonban komoly hátránynak számított, hogy csak egy dologra volt képes. Kódot fejteni.

A kor másik széles körben ismert elektronikus működésű számítógépét is katonai célokra, lőtáblázatok készítésére építették. Az Egyesült Államokban megalkotott ENIAC (Electronic Numerical Integrator and Computer) 1945-ben készült el. Az ENIAC lényegében Pascal mechanikus arithmóméterének volt a modernebb változata. Akárcsak a többi korai számítógép, az ENIAC is hatalmas méretűre sikeredett. A 18000 elektroncsövet, 70000 ellenállást, 10000 kondenzátort, 6000 kapcsolót és mintegy 1500 jelfogót magába foglaló robusztus számítógép 30 tonnát nyomott, hossza 30 métert, magassága pedig 3 métert tett ki. Decimális számrendszerben működött, programozása, vagyis átállítása egyik feladattípusról a másikra viszont meglehetősen lassú és bonyolult módon történt. A régi telefonközpontok működési elvéhez hasonlóan, egy dugaszoló tábla segítségével programozták. Noha ballisztikai számításokat nem végeztek vele a háború befejezése miatt, meteorológiai előrejelzésekhez szükséges számolásokat viszont igen, és Teller Ede is használta a hidrogénbomba megalkotása során.

Az ENIAC-csoport feltett szándéka volt számítógépük továbbfejlesztése, amikor annak egyik tagja, *Herman Goldstine* 1944 júniusában véletlenül összefutott kora matematikai zsenijével, Neumann Jánossal. Neumann azt megelőzően sohasem foglalkozott számítógépekkel, de amikor Goldstine az ENIAC körüli problémákról kezdett beszélni, a téma rendkívüli módon érdekelni kezdte. Habozás nélkül csatlakozott a kutatócsoporthoz, amely akkor kezdett el az új, EDVAC (Electronic Discrete Variable Automatic Computer) számítógépen dolgozni.

Neumann az ENIAC felépítésének tanulmányozása során feltehetően gyorsan felismerte, hogy kora rendelkezésre álló műszaki eszközeivel a számítógépek sebességét és kapacitását jelentősen növelni már nem lehetséges. A fejlesztés irányát az alkalmazhatóság kiterjesztésében és a programozás műveletének automatizálásában látta. Ez utóbbit pedig oly

módon gondolta megvalósítani, hogy az adatokat és a programokat is egy helyen, a memóriában kell tárolni, hiszen valójában a programok is számokkal kódolt információk. Ekkor született meg a tárolt programú számítógép elve. A zseniális magyar matematikusnak a számítógépek vezérlésére és logikai konstrukciójára vonatkozó téziseit ma Neumann-elvként ismeri a világ, s noha a számítástechnika eszköztára az eltelt idő alatt a felismerhetetlenségig megváltozott, elvi felépítésük semmit nem módosult. Elgondolásait *a First Draft of a Report on the EDVAC* című tudományos értekezésben összegezte, amelyet 1945. június 30-án adott közre. Ezzel az volt a szándéka, hogy az üzletre is kellően fogékony kollégái ne szabadalmaztathassák az új konstrukciójú számítógépet, hanem váljon az közkinccsé. Ez a lépése később több bonyodalomhoz is vezetett, ugyanis a szóban forgó konstruktőrök ezen önkényes lépést enyhén szólva is nehezményezték.

Második generáció (félvezetők, diódák, tranzisztorok)

A második generációs gépekben már alkalmazták a félvezető eszközöket, a diódákat és a tranzisztorokat. A méret, teljesítményfelvétel és a hőtermelés csökkent, a megbízhatóság viszont tovább nőtt.

Harmadik generáció (integrált áramkörök)

A szerkezetek méretének ilyen radikális csökkenése nyomán az elektronikai ipar és a számítógépek fejlesztőmérnökei vérszemet kaptak. Az újabb és újabb típusok tervezésekor a gyorsaság növelése, a felhasználhatóság kiterjesztése és a megbízhatóság növelése mellett legalább ilyen hangsúlyt kapott a méretek zsugorításának követelménye is. 1949-ben *Geoffrey William Arnold Dummer* brit mérnök fogalmazta meg elsőként, hogy az egyes elektronikai alkatrészeket (ellenállások, kondenzátorok, tranzisztorok, diódák stb.) kis térfogatba kellene összezsúfolni, csökkentve a vezetékek mennyiségét és hosszát. Sőt ez utóbbit úgynevezett nyomtatott áramkörökkel kellene helyettesíteni.

Dummer ötletének a gyakorlatba való átültetésére még tíz évet kellett várni, amikor *Jack Kilby*, a Texas Instruments elektromérnöke elkészítette az első integrált áramkört. Kilby azonban az eredeti ötletet továbbgondolta, s az ő tervezőasztalán már egy olyan szerkezeti egység született, amelyben az egyes elektronikai elemek (ellenállások, kondenzátorok, tranzisztorok) ugyanabból a félvezető anyagból készültek. Ennek szellemében készítette el 1958 októberében az első *chipet*.

Az új technológia újabb hatalmas előrelépést jelentett a számítógépek fejlődésében. Ettől az időtől számítjuk a számítógépek harmadik generációját. Kilby szabadalmat nyújtott be találmányára, de azt sikerrel támadta meg a National Semicondutor cég, ugyanis az ott dolgozó *Robert Noyce* ugyanabban az időben dolgozta ki saját eljárását. De az idő Noycét igazolta, a szilíciumé lett a jövő, kiderült, hogy az elektronika fellegvárát homokra kell építeni. A XIX. század derekán tört ki a kaliforniai aranyláz, aranyásók mosták ki az aranyszemcséket lázas buzgalommal az értéktelen homok közül. Száz évvel később ugyanott épült ki a Szilíciumvölgy, ahol a szilícium (a homok alapanyaga) immáron az aranynál is értékesebb anyagnak bizonyult.

A korszakváltást nemcsak a miniatürizálás jelentette. Nőtt ugyanis a programok nagysága és a feldolgozni kívánt adatok mennyisége is, ezért növelni kellett a tárolók és a perifériák kapacitását is. Nagyjából ezzel egy időben jelentek meg a mágnesszalagok is, amelyeken gyorsabban és több adatot lehetett elhelyezni és előkeresni. A gépek működését ekkorra már minden esetben egy operációs rendszer irányította, amely emberi beavatkozás nélkül hangolta össze a számítógép legfontosabb elemeit. Leginkább azon volt a hangsúly, hogy a gépidő maximális kihasználásának céljából adott időben több programot is futtathatott a számítógép úgy, hogy amíg az egyik éppen szünetelt, áttért egy másik program lebonyolítására. Értelemszerűen megnőtt a jelentősége a magas szintű programozási nyelveknek, napvilágot látott a FORTRAN, az ALGOL és a COBOL, majd a BASIC és a PASCAL, hogy csak a legjelentősebbeket említsük.

Magától értetődően az újfajta számítógépeknél a szöveges információk kiírására már nem feleltek meg a világító diódákból álló számkijelzők. Szükségessé vált olyan eszköz kialakítása, amely olvasható formában tudta megjeleníteni az információkat. Ezek az eszközök lettek a számítógépekhez csatlakoztatható nyomtatók. Kezdetben hengeres, majd a lánc-, a tintasugaras, végül a lézernyomtatók.

Negyedik generáció (mikroprocesszor)

Minőségbeli változással köszöntött be az emberiség korszakváltó gépeinek negyedik generációja. Már a XX. század hatvanas éveiben próbálkoztak olyan műszaki megoldásokkal, hogy egyetlen integrált áramkörön belül valósítsák meg a számítógép feldolgozó- és vezérlőegységeit.

Az Intel cég fejlesztőmérnöke, *Ted Hoff* volt az első, akinek 1969-ben sikerült létrehoznia a világ első mikroprocesszorát, az Intel 4004-est. Ez az a mérföldkő, ahonnét a számítógépek

robbanásszerű elterjedése elkezdődött, kapacitásuk és sebességük évről évre exponenciálisan növekedett, ezzel arányosan viszont a beszerzési áraik folyamatosan csökkentek. Ez utóbbi tényező lényegesen hozzájárult ahhoz, hogy egyre szélesebb tömeghez jutott el a számítástechnika, szinte teljesen átformálva addigi életet.

Az Intel első, kereskedelmi forgalomban kapható 4004-es mikroprocesszora elkészültét hivatalosan 1971. november 15-én jelentette be. A mindössze bélyeg nagyságú alkatrész 2300 tranzisztorból állt, órajele 108 kHz volt, ami másodpercenként 60 000 utasítás végrehajtását tette lehetővé. Ez a mai chippek tízmilliárdos teljesítménye mellett eltörpül, akkoriban azonban még elképesztőnek számított.

Egy csapásra elavulttá váltak környezetünk megszokott gépei, berendezései, és egyik napról a másikra olyanok születtek, amelyekről korábban álmodni sem mertek. A fejlődés egyre szédítőbb tempóra vált, és naponta nyit újabb és újabb távlatokat. Az egyik nap még ultramodernnek hitt gép vagy szerkezet másnapra elavulttá lesz.

A rohamos méretcsökkenés eredményeként a gépek megjelentek a háztartásokban is, ezért elterjednek a játék- és alkalmazói programok. Érdekesség, hogy az informatikai ipar későbbi neves személyiségei is kapcsolatba kerültek az Altair gépekkel. Például Bill Gates is az Altair 8800 gépen írta első programjait. A Commodore lemezegysége az 5,25" méretű floppyt használta, a szalagos egységbe pedig azt a kazettát használhattuk, amelyen ma is tárolhatjuk hangfelvételeinket. A Spectrum gép arról is nevezetes, hogy készítője, Clive Sinclair a munkásságáért 1983-ban megkapta az Angol Királynőtől a lovagi címet, a Sir Sinclair megtisztelő megszólítást. Ma már furcsa, de a Commodore és a Spectrum gépek megjelenítő egységeként elterjedten használták a televíziókat. Sőt, ezek a gépek már színes képpel büszkélkedhettek. Ezeknél a gépeknél a központi egységet egybeépítették a billentyűzettel, és az operációs rendszert ROM-ban tartalmazták.

Olyan szerencsés korban születtünk, hogy mindezeknek szemtanúi és részesei lehetünk. Az űrhajózás megvalósulásának, az internet információs háló kiépülésének, a műholdas kommunikáció, navigáció és helymeghatározó rendszer megszületésének, és még hosszasan sorolhatnánk a technológiai szemléletváltás számtalan elemének a világra jöttét. Persze, szerencsésebbnek mondható a legifjabb generáció. Ők már ebbe születtek, és a világ elképesztő gyorsasággal megújuló eszköztárának alkalmazása nem okoz számukra nehézséget.

Ötödik generáció

Ma már az ötödik generációs számítógépek korát éljük. A hőskor több tonnás gépeinek leszármazottai mára már egy tenyérben elférnek, és azok teljesítményét igen jelentősen felülmúlják. Továbbra is törekvés az egyre gyorsabb, egyre kisebb gépek elkészítése. *Moore tapasztalati törvénye* szerint az egy lapkára szerelt áramköri elemek száma körülbelül 18 havonként megduplázódik. Eszerint azonban a közeljövőben technikai korlátba ütközünk, hiszen jelenleg egy áramköri lapkán az elemek távolsága 65 nm a néhány 100 pm pedig már az atomok átmérőjének mérettartománya. Érdekes kérdés tehát, hogy merre fejlődhetünk tovább. Moore törvénye mellett az internet térhódításával további törvényszerűségekre figyeltek fel. *Ruettgers törvénye* a tárolási kapacitásról: a tárolási kapacitás 12 havonta megduplázódik. *Gilder törvénye* a sávszélességről: a kommunikációs rendszerek teljes sávszélessége 12 havonta háromszorosára növekszik. *Metcalf törvénye* a hálózatok értékéről: a hálózatok értéke az előfizetők számával „négyzetesen” nő.

Az ötödik generáció esetében már nagy hangsúlyt kapnak a hálózatok, a többprocesszoros (többmagos processzorokkal szerelt) gépek, a párhuzamos feldolgozás. A programozási nyelvek kezdetben eljárás-orientáltak voltak, de manapság már egyre hangsúlyosabb a problémaorientáltság. A problémaorientáltságból született meg például a PROLOG programozási nyelv. Ebben a generációban terjednek el az optikai technológiák.

Korai rendszerek

Az elektronikus számítógépek megjelenése forradalmi változásokat indított el azáltal, hogy hihetetlen mértékben megnövelte az adatfeldolgozás sebességét. Az emberre azonban még mindig nagy feladat hárult, a megoldandó problémák programozásának feladata. Egyáltalán nem meglepő tehát, hogy kezdettől fogva nagy hangsúlyt fektettek az olyan módszerekre, amelyekkel a programozók terhein lehetett könnyíteni.

1945-től a számítógép-tudomány a világ legkreatívabb elméit vonzotta magához. Jellemzően mérnöki vagy fizikai háttérrel rendelkeztek, gyakran rádióamatőrök voltak. Fehér zoknit, nejloninget, nyakkendőt és szemüveget hordtak, és gépi nyelven, assemblyben, FORTRAN-ban, illetve fél tucat mára elfeledett nyelven kódoltak. A második világháború végétől a 70-es évek elejéig – a kötegelt feldolgozás és a nagygépek aranykorában – az „*Igazi Programozók*” uralták a számítástechnikát. Az első ENIAC komputerétől többé-kevésbé

folyamatos és öntudatos technikai kultúra létezett, azoké a lelkes programozóké, akik szórakozásból építettek szoftvert.

Egyesek, akik az Igazi Programozók kultúrájában nőttek fel, még a 90-es években is aktívak maradtak. *Seymour Cray*, a Cray szuperszámítógépek tervezője volt az egyik legnagyobb köztük. Egyszer egy teljes, saját tervezésű operációs rendszert vitt be egy saját tervezésű számítógépbe, annak előlapi kapcsolóin keresztül. Oktálisan. Hiba nélkül. És működött.

Az ARPAnet volt az első földrészeken átívelő, nagysebességű számítógépes hálózat. Az Egyesült Államok védelmi minisztériuma a digitális kapcsolattartás egyik kísérleteként hozta létre, de végül egyetemek, hadiipari cégek, és kutatólaboratóriumok százait összekötő hálózattá nőtte ki magát. Lehetővé tette a kutatóknak, hogy addig soha nem látott sebességgel és rugalmassággal cseréljenek információt, és ezzel hatalmas lökést adott a csapatmunkának, hihetetlen mértékben növelve a technikai fejlődés ütemét és intenzitását.

Unix története

1969 az ARPAnet születésének éve, ugyanabban az évben, amikor a Bell Labs egyik programozója, *Ken Thompson* megalkotta a Unixot. Thompson a Multics nevű időosztásos operációs rendszer fejlesztésén dolgozott. A Multics egyfajta próbaként szolgált. Olyan megoldásokat próbáltak ki rajta, amelyek arra irányultak, hogy az operációs rendszer bonyolultságát elrejtse a felhasználók, sőt a legtöbb programozó elől is. Az alapötlet az volt, hogy a rendszer kívülről minél egyszerűbben használható és könnyebben programozható legyen, hogy több „valódi” munkát lehessen végezni vele.

A Bell Labs kihátrált a tervből, amikor a Multics használhatatlan fehér elefánttá kezdett dagadni. Thompsonnak hiányzott a Multics környezet, ezért játszani kezdett néhány saját, illetve ott felhasznált ötlet megvalósításával.

Egy másik programozó, *Dennis Ritchie*, új nyelvet dolgozott ki Thompson embrióállapotú Unix rendszere számára, ez volt a C nyelv. A Unixhoz hasonlóan a C-t is úgy tervezték, hogy kellemesen használható, a kötöttségektől mentes és rugalmas legyen. A Bell Labsnál egyre többeket érdekelt a dolog, és az eszközök fejlesztése nagy lökést kapott, amikor 1971-ben Thompson és Ritchie megbízást kaptak egy belső használatra szánt (mai fogalmakkal irodai automatizálási) rendszer elkészítésére. A Thompson és Ritchie páros azonban nagyobb álmokat kergetett.

Az operációs rendszereket addig hagyományosan szigorú assemblyben írták, hogy az adott gépeken a lehető legnagyobb hatékonyságot éri el. Az elsők között jöttek rá, hogy a hardver- és fordítói technológia már elérte azt a szintet, hogy egy teljes operációs rendszer elkészíthető legyen C nyelven. 1978-ra a teljes környezetet sikeresen átültették számos különböző géptípusra.

Ilyen még azelőtt soha nem történt, hatása pedig meghatározónak bizonyult. Ha a Unix képes ugyanazt a külsőt és ugyanazokat a képességeket mutatni többféle géptípuson is, mindnyájuk számára közös szoftverkörnyezet lehet. Soha többé nem kell teljesen új szoftvert venni, ha egy gép elavul. A programozók átvihetik szoftverelem-készleteiket a különböző gépek között, és nem kell újra és újra felfedezniük a „tüzet” vagy feltalálniuk a „kereket”.

A kombinációt sikeresen alkalmazták számítási feladatok széles körére, köztük olyanokra, amelyekre a tervezők a legkevésbé sem gondoltak. A megoldás gyorsan elterjedté vált, annak ellenére, hogy nem létezett hozzá formális programtámogatás. 1980-ra számos egyetem és kutatóintézet átvette, és programozók ezrei érezték sajátjuknak.

A Unix még egyfajta saját hálózatot is biztosított. Bármely két Unix-gép képes volt elektronikus leveleket küldeni egymásnak közönséges telefonvonalas pont-pont kapcsolaton keresztül, és ezt a szolgáltatást a rendszer beépítve, nem választható extraként tartalmazta. 1980-ban az első Usenet-helyeken megindult a hírek áramlása, és kialakult az a gigantikus elosztott hirdetőtábla, amelynek mérete hamarosan meghaladta az ARPAnetét. A Usenet körül a Unix-helyek megteremtették saját hálónemzetüket.

A Minix története

A Unix korai verzióinak forráskódját az érdeklődők szabadon felhasználhatták az AT&T engedélye alapján, és gyakran tanulmányozták is. Az egyik egyetem még egy kis füzetet is kiadott, amely sorról sorra kommentálja a kódot. Ezt használta sok egyetem az operációs rendszerek tárgy tankönyveként.

A Unix 7. verziójának megjelenésekor az AT&T, kezdte észrevenni, hogy a Unix értékes üzleti áru, ezért nem engedélyezte az egyetemi kurzusokon ennek forráskódját felhasználni, nyilván azért, hogy ne veszélyeztesse az üzleti titkot. Sok egyetem azzal reagált erre, hogy egyszerűen nem oktatták a Unixot, csak elméletet.

A helyzet orvoslására *Andrew Stuart Tanenbaum* az informatika professzora és számos informatikai könyv szerzője elhatározta, hogy teljesen az elejéről kezdve ír egy új operációs rendszert, amely felhasználói szempontból kompatibilis, felépítésében viszont teljesen

különbözik a Unixtól. Egyetlen sort sem fog használni az AT&T kódjából, így nem sért szerzői jogokat, ha csoportos vagy egyéni tanulásra felhasználják. Az olvasó egy valódi operációs rendszert boncolgathat, hogy lássa, milyen az belülről, ahogy a biológushallgató, mikor békát boncol. A Minix név a mini-Unixból származik, mivel elég kicsi ahhoz, hogy kevésbé jártas hallgatók is átláthassák működését.

A jogi problémák kiküszöbölése mellett a Minix más előnyökkel is rendelkezik a Unixhoz képest. Egy évtizeddel a Unix után készült, annál sokkal strukturáltabb. A fájlrendszer például nem az operációs rendszer része, hanem felhasználói programként fut. A másik különbség, hogy a Unixot hatékonyra, míg a Minixet áttekinthetőre tervezték (ha egyáltalán lehet áttekinthetőségről beszélni több száz oldalas programok esetében). A forráskód több ezer kommentárt (magyarázatot) is tartalmaz.

Megjelenésekor a Minix egy új szabvánnyá kezdett válni, de megtartotta a korábbi programokkal való kompatibilitást is. Az ilyen fejlesztés általános a számítógépiparban, mert egyetlen gyártó sem szeretné, ha új gyártmányát a régi vevői csak nagy átállásokkal tudnák használni.

A Minix is a C programozási nyelven készült, és a különböző számítógépek közötti hordozhatóság igen lényeges szempont volt. Az első implementáció IBM PC-re készült, mivel ezt sokfelé használják. Később Atari, Amiga, Macintosh és SPARC gépekre is átkerült. A „kicsi a szép” filozófiáját követve, a Minix futtatásához eredetileg még merevlemez sem kellett, ezért sok hallgató pénztárcája is elbírt a szükséges gép megvásárlását (mai szemmel furcsa, hogy az 1980-as évek közepén, amikor a Minix napvilágra jött, a merevlemez költséges újdonság volt). A Minix szolgáltatásainak és méretének növekedése következtében a futtatásához ma már szükséges merevlemez, de hála a Minix filozófiának, elegendő egy 30 megabájtos partíció, szemben egy kereskedelmi Unix rendszerhez legkevesebb 200 MB-os partíciót ajánlanak.

Egy IBM PC-a futó Minix felhasználó Unix felhasználónak érezheti magát. Az alapvető programok többsége megvan, és ugyanazokat a funkciókat hajtja végre, mint a Unix megfelelők (pl. *a cat, grep, ls, make* és a parancsértelmező). Ezeket a segédprogramokat ugyanúgy, ahogy magát az operációs rendszert, a szerző és hallgatói, továbbá még néhány korábbi forráskódok felhasználása nélkül teljes egészében újraírták.

Megjelenését követően egy témacsoport (newsgroup) alakult a Minix értékelésére. Néhány héten belül 40 000 előfizetője lett, majdnem mindegyikük rengeteg új szolgáltatást akart a Minix-be építeni, ezzel nagyobbá, jobbá (de nagyobbá biztosan) akarták tenni. A Minix szerzője éveken keresztül sikeresen hárította el ezeket a támadásokat, így maradt a hallgatók

számára a Minix elég kicsi, világos és áttekinthető. Ekkor jött egy finn hallgató, Linus Torvalds, aki elhatározta, hogy ír egy Minix változatot bő szolgáltatásokkal, de ez már egy éles rendszer lesz és nem oktatási segédeszköz. Így született meg a Linux.

Fizetős szoftverek

Mindazoknak, akik a nyolcvanas kilencvenes években a „cybertér” meg az „információ szabadságáért” harcolnak, legfeljebb annyi közük van a hackerek eredeti célkitűzéseéhez, mint annak, aki illegálisan lemásol egy kereskedelmi forgalomban is kapható szoftvert (és ezzel gazdasági bűncselekményt követ el). A helyzet ugyanis az első hackerek és a hackeretika első megfogalmazása óta gyökeresen megváltozott (a programok legyenek mindenki számára ingyenesen elérhetőek). Akkoriban jó ha néhány egyforma komputert volt egész Amerikában, ma viszont több százmillió gépen fut azonos operációs rendszer, és már leginkább csak tíz- vagy százmilliárd dollárban mérhető üzlet rejlik magukban a szoftverekben is. Ahogyan azt Bill Gates, a Microsoft társalapítója is előre látta már az 1970-es évek közepén, amikor a BASIC programnyelvet barátjával, Paul Allennel átültette a világ első személyi számítógépére, az Altair 8800-ra, mert azt remélte, óriási lesz a kereslet iránta. Akkor persze közel sem ez történt. Gates rettenetesen felháborodott, amikor azt vette észre, hogy a felhasználók gátlástalanul másolják a szoftverét. Írt is egy nyílt levelet hozzájuk. *„Miért tesztek így? Mint egyéni felhasználók, jól tudják, hogy legtöbbször lopja a szoftvert. Megveszik a gépet, mert másképp nem lehet hozzájutni..., de az, hogy a szoftver írója semmit sem kap, a jelek szerint nem izgatja Önöket... pedig ki engedhetné meg magának, hogy ingyen dolgozzon? Melyik felhasználó vállalná, hogy életéből három évet szán egy olyan szoftver kifejlesztésére... amiért aztán egy fillért sem kap?”* A sértődött felhasználók is meglehetősen indulatosan reagáltak. Azzal érveltek, hogy Gates és Allen egy egyetemi gépen fejlesztette ki ezt a BASIC-verziót, tehát olyan gépen, amit az állam tartott fenn. Mivel az állam az adófizetők pénzét használta fel, logikusnak tűnt számukra, hogy a hardver megvásárlásával minden el is van rendezve. A szoftverrel az adófizetők megkapták az ellenszolgáltatást a pénzükért – mondták –, és ez így van jól. Ebben a korban még akadtak olyan hardvercégek, amelyek közzétették fejlesztéseik eredményeit, hogy a konkurenciának ne kelljen ugyanazokkal a problémákkal bajlódni, és ehhez képest Gates-ék viselkedése egyszerűen vérlázítónak tűnt. A komputerklubok az általuk egyedül elfogadhatónak tekinthető áron, vagyis ingyen adták tovább a programot, és az új tulajdonosoknak mindössze az volt a kötelességük, hogy ne egy, hanem két másolattal jelenjenek meg a következő számítógépes

összejövetelen. Még olyan klub is akadt, ahol be akarták perelni a Microsoft későbbi alapítóját rágalmazásért. Erre persze végül nem került sor, és lassanként a Gates által képviselt, üzleties szemlélet kerekedett felül. Azok a gyártók ugyanis, amelyek tartották magukat a hackeretika szabályaihoz, pillanatokon belül azon vették észre magukat, hogy a többiekkel szembeni konkurenciaharcban csődbe mennek.

Ingyenes szoftverek

Steven Levy éppen ekkor írta a „Hackers”-t. Egyik fő forrásának *Richard M. Stallman*, a Lab egyik vezetője számított, aki a leghesebben tiltakozott a Lab technológiájának kiadására ellen. Stallman akit általában monogramjáról és bejelentkezési nevééről, az RMS-ről ismernek, megalapította a Free Software Foundationt, és elkötelezte magát a kiváló minőségű szabad szoftver készítése mellett. *Levy* őt jellemezte úgy, mint „az utolsó igazi hacker”-t, de szerencsére ez a leírás nem bizonyult igaznak. Stallman legnagyobb vállalkozása pontosan jelezte, milyen változáson ment keresztül a hackerség a 80-as évek elején. 1982-ben egy teljes Unix-klón készítésébe fogott, amely C nyelven íródna, és ingyenesen hozzáférhető lenne. Terve (a Gnu’s Not Unix-ból alkotott betűszóként – a „GNU nem Unix” rekurzív rövidítése) mint a GNU nevű operációs rendszer vált ismertté.

A munkaállomások grafikájának megszelídítésére számos kísérlet történt. Végül az MIT a tucatnyi cég több száz munkatársának segítségével megalkotott X Window System terjedt el. Sikerének egyik kulcsát az jelentette, hogy az X fejlesztői készek voltak ingyen közzétenni a forráskódot és terjeszteni az Interneten. Az X diadala a magántulajdonú (köztük a Sun által kínált) grafikai rendszerek felett már előre jelezte azokat a változásokat, amelyek pár évvel később alapjaiban alakították át a Unix világot.

De hol volt a szoftver? A kereskedelmi Unixok továbbra is drágák voltak. A 90-es évek elején több cég is megpróbálkozott AT&T és BSD Unix-változatok piacra dobásával PC osztályú gépek számára, de a siker elmaradt, mert az árak alig csökkentek, ráadásul a vásárlók nem kaptak módosítható és terjeszthető forráskódot az operációs rendszerhez. A hagyományos szoftverüzleti modell nem adta meg a hackereknek azt, amire vágytak.

A Free Software Foundation sem. RMS régóta ígért ingyenes Unix magjának, a HURD-nek a fejlesztése évekre elakadt, és 1996-ig a közelébe sem került egy használható rendszer megalkotásának (bár 1990-re az FSF a Unix-szerű rendszer szinte minden más komolyabb összetevőjét elkészítette).

Ami még rosszabb, a 90-es évek elejére világossá vált, hogy a magántulajdonú Unix kereskedelmivé tételére fordított tízéves erőfeszítés kudarcot vallott. A Unix által ígért gépközi hordozhatóság elveszett a fél tucat szabadalmaztatott Unix-változat marakodása közt. A játszma résztvevői olyan nehézkesnek, vaknak és piacérzéketlennek bizonyultak, hogy a Microsoft könnyedén lenyúlhatta piacuk nagy részét a jóval alacsonyabb szintű technológiát képviselő Windows operációs rendszerrel.

A Free Software Foundation befejezetlen HURD-je által hagyott ürt a helsinki egyetem Linus Torvalds nevű diákja töltötte be, aki 1991-ben egy szabad Unix rendszermagot kezdett fejleszteni 386-os gépekre az FSF eszközkészletének segítségével. Kezdeti gyors sikerei számos Internet-hackert arra ösztönöztek, hogy segítsenek neki kifejleszteni a Linuxot, egy teljes szolgáltatáskörű, teljes egészében ingyenes és továbbadható forrással rendelkező Unix rendszert.

A Linuxnak is voltak versenytársai. A Linux legfontosabb vonása azonban nem technikai, hanem közösségi volt. A Linux fejlesztéséig mindenki azt hitte, hogy egy olyan bonyolult szoftvert, mint egy operációs rendszer, csak programozók gondosan szervezett, viszonylag kicsi, szoros kapcsolatban álló csoportja alkothat meg. Ez a modell jellemzi a mai napig a kereskedelmi programok fejlesztését. A Linuxot azonban kezdettől fogva rendszertelenül foltozgatta egy csomó önkéntes, akiket csak az Internet fogott össze. A minőséget nem szigorú szabványok vagy hivatalos felügyelet biztosította, hanem az a naivan egyszerű módszer, hogy hetente újabb változat jelent meg, amire napokon belül százak reagáltak, így a különböző mutációk egyfajta gyorsított darwini kiválasztódáson mentek keresztül. Mindenki meglepetésére a módszer egészen jól működött.

1993 végére a Linux a legtöbb kereskedelmi Unix rendszerrel felvehetette a versenyt stabilitásban és megbízhatóságban, ráadásul jóval több programot írtak rá, sőt egyes kereskedelmi alkalmazásokat is átültettek. A fejlemények egyik közvetett következményeként a kisebb Unix-gyártók tönkrementek, hiszen nem maradtak fejlesztőik, és nem volt kinek eladni terméküket.

A Linux feltörekvése egybeesett egy másik jelenséggel, az internet nyilvános felfedezésével. A 90-es évek elején virágozni kezdett az internet-szolgáltatók ipara, akik már elérhető áron csatlakozást kínáltak a nagyközönségnek. A képes világháló (world wide web) feltalálását követően pedig az internet addig is gyors növekedése nyaktörő tempót vett fel. A Linuxot már CD-ROM-on terjesztették, és vitték, mint a cukrot. 1995 végére a nagyobb számítógép-vállalatok színes hirdetésekkel reklámozták internet barát szoftverüket és hardverüket.

A 90-es évek végén a hackerek fő tevékenységévé a Linux fejlesztése és az internet közkinccsé tétele vált. A world wide web végre tömegkommunikációs eszközzé tette az internetet, a 80-as és 90-es évek hackerei közül pedig sokan internetes szolgáltatást indítottak, hogy a tömegeket a hálóra kapcsolják.

Az internet beszivárgása a mindennapokba tiszteletet hozott és politikai erőt adott a hackereknek. 1994-ben és 1995-ben a hackerek fellépése süllyesztette el az Egyesült Államokban a „Clipperjavaslatot”, amely az erős titkosítási módszereket kormányzati ellenőrzés alá vonta volna. 1996-ban a hackerek széles összefogást hoztak létre, hogy a félrevezetően „kommunikációs tisztasági törvénynek” (Communications Decency Act) nevezett tervezet elfogadását és az internet cenzúrázását megakadályozzák.

A CDA-val szemben elért győzelemmel kilépünk a történelemből, és megérkezünk a jelenbe, amelyben a felhasználó már nem csak megfigyelő, de az események alakítója is.

A Linux története

A Linux történetébe való bepillantás tehát egy olyan világba vezet minket, ahol a programozók „dicsőségért” programoznak, mindenki szabadon átadja ismereteit a többieknek, és mégis a szoftvernagyhatalmakkal összevethető eredményességgel dolgoznak.

Ez a mentalitás nemcsak a Linux-ot jellemzi, hisz már a 70-es években jelentkeztek a Unix-os világban az első szabadterjesztésű programok (hiszen maga a Unix is az volt eredetileg). Ezeket a szabad szoftvereket a *GNU project*, valamint a *Free Software Foundation* fogja össze, melyeknek tevékenysége szélesebb körű, mint a Linux rendszer.

Végigkövettük, ahogy egy hobbiprogramból világméretű mozgalommá vált a Linux, és ez talán egyedülálló a számítástechnika történetében. Mindez úgy történt, hogy lényegében ingyen juthat mindenki hozzá, így még hihetlenebb a siker. De hogyan is kezdődött?

Több évtizede csiszolódtak a megszállott programozók szoftverei, ötletei, amire a Linux elkezdődött. A programokba mindenki azt adta bele, amihez a legjobban értett, nem pedig valami kívülről ráerőltetett feladaton dolgozott. A programok tesztelése is igen széleskörű volt. A freeware programok nem üzleti célból készültek, így alkotóik nem a maximális anyagi hasznot keresték, hanem maguk számára akartak használható rendszert összehozni, és villogni akartak a többiek előtt tudásukkal. Ez a légkör sokkal jobban kedvezett a hatékony, stabil programok kialakításának, mint a szoftverbirodalmak pénzorientált rendszere.

1991 nyarának elején, a Linux fejlesztésének kezdetén Linus Torvalds a 80386 processzor védett módú, feladatváltó lehetőségeivel szeretett volna megismerkedni. A program fejlesztése Minix alatt történt, eleinte assembly nyelven.

Később, amikor Linus áttért a C nyelvre, a fejlesztés lényegesen gyorsabbá vált, és olyan nagyratörő tervek fogalmazódtak meg, hogy valaha le lehessen fordítani a GNU C fordítóját Linux alatt. Ma már csak csodálkozni lehet azon, hogy 1991-ben ez volt a nagy álom, és azóta hol tart a rendszer.

1991. október 5-én hirdette meg Linus az első „hivatalos”, 0.02-es Linuxot az interneten. Ekkor már néhány alapprogram futott a rendszeren (pl. a GNU C fordítója, valamint a „bash” burokprogram), így már el lehetett kezdeni használni a rendszert. Ekkor nem is a rendszer használhatóságának növelése volt a fő cél, hanem a rendszermag fejlesztése. Ezért ekkor nem készültek dokumentációk, installációs csomagok stb. A Linux ekkor még csak a megszállott hackereknek készült. Linus ekkor elhatározta, hogy az interneten keresztül bevonja a fejlesztésbe a szabad kapacitással rendelkező programozókat, és a következő hirdetményt tette közzé az egyik hírcsoportban:

„Sóvárogsz a Minix 1.1 szép napjai után, amikor a férfiak igazi férfiak voltak, és mindenki maga írta a saját eszközmeghajtóját? Egy szép project nélkül vagy, és épp fened a fogad egy operációs rendszerre, amit igényeidnek megfelelően alakíthatsz? Frustrálónak találsz, ha minden működik Minix alatt? ... Akkor ez a levél lehet, hogy pont neked szól.”

A 0.03-as verzió két-három hét alatt megszületett, majd 1991 decemberében Linus kibocsátotta a 0.10-eset is. Ez az ugrás a számozásban azt tükrözte, hogy jelentősen megnőtt a Linux alatt futtatható alkalmazások száma, de a Linux még mindig nem volt önálló, szerzője szerint is „egy hacker által hackereknek írt” rendszerről van szó, így a rendszernek csak fejlesztői vannak, felhasználói nem.

A 0.12-es változat 1992. január 15-én látott napvilágot, néhány bővítéssel. Már volt init/login szolgáltatás (nem rootként kellett először bejelentkezni, és inicializálni a rendszert), közeledett a POSIX szabványhoz, virtuális memóriát is használt, és kisebb korrekciókat tartalmazott. Ez egy elég stabil változat lett, ekkortól kezdődött el a Linux igazi hódítása. Linuxot ugyanis elkezdtek használni „egyszerű” felhasználók is, nemcsak megszállottak. Ekkortól kezdve hihetetlen ütemben gyarapodott a Linux-felhasználók és programozók száma. Az így előálló rendszer már több vonatkozásban jobb volt a Minixnél, de még mindig nem volt látható, hogy ebből akkora mozgalom lesz, mint ami mára kialakult.

A 0.95-0.99 rendszermagra épülő rendszereknek óriási népszerűségük volt. Egyes egyetemeken, pontosabban azok bizonyos intézeteiben gyakorlatilag likvidálták az összes

nem Linuxos programot, és a PC-ken nem lehetett DOS-t vagy Windowst találni (legfeljebb a titkárságokon). Ez főleg olyan helyeken következett be, ahol a kutatók Unix alatt dolgoztak, mert egy Linuxos PC-n otthon is fejleszthették a programjukat, és ezeket egyszerű volt az intézet nagykapacitású gépeire áttenni.

A Linux és a Minix szétválását meggyorsította, hogy a Minix szerzője, Andrew Tanenbaum nem nézte jó szemmel a Linuxot. Alapvetően elhibázottnak tartotta a Linux rendszermag típusát. Linus Torvalds ugyanis ún. „*monolitikus kernelt*” írt, míg Andrew Tannenbaum (elméleti megfontolások alapján) a „*mikrokernelt*” jobb választásnak tartotta. Sajnos, a vitába személyes elemek is keveredtek, és a vita jórészt az internet hírcsoportjaiban zajlott, meglehetősen nagy nyilvánosság előtt. Így kissé ideges hangulatban zajlott le a Minix és a Linux szétválása.

Andrew Tannenbaum: *„Továbbra is fenntartom azt, hogy 1991-ben monolitikus kernelt tervezni alapvető hiba. Örülj, hogy nem vagy a tanítványom. Nem kapnál túl jó minősítést egy ilyen tervezésre :-)”*

Linus Torvalds: *„Az Ön foglalkozása professzor és kutató: Ez egy pokolian jó mentség a Minix némely agysérülésére.”*

Andrew Tannenbaum (1992-ben): *„A Linux elavult!”*

A Minix azért sem terjedhetett annyira, mint a Linux, mert nem szabadterjesztésű. Emellett valószínű, hogy Andrew Tanenbaumnak nem volt igaza abban, hogy a Linux alapvető szervezése teljesen hibás, mert alapvető hibákkal nem lehetne egy rendszer ennyire stabil, és nem is terjedt volna el. Talán személyes ambícióit sértette, hogy egy egyetemista az övénél használhatóbb rendszert hozott össze, mely mellett a Minix elhanyagolható szerepet játszik. Mindenesetre sajnálatos, hogy ilyen veszekedésekre is sor kerülhet komoly szakemberek között.

A POSIX-szabványosítás megfelelő szintű elérésével 1994 márciusában megjelent az 1.0.0 sorszámú kernel. Ekkortól kezdve egy speciális sorszámozási eljárást vezettek be a fejlesztők. A verziószámot három, ponttal elválasztott egész szám jelzi. Az első a fő verziószám, ami csak a rendszermag lényegét érintő változásoknál vált eggyel nagyobbra. A második szám elég speciális jelentésű. Ha páros, akkor stabil, tesztelt kernelről van szó, amit bárkinek ajánlanak használatra, míg a páratlan szám tesztváltozatot jelöl, amit inkább azoknak javasolnak, akik tesztelni, fejleszteni szeretnék a kernelt, és akiknek nem számít, ha a rendszer néha „elszáll”. A harmadik szám pedig kisebb módosításokkor ugrik egyet. Ez a fura sorszámozás lehetővé teszi, hogy az egyszerű felhasználók csak a valóban használható

változatokat kapják meg, de közben az esetleg még hibákat tartalmazó fejlesztői változatok is hozzáférhetőek legyenek.

A fejlesztés során a rendszermag egyre hatékonyabb lett, beépítették a legújabb hardverek meghajtóit (CD-olvasók, PCI-buszok, újabb SCSI-eszközök stb.).

Ebben az időben a Linux alatti felhasználói programok száma nőtt meg hihetetlenül. Míg korábban főleg már meglevő szoftvereket vittek át a Linux alá, eddigre már megjelennek azok a programok, melyeket Linux alatt fejlesztenek, és innét viszik át a többi rendszerre. Ekkor már nagy szoftvercégek is elkészítik programjaik Linuxos változatát (pl. Maple V, Motif 2.0). Ezek természetesen nem szabadterjesztésűek, és az, hogy megéri Linuxra is adaptálni őket, egyértelműen jelzi, hogy a Linux-felhasználók tábora világméretben is piacot jelent.

Ekkortájt egyre több Linux-disztribúció jelenik meg, azaz több cég olyan programcsomagot állít elő, amelyekkel a Linux telepítése, karbantartása sokkal könnyebb, mintha mindenki egyenként gyűjtené be a rendszer részeit.

Manapság a Linuxnak akkora tábora van, hogy még Linus Torvalds és a többi vezető programozó kilépése esetén is tovább fog folytatódni a munka. Különösen igaz ez azért, mert mára nemcsak IBM PC-ken, hanem a legelterjedtebb munkaállomásokon is fut Linux.

A mai napig folyamatosan növekszik a Linuxos szoftverek, a felhasználók száma, és az alkalmazások sokrétűsége. Csak egy példát említsek: megépítettek egy „LOKI” nevű Linuxos szupergépet, amely 16 db, hálózatban összekapcsolt PC-ből áll, és ezt a Los Alamos National Laboratory-ban komoly kutatási feladatokra használják, mert számítási kapacitása egy kisebb CRAY szuperszámítógépével egyenértékű, az ára pedig annak töredéke.

A rendszer kidolgozottsága az idők folyamán olyan fokú, hogy egyre több helyen alkalmazzák Unixos munkaállomásként vagy hálózati szerverként. Mindkét esetben hatalmas előny a szokásos IBM PC-s programokkal szemben a nagyfokú megbízhatóság és az alacsony ár, valamint az sem elhanyagolható, hogy nagyon nagy a hasonlóság a Linux és a „nagygépek” operációs rendszerei közt. Egy linuxos program könnyen átvihető mondjuk egy *Sun SPARC* gépre, de gondos programozás esetén akár egy *CRAY* szupergépre is.

A médiában is egyre gyakrabban merül fel a Linux név. Szinte minden nap jelennek meg hírek, amelyek dicsérik, és arról tájékoztatnak, hogy milyen nagy cégek csatlakoztak a „Linux mozgalomhoz”. De arról nem olvashatunk (hallhatunk), hogy tulajdonképpen mire is használják ezt az operációs rendszert. Sokáig tartotta (talán még most is tartja) magát az a nézet, hogy otthoni játékszernek kitűnő, de ipari környezetben, igazi munkára nem alkalmas. Ennek az is lehet az oka, hogy a cégek büszkén hirdetik, ha valamilyen „pénzes” operációs

rendszerrel használnak, de nem dicsekszenek azzal, ha valamilyen nyílt forráskódú (ingyenes) rendszerrel használnak.

Ezt a tartózkodást külföldön már leküzdötték, nem tartják „szégyennek”, ha Linuxot használnak. Egészen nagy cégek is önként – büszkén – bevallják, hogy ahhoz az egyre népesebb táborhoz tartoznak, amely Linuxot használ. Például: NASA, Boeing Company, Cisco Systems Inc., Corel Computer Corp., Mercedes-Benz AG, Sony Electronics Inc. stb.

Az IBM az első – de már nem az egyetlen – cég, amely hardverrel, szoftverrel és támogatással teljes megoldásokat szállít Linuxra. Átültették a Linuxot majdnem minden géptípusukra.

Nemcsak a hardvergyártók ismerték fel a Linux előnyeit, hanem a szoftvergyártók is. A nagy (és kis) cégek sorra jelentik be, hogy átültetik különböző szoftvereiket Linux alá. Ezek között vannak: IBM, Borland, Oracle, Compaq, Sybase, Lotus, Macromedia Inc.

A nyílt és a zárt forráskód védelmezői időről időre vitákban csapnak össze igazuk védelmében. Előbbiek a zárt kódú fejlesztések kapcsán leginkább a felhasználók kiszolgáltatottságát sérelmezik, hiszen a zárt kódú programok esetében a gyártó kezében van a piac szabályozása, ő dönti el, mikor milyen termékkel jelentkeznek, és milyen ütemben fejleszti azt tovább. A zárt kód miatt ráadásul a felhasználó nem is tudja, hogy milyen hibákkal és biztonsági résekkel rendelkezik a megvásárolt program. A zárt forráskód védelmezői szerint viszont a nyílt kódú fejlesztéseknek nincs gyújtópontja, az ilyen programok által okozott károkért senkit nem lehet felelősségre vonni. Emellett képmutatónak is tartják a nyílt kód védelmezőit, mondván hogy azok az ingyenesség látszatát keltve rejtett módon jutnak profithoz. Ilyen például az a megoldás, amikor a program és a forráskód ingyenes ugyan, de a telepítésért és a támogatásért pénzt kérnek, más nyílt kódú programokhoz pedig olyan alkalmazások és/vagy szolgáltatások kötődnek, amelyek szintén nem ingyenesek.

Az internet története

Az amerikaiak a Szputnyik 1 fellövése után a szovjetek űrversenybeli előnyének ellensúlyozására beindították a DARPA programot, amely tartalmazta egy olyan számítógépes hálózat kialakítását, amely néhány részének kiesése esetén is működőképes marad. Ez lett az ARPANET. Ők fejlesztették ki a csomagkapcsolt hálózatot, amely az internet mai működésének is az alapja. Az internetnek nincs központja, szerkezete leginkább egy úthálózathoz hasonlítható. Hiba esetén más útra kényszerülnek az adatok, mint egy lezárt közút esetén.

Az internet is, mint megannyi technikai eszköz a háborúnak, illetve a katonai fejlesztésnek köszönhető. Az 1960-as években tetőzött a hidegháború az Amerikai Egyesült Államok és a Szovjetunió között. A hálózat története akkor kezdődött, amikor az Amerikai Egyesült Államok védelmi minisztériumának felkérésére kifejlesztettek egy olyan hálózatot, amely földrajzilag távol levő számítógépeket és hálózatokat kötött össze, amely túlél egy atomtámadást. A feladatot kiadták a kutatási részlegnek, ez volt az ARPA (Advanced Research Projects Agency). Az ARPA a hálózat védelmét két dologban látta. Az első, hogy a hálózatnak ne legyen központja, a hálózat minden csomópontja több másik (legalább kettő) hálózati csomóponttal legyen összeköttetésben. A másik, hogy az üzenetek csomagokra bontva, egymástól függetlenül haladjanak, akár más és más útvonalon.

Csomagkapcsolt hálózat egy óriási ötlet. Az elvárás az volt, hogy a hálózatba kötött gépek között akkor is megmaradjon a kommunikáció, ha néhányat támadás ér, és így kiesik a rendszerből. A hagyományos telefonos kapcsolat nem jó, hiszen a felépített kapcsolaton keresztüli adatfolyam vonalszakadásnál megszakad, és az információ csak újabb vonal kiépítése után továbbítható. Ha nincs központ, akkor biztonságosabb a hálózat. Ha több „út” van, akkor bármelyik hálózati csomópont vagy összeköttetés kiesése esetén is eljut az információ a hálózat többi pontjára.

A csomagkapcsolt hálózatban az információt kis részekre bontják, és minden rész tartalmazza a címzett számítógép címét, a küldő címét, és azt, hogy az eredeti információnak melyik részét tartalmazza, hogy aztán a címzett össze tudja rakni az eredetit a részekből. A továbbítás általában nem rögtön a címzethez történik, hanem a csomagok egymástól függetlenül vándorolnak gépről gépre úgy, hogy ha valamelyik gép felé a kapcsolat túlterhelt, akkor más irányt választ a továbbküldő gép. Ha egy gép kiesik a rendszerből, azt a hálózat úgy látja, hogy túlterhelt, ezért automatikusan kikerüli. A címzett gép gyűjtögeti a csomagokat, amelyek nem biztos, hogy sorban érkeznek meg, de mivel tartalmazzák a helyüket az információban, a gép sorba tudja rakni őket. Ha egy csomag éppen egy lerobbant gépben van, nem jut tovább, elvesz. De akkor a címzett gép kéri a küldőt, hogy a hiányzó csomagot küldje el újra. Amikor az információ teljesen megérkezett, a címzett gép megjeleníti az aktuális kimeneten (képernyő, nyomtató, hangszóró stb.)

A kísérleti hálózatot (ARPANET) 1969-ben hozták létre, és rögtön nőni kezdett, az előnyei ugyanis hamar megmutatkoztak. Az, hogy az információ másodpercek alatt száz kilométerekről megszerezhető, új távlatokat nyitott főleg a tudósok között. Azelőtt egy matematikai levezetés, egy információ vagy személyes találkozókon, vagy levélben jutott az egyik tudóstól a másikig. Most egy fájl letöltése volt az egész. Nem véletlen, hogy főleg

egyetemek és kutatóintézetek éltek a lehetőséggel. Az ARPANET méretének növekedésével világossá váltak a technikai problémák is.

A csomagok akár több számítógépen keresztül is eljuthattak a célállomásra, s így az egymással közvetlenül össze nem kötött és különböző gyártóktól származó számítógépek is adatokat cserélhettek egymással. Ehhez meg kellett oldani az egyes gépek azonosítását, az adatsomagok címezését és az egyes csomagok sorrendjének azonosítását is. Ez vezetett el az azóta ipari szabvánnyá vált TCP/IP protokollok, valamint az IP címek kialakulásához. Ez a fejlődés azonban már a civil, nem katonai kutatóintézetekben és felsőoktatási intézményekben bontakozott ki. Vinton „Vint” Cerf, akire általában az internet egyik alapító atyjaként hivatkoznak, kulcsszerepet töltött be az internet, valamint a TCP/IP protokollkészlet megalkotásában. Ez volt az a protokoll, amelyet kifejezetten erre a hálózattípusra terveztek, és amely 1983-tól lett hivatalos protokollja az ARPANET-nek. Segítségével olyan szolgáltatások születtek mint a TELNET, amellyel felhívhatjuk a kiválasztott gépet és bejelentkezhetünk. A távoli bejelentkezés lehetővé teszi a felhasználónak, hogy saját gépe mellett ülve kapcsolódjon egy távoli géphez, és azt interaktív módon használja, úgy, mintha a távoli terminál mellett ülne. A TELNET áthidalja a helyi és a távoli rendszerek közötti különbségeket, biztosítva az egymástól eltérő típusú, felépítésű, rendszerű gépek közötti kommunikációt. A legtöbb gép a bejelentkezéshez azonosítót, illetve jelszót kér.

1983-ban már akkora lett a hálózat, hogy biztonsági okokból az ARPANET-ről levált a katonai rész. Ezt nevezték MILNET-nek. Majd az 1980-as évek végére az ARPANET átadta helyét az internetnek.

Ezen a hálózaton nincsen központ, nincs „egy” központi gép. Minden hálózatra kötött gép egyszerre fő- és alállomás. Az internet tehát egy olyan szerveződése a számítógépeknek és telefonvonalaknak, amelynek bármely pontja képes kapcsolatot teremteni bármely másik pontjával. A valóságban persze néhány tízezer nagy gép nem felhasználó, hanem kizárólag szolgáltató feladatokat lát el, például a kereső szerverek. Az internet pár év alatt a világ legnagyobb hálózatává vált, és eddig nem tartozott egyetlen kormány vagy szervezet irányítása, ellenőrzése alá sem. Az internet nem szervezetként működik. Nincsen központi irányító szerve és ellenőrzése. Az interneten bárki bármilyen információs forrást elhelyezhet, akár saját programját is terjesztheti rajta. Tehát az internet virtuális közösséget is nyújt használói számára, akik gyakran létrehozzák különféle csoportjaikat és elkülönült közösségeiket.

Az eredetileg katonai és szakmai célokra tervezett hálózat gyorsan általános kommunikációs, információtovábbító médiává vált, majd maguktól adódtak az emberi

kapcsolatteremtés újabb, sokszor korábban soha nem ismert formái. Az eredetileg elsősorban oktatási intézményekben elérhető hálózatra egyre több intézmény, szervezet, cég kapcsolódott, a szolgáltatást hamarosan a nagyközönségnek is felkínálták. Az elektronikus levelezés (e-mail) forradalmát gyorsan követte a hírcsoportok (newsgroup) forradalma, majd az egyre újabb és sokoldalúbb információkereső- és továbbító eszközök elterjedése, amelyek 1992-ben úgy tűnik, egy „természetes” végponthoz, a www-hez (world wide web) vezettek. Ekkorra fejlesztettek ki egy új alkalmazást, a világhálót, vagyis a www-t. Ez az alkalmazás grafikus felületet biztosít az internet felhasználói számára. Az internet egyik legnépszerűbb szolgáltatása. Lehetőséget biztosít információk közlésére, szórakoztatásra és üzleti tevékenységre, mindezt ma már teljes multimédiás megvalósításban.

Az egész történet 1989-ben kezdődött. Európai országok tudósainak kommunikációjának, munkájának megkönnyítésére szerettek volna valamilyen kapcsolatot kialakítani. A www az európai részecskefizikai kutatóintézet, a CERN szülötte. Tim Berners-Lee és Robert Cailliau elgondolásai alapján olyan rendszer született, ami a következő tíz évben forradalmasította a kommunikációt. 1998-ra mintegy 300 millióra nőtt a webdokumentumok száma, és a web azóta is nap mint nap nagy ütemben tovább fejlődik. Innentől a számítógépekhez nem értő laikusok is könnyedén, minden tanulás nélkül navigálhatnak az internet óceánján. Ehhez természetesen hozzájárultak az ekkorra már magas színvonalú grafikus operációs rendszerek, és internetes böngészők, amelyek leegyszerűsítették a számítógépes munkát. 1993-ban megjelent az első grafikus megjelenítő, a Mosaic. Szerzője Marc Andreessen, a későbbi Netscape Communication Corporation alapítója.

Ma már az interneten nemcsak fájlokat cserélnek vagy leveleznek az emberek, mint a régi időkben, hanem barangolnak a hálózaton, beszélgetnek, akár videó kapcsolatot is létesíthetnek, vásárolnak, tőzsdéznek, távmunkában dolgoznak, és a távolság nem akadály.

Xerox PARC

1970-ben a Xerox Corporation létrehozott Kaliforniában egy fejlesztő részleget, a Palo Alto Research Centert (PARC). Ennek a kis gyárnak az egyik legjobb fejlesztése az ALTO nevű számítógép volt, amelynek egyik legszembeűnőbb újdonsága, hogy új típusú kommunikációt folytatott a felhasználóval. A gyermekekkel végzett kísérletek megmutatták, hogy a szöveges helyett a grafikus és hangos információk jóval gyorsabban hatnak a tanulási folyamatban. Ezért készítettek a PARC kutatói olyan számítógépet, amely intenzíven grafikát és animációt használt az ember-gép kapcsolat megteremtésére. Ezt nevezzük ma GUI-nak,

grafikus interfésznek, ablakos technológiának, amely számtalan változatban terjedt el (Atari és Mac grafika, MS Windows, UNIX/Linux stb.). A billentyűzet használata mellett az ALTO felhasználóinak lehetőségük volt a képernyőn megjelentetett grafikai szimbólumok (ikonok) között válogatni. A kiválasztást egy könnyen mozdítható „egér” segítségével végezheték el. Az ilyen típusú funkcióválasztás nagymértékben megnövelte a gép hatékonyságát.

A PARC-nál dolgozott Alan Kay, az első dinamikus objektumorientált programozási nyelv, a SmallTalk kidolgozója, és a számítástechnika egyfajta (apró modulokból, „sejtekből” építkező) biológiai modelljének a megalkotója. A technológia alapelve, többször újra használható modulok alkalmazása a programozásnál, aztán egy sereg más programozási nyelvben is központi szerepet kapott. Elméleti biológusi háttérével, biológiai analógiák nyomán kezdett azon gondolkodni, hogy az ideális számítógépnek a „sejt”-ekből álló élő anyag mintájára kellene szerveződnie és működnie. A sejtek szervenként együttműködve valósítanak meg egy összetett célfeladatot, de amúgy mindegyikük független és önálló rendszert képez. Alkalmassint viszont gyorsan átszervezhetőek egy-egy újabb cél elérésére. Ezt az elvet alkalmazták már az ALTO gép programozásakor is.

Az ALTO drága volt, és nem is volt igazi mikroszámítógép. Az INTEL-8008 még fejlesztés alatt állt, amikor az ALTO már megjelent. Mivel ez a gép kifejezetten professzionális felhasználásra készült, néhány jellemzőjében eltért a későbbi mikroszámítógépektől. Úgy kezelték, mint egy munkaállomást, és számos későbbi típus modelljéül szolgált. Ennek alapján fejlesztette ki a Xerox a STAR-t. Ez egy nagy képernyővel rendelkező olyan munkaállomás volt, amely ALTO típusú ikonos felhasználói felülettel rendelkezett. Az igazi sikert a fenti típusú rendszerek között az Apple-Machintosh és a Sun System érte el.

Az egy-felhasználós munkaállomások egy új típusú operációs rendszer kifejlesztésének az alapjául szolgáltak. Az operációs rendszert sokáig úgy tekintették, mint a számítógépes rendszer irányítóját. Az új elképzelés szerint az operációs rendszer a felhasználó kiszolgálója lett. Az ilyen típusú operációs rendszer középpontjában a kényelem és nem az ellenőrzés áll. Az operációs rendszer szolgáltatásokat nyújt, de nem lép kapcsolatba a felhasználói programokkal, ezért úgy tekinthető, mint egy szubrutin gyűjtemény. Így eltűnt az éles határ a felhasználói programok és az operációs rendszer között, megszületett a nyitott operációs rendszer gondolata. Egy ilyen rendszer nem korlátozza a felhasználót, bár ha valamilyen hiba lép fel, akkor a programok sokkal sebezhetőbbekké válnak.

A PARC másik fejlesztése a mai világháló TCP/IP protokollját megalapozó Ethernet technológia, amely *Robert Metcalfe* nevéhez fűződik. Ez lehetővé tette, hogy később ne csak a nagyvállalatok vagy bankok által fenntartott drága, légkondicionált termeket igénylő

központi számítógépek, hanem a kispénzű felhasználók olcsó személyi komputeri is hálózatba kapcsolódhassanak.

Ilyen Ethernet-hálózat már az 1970-es évek közepén is létezett a PARC-ban, és ez adta az ötletet két kutatónak. John Shoch és Jon Hupp a „distributive computing” (kb. megosztott számítógép-működtetés) elvével játszottak el, vagyis azzal a gondolattal, hogy az Etherneten keresztül összekapcsolt gépek közös kapacitását úgy használják fel egy-egy probléma megoldására, mintha csak egyetlen, sokprocesszoros komputerrel dolgoznának. A kérdés csak az volt, miként lehetne összehangolni ezeknek a processzoroknak a működését. *„Igazán ostoba dolog lett volna körbejárni az épületben, és mindegyik gépre rátelepíteni ugyanazt a programot.”*

Kidolgoztak egy creeperszerű („futónövény”) szoftvert, amely a belső hálózaton vándorolva szabad kapacitást keresett magának, hogy aztán különböző műveleteket hajtson végre. Rendszerint talált is ilyen kapacitást, még hozzá főleg éjszaka, mert a PARC dolgozói a munkaidő végén általában bekapcsolva hagyták a gépeiket. A Shoch és Hupp által írott több-féle féreg egyike nem véletlenül kapta éppen a „Vámpír” nevet. Napközben ugyanis nem csinált semmit (mintha az igazi vámpírokhoz hasonlóan ő is félne a fénytől), ám éjszaka nagyon is aktívvá vált, és olyan, összetett feladatokat futtatott le, amelyekhez különösen nagy számítási teljesítményre volt szükség, hogy aztán a reggel közeledtével elmentse az eredményeket, és elkezdje várni a következő alkonyatot.

Megemlítendő még a Xerox egy fejlesztése: a meghajtó szerkezetes lézernyomtató.

Közben a mikroprocesszorok is rohamléptekkel fejlődtek. A 80-as években az INTEL gyors egymásutánban dobta piacra az új 16, 32 és 64 bites processzorait, és ezzel párhuzamosan alakították az MS-DOS különböző változatait is. Ezek az új verziók azonban már nem hoztak forradalmi változást. Az újabb lökést a fejlődésnek az adta, amikor a 90-es évek elején – felismerve az ikonos rendszerek előnyeit – a Microsoft kifejlesztette az Intel processzorokra alapozva a Windows operációs rendszert, amelynek egyre frissebb generációi fokozatosan szorították ki a korábbi operációs rendszer változatokat a mikrogépek világából.

Apple története

A 1971 nyarán összeismerkedett két Steve-nek (Steven Paul Jobs és Stephen Gery Wozniak) az Esquire magazin októberi számában olvasott cikk meglódítja fantáziáját. Az írás olyan csalássorozatról szól, amelyet a telefontársaságok rovására követnek el. Híváskor a telefonközpontok ugyanis apró jeleket vittek át a beszélgetések alatt. A csalók ilyen jelek

adására képes készüléket építettek, amellyel így ingyen vagy jóval olcsóbban tudtak telefonálni. Wozniak számára kihívás volt hasonló eszköz megalkotása. Jobs 40 dollárért vásárolt alkatrészt, amelyből Wozniak elkészítette az általuk későbbi interjújukban „kék doboznak” nevezett eszközt. Ezt Jobs házalással eladta 150 dollárért, a hasznot megfelezték. Persze egyetemistákként nem riadtak vissza egy kis telefonbetyárkodástól sem.

Jobs az Oregon állambeli Portland Reed Főiskoláján hallgatott egy szemesztert 1972 októberéig, de továbbra is a főiskola kollégiumában dekkolt, kihasználva az üres ágyhelyeket, előadásokat hallgatott, de vizsgatárgyként nem vette fel őket, barátaival élte a boldog főiskolás életet. Később belépett az Atarihoz, a Nolan Kay Bushnell által 1972-ben alapított legendás játékfejlesztő cég alkalmazottja lett. Az ötdolláros órabérért dolgozó Jobs annyira arrogáns volt és munkatársaival összeférhetetlen, hogy közvetlen főnöke rendszeres éjszakai munkára osztotta be. Így Jobsnak nem okozott nehézséget, hogy rendszeresen beszöktesse Wozniakot a céghez, és egész éjszaka játsszák kedvenc játékukat, a Gran Trakot. Cserébe a korlátlan és ingyenes játéklehetőségért Wozniak segített Jobsnak technikai problémák megoldásában. Az Atari sikere akkor a Pong játék volt – a képernyő alján vízszintesen mozgó „ütővel” kellett egy „labdát” visszaütni, amely visszapattant a képernyő széleiről és tetejéről. Később elkészült a két játékos változata is a Pongnak. Akkoriban ez a játék tarolt, Bushnell pedig igen aggódott, milyen új játékkal tudná ezt a sikert is felülmúlni. Legjobbnak az az ötlet tűnt, amikor a Ponghoz hasonlóan kell visszapattintani a „labdát”, ám a feladat nem csak a sikeres visszapattintás, hanem a képernyő tetején lévő háromsornyi „téglafal” lebontása. Jobsé lett a feladat, készítse el a szükséges áramköröket. Ez a hőskor, nem programozni kellett, hanem megépíteni. Jobs nagy lendülettel látott neki a megoldásnak, de hamarosan szembesülnie kellett azzal, hogy tudását meghaladja a feladat. Ezért éjszakai játszótársától kért segítséget. „Steve sohasem volt képes összetett dolgokat megtervezni – emlékszik vissza Wozniak – Az Atarinál dolgozott, amikor elmondta, hogy milyen játék megtervezésével bízták meg, és ő tovább passzolta nekem a feladatot. Ráadásul négy napom volt csak rá.” Nehéz feladat és szűk határidő, Wozniak az ilyen kihívásokért élt-halt. Amellett, hogy nappal a Hewlett-Packardnál dolgozott, négy teljes éjszakát átdolgozva Jobsszal elkészítették a mintapéldányt. Bushnell igen elégedett volt, de szeretne volna a legkevesebb alkatrészből megépíteni a játékot, amely akkor már a Breakout (Kitörés) nevet kapta.

Wozniak és Jobs akármerre is tanultak vagy dolgoztak éppen, tagjai maradtak a Homebrew Computer Clubnak, amely összegyűjtötte az amatőr számítógép tervezőket és építőket, és a Palo Alto-i klub rövid idő alatt több száz fős tagságra tett szert. A klubtagok többsége a 179 dolláros Intel 8080-as chip köré tervezte gépét. Ezt a processzort használta a MITS az Altair

8800 otthoni, összeszerelhető számítógépéhez is, melyet úgy kellett összeilleszteni, mint egy repülőgépmodellt. Az Intel processzor jó volt, viszont Wozniak túl drágának találta, legalábbis akkori anyagi helyzetéhez mérten. Egy elektronikai kiállításon beleszeretett a MOS Technology 6502 programozható mikroprocesszorba, amely csak 20 dollárba került. Megvéve az első darabot, írt egy BASIC fordítót, hogy HP gépén letesztelhesse a 6502-t. A teszt megnyugtatta, és nekiállt megépíteni első komoly számítógépét. Eldöntötte, hogy nem az Altair nyolckapcsolós adatbeviteli módját követi, hanem szabványos qwerty-billentyűzetet fog majd használni. Kimenetként sem kívánt drága monitort vagy nyomtatót alkalmazni, hanem a tévé képernyőjét célozta meg. Március elsején a Homebrew rendszeres találkozásán bemutatta a gépét, ahol nagy érdeklődéssel fogadták a többiek. Jobs egy pillanat alatt felismerte Wozniak munkájának értékét, fontosságát, épp úgy, mint a „kék doboz” esetében. Jobs hosszan győzködte Wozniakot, hogy ahelyett, hogy a kapcsolási rajzot ingyen közreadná, árulják a kész gépet termékként, sok pénzért. Wozniak nem érezte a készletet, hogy csupasz nyákokkal (nyák: nyomtatott áramkör) házaljon. Nem osztotta Jobs látomását a hatalmas számítógépes piacról, nem gondolkodott saját cég létrehozásában, menedzselésében. Megelégedett munkavállalóként Wozniak arra készült, hogy cégét, a HP-t minél jobb kalkulátorok tervezésével örvendeztesse meg. Azért az összerakott gépet megmutatta főnökének is: „Érdeklé egy 800 dolláros gép, amelyen BASIC fut és a tévéhez kapcsolható?”. A válasz egybehangzó volt: „A HP nem kíván ezen a piacon jelen lenni.”.

A letört Wozniak ekkor Jobsszal ez utóbbi főnökeinek mutatta be a később Apple-I néven emlegetett számítógépet. Az Atari ebben az időben mutatta be első Home Pong játékát, így gyártósorai mind teljes kapacitással működtek. Az Apple-I gépet ragyogó megoldásnak tartották, de nem kívántak semmiféleképpen sem részt venni a gyártásában, terjesztésében. Sem a HP, sem az Atari, tehát maradt Jobs.

A két Steve leült, osztott-szorzott. Jobs eladta 1500 dollárért Volkswagen kisbuszát, Wozniak megvált szeretett programozható HP-65 kalkulátorától, amiért 250 dollárt kapott. Mivel üzletkötésre készültek, kellett a vállalkozásnak egy név. Apple Computer!

1977. április 17-én nyitotta meg kapuit a San Franciscóban a Nyugati Part Számítógépes Vásár, itt mutatkozott be az Apple-II 1298 dolláros áron. Sikeres volt, lenyűgözte a megjelenteket. A Jobs vesszőparipájává vált a házat, billentyűzetet, tápot tartalmazó gép, amely grafikus megjelenítésre volt képes. Az Apple-II 15 éves pályafutása alatt 5 millió felhasználóhoz jutott el. A cég 1980-ban jelent meg a tőzsdén, amely 30 éves kora előtt milliommossá tette Steve Jobs-t. Mivel a cég mérlege 1977 augusztusában már pozitív volt, így a Microsofttól megvásárolták a BASIC nyelv használati jogát nyolc évre 21 ezer dollárért. A

kódon kicsit dolgozott Jobs volt egyetemi cimborája, Randy Wigginton (ő írja meg később a MacWrite szövegszerkesztőt), majd az egészet kiadták Applesoft (lebegőpontos-BASIC) néven. Az Applesoft remek fejlesztői környezet volt, számos kiváló programot írtak a segítségével az Apple gépekhez.

Az Apple-II a fenti kiállítást követő évben vált igazi sikerré. A géphez ugyanis elkészült az Apple-II Disk, ami 475 dollárért meg is volt vásárolható. Az Apple-II bemutatását követő évben megrendezett vásáron már VisiCalc névre hallgató program volt a kiállítás egyik slágere, a világ megtanulta, hogy mi az a táblázatkezelő program. Az Apple ezen a vásáron már az Apple-II-Pluszt kínálta. A gépet 48 KB memóriával szállították, az Applesoftot már ROM-ba égették, így azt nem kellett külön betölteni. A II Plus, a Disc II és a VisiCalc épp azt kínálta, amit a vevők kerestek. A VisiCalcból több mint kétszáz ezer példány kelt el két év alatt, ez volt az első sikerprogram. És mivel ez a program csak Apple-ön futott, így az Apple-t is vásárolták szépen. Az Apple II-ből több milliót adtak el világszerte.

Az Apple következő nagy dobása, az 1983-as Lisa volt (amit Jobs lányáról nevezték el). A számos újítást felvonultató gép azonban bukás volt, ezzel együtt ez a cég egyik legfontosabb terméke. A Lisával vezették be a grafikus felhasználói felületet, aminek az első Macintoshban bemutatkozott utódját lenyúlta, átdolgozta, és Windows néven piacra dobta a Microsoft. A sors fintora, hogy Jobs önként szolgáltatta ki a grafikus felületet, ő adta Bill Gates kezébe a rendszert, hogy a Microsoft szoftvereket írjon az Apple-nek.

Az igazsághoz hozzátartozik, hogy az Apple is lopta az elvet, méghozzá a Xeroxtól. Jobs és csapata még 1979-ben látogatott el a társaság főhadiszállására, ahonnan a grafikus felhasználói felület és az eger ötletével tértek haza. Az egeret eredetileg szappantartóból és pingponglabdából fabrikálták, ez utóbbit aztán gumilabdával helyettesítették, hogy ne csúszkáljon az asztalon. A Xerox vezetői azt mondták a mérnökeiknek: *„Ti se gondoljátok komolyan, hogy a Xerox egy patkányhoz adja a nevét...”*.

A Lisa sikertelenségének oka leginkább az volt, hogy a nagyközönségnek szánt gép árazásánál elszámolták magukat, tízezer dollárja keveseknek volt egy számítógépre. Aztán 1984-ben bemutatták a Macintosht, ami már meghozta a világsikert. Ebben a gépben mutatkozott be a MacOS is, és a kétezer-ötszáz dolláros, fekete-fehér monitorral egybeépített számítógépet elkapkodták a vásárlók. Az Apple „1984” reklámjának nevezett televíziós reklám indította útjának az Apple Macintosh személyi számítógépet 1984-ben. Azóta elképesztő magasságokat és mélységeket élt meg a társaság: sokáig úgy tűnt, a Macintosh lesz az otthoni számítógép, aztán jött az IBM meg a Microsoft, és átvette az uralmat.

A PC és a Windows története

A személyi számítógépek hőskorának egyik legismertebb típusa az Altair 8800-as számítógép volt, amelynek sikeréhez három cég is hozzájárult. Elsősorban az Intel, amelynek a 8008-as mikroprocesszora felettébb sikeresnek bizonyult. A 6000 tranzisztort tartalmazó chip órajele 2 MHz volt és 640 000 műveletet tudott elvégezni másodpercenként. Magát a személyi számítógépet a New Mexico állambeli Albuquerque-ben székelő MITS (Micro Instrumentation Telemetry Systems) szerkesztette meg 1974-ben. A computert nem összeszerelve dobták piacra, hanem félkész állapotban, azaz a vásárló a készletből otthon barkácsolta össze a számítógépet. Az adatok bevitelére még nem billentyűzet, hanem egyszerű kapcsolótábla szolgált.

Az egyre népszerűbbé váló Altair 8800 felkeltette a figyelmét két ambiciózus fiatalembernek, akik ugyanebben az Új Mexikó-i városban alapították meg abban az időben Microsoft nevű cégüket. *Bill Gates* és *Paul Allen* számítógépes programok fejlesztésével próbáltak megkapaszkodni a még csak kialakulóban lévő piacon, s mint tudjuk, ez a törekvésük minden képzeletet felülmúlóan sikerült. Gates és Allen megalkották az Altair Basic programnyelvet, és eladták a MITS vállalatnak. Ez a szoftver nemcsak a Microsoft szerencséjének a kovácsává vált, hanem a személyi számítógépek elterjedésének is nagy lökést adott.

A PC története 1981-ben kezdődött, amikor az IBM először jelentette be, hogy személyi számítógépet készít (IBM Personal Computer). A cég egy tervezőcsoportjának csak egy évre volt szüksége, hogy előkészítse az IBM személyi számítógépét, ami ennél a megfontolt, nagy cégnél igazán nem nagy idő. 1982 tavaszára megindult a PC sorozatgyártása, és a kereslet messze meghaladta a kínálatot. Hirtelen mindenki ráébredt azokra a lehetőségekre, amelyeket a PC teremtett.

A DOS, amely mindenki számára egybeforrt a Microsoft nevével, vásárlás útján került a Microsofthoz. Az eredeti programot, melynek QDOS (Quick and Dirty Operating System) volt a neve, a Seattle Computer Products fejlesztette ki. Az MS-DOS 1.0 valójában a QDOS egy minimálisan átdolgozott változata volt, amelyet a Microsoft az eredeti gyártó Seattle Computer Products-tól kizárólag abból a célból vett meg, hogy azt tovább értékesíthesse az IBM felé, utóbbi akkor induló PC számítógépei operációs rendszereként. A jól jövedelmező lépések között említsük még meg Bill Gates azon sikerét is, hogy sikerült rávennie az IBM-et, hogy az MS-DOS-szal kapcsolatos minden jogot hagyja meg a Microsoftnál. A Microsoft a

Seattle Computer Products-nak a QDOS nem exkluzív terjesztési jogaiért 50 000 dollárt fizetett.

Az első IBM PC 1981 augusztusában jelent meg. Ekkor jelent meg az MS-DOS 1.0 is. Az év szeptemberében a Microsoft megkezdte a később Microsoft Windows néven megjelenő program fejlesztését, melynek megjelenéséhez több mint 4 évre volt szükség. Bill Gates a GUI ötletét az Apple cég Lisa nevű gépéből leste el, illetve a későbbi, de még a Windows előtt megjelent Macintosh-ok GUI-ja is inspirálhatta.

Egy évvel a PC megjelenése után a Compaq Computer Corporation piacra dobott egy hordozható PC-t, majd az IBM hozott ki új családtagot, az IBM XT-t. Ennek már merevlemez tárolója volt, és hamarosan teljes egészében felváltotta az eredeti PC-t. Az XT-vel már az MS-DOS 2.0 került kiszállításra. Utóbbi egy szinte az alapoktól újraírt rendszer volt, amely immár képes volt a könyvtárak és merevlemezek kezelésére is, bár utóbbiból csak a maximum 10 MB-osokat tudta kezelni. Mivel az akkori PC-kben nemhogy az ekkora kapacitású, de egyáltalán a merevlemez igencsak ritkaságnak számított, ezért ez nem okozott különösebb problémát a felhasználók számára. Az XT-t felváltó IBM 1984-es csúcsgépének, az IBM AT-nek egyértelmű sikere lett. Ez a siker a klóngyártóknak is újabb ösztönzést adott, akik közül sokan az eredetinél több szolgáltatást és alacsonyabb árat nyújtottak. Az egyik legnagyobb változtatás a 101 gombos billentyűzet bevezetése volt, ami ma ipari szabvánnyá vált. 1983. november 10-én New Yorkban, jelentette be hivatalosan a Microsoft a Microsoft Windows tervezett megjelentetését. Saját szavaik szerint a program az operációs rendszerek új generációjába tartozik, mivel grafikus felhasználói felületet és egyszerre több feladat végrehajtását is lehetővé tevő multitasking környezetet biztosít az IBM számítógépei számára. Az Intel 80386-os processzora után egy hónappal, 1985 novemberében adták ki. A feljegyzések szerint meglehetősen használhatatlan darab volt, holott a 386-os processzor már lehetővé tette volna a valódi többfeladatos működést, a multitaskingot.

1987 áprilisában viszont az IBM drámai módon megváltoztatta korábbi stratégiáját. A személyi számítógépek teljesen új családját indította el, amelyet Personal System 2-nek, röviden PS/2-nek nevezett el. A nem PC-kompatibilis 386-alapú géppel, és a Microsoft-tal közösen bejelentették az OS/2-t, amely csak decemberben került a piacra. Még áprilisban a Microsoft is bejelentette az MS-DOS 3.3-at és a Windows 2.0-t. Ez utóbbi már júniusban piacra is került. A PC-k elkezdtek még jobban hasonlítani a Macintoshokra. A Windows 2.0-ban már ikonok voltak, amelyek programokat és bármi egyebet jelképezhettek, és megjelentek azok az ablakok is, amelyek között egy mozdulattal ugrálhatunk. Az Apple természetesen azonnal beperelte a Microsoftot, mondván, hogy azok nem tartották be az 1985-ös

szerződésben foglaltakat. Microsoft azzal védekezett, hogy a licence-szerződés engedélyt adott nekik, hogy az Apple minden eredményét felhasználják. Az Apple ezzel szemben azt hangoztatta, hogy ellenfelei 170 alkalommal sértették meg az ő szerzői jogait. Végül Gates megpendítette, hogy az Apple a Xerox által az Alto és a Star nevű számítógépekhez fejlesztett GUI-kból lopta a levédett fejlesztések egy részét. A pert a Microsoft nyerte 1993 januárjában.

1988 októberében megjelent az OS/2 1.1-es verziója. Ugyanekkor a VMS egyik volt fejlesztője – David Cutler – a Microsoft-nál belefogott az NT tervezésébe. Egy hónappal később kiadták az MS-DOS 4.0-át, amely már a 32 MB-nál nagyobb merevlemezekkel is elboldogult. A Microsoft és az IBM szakítása után a 4.0 újításait az IBM az OS/2 nevű operációs rendszerében vitte tovább.

A hardverek fejlődése is haladt közben, 1989 tavaszán az Intel bemutatta a 80486-os processzort, amely 1 mikronos technológiával készült.

1989 májusában megjelent a Windows 3.0, amely már tudta használni a 640 KB feletti memóriaterületet is. Márciusban az IBM megjelenik az OS/2 2.0-val. Áprilisban a Microsoft kiadja a Windows 3.1-et és a DOS 5.0-t. A Windows 3.x-ek abszolút piacvezetők voltak egészen 1997-ig, amikor a már két éve kapható Windows 95 kiszorította a programokat.

Júniusban megjelenik a PCI sín, majd 1993 márciusában a Pentium processzor. Az év májusában megjelenik az OS/2 2.1. Augusztusban piacra kerül a Windows NT első verziója, 3.1-es verziószámmal, valamint a DOS 6.0, később pedig a DOS 6.22.

1994 októberben megjelenik az OS/2 Warp 3. 1995 augusztusában pedig kiadják a Windows 95-öt, amely még mindig nem tudott megszabadulni a DOS korlátaitól.

1995 novemberében az Intel bemutatja a Pentium Pro-t, majd 1996 márciusában bejelenti az MMX technológiát. A ráépülő processzorok azonban csak 1997 januárjában jelennek meg. Abban az évben tűnnek fel a piacon a Pentium II-es processzorok is.

1998-ban a Microsoft kiadja a Windows 98-at. Ez volt az utolsó változat, amelynek még bármi köze volt a DOS-hoz, mivel még a DOS kernelt használta. Ebben a változatban szerepelt először az Internet Explorer 4, és ez az operációs rendszer már támogatta az USB portot, és több más csatlakozási felületet is.

2000 februárjában megjelenik a Windows 2000. A Windows 2000 után jött a Millennium Edition és az XP, amelyek mindig egyre stabilabbak, egyre szebbek és gyorsabbak lettek – legalábbis a fejlesztők szerint. Ennek némileg ellentmondani látszik, hogy a Windows 98-ból létezett Second Edition, amely bizonyára még stabilabb volt, és hogy az XP-hez is kiadtak már szervizcsomagot, nem is egyet. 2007 elején Microsoft megjelentette legújabb operációs rendszerét, a Windows Vista-t.

Lassan már olyan stabilnak kellene lennie a gépünknek a sok fejlesztés következtében, hogy lelőni sem lehetne. A felhasználói oldalról valamit biztosan kijelenthetünk. Egyre nagyobb winchester, egyre több memória és egyre gyorsabb processzor kell, hogy az új operációs rendszereket futtathassuk. Meg persze egyre több pénz, hiszen ma az XP és az Office árából könnyedén megvehetünk egy középkategóriás számítógépet.

Mesterséges élet

A történelem legelső vírusai csak elméleti alapon léteztek. Feladatuk ugyanis a Neumann Jánostól származó teóriának az igazolása volt, hogy mesterséges életet lehet létrehozni a bináris világban, azaz lehet olyan programot írni, amely az élet alapvető jellegzetességeit (legalább részleteiben) megvalósítja. Az elmélet napjainkra kissé elfajult...

A (számítógépes) vírus egy intelligens, önmagát reprodukáló számítógépes program. Terjedéséhez más programokat használ fel, hogy magát álcázhassa. Intelligenciáját a programozójától kapta, és olyan erkölcstelen dolgokat képes művelni, amelyekkel a programozója felruházta. Intelligencia, értelem nélkül.

A számítógép legértékesebb részét az adatok jelentik. Ezek lehetnek táblázatok, szerkesztett szövegek, saját programok, nagyobb adatbázisok, vagy esetleg ott lehet a cég teljes könyvelése. Az adatok értéke mellett eltörpülhet a hardver és a szoftver értéke. Sajnálatos módon az adatokat nem csupán a műszaki vagy programhibából eredő megsérülés veszélye fenyegeti. Egyes emberek szántszándékkal ezeknek az adatoknak és programoknak a megsemmisítésére készítene (erkölcsileg nagyon alacsony, programozói tudásban elég magas színvonalon állva) sajátos programokat.

Az USA-ban már az ötvenes évek végén, később Németországban a hadsereg keretein belül is foglalkoztak olyan vírusok előállításával, amelyek megbéníthatják az ellenfél gépét. A vírusokat elméletileg csak háborús célokra akarták felhasználni, de valahogy mégis sikerült jó párnak kiszabadulnia. Ezek a vírusok folyamatos mutációs lehetőségeikkel és a hagyományos módszerekkel, észrevehetetlen terjedésükkel ideális hadviselési eszközök.

Európában a dortmundi egyetemen a kutatás ekkor még a legteljesebb titoktartás mellett folyt. Egyes katonai körök úgy látták, hogy a vírusprogramok alkalmasak egyes érzékeny technológiák és szoftverek le- és ellopásának megakadályozására és az ellenséges hatalmak számítógéprendszerének totális megbénítására.

Az információt egy idő után már nem lehetett visszatartani. Tévedés volt azt hinni, hogy a szakirodalom kirekesztésével nem terjed tovább ennek az új programozási lehetőségnek az

ismeretanyaga. 1984-ben az NSZK-ban egy rövid cikk számolt be az önreprodukáló programok létéről, felhívva a figyelmet a számítógépes technikai kultúrára leselkedő veszélyekre is. Ezután már nem lehetett letagadni létüket.

A vírusok kialakulásában egy másik fontos történet is szerepet játszott. A nyolcvanas évek legelejére a számítógépek már tudtak kommunikálni egymással hálózatokon, telefonvonalakon keresztül, és az amerikai telekommunikáció olcsósága miatt ez nem volt egyedi, ritka esemény. Eme számítógépes vonalakon keresztül cseréltek egymással adatokat, illetve információkat.

A témával konkrétan foglalkozó elméleti publikációk sorát egy amerikai kutató, Fred Cohen „Computer Viruses: Theory and Experiment” című tanulmányában alkalmazta a gyakorlatban. Ő végzett először valós kísérleteket az egyetem VAX 11/750 típusú gépén UNIX multitasking (többfelhasználós) operációs rendszerkörnyezetben, amit megismételt egy VMS-VM/370 operációs rendszerű hálózati rendszerkörnyezetben is. Az eredmény több mint megdöbbentő volt.

A multitask környezetben a vírus elindítása után gyakorlatilag nulla időpillanatban mind a 33 rendszerállományt és az adminisztrátor programállományát megfertőzte, majd az elindítás utáni 18. másodpercben a négy felhasználó állományai is fertőzöttek voltak. A hálózatos rendszerben a hatszázadik másodpercben vált teljessé a fertőzés. Ezek a rendszerek annak idején semmilyen külön beépített védelemmel sem rendelkeztek a vírusok ellen. Ennek azonban akkor még nem sokan mérték fel a veszélyeit. Megjelentek a vírusprogramot kibocsátó, mint az illegális programmásolókat megbüntető – önbíráskodó – másolásvédelmi programrendszerek, ugyanakkor a fiatalok is „jó tréfának” tekintették a hálózatok vírusokkal történő megfertőzését.

Fred Cohen 1983 novemberében, akkor éppen PhD-jára készült, amikor szemináriumon vett részt. A téma a számítógépes rendszereket megtámadó trójai falovak voltak. Ezeknek az a lényegük, hogy többet, illetve mást tesznek, mint amire a felhasználó számít, és eközben persze kárt okoznak. Például egy programot elindítva azt hisszük, hogy szövegszerkesztőt fogunk működésbe hozni, ehelyett azonban letöröljük a merevlemezt. Vagyis a trójai is végtelenül kártékony lehet, bár nem képes arra, amire a vírusok: szaporodni. Egy trójai faló rendszerint csak akkor jelenthet komolyabb veszélyt, ha valamilyen módon mesterségesen terjeszti el készítője, miként például az „AIDS ismeretterjesztő floppy”, amelyből 1989-ben 26000 fertőzött floppyt postáztak.

Cohen ezen a szemináriumon döbbsent rá, hogy milyen végtelenül alacsony hatásfokú ez a módszer. „*Mintha csak egy függöny választott volna el az igazságtól, és most Isten félrehúzta*

volna a függőnyt, mondván: »Íme, lássad!«. És én rögtön megértettem, hogy miről van szó.» Ekkor persze már régóta ismerte a Neumann-féle, önreprodukcióra képes automaták elméletét, dehát ezek meglehetősen bonyolult matematikai konstrukciók. Átgondolta, hogy egy egyszerű programcska képes a saját, esetleg továbbfejlesztett másolatát bejuttatva a befolyása alá vonni és a saját céljaira kihasználni egy nagyobb programot éppen úgy, mint egy parazita a gazdaállatot. És ezzel meg is született a számítógépes vírus definíciója.

Cohen viszont nagyon is átlátta az ötlet fontosságát. Sőt, hamarosan azt is hozzátette, hogy többről van itt szó a biológiai és a számítógépes vírusok felületes hasonlóságánál. Ha ugyanis az élőlényt nem önmagában, hanem környezetével együtt tekintjük élőnek, akkor a számítógépes program is több egy halom logikai műveletnél. Ha leírjuk a szaporodásra, a mutációra, a környezethez való alkalmazkodásra alkalmas számítógépes vírusok viselkedését, csak azt felejtjük el megemlíteni, hogy nem létező teremtményekről van szó, hanem pusztán kódról, akkor nem lesz az a biológus, aki ne tekintené őket valóban élőnek. Az élő és a mesterséges közötti különbségeket kutató, Artificial Life (Mesterséges Élet) nevű új tudomány egyik legjelentősebb képviselője, Christopher Langton szerint: *„Bármely olyan definíció, amely eléggé széles ahhoz, hogy átfogja az egész állatvilágot, szükségszerűen ki fog terjedni bizonyos számítógépes folyamatokra is, és ekkor ezeket valóban élőnek kell tekinteniünk.”*

Cohen írta meg az első ismert vírust is. Még aznap, 1983. november 3-án délután nekiült, és öt perc alatt el is készült a C nyelvű kódnak a behatolásra és rombolásra szolgáló részével – aztán a nap hátralévő részét egészen kora estig azzal töltötte, hogy megírja a vírus terjedésének ellenőrzését és szabályozását szolgáló részt. Nem véletlen, hogy a kétszáz soros program túlnyomó – és összehasonlíthatatlanul időigényesebb – része a kontrollra szolgált. Cohen azt akarta, hogy kizárólag az ő engedélyével lehessen megfertőzni egy-egy fájl a megtámadott komputeren. A mai vírusírókkal ellentétben úgy gondolta, hogy egy vadul terjeszkedő, ellenőrizhetetlen program létrehozása nem dicsőség, hanem szégyen – és még csak nem is olyan hasznos, mintha „fékek” volnának beleépítve. Ő ugyanis a UNIX alatt dolgozó egyetemi gépen a szeminárium vezetőjének engedélyével – meg persze az engedelmes vírus segítségével – rombolás helyett villámgyorsan átvette a hatalmat.

Magyarországon a 80-as éves közepén bukkant fel az első vírusprogram, igaz, még Commodore 64-es gépen. Ennek hordozója néhány népszerű játékprogram volt. Terjesztője pedig egy, a gépek javításával foglalkozó „szakember”, aki ezzel a piszkos trükkel ért el magának nagyobb forgalmat, könnyű kereseti lehetőséget. Programvírusa ugyanis olyan külső pályára vitte a lemez meghajtó olvasófejét, ahonnan csak kézzel, a lemezegység

szétszedésével lehetett visszavezényelni. Magyarországon ezt a vírust használták először másolásvédelemre egy kereskedelmi forgalomban árusított könyvelőprogramban.

A jövő

Hogy mi lesz a jövőben a fejlődés iránya a számítástechnikában, az megjósolhatatlan. Nem lehet tudni, hogy mi lesz 1 év múlva. Ugyanis nem tudjuk, hová fejlődik a számítógép holnap, vagy akár csak ma. A következőkben egy lehetséges irányt szeretnék megmutatni.

A gépszerkesztés alternatívája a mesterséges intelligencia létrehozásában az egyik megközelítés, a biológiai evolúció folyamatának utánzása a számítógépben. A szimulált evolúció eltérő utat kínál a bonyolult hardver és szoftver tervezésére. Olyan utat, ami megkerüli a műszaki tervezés számos problémáját. A szimulált evolúció működését példázzuk egy számokat csökkenő sorrendbe rendező szoftverrel. A szokványos műszaki megközelítés az lenne, hogy egy rendező algoritmus valamelyikének alapján írunk egy programot; de most nézzük azt az esetet, hogy ehelyett hogyan „fejleszthetnénk ki” a szoftvert.

Az első lépés véletlenszerű programok „populációjának” a generálása. Ezt a populációt létrehozhatjuk álvéletlenszám-generátor használatával, amellyel megalkotjuk az utasítások véletlenszerű sorozatát. A folyamat felgyorsítására alkalmazhatjuk a csak a rendezés műveletére használható utasításokat, például az összehasonlító- és csereutasításokat. Az utasításoknak ezek a véletlenszerű sorozatai jelentik a programot. A véletlenszerű populáció mondjuk tízezer ilyen programot fog tartalmazni, melyek mindegyike néhány száz utasítás hosszúságú.

A következő lépésben megvizsgáljuk a populációt, hogy kikeressük közülük a legsikeresebb programokat. Ehhez minden egyes programot le kell futtatnunk, hogy lássuk, melyik rendezi helyesen a próbasorozatot. Minthogy a programok véletlenszerűek, valószínűleg egyik sem állja ki a próbát, de a pusztán szerencse némelyiket közelebb viszi a helyes rendezéshez, mint a többieket. Az egyik program például véletlenül a sorozat végére helyezheti az alacsony számokat. Miután a programokat kipróbáljuk egy néhány számból álló sorozaton, minden programhoz egy hozzáillő pontszámot rendelhetünk. A következő lépés az olyan új populációk létrehozása, amelyek a magasra értékelt programok leszármazottai.

Ennek megvalósításához először is töröljük az átlagos pontszámnál kevesebbel rendelkező programokat, hogy csak a legalkalmasabb programok maradjanak életben. Az új populációt úgy hozzuk létre, hogy kisebb véletlenszerű variációkkal másolatokat készítünk a fennmaradó programokról. Ez az eljárás megfelel az aszexuális mutációs reprodukciónak. A másik

lehetőség, hogy a következő generáció új programjait az életben maradt programok párosításával „tenyésztjük”. Ez a folyamat pedig a szexuális reprodukciónak felel meg. Ez oly módon vihető végbe, hogy a „szülőprogramok” mindegyikéből utasítássorozatokot kombinálunk a „gyermek” létrehozására. A szülők feltételezhetően azért maradtak fenn, mert hasznosítható utasítássorozatokot tartalmaztak, és így jó esély nyílik rá, hogy a gyermek örökölni fogja szüleitől a leghasznosabb részleteket.

A programok létrejött új generációját ismét ugyanannak az elemző és szelekciós eljárásnak vetjük alá, úgyhogy ismét csak a legalkalmasabb programok maradnak életben és szaporodnak. Egy párhuzamos számítógép néhány másodpercenként hoz létre újabb generációt, így a szelekciós és variációs eljárást sok-sok ezerszer is könnyedén megismételhetjük. A populációk átlagos alkalmassága minden generációval növekszik, azaz a programok egyre alkalmasabbak a rendezésre. Néhány ezer generáció múlva a programok tökéletesen fognak rendezni.

Egy kísérletben alkalmazták a szimulált evolúciót, hogy az különleges rendezési feladatok megoldására kifejlesszen egy programot, majd leírták a folyamat működését. A kísérletben előnyben részesítették azokat a programokat, amelyek gyorsan rendezték a próbasorozatokat, így a gyorsabb programoknak nagyobb esélyük volt a fennmaradásra. Ezzel az eljárással igen gyors rendezőprogramok jöttek létre. Az evolúciós folyamatban létrejött programok valamivel gyorsabbnak bizonyultak, mint azok, amelyek algoritmusok alapján íródtak. Gyorsabban rendezték a számokat, mint bármely olyan program, amelyet programozók írtak volna egy ismert algoritmus alapján. Az evolúciós folyamat során létrejött programok esetében az az egyik legérdekesebb mozzanat, hogy nem érthető, hogyan is működnek, hiába vizsgálták meg utasítássorozataikat a leggondosabban. Könnyen lehet, hogy ezek a programok nem megérthetőek, más szóval, nem bonthatjuk a program működését a megérthető részek hierarchiájára.

Matematikai tesztekkel használták annak bizonyítására, hogy a kifejlesztett rendezőprogramok tökéletes rendezők. Jobban bízhatunk az őket létrehozó folyamatban, mint a matematikai tesztekben. Mégpedig azért, mert az evolúciós folyamat során kifejlődött rendezőprogramok olyan programok hosszú sorának a leszármazottai, amelyek fennmaradása kizárólag rendezési képességüktől függött.

Az a tény, hogy az evolúciós folyamat során létrejött programok nem mindig megérthetőek, egyes embereket aggodalommal tölt el az alkalmazásuk tekintetében, azonban ez az aggodalom téves feltételezéseken alapul. Ezeknek a feltételezéseknak az egyike, hogy a szigorúan műszaki alapon létrehozott rendszerek mindig jól megérthetőek, ám ez csak a

viszonylag egyszerű rendszerek esetében igaz. Például manapság egyetlen személy sem láthat át teljes mértékben egy operációs rendszert. A téves feltételezés az is, hogy a nem megmagyarázható rendszerek kevésbé megbízhatóak. Ha választani lehetne, hogy egy műszakilag tervezett számítógépprogram, illetve egy emberi pilóta által irányított repülőgépen utazzon-e, melyiket választaná? Részemről egészen biztosan az embert választanám, bár fogalmam sincs az emberi pilóta működéséről. Szívesebben vetem a bizalmam abba a folyamatba, amely a pilótát létrehozta. Akárcsak a rendezőprogramok esetében, tudom, hogy a pilóta az életképesnek bizonyult egyedek hosszú sorának a leszármazottja. Ha a repülőgép biztonsága a számok helyes rendezésétől függene, akkor inkább bíznam magam egy evolúciósan kifejlesztett rendezőprogramra, mint egy olyanra, amit egy csapat programozó írt.

Az előzőekben leírt kísérlet is rámutat, milyen lehetőség van a jövőben a számítógépek egyik lehetséges fejlődési irányában a mesterséges intelligencia fejlesztésében. Gondoljunk csak a Mars meghódítására, lakhatóvá tételének egyik lehetősége lehetne pl. gondolkodó gépekre bízni a marsi felszín átformálását. Pusztán azzal, hogy kijelöljük, mi a cél, az eszközt és annak kifejlesztését pedig a gyorsan fejlődő gondolkodó gépekre hagyjuk.

Összefoglalás

Tapasztalataim szerint sok középiskolában nem foglalkoznak megfelelő részletességgel a számítástechnika és informatika fejlődéstörténetével. Szakdolgozatom írásánál a célom az volt, hogy olyan munkát készítssek, amely nélkülözi az egyes területek részletes taglalását. Inkább azoknak szól, akik az adott tananyagrészt, tanítani szeretnék. Dolgozatommal iránymutatást kívánok adni nekik a tanításhoz.

A kidolgozásnál fontosnak tartottam az ok-okozati összefüggések feltárását, elősegítve a könnyebb érthetőséget.

Munkámban bemutattam a számok kialakulását, a számításokat segítő egyszerű gépek történetét. A számolás fejlődését, amely a formális matematika, a matematikai logika és a matematikai nyelvészet megalkotásához vezetett. Megvilágítottam, hogy a XX. század első felében miként indult meg a számítógépek kifejlesztése, amelyek megszületésüket a háborúnak köszönhetik. A század második felében az addig is lendületes fejlődés további gyorsulását a technikai haladásnak köszönhetően, melynek végeredménye egy a mindenki számára elérhető könnyen kezelhető gép lett, amely úgy vált a hétköznapok részesévé, mint előtte a televízió vagy a telefon. Utolsó nagy áttörést az internet megjelenése hozta, amely eredményeként a kommunikáció új szintre emelkedett.

Úgy látom, hogy az internet elterjedésével a határ egyre inkább elmosódik a telefon a televízió és a számítógép között, melynek következtében egyfajta univerzális kommunikációs csatorna van kialakulóban, amely már nem utópia.

A számítástechnika megállíthatatlanul tovább fejlődik, a zseniális elmék kitartó munkájának és sokszor a véletlen felfedezéseknek köszönhetőn. Nehezen kiszámítható, hogy mit hoz a holnap, de remélem, hogy az emberiség javát szolgálja.

Úgy vélem, hogy a kitűzött céloimat sikerült oly mértékben megvalósítanom, amennyire szerettem volna. A dolgozatomhoz készítettem egy bemutatót, melyet kiváló oktatási segédanyagnak tartok a téma iránt érdeklődő oktatóknak, tanulóknak, a számítástechnika és az informatika fejlődésének megismertetéséhez.

Melléklet

A szakdolgozathoz készített bemutató.

Irodalomjegyzék

- Kőfalvi Tamás: *Informatikai alapismeretek*, Nemzeti Tankönyvkiadó 2006.
- Raffai Mária: *Az informatika fél évszázada*, Springer 1997.
- Herman H. Goldstine: *Pascaltól Neumannig*, Műszaki 2003.
- F. W. Winterbotham: *Az Ultra titka*, OMMIK 1990.
- Stephen Budiansky: *Elmék harca*, Vince 2005.
- T. Dénes Tamás: *Titkos-számítógép-történet*, Aranykönyv 2003.
- Simon Singh: *Kódkönyv*, Park 2001.
- Simon Singh: *A nagy Fermat-sejtés*, Park 1999.
- Paul Hoffman: *A Prímemberek*, Scolar 1998.
- Bach Iván: *Formális nyelvek*, Typotex 2001.
- William Aspray: *Neumann János és a modern számítástechnika kezdetei*, Vince 2004 .
- Bödök Zsigmond: *Magyar feltalálók a számítástechnika történetében*, Nap 2006.
- Dr. Galambos Gábor: *Operációs rendszerek*, Műszaki 2003.
- Andrew S. Tanenbaum - Albert S. Woodhull: *Operációs rendszerek*, Panem 1997.
- Eric S. Raymond: *A katedrális és a bazár*, Kiskapu 2004.
- Bill Gates: *Üzlet @ gondolat sebességével*, Alexandra 1999.
- Daniel Ichbiah: *Bill Gates és a Microsoft regénye*, K.u.K. 1996.
- Galántai Zoltán: *A nagy adatrablás*, Kossuth 1998.
- Kazári Csaba: *Hacker, cracker, warez*, Computer panoráma 2003.
- Farmosi István – Kis János – Szegedi Imre: *Víruslélektan*, Cédrus 1990.
- Daniel Hillis: *Üzenet a kövön*, Vince 1999.

A SZÁMÍTÁSTECHNIKA ÉS AZ INFORMATIKA FEJLŐDÉSÉNEK TÖRTÉNETE

Készítette:
Becskeházi Zoltán
informatika tanárszak
levelező tagozat

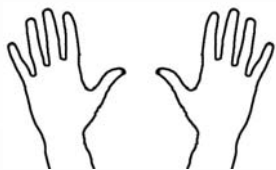
DEBRECENI EGYETEM – INFORMATIKAI KAR

Debrecen
2008

Ajánlott irodalom

- Herman H. Goldstine: Pascaltól Neumannig, Műszaki 2003
- Bődök Zsigmond: Magyar feltalálók a számítástechnika történetében, Nap 2006
- Raffai Mária: Az informatika fél évszázada, Spinger 1997
- Kőfalvi Tamás: Informatikai alapismeretek, Nemzeti 2006
- T. Dénes Tamás: Titkos-számítógép-történet, Aranykönyv 2003

Számrendszerek

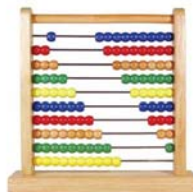


tízes számrendszer

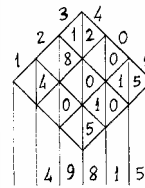


hatvanas és tizenkettes
számrendszer

Számszerszámok



abakusz



gelosia módszer

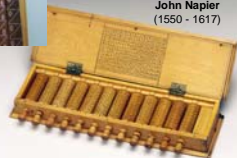
Számszerszámok



Napier-pálcák



John Napier
(1550 - 1617)



logarléc

Számológépek



Wilhelm Schickard
(1592-1635)



Schickard-gép

Számológépek



Blaise Pascal
(1623 - 1662)



Pascal kalkulátor

Számológépek



Gottfried Wilhelm Leibniz
(1646-1716)



Leibniz kalkulátor

Programvezérlés



vezérelt szövőszék



Jacquard-kártya

„Az első számítógép”



differenciagép



Charles Babbage
(1791 - 1871)

Programozható gép




analitikus gép



Ada Lovelace
(1815-1852)

Boole algebra



George Boole
(1815 - 1864)

A logikai algebra, amelyet
Boole algebrának nevezünk,
megteremtésével a számítástechnika
fejlődéséhez jelentősen hozzájárult.



Herman Hollerith
(1860-1929)

Népszámlálás



Hollerith népszámlálógépe

Ajánlott irodalom

- F. W. Winterbotham: Az Ultra titka, OMMIK 1990
- Stephen Budiansky: Elmék harca, Vince 2005
- Simon Singh: Kódkönyv, Park 2001
- T. Dénes Tamás: Titkos-számítógép-történet, Aranykönyv 2003

Az Enigma

Felépítése

- Billentyűzet
- Keverőegység
- Kijelzőpanel

A forgótárcsák alkalmazása

- A forgótárcsa minden betű leütése után elfordul egy beosztással.
- A tárcsa egyik oldalán lévő érintkezők bonyolult huzalozással kapcsolódnak a túlsó oldalhoz.
- 3 forgótárcsát alkalmaztak



Az Enigma biztonsága

- 17576 kódtárcsa állás. 6 ember 1 nap alatt végigpróbálhatja nem elég.
- Az Enigma biztonságos, mert...
A bemeneti keverő fokozza a variációk számát
A tárcsák helyét is lehet cserélni és a tárcsákat meg lehet fordítani.
- Az Enigmához napi kódkönyvet használtak, amin az aznapi enigma tárcsák beállítása és a bemeneti kapcsolótábla huzalozása volt.
- **Elég biztonságos, mert a variációk száma több, mint 10 000 000 000 000 000!!!**



Bemutkozik az Enigma

- 1926-tól a németek használni kezdték az Enigmát.
- A franciák, angolok nem tudták feltörni a német kódokat. Hamarosan abbahagyták a próbálkozást!
- A Lengyelek félték a németektől és a Szovjetuniótól is. Szereztek egy kereskedelmi változatú Enigmát.
- Egy német Hans-Thilo Schmidt 1931-ben átadott egy Rex nevű francia ügynöknek információkat az Enigmáról, a huzalozásáról és egyéb paramétereiről



Az Enigma megfejtése

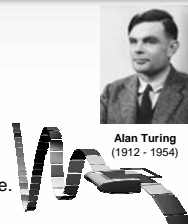
- A megfejtés kulcsa az alapbeállítás
- A franciák nem jutottak semmire, átadták az információt a Lengyeleknek
- Megtudták, hogy napi kulcsok vannak
- Mivel a napi kulcs sok üzenetet jelent, ezért meg lehet fejteni. A németek ezért minden nap elején üzenetkulcsot küldtek, amely a továbbiakban küldött üzenetek kulcsát tartalmazta. Így naponta csak néhány ezer betűt kódoltak ugyanazzal a kulccsal.
- A Lengyelek nem irodalmárokat, hanem matematikusokat, mérnököket állítottak rá a megfejtésre, mivel ez már egy gépesített kor...
- A németek minden nap elején kétszer küldték el a kulcsot, hogy a zavarokat kiküszöböljék. Ez alapján olyan rendszert talált, amely a bemenet és a kimenet közötti bizonyos összefüggéseket mutatott meg.
- Egy év alatt készített egy táblázatot, amely a kipróbálandó esetek számát csak 105 456 keverőtárcsa beállításra csökkentette.

A biztonság további fokozása

- A németek módosították az üzenetküldés módját. Rejewski táblázatai használhatatlanná váltak, de ő gépesítette a táblázatok alkalmazását.
- Készítettek 6 módosított Enigmából álló „Bombát”, amely végigpróbálta a 17 578 keverőtárcsa beállítását, majd megtalálhatta a helyes beállítást.
- A németek növelték a tárcsák számát és megváltoztatták a tárcsák és a kapcsolótábla huzalozását!
- A variációk száma nőtt
- A „bomba” méretét növelni kellett volna
- A Lengyelek a továbbiakban nem tudták megfejteni az üzeneteket.
- A lengyelek 1939 júliusában megmutatták az angol és francia kriptográfusoknak a „bombát” és átadták a teljes dokumentációt. Pár héttel később a németek lerohanták Lengyelországot.

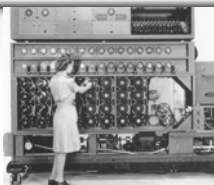
Alan Turing

- Zseniális matematikus, különc tudós.
- Legfontosabb publikációja „Kiszámítható számok c. dolgozata”
- Turing gép, Tetszőleges algoritmikus feladatot végrehajtó berendezés. Az algoritmikus számítógépek modellje.
- 1938-ben meghívták kriptográfusnak.
- Turing feladata volt olyan módszer megtalálása, ami akkor is működik, ha a németek már ismételnék üzeneteket.
- Rájött, hogy egyes üzeneteket naponta ismétlik a németek. Ezek lettek a támpontok



Turing bombái

- Turing olyan berendezést szerkesztett, amely elektromosan összekötötte három berendezés kimenetét a bemenettel és így lecsökkentette a kipróbálandó esetek számát.
- 12 készlet Enigmát kötöttek megfelelően sorba, utána 17576 beállítást kellett csak végigpróbálni. Ha a lámpák kigyulladtak megvolt az aznapi beállítás.
- A bombák sokat segítettek. Churchill támogatta a kódfejtőket. 1942-ben már 42 bomba járt.



Ajánlott irodalom

- Herman H. Goldstine: Pascaltól Neumannig, Műszaki 2003
- Dr. Galambos Gábor: Operációs rendszerek, Műszaki 2003
- Andrew S. Tanenbaum - Albert S. Woodhull: Operációs rendszerek, Panem 1997
- William Aspray: Neumann János és a modern számítástechnika kezdetei, Vince 2004
- Bach Iván: Formális nyelvek, Typotex 2001

Neumann János

„A számítógép nem egy vagy több ember tulajdona, hanem az egész emberiségé.”



Neumann János
(1903 - 1957)

Az elektronikus számítógépek logikai tervezésében kiemelkedő érdemeket szerzett. Ennek alapvető gondolatait (a kettes számrendszer alkalmazása, memória, programtárolás, utasítás rendszer) Neumann-elvekként emlegetjük.

Neumann János

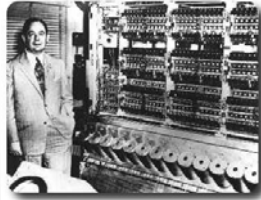
Neumann-elvek

- soros utasításvégrehajtás
- bináris (kettes) számrendszer használata
- belső memória (operatív tár) használata a program és az adatok tárolására
- teljesen elektronikus működés
- központi vezérlőegység alkalmazása

Neumann János

A Neumann-elvű számítógépek elméleti felépítése

- központi egység
 - központi feldolgozó egység
 - központi vezérlő egység
 - aritmetikai-logikai egység
 - regiszterblokk
 - gyorsítómemória
 - matematikai társprocesszor
 - operatív tár (memória)
- háttértárak
- perifériák
 - input perifériák
 - output perifériák



Számítógép generációk

Első generáció 1943-1954

- rendelkezésre készült műveletek, az elvégzendő feladathoz: tudományos műszaki számítások
- binárisan kódolt gépi nyelvű program (minden gépnek különböző)
- programozás nehezen megtanulható, gépi nyelven
- **processzorcentrikus**
- soros feldolgozás
- vákuumsövek (nagy méret)
- adat tárolók: mágnesdobok
- műveletvégzéshez **elektroncsöveket** használnak
- néhány tízezer művelet/mp
- nagy energia felhasználás
- kis megbízhatóság
- magas ár
- néhány darab

Számítógép generációk

Első generáció 1943-1954

- 1941 *Konrad Zuse, Z3*, elektromágneses relék, repülő és rakéta tervezés
- 1943 *Alain Turing, Colossus*, német rejtjel visszafejtés (célgép)
- 1944 *Howard H. Aiken, Mark I.*, lövedékpálya táblázatok, fél focipálya méret, 800km vezeték, relé, 3-5 sec/számolás, alapsműveletek, komplex egyenletek

Számítógép generációk

Első generáció 1943-1954

- 1946, **ENIAC** első elektronikus digitális számítógép
18.000 vákuumszó, 70.000 ellenállás, 5 millió forrasztás, 160 kW fogyasztás
5000 +/sec, 400 */sec, 10 jegyű számok, 20 regiszter, 1000* gyorsabb mint Mark I.
külső programvezérlés (huzalozás)
30 Tonna
- 1945 **EDVAC**, memória tárolja az adatokat és a programot feltételes vezérlés átadás központi vezérlő egység
- 1951 **UNIVAC I.** első kereskedelemben kapható számítógép

Számítógép generációk

Második generáció 1954-1964

- az elektroncsövek helyett megjelenik a jóval kisebb dióda és **tranzisztor**
- a tranzisztor révén sokkal megbízhatóbb gépek
- kapcsolási idő, gépi méretek, energia igény csökken
- teljesítmény/ár arány megnő
- önálló (a központi feldolgozó egységtől függetlenül) párhuzamosan működő csatornák (I/O)
- **memória centrikus**
- perifériák, háttértárak
- ferritgyűrűs memória (megbízhatóbb, olcsóbb, gyorsabb, nagyobb kapacitás)
- a nagy univerzális számítógépek
- megjelennek az első programozási nyelvek: assembly nyelv (rövidített kódok), COBOL, FORTRAN, ALGOL, software ipar...
- kötegelte (batch) feldolgozás, gazdasági adatfeldolgozás, ipari folyamatirányítás

Számítógép generációk

Harmadik generáció 1964-1971

- 1958 *Jack Kilby* (Texas Instruments) **Integrált áramkör** (IC)
- az integrált áramkörök a gépekben
- 10e5..10e6 művelet /sec
- **godularitás gépfelépítés**, bővíthetőség
- modulás a gépek ára és mérete rohamosan csökken, megbízhatóságuk nő
- párhuzamos működés, több processzor
- I/O processzorok
- olcsó nagy táruk (félvezetőkől készült memóriák)
- megjelennek a korszerű operációs rendszerek, szoftverek
- multiprogramozott üzemmód
- időosztásos rendszerek, távoli terminálok
- **IBM 360 / 370, PDP 11 (DEC másolat)**



Számítógép generációk



Negyedik generáció 1971-1991



- egyre több elem egy tokban (chipben) LSI, VLSI,
- csökkenő méret, csökkenő ár
- növekvő teljesítmény, megbízhatóság
- 1971 Intel 4004: központi feldolgozó egység, memória, I/O vezérlés 1 chipben (egy **mikroprocesszor** - több feladatra programozva)
- **mikroszámítógépek**
- 1976 **Cray** 198 MFLOPS
- mini-számítógépek (**Comodore, Apple, Atari**)
- 1981 **IBM PC** „személyi számítógép”
- desktop, laptop, palmtop
- 1984 **Macintosh Apple**, grafikus operációs rendszer
- **hálózatok**, LAN, internet

Számítógép generációk

Ötödik generáció 1991-

- Mesterséges intelligencia...
- Párhuzamos (nem Neumann elvű) feldolgozás
- Új technológia, új elvek?
- **Kvantum számítástechnika...**

Egyik jellemzőjük, hogy párhuzamos és asszociatív működésű mikroprocesszorokat alkalmaznak. A problémaorientált nyelveket próbálják tökéletesíteni, erre egy kezdeti kísérlet a PROLOG programozási nyelv. A számítógépeket úgy tervezik, hogy minél több áramkörti elemet szűksítsenek bele egyre kisebb méretű mikrochipekbe, azonban ennek hamarosan elérjük a fizikai határait, ezért új gyártási módszerekre és működési elvekre van szükség.

Ajánlott irodalom

- Eric S. Raymond: A katedrális és a bazár, Kiskapu 2004
- Daniel Ichbiah: Bill Gates és a Microsoft regénye, K.u.K. 1996
- Bill Gates: Üzlet @ gondolat sebességével, Alexandra 1999
- <http://www.nhh.hu/dokumentum.php?cid=11475>
- http://apple1.buzz.hu/archives/2006/12/11/Apple_tortenete/
- <http://www.fallerjeno.tvn.hu/Tanarok/HCS/TAN/70/70.htm>

Xerox PARC



Apple Computer



Apple I
(1976)



Apple II (1978)



Lisa (1983)



Machintos
(1984)

Személyi számítógép



IBM PC (1981)



IBM AT (1984)



IBM PS/2 (1987)

Operációs rendszerek



MS Windows (1985-)



MacOS (1984-)



Linux (1991-)

Microsoft Windows



Windows asztali termékek

Windows 1.0 (1985)
Windows 2.0 (1987)
Windows 3.0, 3.1 és Windows for Workgroups 3.11 (1993)
Windows NT 3.1 (1994)
Windows NT 3.5
Windows 95 (1995)
Windows 95 második kiadás (1996) (OSR2)
Windows NT 4.0 (1997)
Windows 98 (1998)
Windows 98 második kiadás (1999) (SE)
Windows Me (2000) (Millennium Edition)
Windows 2000 Professional (1999)
Windows XP (2001)
Windows Vista (2006-2007)

Windows kiszolgálótermékek

Windows NT Advanced Server 3.1
Windows NT Server 3.5
Windows NT Server 3.51
Windows NT Server 4.0
Windows 2000 Server
Windows Server 2003
Windows Server 2008

Az internet



Az internetnek nincs központja, szerkezete leginkább egy úthálózathoz hasonlítható. Hiba esetén más útra kényszerülnek az adatok, mint egy lezárt közút esetén.

Az üzenetek csomagokra bontva, egymástól függetlenül haladnak, akár más és más útvonalon.

Az internet fejlődése

- 1960 - A csomagkapcsolásos technika megjelenése
- 1968 - Az ARPANET hálózat építésének a kezdete
- 1969 - Négy számítógép összekapcsolása
- 1972 - Az NCP (Network Control Protocol) kidolgozása, az első e-mail szoftver megszületése
- 1983 - A TCP/IP bevezetése az Internet hálózatban
- 1985 - A hálózat kilép a hadügy keretei közül
- 1989 - A World Wide Web megszületése a CERN-ben (Genf)
- 1990 - Az első kereskedelmi Internet szolgáltató megjelenése
- 1991 - Magyarország csatlakozása az Internetre
- 1992 - Megjelenik az első internet böngésző (Mosaic)

A hálózati világ tapasztalati törvényei

- **Moore törvénye** a feldolgozási kapacitásról: a feldolgozási kapacitás 18 havonta megduplázódik
- **Gilder törvénye** a sávszélességről: a kommunikációs rendszerek teljes sávszélessége 12 havonta háromszorosára növekszik
- **Ruettgers törvénye** a tárolási kapacitásról: a tárolási kapacitás 12 havonta megduplázódik
- **Metcalf törvénye** a hálózatok értékéről: a hálózatok értéke az előfizetők számával „négyzetesen” nő

Ajánlott irodalom

- Galántai Zoltán: A nagy adatrablás, Kossuth 1998
- Farnoszi István – Kis János – Szegedi Imre: Víruslélektan, Cédrus 1990
- Kazári Csaba: Hacker, cracker, warez, Computer panoráma 2003
- Daniel Hillis: Üzenet a kövön, Vince 1999