Garai Géza Szabadegyetem I.

TÁMOP-4.2.3-12/1/KONV-2012-0039
Alba Regia Egyetemi Központ tudományos eredményeinek disszeminációja, mérnöki és kutatói utánpótlás biztosítása a Közép-dunántúli Régióban

Készült az „Alba Regia Egyetemi Központ tudományos eredményeinek disszeminációja, mérnöki és kutatói utánpótlás biztosítása a Közép-dunántúli Régióban” (TÁMOP 4.2.3-12/1/KONV-2012-0039) című projekt keretében.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Szerkesztette: dr. Nagy Rezső

Lektorok: Dr. Hajnal Éva (1-55. oldal), Dávid András (56-108. oldal)

ISBN 978-615-5460-34-0

Felelős kiadó: Prof. Dr. Fodor János rektor

Felelős szerkesztő: Dr. Györök György

Óbudai Egyetem

1034 Budapest Bécsi út 96/b

http://uni-obuda.hu

Nyomdai előkészítés: Dr. Hajnal Éva

Nyomdai munkálatok: Copystore Nyomdaipari Kft.

Printed in Hungary

Tartalomjegyzék

Előszó

Az egyetemek elsődleges feladata, hogy szakterületeiken diplomásokat képezzenek és kutatásokat végezzenek. Sok egyetemi oktató és kutató azonban joggal hivatottnak érzi magát arra, hogy részt vállaljon szakterületén a magas szintű – régies kifejezéssel élve a „művelt nagyközönségnek" szóló – tudományos ismeretterjesztésben is. Számos példát lehetne erre felhozni, így Bugát Pál orvosprofesszort, aki a Tudományos Ismeretterjesztő Társulat első elődszervezetének, a Magyar Természettudományi Társulatnak (1841.) kezdeményezője és első elnöke volt.

Sokunk példaképének, Simonyi Károly professzornak valószínűleg utolérhetetlen teljesítménye „A fizika kultúrtörténete" című könyve. Fia, Charles Simonyi adományából jött létre 1995-ben az Oxfordi Egyetemen a Simonyi Professorship Chair for the Public Understanding of Science nevű tudománynépszerűsítő tanszék.

Az Óbudai Egyetem Alba Regia Műszaki Kara részt kíván venni Székesfehérvár szellemi életében. Ennek egyik megvalósulási formája a Garai Géza Szabadegyetem, amelynek keretében egyetemünk oktatói, valamint az egyetemmel szoros kapcsolatban álló szakemberek tartanak magas szintű ismeretterjesztő előadásokat.

Garai Géza a Videoton egykori kiemelkedő fejlesztőmérnöke, majd fejlesztési vezetője, aki többünknek nem csupán főnöke, hanem mestere is volt. Bár ismeretterjesztő előadásokat nem tartott, széles körű tudását rendszeresen megosztotta velünk, tudományos ismeretterjesztést végző kollégáit elismerte, támogatta.

Az előadássorozat évek óta dédelgetett terve egy TÁMOP pályázat kapcsán vált valóra két évvel ezelőtt, az akkor még Alba Regia Egyetemi Központban. A pályázat tette lehetővé e könyvecske megjelentetését, amely az első két év előadásainak egy részét tartalmazza.

Az alábbiakban felsoroljuk az első két év összesen 12 előadását, amelyek mindegyikének a felvétele megtalálható a következő webhelyen: http://archive.galileowebcast.hu/.

- Dr. Tóth Mihály professor emeritus: Infotechnika az őskortól napjainkig
- Dr. Seebauer Márta egyetemi docens: Intelligens otthonok
- Dr. Györök György egyetemi docens: Processzorok mindenütt
- Dr. Fűrész Gábor műszerfejlesztő csillagász: Modern eszközök és módszerek a csillagászatban
- Dr. Budavári Tamás fizikus: Távoli galaxisokkal a Nobel-díj közelében
- Dr. Sima Dezső professor emeritus: A népvándorlás kora az informatikában?
- dr. Hudoba György főiskolai docens: Bolygószonda modell építése az Alba Regia Egyetemi Központban
- Dr. Ujvári Sándor adjunktus: Magfizika magyar szemmel
- Dr. Horváth Árpád adjunktus: A részecskefizika rejtelmei
- Dr. Lakner József c. egyetemi tanár: A múltban gyökerező jelen (200 éve született Ybl Miklós)
- Dr. Hajnal Éva egyetemi docens: Édesvizek ökológiájáról egy informatikus szemével
- dr. Nagy Rezső főiskolai docens: Távcső helyett számítógép?

Az előadássorozat természetesen a pályázat lezárultával is folytatódik, immár az Alba Regia Műszaki Karon. Az előadók és a témák köre is bővülni fog, mivel a karnak része lett a Geoinformatikai Intézet, amely (más keretek között) több mint fél évszázada működik városunkban.

Az ICT és az adatbiztonság

Az összegyűjtött tudás (információ) és a kommunikáció szerepe az emberi faj fejlődésében és hangsúlyozott szerepük jelen korunkban.

Dr.habil. Tóth Mihály, prof emeritus
Óbudai Egyetem, Alba Regia Műszaki Kar (OE-AMK) Székesfehérvár,
toth.mihaly@arek.uni-obuda.hu

***Abstract*—Az információ fogalma és megosztása az emberi faj történeti fejlődésében. A kommunikáció és az írás kialakulása és fejlődése. A kumulált tudás mérföldkövei az elektronikus kommunikációig. A kommunikáció védelme. A titkosítások. A kriptorendszerek generációi. A titkosítási transzformációk és erősségük. A mai kriptorendszerek. Iterációs rendszerek. A nyíltkulcsú rendszerek és alkalmazásaik. Az e-aláírás. Hibrid rendszerek. Néhány szó az alkalmazásokról.**

I. Bevezetés: Az ICT fogalmai

A tapasztalattal vagy tanulással megszerzett *tudás* és annak befogadása, megosztása, továbbadása a legelső, még történelem előttinek nevezett emberektől kezdve az Embernek, mint társas és gondolkodó lénynek mindig is veleszületett, természetes adottsága volt. A Föld minden élőlénye közül csakis az Ember rendelkezik ezzel a kivételes tulajdonsággal, amely igen nagy szerepet játszott és játszik ma is az emberiség mindenféle fejlődésében. Tulajdonképpen e fejlődés motorja ez az egyéni és a közösségi tudás, amelynek a ma használt gyűjtőfogalma az *információ*.

Az információ rendkívül tágan értelmezett fogalom és nagyon sokféle megjelenési formája van. Éppen ezért nincs is átfogóan érvényes és pontos definíciója. Erre ez az írás sem tesz kísérletet. Helyette a kifejezése és fejlődése néhány mérföldkövét villantja fel, mutatja be a tízezer évesnél is régebbi barlangrajzoktól az írott információkon keresztül a mai, elektronikus formákig. Természetesen messze a teljesség igénye nélkül, önkényesen kiválasztva a „mérföldköveket”.

Mindegyik ilyen „mérföldkővel” kapcsolatban megemlítünk néhány mennyiségi és minőségi jellemzőt, valamint a fejlődéssel együtt járó

problémákat is. Így a mai „információs forradalom" elképesztő mennyiségű információs kincsének a védelmével kapcsolatos néhány dolgot is.

Az Ember, mint olyan, vele született tulajdonságaként említettük az információ befogadásának és *megosztásának* a problémakörét is. Ma erre a *kommunikáció* megnevezést használjuk, ami ugyanannyira tág fogalom, mint maga az információ.

A problémakörhöz tartozik az információ *tárolásának* a kérdése is, amire technikai szempontból egyáltalán nincs igazán megbízhatónak nyilvánítható megoldás.

Mind a kommunikáció, mind a vele szorosan összefüggő tárolás és egyéb járulékos problémák (mint pl. az információ védelme, stb.) az információ kezelésének/feldolgozásának *technikai* kérdése.

Mindezekre együttesen manapság az információ (I) és kommunikáció (C) technikája (T) vagy technológiájaként szoktunk hivatkozni és az ICT rövidítést használjuk.

II. A KEZDETEKTŐL AZ ÍRÁSOKIG

Az utolsó jégkorszak utolsó harmadában, kb. 30 ezer évvel ezelőtt Afrikából az európai kontinensre vándorolt a Homo Sapiens Sapiens: Ádám népe.

Az Ibériai félsziget déli tengerpartjain felfedezett, legalább 10-20 ezer éves barlangok rajzai [1] úgy is értelmezhetők, hogy az azokban lakó emberek – a barlangi festmények segítségével – már igyekeztek átadni más embereknek ill. csoportoknak bizonyos ismereteket és kultuszokat. (Ha nem tudták megmondani valakinek pl. a bölény nevét, *megmutatták* neki a rajzon, hogy miről van szó.)

A barlangrajzok kutatóinak többsége azzal ért egyet, hogy ezek a rajzok és festmények kultikus célokat (is) szolgáltak.

Az egymástól néhányszor tíz kilométerre fekvő barlangokban talált, azonos megmunkálási módszerrel készült kőszerszámokból arra lehet következtetni, hogy az ilyen szerszámok készítési technikáját is átadták egymásnak valahogyan, tehát az ősök egymástól távolabb élő csoportjai között is volt valamilyen kommunikáció.

Mind a fellelt vadász-eszközök, mind a barlangrajzok arra utalnak, hogy nagy vadakra is vadásztak, ami csakis csoportosan, előre *megbeszélt* taktikával volt lehetséges.

Szükségképpen volt tehát az együtt élő csoportok között szóbeli kommunikáció. Az erre való képességük lehetőségére (t.i. a beszéd képességére) mutatnak az emberi csont-leletek bizonyos anatómiai jellegzetességei is. (A neandervölgyi ember állítólag nem volt képes szóbeli kommunikációra, pedig nagyobb agytérfogata volt, mint a homo sapiensnek.) Az ilyen kommunikáció segíthette a beszélt nyelv kifejlődését is.

Az írástörténet kutatói feltételezik, hogy a piktogramok (képi szimbólumok) sokkal előbb jöttek létre, mint a mai értelemben írásnak nevezhető információrögzítés. Ilyen, a beszélt nyelvhez nem kötött piktogramokat ma is széles körben használunk. (Pl. a KRESZ táblák, menekülési utat jelző táblák, dohányzás vagy mobil telefon használatát tiltó táblák, stb.) Ezeket az egy kultúrkörhöz tartozó, de a legkülönbözőbb nyelveken beszélő emberek mindegyike megérti, de mindegyike másképp nevezi. Bizonyos szempontból ilyen piktografikus jeleknek tekinthetők az ú.n. arab számokat használók körében a számjegyeink, vagy egyes írásjelek, matematikai jelek. Ilyenek pl. a vallásokhoz kötődő szakrális szimbólumok, a heraldika címerei és sok más is. Mindez arra mutat, hogy a piktogramok fogalmak, megnevezések, figyelmeztetések stb. jelzésére nagyon is alkalmasnak bizonyultak már évezredekkel ezelőtt is, de beszéd leírására, vagy történetek „elbeszélésére” azért nem voltak alkalmasak.

1. ábra
Egy kb. öt és fél évezreddel ezelőtti ún. protosumér piktogram, amely vélelmezhetően valamely akkor tisztelt isten szimbóluma.[2]

Érdemes megjegyezni, hogy a mai tudásunk szerint egyáltalán nincs értelme i.e. 3000 évvel ezelőtti írásokról (és pláne nem betűírásokról) beszélni, jóllehet a neten találhatók ilyen hivatkozások.

A piktogramok ókori használatát szó-írásnak is szokták nevezni, bár nem valamely nyelvhez köthető szavakat, hanem azok szemantikai (jelentés) tartalmát rögzítették.

Az i.e. harmadik évezred közepére teszik azt az igen jelentős lépést, hogy a képírásból egy nyelvhez (az ú.n. protosumérhoz) kapcsolódó írás alakult ki Mezopotámiában. Ez a sumért megelőző nyelv ma nem ismert, de az tudható, hogy az „írásjeleit" vízszintes sorokban, balról jobb felé írták.

Az íróeszköz egy háromszög keresztmetszetű pálca volt, amellyel puha agyagtáblába nyomtak bele kombinált írásjeleket. A korábbi piktogramok szemantikai tartalmát az írásjelek fonetikai tartalma váltotta fel, bár egyes összetett jelek, akár 20-30 ékből álló ú.n. ligatúrák, megnevezéseket vagy szemantikai tartalmat is megőriztek. Az „egyszerű" ékírásos jelek is 5-10 ékből álltak. Nem szabad abba a tévedésbe esni, hogy az ékírást a mai értelemben vett betűírásnak véljük. Közelebb áll talán a szótag-írásokhoz, de ennek a cikknek nem célja az írástörténet részletezése.

2. ábra
A sumér SAG (=fej) ékírásos jel kialakulása egy piktogramból és mintegy 2 évezredes továbbfejlődése (Borger nr. 184, U+12295).[11]

Mindazonáltal nagyon is jelentős kultúrtörténeti mérföldkövek voltak, amikor egy-egy, ma már ismeretlen nyelvhez kötődő, „egzotikus" írást sikerült a régészeti leletekből megfejteni.

Pl. a sumér ékírás és nyelv (Rawlingson és Rónai Jácint), az ókori egyiptomi írások (Champollion) vagy a krétai lineáris B írás és a hozzá tartozó nyelv (akháj nyelv Michael Ventris) megfejtése.

Az agyag „táblákon" rögzített információ megfejtésének a nehézségére álljon itt egy példa (3. ábra):

3. ábra
Egy i.e 2400-ból származó ékírásos levél,[3]

A KÖNYVTÁRAK

Az utolsó jégkorszak utolsó harmadából, kb. 30 ezer évvel ezelőttről leltek fel egyáltalán értelmezhető valamilyen rögzített jelzéseket, amelyek az Embernek voltak tulajdoníthatók. A fentiekben leírtak lényege a szempontunkból az, hogy az ékírás és az agyagtáblák igen alkalmasak voltak mindenféle információ – az adófizetési leltárakon kívül akár történeti leírások vagy legendák – leírására és az agyagtáblák kiszárítása, vagy kiégetése után ezredévekre *megőrizték ezeket az információkat*.

Nagy kérdés hogy a mai információ-rögzítési technikák (papír, film és hangrögzítési anyagok, stb.) élettartama vajon mennyi lehet.

Az információ rögzítésének ez az agyagtáblás módja olyan hatékonynak bizonyult, hogy Asszurbanipal ninivei, ókori „könyvtárának" a régészeti feltárásakor mintegy 22 ezer agyagtáblát találtak. Más régészeti feltárásokkal együtt ma mintegy 400 ezer ókori agyagtábla megfejtésével foglalkoznak filológusok, paleo-lingvisztikusok, archeológusok és más szaktudósok.

Ez által a megszerzett és ***összegyűjtött tudás tértől és időtől függetlenül megoszthatóvá vált***.

Ez rendkívül jelentős fejlődési lépés volt az emberiség kumulált tudása, azaz az információ kezelési technikájának a kialakulásában.

4. ábra
A XX. század végén újra felépített alexandriai könyvtár [16]

Tulajdonképpen nagyon érdekes lenne tudni, hogy vajon mi indította az ókori Ptolemaios dinasztia első, Nagy Sándor által „kinevezett" egyiptomi uralkodóját (i.e. 367-283) arra, hogy az akkori Egyiptom Nagy Sándor által alapított fővárosában, Alexandriában összegyűjtse az ókori világ akkoriban fellelhető *valamennyi* tudását. Erre alapította meg a híres ókori, alexandriai könyvtárat, amelyben mintegy 700 ezer papirusz tekercset gyűjtött össze (ógörög nyelvre lefordítva) és amely az első olyan, könyvtárnak nevezhető gyűjtemény volt, amelyben *katalogizálták* is a dokumentumokat.

Jóllehet többször is elpusztították ennek a könyvtárnak a tartalmát, mindig is újraéledt és máig is neves ókori, görög tudósoknak nyújtott otthont. (Csak néhány, ott munkálkodó, ismert ókori tudós nevét megemlítve: Demetriosz, Erasztothenesz, Arisztarkhosz, Diofantosz.)

Legutóbb az egyiptomi Hoszni Mubarak elnöksége alatt, nemzetközi összefogással és segítséggel 1995-től 2002-ig építették újjá. Nem egészen az ókori könyvtár helyén, mert azt a helyet ma már tenger borítja, de nem messze attól. [14]

Az ókori alexandriai könyvtár minden esetre igen jelentős mérföldkő az emberiség kultúrtörténetében.

Érdemes meggondolni, hogy maga a létrehozás indítéka is az Ember eredetétől fogva meglévő (originális) tulajdonságának a következménye.

A történeti továbblépés előtt visszatérve még egy kicsit az információ összegyűjtésének és megosztásának történelmi mérföldköveire, feltétlenül meg kell említeni a cordobai (mór) könyvtárat, amely az európai középkor vitathatatlanul legnagyobb tudásanyagát gyűjtötte össze.

5.ábra
Részlet az új alexandriai könyvtár belső teréből (Saját fotó)

A mórok VIII. századi, európai hódítását követően az andalúziai Cordóba lett az (európai) iszlám kalifátus fővárosa. A X. században ez volt a világ legnépesebb városa. (Ma a lakóinak száma alig több 300 ezernél.)

A X. századtól a mórok egyetemet alapítottak és létrehozták az akkori Európa legfejlettebb kulturális központját, valamint a cordóbai könyvtárat, amely az első ezredforduló után a Világ legnagyobb könyvtára volt. Az ókori filozófusok műveit arab nyelvre fordították, és később, az európai reneszánsz idején nem az eredeti, görög forrásokat, hanem a sokkal inkább érthető, cordobai arab forrásokat fordították vissza az európai nyelvekre. Csak becsléseket lehet tenni arra, hogy mekkora is volt Cordóbában a mórok által alapított könyvtár információs anyaga. A fénykorában állítólag legalább félmillió, de lehet, hogy egymillió iratot tároltak.

Összehasonlításul meg kell jegyezni, hogy a középkori szerzetesrendek regulái szerint a szerzeteseknek kötelező elfoglaltságuk volt a kódexek másolása, de a kolostorokban és más egyházi centrumokban a cordóbainál több nagyságrenddel kevesebb írott anyagot tároltak.

Adatunk van arra például, hogy a pannonhalmi apátságban 1093-ban 80 kötetben összesen kb. 200 írás másolatát tárolták. A kézírásos másolás tehát egyáltalán nem volt hatékony és különben is csak az egyházi szövegekre terjedt ki. Az ókori filozófusok hagyatékára és a nem keresztény történeti írásokra egyáltalán nem. Minőségi (és mennyiségi) változást hozott a könyvnyomtatás feltalálása és ezáltal az információ megosztás nagyságrendi változása a XV. században. Ezt a változást ma Gutenberg galaxis néven emlegetik, és természetesen mérföldkőnek számít ez is a diszkussziómban. [5]

6. ábra
A kumulált tudás a középkorban [17] és [18]

A Gutenberg galaxis utáni (azaz az elektronikus média: TV, internet, rádió, elektronikus „könyvek", stb.) világgal szembeállítják a nyomtatott médiumokat és az utóbbi válságáról beszélnek, írnak. [5]

A kérdés nem eldöntött és kihat az oktatási rendszerünkre is. Mindenesetre a könyvnyomtatás feltalálása és elterjedése nagyságrendi változást hozott a XV. században a ma információ technikának nevezett fejlődésben is, tehát ez is mérföldkőnek számít.

Manapság a világ nagy könyvtáraiban – nem „csak" nyomtatott, hanem más hordozókon is – tárolt információ mennyiségét 10^{19} – 10^{20} byte mennyiségűnek becsülik. (Ez gyakorlatilag ugyanennyi karakterrel ekvivalens.)

Összehasonlításul vegyük figyelembe a következő (nagyon durva) közelítést:

Egy A4-es oldalon 25 sorral és soronként 50 karakterrel számolva 1251 byte-nyi információ van. 1000 oldalas könyvekkel számolva egy-egy könyvben $1{,}251\times10^6$ byte mennyiségű információ található. Vagyis a 10^{19} byte mennyiségű információ valamivel kevesebb, mint 10^{13} ilyen, egyenként 1000 oldalas könyvben „férne el", más szóval ez 10×milliószor millió ilyen, egyenként 1000 oldalas kötetet jelentene. Elképzelni sem lehet.

Ezt az összehasonlító szemléltetést tovább fejlesztve feltételezhetnénk, hogy egy-egy ilyen 1000 oldalas kötet pl. 5 cm vastag és kiszámolhatnánk, hogy hány kilométer hosszú polcra lenne szükség valamennyi elhelyezésére és mekkora „könyvtárban" férne el mindez. Ehelyett fontoljuk meg inkább azt, hogy vajon érdemes-e egyáltalán ennyi információt tárolni, hogyan is lehet e tömegben eligazodni és vajon hogyan lehetne a nyomtatott formánál sokkal koncentráltabb módon tárolni ekkora információ-mennyiséget.

E három kérdés közül az első kettő napjaink még nem igazán megoldott problémája. A harmadik, vagyis az emberiség eddig elért, elképesztően nagy tudásmennyiségének a koncentrált tárolására már léteznek folyamatban lévő megoldások:

A könyvtárakban eleddig összegyűjtött tudás-mennyiség digitalizálásáról, elektronikus tárolásáról és az interneten való hozzáférhetőségéről van szó. Ez az ICT mérföldköveinek napjainkra tehető eseménye, amely nem nevezhető állomásnak, mert folyamatában létezik és itt csak felvillantani kívánjuk.

A következő képen az USA Washingtonban lévő Kongresszusi könyvtárának a fő olvasóterme látható. Az 1800-ban alapított könyvtár katalogizált könyv állománya ma meghaladja a 30 millió tételt

Nem is számolva a kéziratokat, újságokat, okiratokat, hang és kép anyagokat, stb.

Ezekből mára már több petabájtnyi anyagot digitalizáltak.

Az interneten hozzáférhető, digitalizált könyvtári anyag létezik Magyarországon is a Magyar Elektronikus Könyvtár (MEK) formájában, de létezik nagyon sok ú.n. hangos könyv és sok más formátumú információ is, mint pl. internetes folyóiratok. Felsorolni sem lehet mindet.

7. ábra
Az USA kongresszusi könyvtárának fő olvasóterme [19].

Ezek az információkszolgáltatókon keresztül érhetők el és esetenként csak díjfizetés ellenében. Egyébként általában fizetős maga az internetes szolgáltatás is, de léteznek olyan országok is, ahol ez ingyenes, pontosabban az állam finanszírozza.

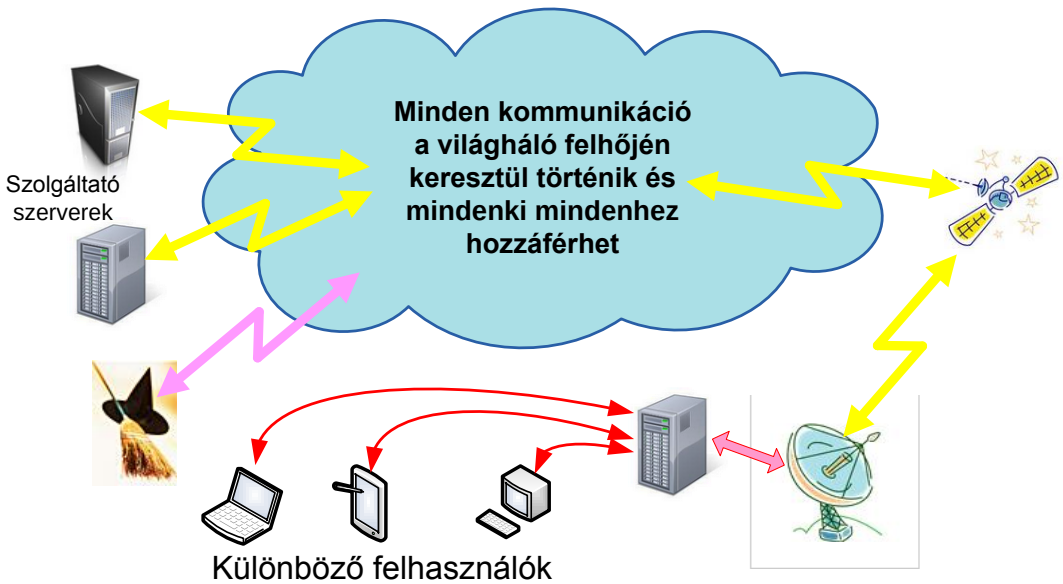
III. A "FELHŐ" ÉS AZ INFORMÁCIÓ SZOLGÁLTATÓK

Az információ szolgáltatók és a felhasználók bonyolult kapcsolatrendszerét egy ú.n. *felhő* reprezentálja.

Valójában ma már nem nagyon érdemes drága felhasználói szoftvereket egyedi felhasználói számítógépekre telepíteni (mint amilyen pl. egy képeditor vagy egy matematikai szimulációs program), hanem az ilyen igényeket is a felhőn keresztül (fizetős) szolgáltatásként veheti igénybe a felhasználó.

No és az internetes felhőn keresztül tölthet le saját használatra pl. zenéket vagy filmeket – egyre inkább fizetős szolgáltatásokként.

A felhő gazdaságossága és előnyei mellett a teljes nyitottsága hátrányt is jelent, mert rajta keresztül a rosszindulatú „fekete kalaposok" kéretlenül hozzáférhetnek a kommunikációnkhoz, lehallgathatják és/vagy módosíthatják a letöltött információinkat és megtévesztő információkat is küldhetnek.

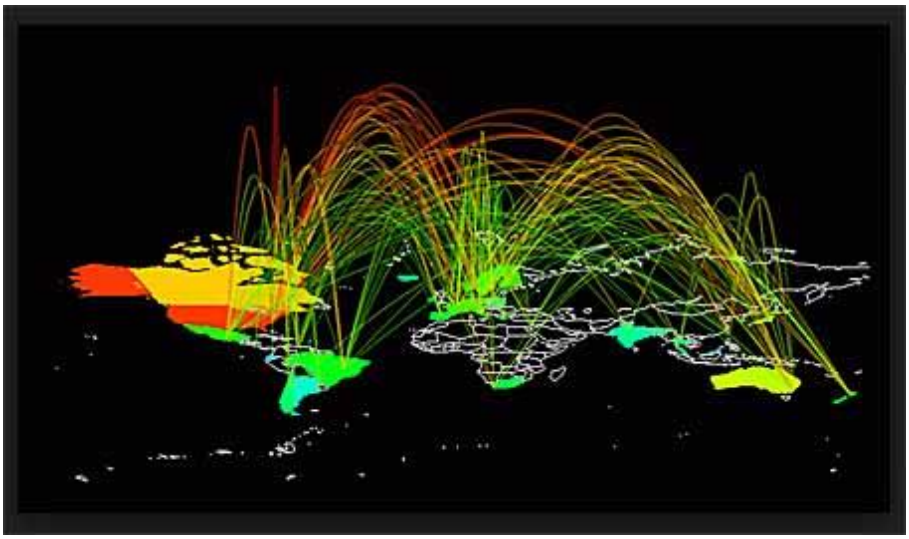


8. ábra
A felhő fogalom szemléltetése

IV. A FORGALOM

Már a bevezetőben említettük, hogy az információ megosztása, vagyis a kommunikáció milyen lényeges szerepet játszott a kezdetektől fogva egyének és csoportok között, és manapság ide sorolható az intézmények és eszközök *információ forgalma* is. Mindez a világhálós felhőn keresztül bonyolódik. A következő ábra azt szemlélteti, hogy a Föld egyes pontjai között milyen a kapcsolatok megoszlása.

Az internetes adatforgalom volumenét jól reprezentálja az USA gerinchálózatának a statisztikája.



9. ábra
Információ megosztás a Föld felszíni pontjai között [20]

Az éppen aktuális forgalom helyett azonban érdekesebb annak a fejlődését, növekedését vizsgálni.

Az internet forgalomra egészen 1990-ig visszamenőleg találhatunk adatokat, de a mobil (telefonos) forgalomra gyakorlatilag csak 2005-től. A következő táblázatban az USA gerinchálózatainak havi forgalmi adatmennyisége van megadva petabájtokban (1 PB = 10^{15} bájt.) [8]

Global Internet traffic by year

Year	IP Traffic (PB/month)	Mobile Internet Traffic (PB/month)
2005	2,426	0.9
2006	3,992	4
2007	6,430	15
2008	9,927	38
2009	14,414	92
2010	20,197	256
2011	27,483	597

V. AZ E-ALKALMAZÁSOK ALAPPILLÉREI

Az internetes kommunikációt használó elektronikus alkalmazásoknak ma már rendkívül nagy választéka létezik az üzenetváltásoktól kezdve az internetes műsor- vagy hírközlésen keresztül az elektronikus bankolásig és kereskedelemig.

Ezek az alkalmazások három alappilléren nyugodnak:

Az egyik az ilyen alkalmazások kommunikációjának az eljárásrendje. Ezt *protokollnak* nevezik, amelybe nem csak technikai kérdések tartoznak bele, hanem pl. a kommunikációban résztvevők megbízható azonosítása, a továbbítás közbeni illetéktelen beavatkozásnak az észlelése, az interneten kötött megállapodások letagadhatatlansága, biztonságos elektronikus aláírása, ú.n. időbélyegzővel való ellátása és hasonlók.

Egy másik pillér, amit külön ki kell emelni az „érzékeny” *adatok titkosítása*, és ily módon való *védelme*. Az előző pillér kapcsán említett néhány, nem kifejezetten technikai dolog is kapcsolódik ehhez. Ez az egész speciális témakör ma már annyira bonyolult és annyi járulékos vonzata van, továbbá annyi igen fontos alkalmazása, hogy külön pillérnek lehet tekinteni.

A harmadik, vagyis a *törvényi háttér* tulajdonképpen a társadalmi környezethez illeszti az adott e-alkalmazást (és nem is technikai ügy).

A három alappillérből tehát kettő az adott alkalmazást illeszti a technológiához, nevezetesen

a kriptográfiai technológiához és

a **kommunikációs folyamatokhoz**

Más szóval a technológiát szabványok kontrollálják a társadalmi-gazdasági környezethez való illeszkedést pedig a jogi eszközök.

A továbbiakban a titkosítással kapcsolatos kérdésekkel foglalkozunk.

VI. A TITKOSÍTÁSOK ELVEIRŐL

Titkosításkor az ún. *nyílt szöveget* (amit az angol Plaintext elvezés alapján P-vel jelölnek) egy titkosítási, vagy – más néven – kódolási eljárással, csak a beavatottak által visszafejthető ú.n. *kriptogrammá* (C) alakítják. Ezt az eljárást siffrírozásnak is nevezték régebben és a végrehajtásához valamilyen *kulcsra* van szükség. A titkosítások matematikai modelljeiben ennek az átalakításnak *transzformáció* a neve, de matematikai értelemben egy egyértelmű leképezést, azaz *függvényt* jelent. A kriptográfiában alkalmazott függvények rendszerint nem adhatók meg a matematikai analízisből ismert képletekkel, hanem inkább csak táblázatokkal vagy a transzformáció eljárási szabályainak másfajta (pl. valamilyen metanyelvi, és/vagy a programozásban szokásos) leírásával.

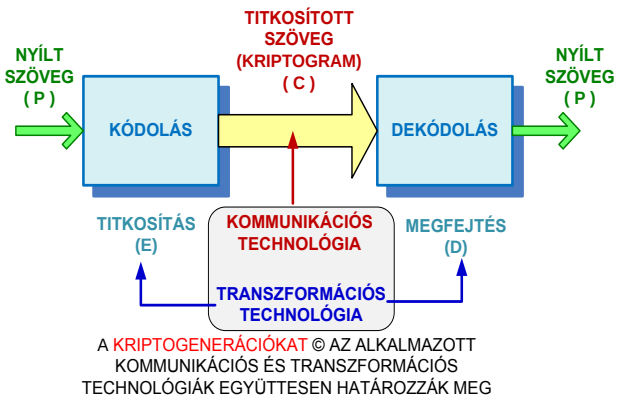
A C kriptogramot valamilyen nyílt, bárki által hozzáférhető információs csatornán továbbítják a címzetthez, aki vagy ami aztán a kódolásnál alkalmazott transzformáció inverzének és a kódolási kulcsnak a segítségével képes visszafejteni, azaz dekódolni a C kriptogramot és megismerni az eredeti nyílt szöveget.

A kódolási és a dekódolási transzformációk a kezdetektől az ún. negyedik kriptogenerációig bezárólag kölcsönösen egyértelmű leképezéseket végrehajtó inverz függvények.

Itt jegyezzük meg, hogy az ú.n. kripto-generációk fogalmát a korábban használt számítógép generációk fogalmának analógiájaként e cikk szerzője vezette be. Előnye, hogy segít „rendet teremteni” és áttekinteni a titkosítási módszereket és azok fejlődését és e témakör oktatásában is hasznos lehet.

A kripto-generációkat a transzformációk jellege és az alkalmazott kommunikációs módszerek együttesen határozzák meg.

A modern, számítógépeket és bonyolult transzformációkat alkalmazó kriptorendszerek a 4. és az 5. generációs titkosítások.

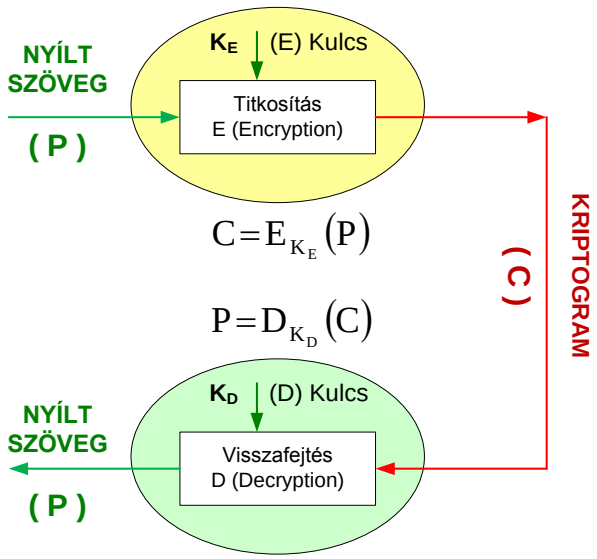


10. ábra
A kriptorendszerek generációinak meghatározásához.

C.E.Shannon (MIT) 1948-ban kétrészes nagy cikkével megalapozta az információelmélet tudományát, és egy évvel később ugyancsak ő a titkosítás elvi alapjait is.

Két alapelvet említett: a *helyettesítést* és a *keverést* (ennél azért általánosabban megfogalmazva, konfúziónak és diffúziónak nevezve, mint titkosító átalakításokat).

A cél az, hogy az érthető nyílt szöveget minél inkább véletlenszerűnek látszó „zagyvasággá" alakítsuk, de úgy, hogy a kulcs ismeretében azért egyértelműen megfejthető legyen. Erre a célra az idők folyamán egyre bonyolultabb transzformációkat találtak ki, de ezeknek azért az adott kor technikájával kezelhetőeknek kellett lenniük és elfogadhatóan gyorsaknak is. Már elég régen alkalmaztak erre egyszerű eszközöktől kezdve bonyolult (pl. elektro-mechanikus) gépeket, de a számítógépek



11. ábra
A kriptotranszformáció-pár modellje

megjelenésével és e célra való alkalmazásával a transzformációk bonyolultsága is rendkívül megnövekedett. Ez jellemző a 4. és az 5. kriptogenerációkra és újabb változataikra. Az utóbbiak szinte mindegyikében alkalmaznak nemlineáris transzformációkat, ú.n. láncolást és még újabban a matematikai káosz elméletet is igyekeznek bevetni.

A 11. ábra felső fele azt mutatja meg, hogy egy P nyílt szövegből egy E titkosító transzformáció és egy K_E titkosító kulcs segítségével előállítunk egy beavatatlanok számára reményeink szerint nem megfejthető C titkosított szöveget.

Az egész dolognak, persze, csak akkor van gyakorlati értelme, ha a dolog a beavatott számára visszafejthető. Ehhez, persze, ismerni kell a D visszafejtő transzformációt és a hozzá tartozó K_D kulcsot.

Az első négy kriptogeneráció titkosításaira az volt a jellemző, hogy azonos kulcs volt mind az üzenet küldője, mind a címzettje birtokában, amit persze titokban kellett tartaniuk. A titkosító és a visszafejtő transzformációk pedig egymás inverzei voltak. (Lehet ugyan kivételt említeni az ú.n. tükörszimmetrikus transzformációk körében, de itt nincs hely a részletekre kitérni.). Ezeket nevezzük *szimmetrikus* titkosító rendszereknek (a kulcsok azonossága miatt). Képletekben megfogalmazva:

$$K_E = K_D; \text{ és } D = 1/E = E^{-1}$$

A számítógépek elterjedésével a korábbiaknál *sokkal* bonyolultabb transzformációk számításait is elég gyorsan el lehet végezni és az 1970-es évek közepén Diffie, Hellman és Merkle publikálták egy olyan rendszer elvét, amelyben az E titkosító és a D visszafejtő transzformációk azonosak voltak és a K_E valamint a K_D (bonyolult módon összetartozó) kulcsok voltak egymás inverzei. Matematikailag tehát:

$$K_E = K_D^{-1}; \text{és } D = E$$

Ezeket a rendszereket nevezzük *aszimmetrikus* titkosító rendszereknek, de nevezik nyíltkulcsú rendszereknek is, mert egy ilyen kulcspár két kulcsa közül az egyiket nyilvánossá is lehet tenni és ez sok olyan alkalmazásra ad lehetőséget, amiről korábban a titkos és bizalmas kommunikáció körében szó sem lehetett. (E-kereskedelem, banking, hitelesített e-aláírás, stb.)

A 11. ábrára tekintve, persze, még másfajta elveken működő rendszerek is létrehozhatók, de a szükséges és elegendő biztonságot nyújtó (és amellett elég gyors) rendszerek túlbonyolításának nem látszanak gyakorlati hasznai. Az információ biztonság növelése természetesen

folytonosan fennálló igény, de ma ezt másutt, más (pl. fizikai) módszerek fejlesztésével valósítják meg.

Néhány lényeges következtetetést összefoglalva:

- Az első négy generáció kriptorendszerei kivétel nélkül mind szimmetrikus (titkos kulcsos) rendszerek.
- Esetenként többszörös transzformációkkal.
- Nem közömbös, hogy a nyílt szöveget nem túl nagy szövegegységenként (pl. betűnként), vagy
- nagyobb szövegegységenként (ú.n. blokkonként) titkosítják-e.
- A 4. és az 5. generáció rendszerei mind blokkos rendszerek. Minimum 128, de akár 2048 bites blokkokkal és ugyanilyen hosszú kulcsokkal.
- A számítás-igény a kulcshosszal nő.

Erről a következő pontban bővebben.

VII. A TITKOSÍTÁSOK ERŐSSÉGE

Jóllehet nem csak a titkosító módszerek elveivel kapcsolatban, de minden esetre azok hatására is megjelent a modern matematikában a matematikai bonyolultság-elmélet. amely – többek között – azzal is foglalkozik, hogy valamilyen problémáról bebizonyítsa, hogy az elvileg sem kiszámítható, de itt és most nem erről van szó, hanem a *gyakorlati kiszámíthatatlanságról*. Még ha található is egy titkosítási módszerhez ú.n. *feltörési algoritmus*, egyáltalán nem mindegy, hogy az a gyakorlatilag rendelkezésre álló számítási kapacitás és időtartam esetében alkalmazható-e. Ezért létezik definició arra, hogy mikor nevezhetünk egy titkosítási módszert (kriptorendszert) erősnek.

Könnyen belátható, hogy ha a titkosítási (és a visszafejtési) módszer ismert, akkor a titkosítás biztonsága a kulcsoktól függ. Az is belátható, hogy elvileg bármilyen kriptorendszer feltörhető úgy, hogy valamennyi lehetséges kulcsot kipróbáljuk. Ha nagyon sok kulcs lehetséges, akkor a feltörés gyakorlatilag lehetetlen. Ezt a kulcs-próbálgatásos módszert nevezik *a nyers erő* (brute force) *módszerének*.

ERŐS az a KRIPTORENDSZER, amelynek a feltörésére NEM ISMERT OLYAN ALGORITMUS, amellyel gyorsabban fel lehetne törni, mint a nyers erő módszerével.

Egy kriptorendszer *erőssége* tehát a mondottak értelmében függ attól, hogy hányféle kulcsa lehetséges.

A kulcsok hosszát ma bitekben szokás megadni. Pl. a 128 bites bináris számokból összesen 2^{128} féle van a csupa nullástól a csupa 1-es bitből álló számokig.

Mivel $2^{10} \approx 1000$, vagyis $\approx 10^3$, ezért $2^{128} \approx (10^3)^{13}$ vagyis 10^{39}. Ha valamivel kevesebb, mint 1 nanoszekundumonként ($= 10^{-9}$ s) lennénk képesek egy-egy kulcsot kipróbálni, akkor a 86400 másodpercből álló 24 órás nap alatt, mondjuk 100 ezer (10^5) kulcsot), akkor „csak” $10^{39-9-5} \approx 10^{24}$ napra lenne szükség az összes lehetséges kulcs kipróbálására. Lehetne még tovább „csökkenteni” a szükséges időt, ha feltételeznénk, hogy mondjuk 1 millió ($= 10^6$) ilyen gyors számítógép dolgozik szimultán a „próbálgatásokon”, de a dolog *gyakorlati* képtelenségét szemlélteti már a körülbelüli számítási eredmény is. Ami, persze, nem zárja ki azt, hogy véletlenül már a próbálgatások első 5 percében rábukkanhatunk a megoldó kulcsra.

Az összes lehetséges kulcsok számát egy adott kriptorendszerben *kulcstérnek*, pontosabban *a kulcstér számosságának* (halmazelméleti terminológiával a kulcshalmaz rangjának) nevezik.

Az Olvasót ennyi is meggyőzi talán, hogy a kriptorendszer biztonságát a kulcstér számossága határozza meg. Manapság a 128 bites kulcsok nem is számítanak nagyon erősnek. Titkos kulcsos (szimmetrikus) rendszerekben nem is használnak már 256 bitnél rövidebb, nyíltkulcsú rendszerekben pedig 1024 bites kulcsoknál rövidebb kulcsokat, de erre alább még visszatérünk. Azt talán bizonyítás, vagy számolgatásos becslések nélkül is be lehet látni, hogy minél hosszabb kulcsokkal történik egy titkosítás, annál nagyobb számítási kapacitást igényel. Mind időben, mind tárolási kapacitásban kifejezve.

A titkosító rendszerekben tehát meghatározó elv a biztonsági szempontból szükséges, de az elégségesnél nem hosszabb kulcsok alkalmazása.

Érdemes talán már itt megemlíteni, hogy egy biztonságos (titkosított) komplex kommunikációs rendszer leggyengébb pontja a rendszerben mindig aktív szerepet játszó *emberi óvatlanság* (Human factor) és nem a rendszer technikai része.

Összefoglalva az ebben a fejezetben elmondottak lényegét:

- Magát a titkosítási módszert nem érdemes titokban tartani,
- sőt: egyenesen szabványosítják.
- A titkosítás annál „erősebb", minél nagyobb az adott kriptorendszerben lehetséges kulcsok száma, a *kulcstér*.
- Elvileg mindig lehetséges lenne az összes kulcs kipróbálása. Ez a nyers erő (brute force) módszere.
- A kulcsok hosszát bitekben szokás megadni (több száz, vagy több ezer bites kulcsok is előfordulhatnak a mai gyakorlatban is).
- Ilyen nagyszámú kulcs végigpróbálása bármilyen reális idő alatt gyakorlatilag kivitelezhetetlen.

VIII. A MAI KRIPTORENDSZEREKRŐL

A következőkben nem célunk e rendszerek működésének a részletes ismertetése, csak valamilyen általános benyomást szeretnénk kelteni a bonyolultságukról. Megmutatva és ezzel sejtetve is a feltörési nehézségeiket, és (talán) a megbízhatóságukat is. Persze mindez relatív és a technika pillanatnyilag adott fejlettségétől függ.

A 4. generációs, titkos kulcsos kriptorendszerek ma is használt, persze mára már továbbfejlesztett változatai az ú.n. *iterációs rendszerek* amelyek archetípusa (mintegy: állatorvosi lova) az 1970-es évek közepére kifejlesztett és szabványosított Data Encryption Standard, a DES. Ez 25 évig igen jól szolgáló titkos kulcsos (azaz szimmetrikus) rendszer, amelyben már a legelején megjelent a később tovább fejlesztett szimmetrikus utódai szinte valamennyi lényeges tulajdonsága.

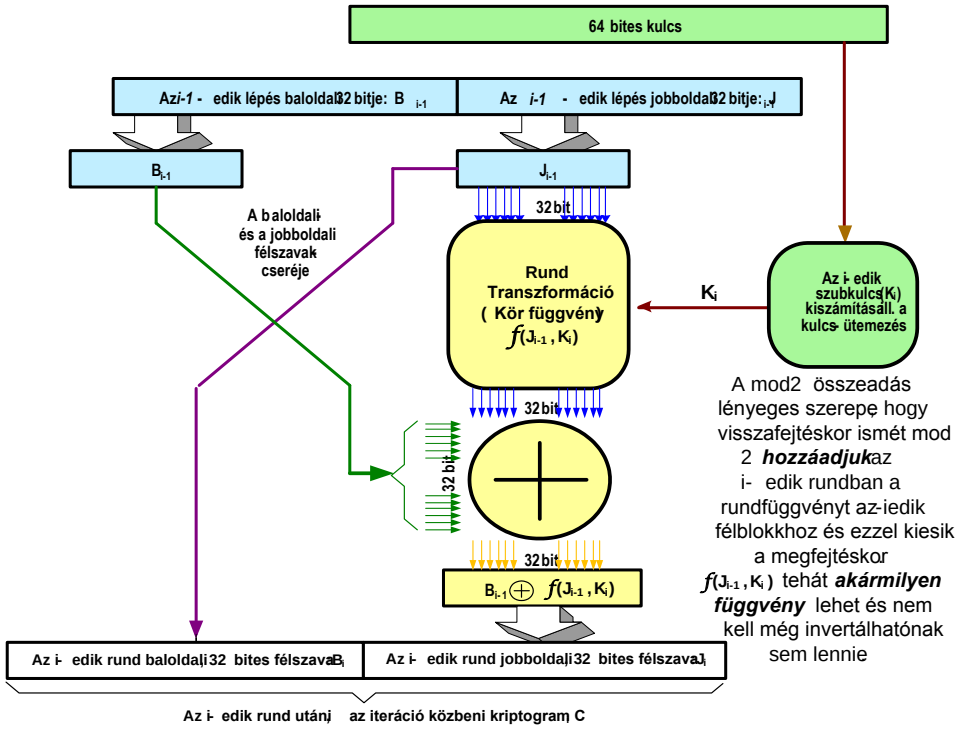
Aránylag egyszerű helyettesítő és keverő transzformációk egy többlépéses sorozatát hajtja végre, egy adott hosszúságú nyíltszöveg blokkon, majd egy másik kulccsal ezt megismétli és így tovább többször is.

Egy-egy ilyen titkosító lépés-sorozatot egy-egy *körnek* (rundnak) neveznek és minden körhöz más-más alkulcsot számolnak ki az aktuális fő-kulcsból.

A DES alapváltozata 64 bites nyíltszöveg blokkokkal és kulcsokkal működött és 16 kört hajtott végre minden egyes blokkon. Fontos, hogy

már a legelső, szabványosított változatának a körfüggvényébe is beépítettek egy nagyon nemlineáris transzformációt.

A bonyolultságát hivatott szemléltetni a következő ábra:



12. ábra

A DES egy körfüggvénye a szubkulcs ütemezéssel együtt.

A DES-hez hasonló blokkos és egy-egy körfüggvényt többször is végrehajtó rendszereket *iterációs (titkos kulcsos)* rendszereknek is nevezik. Jóllehet a DES és némileg bonyolított változatai 25 évig nagyon jól szolgáló erős rendszerek voltak, mára már a min. 128 bites blokkokkal (és kulccsal) dolgozó, belga fejlesztésű AES (Advanced Encryption Standard) nevű utódját szabványosították, de több más iterációs rendszert is kifejlesztettek.

Az iterációs kriptorendszereknek NEM továbbfejlesztett, hanem teljesen más elvű változatai a következőkben bemutatandó *nyíltkulcsú rendszerek*, amelyek célja és alkalmazása is némileg más .
Ez utóbbiakkal szemben az iterációs rendszerek gyorsabbak és kisebb számításigényűek.

A titkosító rendszerekhez elég könnyen lehet mindennapi analógiát találni, ha nem is mindig pontosan megfelelőt: Maga a titkosított üzenet megfeleltethető egy lakattal lezárt valaminek, amihez csak a lakathoz való kulcs birtokában tudunk hozzájutni.

Tehát a lakat (a titkosító transzformáció analógiája) és a kulcs szerepe kb. ugyanaz, mint a titkosításnál is.

Képzeljünk el most egy olyan lakatot, amelynek két, nem azonos kulcsa van és a lakat e kulcspár (bonyolult és nem kiszámítható módon összetartozó) két kulcsa közül bármelyik kulccsal bezárható ugyan, de ezután csakis a kulcspár másik kulcsával lehet kinyitni. Azzal nem, amellyel bezárták.

Szemléltesse ezt a következő ábra:

13. ábra.
A kétkulcsos (aszimmetrikus) kriptorendszerek lakat-analógiája.
A lakat ugyan bármelyik kulccsal bezárható, de ezután csakis a kulcspár másik tagjával nyitható ki.

Ennek a „rendszernek” van kriptográfiai analógiája:

Nevezetesen az aszimmetrikus (nyíltkulcsú) kriptorendszerek, amelyek ötletét 1976-ban publikálta Whitefield Diffie, Martin Hellman és Ralph Merkle Berkeleyben egy konferencián a New Directions in Cryptography c. cikkükben. Ez mérföldkő volt a titkosírások többezer éves történetében, mert előttük még soha senkinek nem jutott eszébe ez a kétkulcsos titkosítási elv. (Kivéve a brit GCHQ 1960-as titkos anyagát.)

Az első, gyakorlatban is használható és máig is legismertebb rendszert, az **RSA**-t a bostoni MIT három hallgatója: Ron **R**ivest, Ady **S**hamir, és Leon **A**dleman találták ki és tették közzé 1977-ben. Ez máig is használt, igen elterjedt rendszer.

A matematikai működési elvük bonyolultabb annál, hogysem egy ismeretterjesztő cikk keretében bemutassuk. E szempontból érdekesebbek a problémáik és a ma már igen elterjedtnek mondható alkalmazásaik.

A 4. generációs, szimmetrikus, egy (titkos) kulcsos rendszerek problémája a titkos kulcs eljuttatása a partnerhez. Nem lehet ugyanazt a kulcsot akármilyen hosszú ideig használni, mert az üzenetek feltörésében

érdekelt fél előbb, vagy utóbb rájön a kulcsra és attól kezdve hiába is titkosítják az üzeneteket. Ilyen problémát jelentett pl. a második világháborúban a német tengeralattjáróknak küldött üzenetek titkosítása ill. az üzeneteknek a Szövetségesek általi megfejtése, de más, nem „csak" katonai, hanem diplomáciai üzenetváltások problémái is megemlíthetők.

Ezeket a kulcsokkal és azok eljuttatásával, titokban tartásával kapcsolatos problémákat ma gyűjtőnéven a **kulcsmegosztás** problémáiként említjük.

Az 5. generációs, kétkulcsos kriptorendszerek kifejlesztését lényegében a kulcsmegosztási probléma égetően fontos megoldása indokolta és valóban sikerült is ezt megoldani. Itt kell megemlíteni, hogy Diffie és Hellman később, már az RSA rendszer bevezetése után kitalált egy olyan, róluk elnevezett kulcs-csere eljárást, amely távoli kommunikációs partnerek titkos kulcs-cseréjét nyitott kommunikációs csatornán keresztül is lehetővé teszi. *DH kulcs-csere algoritmusnak* nevezik és ténylegesen jelentős szerepe van a mai titkosított kommunikációban, de itt nem részletezzük.

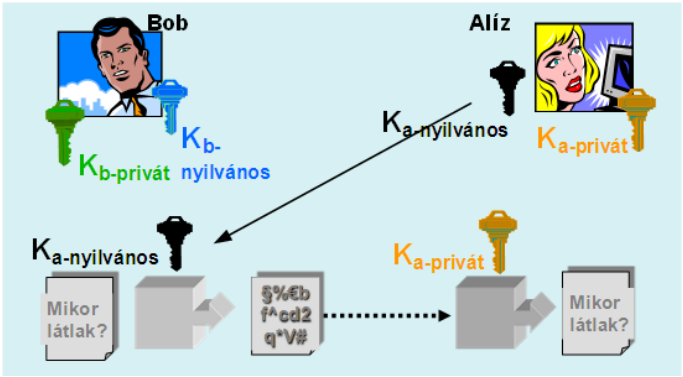
IX. A NYILTKULCSÚ RENDSZEREK ALKALMAZÁSAIRÓL

Az 5. generációs, aszimmetrikus kriptorendszerek kifejlesztését ugyan elsősorban a kulcsmegosztási problémák megoldása erőltette, de kiderült, hogy olyan alkalmazásokra is képesek, amelyek a korábbi, szimmetrikus rendszerekkel elképzelhetetlenek voltak.

A bemutatandó alkalmazások megértéséhez elegendő a 13. ábrán vázolt kétkulcsos lakat-analógiára hivatkozni. Ugyancsak a könnyebb megértést segíti, ha a kommunikációban résztvevő partnereket megszemélyesítjük, személyneveket adunk nekik, jóllehet ezek a partnerek esetleg csak számítógép-szerverek. Ez a „megszemélyesítés" a kommunikációs protokollok leírásakor különben is általános szokás.

A kommunikációban résztvevők mindegyike rendelkezik egy ú.n. privát (titkos) kulccsal és egy nyilvános kulccsal. Az utóbbit pl. egy telefonkönyv-szerűen (de annál biztonságosabban és hitelesebben) működő, központi kulcs szerverről, vagy a partner személyes honlapjáról tölthetik le.

Nevesítsük így „A" és „B" titkosított kommunikációját Aliz és Bob információcseréjének.



14. ábra
Bob küld (Aliz nyilvános kulcsával titkosított üzenetet Aliznak.

Figyeljük meg, hogy ennél a titkosított üzenetküldésnél a küldő, vagyis Bob nem használja egyik titkosító kulcsát sem. Ugyanakkor *meg kell bíznia* abban, hogy Aliz nyilvános kulcsa valóban és hitelesen azé az Alizé, akinek az üzenetet küldi. Azaz azt valóban csak „az" az Aliz lesz képes megfejteni a saját titkos kulcsával, akinek küldeni szánta.

Ez a kérdés a kulcsmegosztás szempontjából nagyon is lényeges. Nem technikai, hanem *bizalmi, garantált hitelesítési ügy*.

Ezen a ponton belép (vagy megjelenik) e kommunikációs rendszerben Aliz és Bob mellett egy harmadik „személy" a *hitelesítés szolgáltató.*

A magyar jogi terminológiában valóban ez a neve. Az angolban az ú.n. Certification Authority: CA.

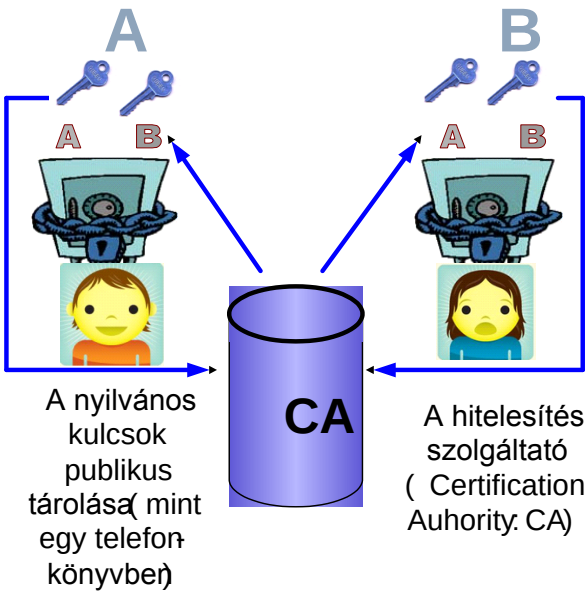
Magyarországon a hitelesítés szolgáltatásra több cég is létezik és a működtetésüket szigorú törvényi előírások szabályozzák. A hitelesítésük akár közjegyzői hitelesítéssel azonos érvényű is lehet, és Aliz nyílt kulcsának Alizhoz való hiteles hozzárendelésén kívül más szolgáltatásaik is vannak.

A hitelesítés szolgáltatás, persze, díjköteles, de magánszemélyek is igénybe vehetik.

Manapság már a **P**ublikus **K**ulcsok **I**nfrastruktúrája (PKI) akár önálló diszciplinának is tekinthető és nagy szakirodalma van.

Ismételten felhívjuk a figyelmet arra, hogy ezekben a nyíltkulcsú titkosítási alkalmazásokban feltétlenül szükség van egy a technikai megoldásokat az adott társadalmi ill. gazdasági környezethez *illesztő* és közbizalmat igénylő törvényi/jogi rendszerre. Ez a PKI.

A következő ábra a hitelesítés szolgáltató (CA) kulcskezelő szerepét kívánja bemutatni. A rendszer résztvevői a nyilvános kulcsaikat egy központi CA szerveren tárolják, amely szerepe leginkább egy nagy biztonsággal hitelesített telefonkönyvéhez hasonlítható.



15. ábra.
A hitelesítés szolgáltató szerepe a publikus kulcsok kezelésében
(ha csak két résztvevő lenne a rendszerben.)
Mind a négy kulcs különböző, de **A** kulcsai egy kulcspárt alkotnak és **B** kulcsai szintén.

A nyíltkulcsú kriptorendszer alkalmazható ú.n.. **elektronikus aláírásra,** vagyis dokumentumok hitelesítésére is. Ebben meghatározó szerepe van a hitelesítés szolgáltatónak, amely a nyilvános kulcsot hatóságilag garantált módon és egyértelműen hozzárendeli a kulcs tulajdonosához.

Ha ezek után Aliz a saját titkos kulcsával aláír egy dokumentumot, akkor azt az aláírást bárki dekódolhatja Aliz, de csakis az ő nyilvános kulcsával és így a hitelesítés szolgáltató hatóságilag garantálja, hogy az az aláírás valóban Alizé. Ez nem technikai, hanem a jogi bizalom kérdése. Ez az eljárás alapelve, de a gyakorlati kivitelezése azért ennél bonyolultabb.

Gondoljuk meg, hogy a mindennapi gyakorlatunkban egy biztosítási szerződés, vagy egy banki beszedési megbízás, stb. aláírásával tulajdonképpen nem annak az okiratnak a szövegét, hanem a szöveg hordozóját, vagyis a papírt hitelesítjük az aláírásunkkal. (Már csak ezért se írjunk alá soha üres papírokat!)

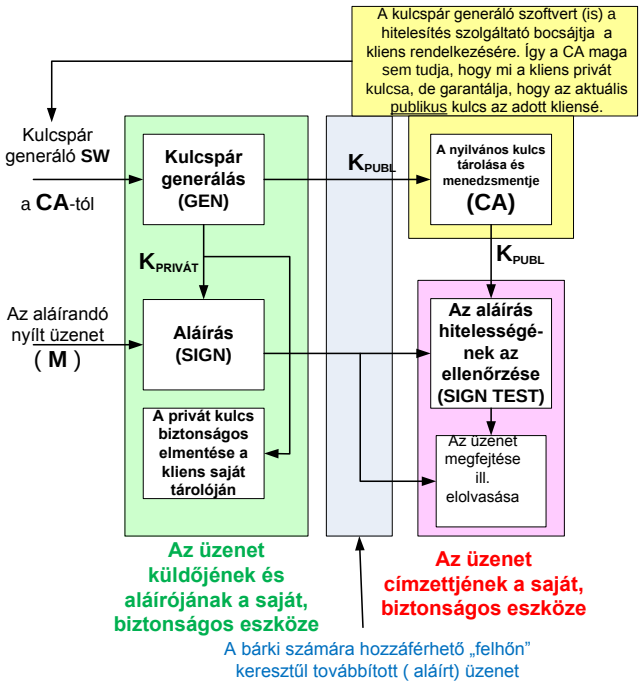
Egy elektronikus dokumentum esetén viszont nem lehet a „hordozót” hitelesíteni, hanem a tényleges szöveget kell „aláírni”.

Ezért egy elektronikus dokumentum hitelesítéséhez az említett privát kulcsos aláírás önmagában nem elegendő. A dokumentum szövegéből – szabványosított eljárással - előállítanak egy az adott dokumentumra gyakorlatilag kizárólagosan jellemző ú.n. HASH jelzőszámot és azt hozzákapcsolják az aláíráshoz, továbbá az egészet ellátja a hitelesítés szolgáltató egy a dátumot és az időpontot is rögzítő – persze szintén hiteles – jelzéssel: egy *időbélyegzővel*.

Mindez a biztonságot szolgálja és annyira automatizált, amennyire csak lehetséges.

A felhasználónak rendszerint fogalma sincs arról, hogy egy-egy üzenetváltáskor, vagy tranzakció folyamán milyen bonyolult folyamatok játszódnak le a háttérben. Persze, manapság nem kell tudni, hogy egy TV készülék vagy egy maroktelefon belseje – és tágabb rendszere - hogyan is működik, és a használója e tudás hiányában is jól elboldogul vele.

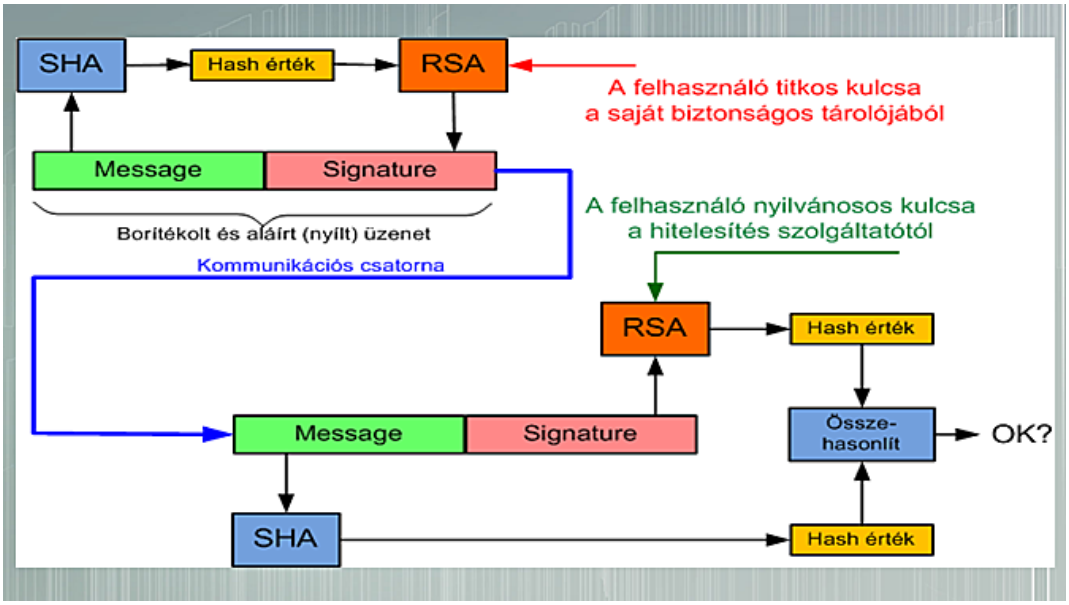
A fent leírt digitális aláírási, ill. az azzal hitelesített dokumentum előállítási folyamatát és szereplőit mutatja a következő blokkvázlat, amelyben ismét csak az eljárás bonyolultságát kell észrevenni.



16. ábra.
A digitalis aláírás működési vázlata és a folyamat szereplői

A fenti ábrán nem szerepeltettük az üzenet titkosítását és az esetleges (továbbítás közbeni) sérülésének az ellenőrzését sem.

Ha egy ilyen folyamatba beillesztjük még a fent említett HASH ellenőrző számot is, akkor egy nem titkosított, de HASH számmal és digitális aláírással ellátott üzenet előállítását és továbbítását szemlélteti a következő ábra:



17. ábra

A HASH ellenőrzőszámmal ellátott – és aláírt – üzenet továbbítása és a vétel helyén való ellenőrzése, hogy nem változott-e meg a továbbítás során.

NB: A Hash ellenőrző szám ma szokásosan egy 168 bites szám, amelynek a hossza független az üzenet hosszától és egy szabványosított eljárással (a magyar terminológiában: hasító függvénnyel) állítják elő.

Azt nem tudjuk megakadályozni, hogy a nyílt interneten való továbbításkor akár véletlenül, akár szándékosan ne változhasson meg egy üzenet, de a HASH jelzőszám alkalmazása alkalmas az ilyen, esetleges változás kimutatására.

Manapság (pl. az internetes banki tranzakcióknál) még más, az internetes világhálót megkerülő további biztonsági azonosítót is használnak. Pl. egy SMS-ben megküldött, csak néhány percig érvényes, véletlenszerű azonosítót, amely nélkül a tranzakció nem hajtható végre. Mindez a PKI témakörébe tartozik és itt nincs hely a részletezésére.

X. A HIBRID KRIPTORENDSZEREK

A 4. generációs, szimmetrikus (modern változataikban iterációs) kriptorendszerek erősek, gyorsak és nem igényelnek relatíve nagy számítástechnikai kapacitást, de a kulcsmegosztással problémájuk van.

Az 5. generációs, azaz a nyíltkulcsú rendszerek megoldják a (személyes találkozást nem igénylő) kulcsmegosztást, de ennek az az ára, hogy a 4. generációs rendszereknél jóval nagyobb számítási kapacitást igényelnek és így lassúbbak is azoknál.

Igaz, hogy a PKI megoldásával együtt nagyon sok olyan, fontos alkalmazásra is képesek, amelyekre a 4. generációs rendszerek egymaguk nem.

Mellesleg azonos biztonsághoz jóval hosszabb kulcsokra is szükségük van, mint a 4. generációs rendszereknek.

Kézenfekvő megoldás, hogy a 4. és az 5. generációs rendszerek előnyeinek együttes alkalmazásával valamilyen HIBRID kriptorendszert hozzanak létre és ezt – többféle változatban is – megtették.

Ma a kommerciális biztonságos kommunikációban szinte kizárólag ilyen hibrid rendszereket alkalmaznak.

Többféle protokoll is létezik. Egy ilyen lépései a következők:

1. Az üzenet küldője előállít egy egyszer használatos véletlen (K_V) kulcsot, amely megfelel a 4. generációs kulcshossz-követelményeknek.

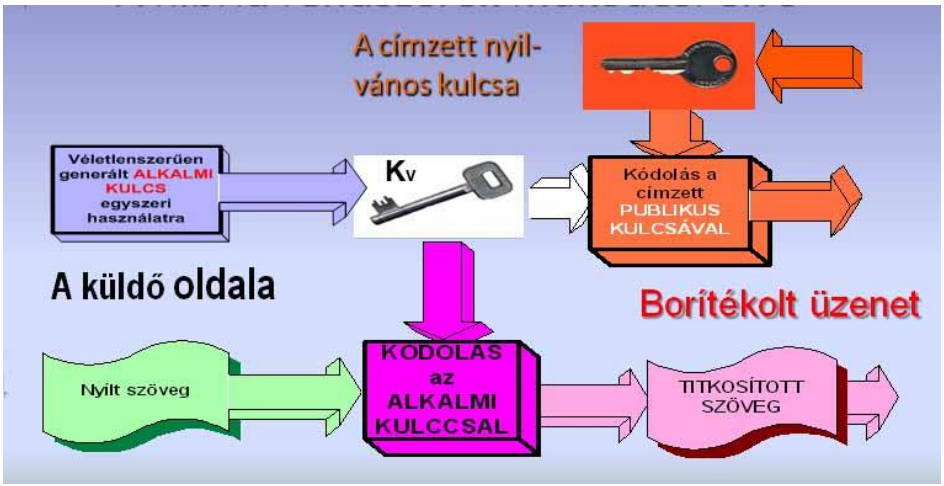
2. Bekéri (pl. a hitelesítő cégtől) a címzett nyilvános kulcsát (K_{CP})

3. Az elküldeni kívánt nyílt (P) szövegét egy megegyezés szerinti 4. generációs eljárással titkosítja a K_V véletlen kulccsal, majd elküldi a titkosított üzenetet (C).

4. A címzett (K_{CP}) nyilvános kulcsával titkosítja az egyszer használatos (K_V) kulcsot, amelyet a címzett visszafejt a saját titkos kulcsával,

5. és így már képes lesz megfejteni a C üzenetet.

Ennek az eljárásnak az elvét szemlélteti a következő blokkvázlat:



18. ábra Egy hibrid kriptorendszer működésének az elvi vázlata.

Látható, hogy a küldő először is *beszerzi* a címzett hitelesített nyilvános kulcsát, majd a küldőtől *két* üzenet megy ki: A nyíltkulcsos rendszerrel titkosított egyszer használatos kulcs, és az egy alkalomra generált kulccsal (4. generációs módon) titkosított üzenet maga.

A címzettnek mindkettőre szüksége van a megfejtéshez. Ez, persze, csak a hibrid rendszer működési elve, mert mind a címzett publikus kulcsának a beszerzésére, mind az aktuális esetekben alkalmazott 4. és 5. generációs kriptorendszerekre többféle változat is létezik.

Ez azért gazdaságos elv, mert az egyszer használatos véletlen kulcs (nagyobb számításigényű) titkosítása, vagy ehelyett egy Diffie-Hellman kulcs csere lebonyolítása csak egy blokkon történik meg és a rendszerint nagyobb terjedelmű üzenet, több blokkos titkosításához már a kisebb számításigényű iterációs kriptorendszerek valamelyikét lehet használni.

Az aktuális protokoll a 17. és a 18. ábrán vázoltakkal is kombinálva, persze már meglehetősen bonyolult szokott lenni, de ezt a felhasználó nem is érzékeli.

XI. NÉHÁNY SZÓ A JÖVŐRŐL

A titkosított kommunikáció „lételeme”, alkalmazása szorosan kötődik a világhálóhoz és az azzal kapcsolatos kommunikációs technikákhoz, a technika fejlődéséhez.

Manapság talán az alkalmazások fejlesztésére, kiterjesztésére fókuszálnak és nem is annyira a számítógépekkel folytatott

kommunikációra, hanem a mobil telefóniára, amely készülékek egyre „okosabbak”.

Nagyon sok és elképesztően nagy méretű ú.n. közösségi webkikötő létezik, amelyekhez csatlakozó személyek önként megadnak magukról nagyon sok információt. Ezek segítségével a nagy kereskedő vállalkozások személyre szabott reklámokkal bombázzák a felhasználókat. Ezt több szempontból tapasztalhatjuk is.

Nagyon sok személyes adatunkat tárolja, persze, a közigazgatási rendszer is. Kevesen tudják, hogy az adatvédelmi törvény lehetővé teszi, hogy a lakóhely szerint illetékes önkormányzati jegyzőnél letilthatjuk ezeknek az adatainknak a harmadik személynek való kiadását. Még kevesebben mennek el a jegyzőhöz és intézkednek erről a letiltásról, amelynek a hiányában az adataink alapértelmezésben szabadon kiadhatók.

Ma már a név és címlistákkal kereskednek is.

Igen sok rosszindulatú szoftver (maleware) is kering a világhálón, amelyeket az óvatlan felhasználó egy e-mail megnyitásával még nem, de egy link, egy kép, vagy valamilyen csatolmány megnyitásával már akaratlanul letölt a gépére, amelyen az működni kezd és kárt okoz. Nem a gép hardver elemeiben, (egyelőre azokban még nem) hanem a működtető szoftverben, vagy elkezd a háttérből „figyelni” és megpróbál érzékeny adatokat ellopni, elküldeni. Pl. banki adatokat, jelszavakat, stb. Sajnos bármennyire is idegen a jóindulatú emberektől, bizony gyanakvónak kell lenni és *odafigyelni*.

Kering egy csomó jóindulatú, de „helyből” látszik, hogy hozzá nem értő figyelmeztetés pl. olyan szövegekkel, hogy „ez a vírus leégeti” a merevlemezt.

Már ma is létezik és kapható egy csomó olyan szoftver (persze nem ingyen) amelyek a különféle rosszindulatú támadások kivédésére valók, de ezek hatékonysága nagyon különböző és ezzel „nagyon finoman” fogalmaztunk.

Világméretű figyelő szolgálata van a Symantecnek és Bruce Schneier: Cryptogram c. ingyenes, internetes havi folyóiratának, amely sok ilyen „védelmi” szoftvert is szokott minősíteni.

Várható, hogy az ilyen adatbiztonsági rendszerek a jövőben fejlődnek és az is, hogy ugyancsak a biztonság növelése céljából az internetes üzenetváltással szimultán más (pl. mobil telefonos) és ú.n. biometriai biztonság-növelő szolgáltatásokat is bevezetnek.

Pl. hang-azonosítás, vagy egy hang-kód bejátszása telefonon, ujjlenyomat érzékelés, stb. Közülük akár többet is egyidejűleg alkalmazva. Ezek a módszerek és a hozzávaló érzékelő eszközök már ma is léteznek. Némelyik ma még igen drága és csak a legnagyobb biztonságot megkövetelő helyeken alkalmazzák.

Mint pl. az írisz-felismerő beléptetést a CERN-ben az LHC gyorsítónál.

Végül, de egyáltalán nem utolsó sorban meg kell említeni, hogy a *felhő* fogalom ma már nem csak a világhálóra (WWW: World Wide Web) hanem más, világméretű összeköttetési rendszerekre is értelmezhető. Ilyen, egyelőre a www-től elkülönített „felhő" az egyre „okosabb" telefonokkal megvalósított, nem csak verbális, hanem képi, sőt: video kommunikáció is.

Beszélhetünk azonban a sokféle TV csatorna által szolgáltatott video és hír- kommunikációról is.

Mindennapjainkban tanúi vagyunk annak, hogy ezek a „felhők" mintegy integrálódnak, részben vagy egészben egymásba olvadnak.

A jövőről szólva tehát meg kell említeni ezeknek az itt nem is pontosan definiált „felhőknek" az integrációját, mint több mint lehetséges fejlődési irányt.

FORRÁSOK ÉS SZAKIRODALOM

A cikk szerzője több évtizedes főiskolai és egyetemi előadásaiból, az azokhoz készült jegyzetekből és prezentációkból válogatva állította össze e cikk anyagát. Ezekhez természetesen nagyon sok forrást felhasznált, amelyeket lehetetlen itt mind felsorolni. Néhány alapvető művet azonban mégis meg kell itt említeni, amelyek a következők.

[1] The CODEBRAKERS, by David Kahn
Scribner, NewYork, 1966. ISBN 0-684-83130-9
A kriptográfia történetének majdnem 1200 oldalas alapműve. Több részes filmet is készítettek belőle, de magyarra nem fordították le.

[2] ICSA Guide to cryptography, by Randall K. Nichols, McGraw-Hill, NY@ other cities in 1999.
ISBN 0-07-913759-8.

Ez a több, mint 800 oldalas alapmű ma már a kriptográfiában egyáltalán nem friss, de feltétlenül említésre méltó, alapvető szakirodalmi forrás.

[3] Applied cryptography, by Bruce Schneier. JohnWiley and Sons Inc. NY…1996.
ISBN 0-471-12845-7.
A szerzó ma, 2013-ban is a kriptográfia talán leghíresebb guruja. Sok és jó könyve jelent meg és ma is van egy internetes folyóirata.

[4] Wireless security, by Randall K.Nichols at al. McGraw-Hill,
NY…2002,
ISBN 0-07-138038-8

Nichols prof (Univ of Washington, NY Columbia) szintén világhíres kriptográfiai guru és sok könyvet, egyetemi jegyzetet írt.

[5] Digital communications, by Bernard Sklar,
Prentice-Hall Inc. New Jersey, 1988.
ISBN 0-13-211939-0.
A címének pontosan megfelelő, nagyon jó alapmű (a tisztes kora ellenéra még ma is.)

[6] Crypto-gram. *Bruce Schneier internetes (ingyenes) havi folyóirata. Feliratkozni lehet rá a*
http://www.schneier.com/crypto-gram.html *webkikötőn*.

A magyar nyelvű szakirodalom köréből jó szívvel ajánlhatom az érdeklődőknek:

[7] Virasztó Tamás: Titkosítás és adatrejtés. Netacademia Kft. Bp. 2004. ISBN 963 214 253 5
Talán az egyetlen és még elég friss magyernyelvű könyv, amely komolyan foglalkozik a kriptorendszerek elméleti hátterével is. Felsőfokú tankönyvként is használható.

[8] Simon Singh: Kódkönyv.Park Könyvkiadó Bp. 2001. *Nem szakkönyv, hanem igényes ismeretterjesztő célú, nagyon olvasmányos és szórakoztató mű a kriptográfia "izgalmas" történeteiről.*

[9] Dr. Berta István Zsolt: Nagy e-szignó könyv.
Microsec Kft, Bp. 2011.
Mintegy kézikönyv az elektronikus aláírás témájához és mindenhez, ami vele kapcsolatos

[10] *Az ELTE egy igen érdekes, a kriptográfiával és "környezetével foglalkozó webkiktője:*
www.**biztostu.hu**/login/index.php

E cikkben ténylegesen felhasznált anyagok forrásai:

[11] http://hu.wikipedia.org/wiki/Barlangrajz

[12] http://hu.wikipedia.org/wiki/%C3%89k%C3%ADr%C3%A1s#Protosumer_.C3.ADr.C3.A1s

[13] http://en.wikipedia.org/wiki/Cuneiform#Proto-literate_period.

[14] http://archnet.org/library/sites/one-site.jsp?site_id=8223.

[15] http://hu.wikipedia.org/wiki/Gutenberg-galaxis

[16] https://hu.wikipedia.org/wiki/K%C3%A9pes_kr%C3%B3nika

[17] https://www.google.com/search?q=k%C3%A9pes+kr%C3%B3nika+k%C3%A9pei&hl=hu&tbm=isch&tbo=u&source=univ&sa=X&ei=R6mvUc69E4z24QTZoIHoDQ&ved=0CCkQsAQ&biw=1280&bih=642

[18] http://www.google.com/imgres?imgurl=http://elismondom.files.wordpress.com/2010/08/0449-cordoba-mecset-belso.jpg&imgrefurl=http://elismondom.wordpress.com/2010/08/17/andaluz-nyar-11-cordobai-nagymecset-a-mezquita/&h=873&w=1164&sz=170&tbnid=6lNs6fSeTA8_KM:&tbnh=98&tbnw=130&zoom=1&usg=__y1-SSkjl23FqsolF11FU0s1hwjc=&docid=qXK8NtWN3K0dZM&hl=hu&sa=X&ei=9zevUerUF43E4gSSwoHYBQ&ved=0CDIQ9QEwAQ&dur=4745

[19] http://www.panoramio.com/photo/5259007

[20] http://en.wikipedia.org/wiki/Internet_traffic

Bolygószonda modell építése az Alba Regia Műszaki Karon

dr. Hudoba György
Óbudai Egyetem, Alba Regia Műszaki Kar
(OE-AMK) Székesfehérvár,
hudoba.gyorgy@amk.uni-obuda.hu

***Abstract* — we report about a planetary probe constructing (called Hunveyor) project running at the Óbuda University, Alba Regia Technical Faculty. The primary aims of the project (engineering, constructing and using an internet controllable exploration robot) are: motivation and education of electrical engineers of the future. Building such a robot (HUNVEYOR-4) integrates many fields of sciences, like physics, electronics, robotics, from microcontroller to web programming, modelling, creating space-inspired animations as well as doing various experiments (like monitoring the environment, e.g. measuring the temperature, wind speed and direction, etc.) and planetary analogue field studies. In this paper we show the evolution of the project from the beginning to the latest international field study, conducted in the desert Sahara in February 2013.**

***Kivonat* - Az Alba Regia Műszaki Karon oktatási céllal egy bolygószonda modell épül. A modell építésének elsődleges céljai: motiváció és oktatás, vonzó és hasznos téma biztosítása projekt- és diplomamunkákhoz a leendő villamosmérnökök számára, hosszú távon. Egy bolygószonda építés számos diszciplínát (mint pl. fizika, elektronika, robotika, programozás, modellezés, ...stb.) egyesít, miközben analóg terepgyakorlatok alkalmával számos tevékenység (mint pl. környezet monitorozás: hőmérséklet, szélsebesség és szélirány mérés, ... stb.) elvégzésére, kipróbálására ad lehetőséget. A cikkben néhány megoldandó műszaki feladaton keresztül bemutatjuk a projekt történetét, és beszámolunk a 2013 februárjában, a marsi körülményekhez hasonló klímájú területen, a Szaharában végzett nemzetközi terepgyakorlat tapasztalatairól és eredményeiről is.**

I. BEVEZETÉS

A XXI. század hajnalán sajátos ellentmondásnak lehetünk tanúi. Míg mindennapi életünkben egyre kiszolgáltatottabbakká válunk a technikának (elektromosság, számítógép, internet, okostelefon, … stb.), ugyanakkor a mérnöki és kutatói életpályák iránti érdeklődés vészesen csökken, a fiatalok hátat fordítanak a műszaki és a természettudományi pályának. Az érdeklődés össztársadalmi szinten megnyilvánuló hanyatlása világméretű jelenség. Pedig a XX. század eredményeinek továbbviteléhez, a fejlődés fenntartásához és megújulásához a lassan kiöregedő korosztálytól a fiataloknak fokozatosan át kell(ene) venniük a stafétabotot. A napjainkra már-már rutinszerűvé váló űrkutatás még mindig érdeklődésre tarthat számot, főként, ha egy-egy speciális űreszközre vagy eseményre a média is aktívan reagál. A HUNVEYOR űrszonda építési programmal a fentiekben vázolt problémákra próbálunk egyfajta választ adni.

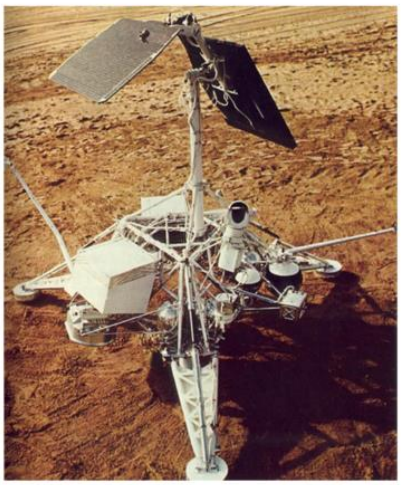
II. A KÍSÉRLETI GYAKORLÓ ŰRSZONDA ÉPÍTŐ PROGRAM CÉLJAI

A kísérleti gyakorló bolygószonda építési program a HUNVEYOR elnevezést kapta, amely a „**H**ungarian **UN**iversity Sur**VEYOR**” megnevezésből alkotott mozaikszó. Az első két tag jelentése magától értetődik, az utolsó tag pedig azt jelzi, hogy mintául az ember Holdra szállását előkészítő amerikai SURVEYOR-7 holdkutató robot szolgált.

Az űrszonda építés alapgondolata az ELTE-n született meg 1997-ben. A programhoz Pécs és Szombathely után székesfehérvári intézetünk[1] 2001-ben negyedikként csatlakozott, így bolygószonda-modellünk a 4-es indexet kapta.

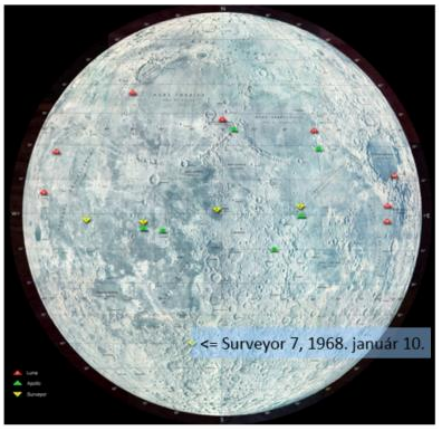
„A Föld környezetét végleg elhagyó űreszközöket űrszondáknak, vagy bolygóközi szondáknak nevezzük. Céljuk a Naprendszer égitesteinek megközelítése és helyszíni vizsgálata, illetve a bolygóközi tér tanulmányozása.”[1]

1, Akkoriban még Kandó Kálmán Műszaki Főiskola, Számítógéptechnikai Intézet



Surveyor-7

Kilövés: 1968. január 7., 06:30:00 UTC
Leszállás: 1968. január 10., 01:05:36 UTC
Hordozórakéta: Atlas-Centaur
Repülési idő: 65 h
Pozíció: 41.01°S 348.59°E
Leszálló tömeg: 305.7 kg



1. ábra A Surveyor 7 és a Hold meghódítása. A piros jelek a szovjet Luna, a sárga az amerikai Surveyor szondák, míg a zöld az Apolló leszálló helyeit mutatják.

Természetesen senki nem gondolja komolyan, hogy a HUNVEYOR-4 elhagyja a Földet. Célként - mint azt a „gyakorló” jelző is mutatja - azt tűztük ki, hogy a hallgatók számára hosszú távra biztosítsunk egy vonzó, értelmes és hangulatos keretprogramot a Tudományos Diákköri tevékenységhez (TDK), a projekt munkákhoz, biztosítsunk lehetőséget a mérnöki készségek (tervezés, szervezés és kivitelezés) gyakorlására, kibontakoztatására, a legújabb technikák és technológiák megismerésére, valamint a tehetségesebb és kitartóbb hallgatók esetén akár diplomamunkák is születhessenek. A programban való részvétel szolgáljon továbbá referenciaként a végzett diákok számára, növelje hallgatóink versenyképességét a munkaerőpiacon, s nem utolsó sorban mutassuk meg, hogy a mai technikával már akár diákok is képesek egy 1960-as évekbeli űrszonda képességeit elérő szerkezetet konstruálni.

Az sosem volt célunk, hogy egy kész, befejezett, „kilövésre kész” bolygószonda álljon elő. Maga az építés, a mérnöki feladatmegoldó tevékenység gyakorlása illetve gyakoroltatása a valódi cél, akár a már meglevő egységek esetleges ismételt újratervezése és megépítése révén, követve a műszaki fejlődést, mint amire majd példát is mutatunk.

III. FELADATKIÍRÁS

A feladat kiírása ezek után a következőképp körvonalazódott. Képzeljük el, hogy egy Földön kívüli égitestre (Holdra, Marsra, a Jupiter, vagy akár a Szaturnusz egyik holdjára) kutató űrszondát küldünk, melynek feladata egy jövőbeli kolónia megalapításának előkészítése. Építsünk egy ilyen távolról vezérelhető mérési adatgyűjtő robotszondát! A korral haladva - a szonda legyen elérhető az Internetről is! (Mindez 2001-ben.)

A fenti követelményeknek megfelelően a megoldandó főbb feladatok:

- az űrszonda fém tartóvázának elkészítése
- különböző műszermodulok építése
- a szonda műszer-együttesének vezérlése
- mérési adatok gyűjtése, tárolása, továbbítása, feldolgozása
- egyéb kiegészítő és kiszolgáló elektronikus és mechanikus elemek készítése
- a szonda energiaellátásának biztosítása
- kommunikáció a „földi irányító központtal”
- a szonda külvilág számára való elérhetőségének biztosítása

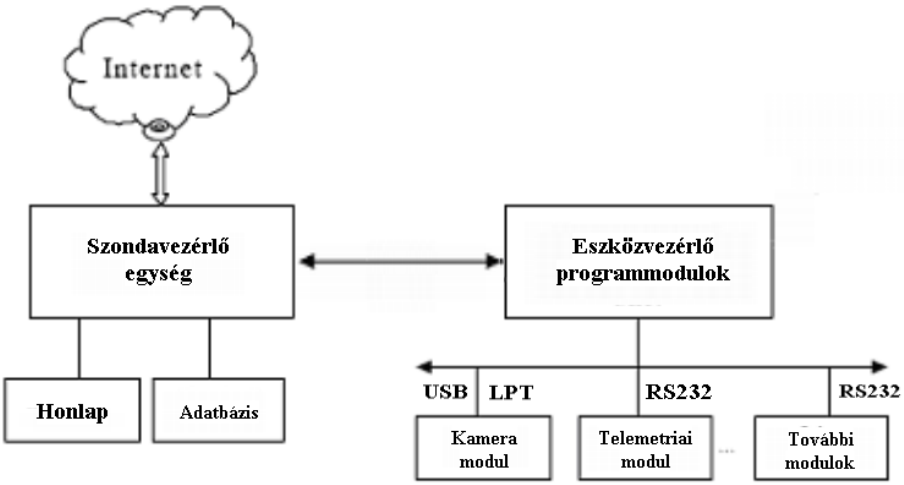
IV. AZ ELSŐ LÉPÉSEK

A projekt meghirdetése eleinte semmilyen érdeklődést sem váltott ki a hallgatók körében, pedig Intézetünk fő profilja a villamosmérnök képzés, így a szonda tartóvázának egyszeri elkészítésén kívül a fenti feladatok jól illeszkednek a diákokkal szemben támasztott követelményekhez. Úgy gondoltuk, ha a mechanikát már készen tálaljuk, akkor a többi feladat már vonzóbbá válik, ezért gépészmérnök kollégánk, Sasvári Gábor révén elkészült az alumínium vázszerkezet. Az elgondolás helyesnek bizonyult, hamarosan több hallgató is jelentkezett.

2. ábra A HUNVEYOR-4 fémváza és alkotója, Sasvári Gábor

V. A HUNVEYOR-4 STRUKTÚRÁJA

A HUNVEYOR-4 struktúrája az évek folyamán többször is módosult. Az első verzió egy PC alaplapra épült, melyen a műszerek kezelése mellett helyet kapott a web szerver és az adatbázis is.

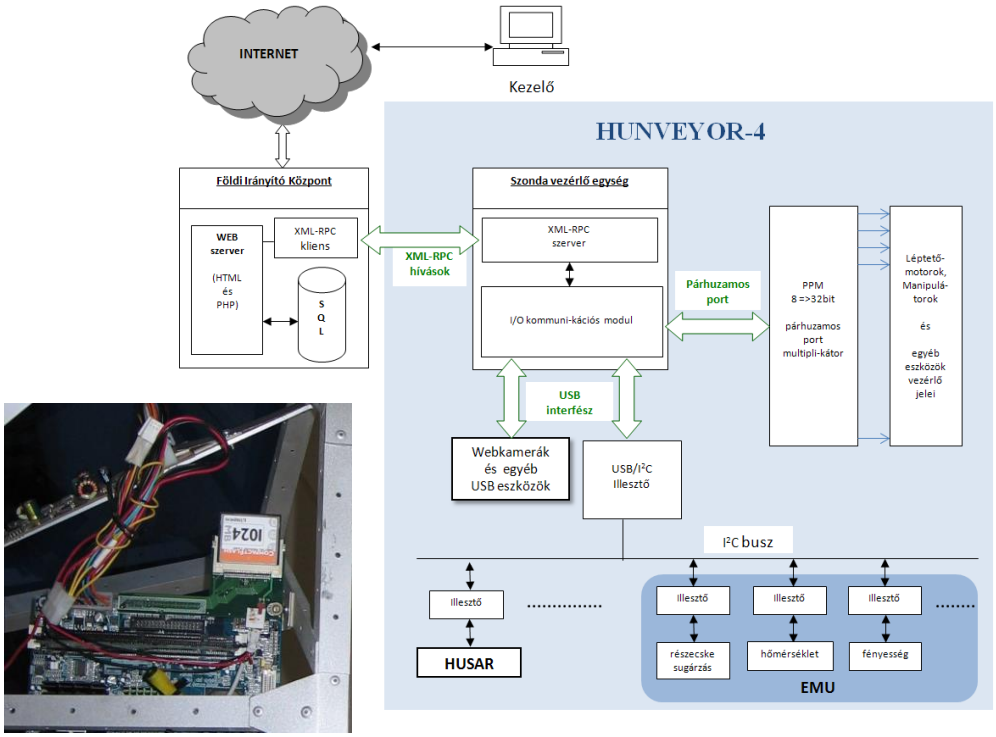


3. ábra A HUNVEYOR-4 első verziójának strukturális felépítése

4. ábra A HUNVEYOR-4 első verziója

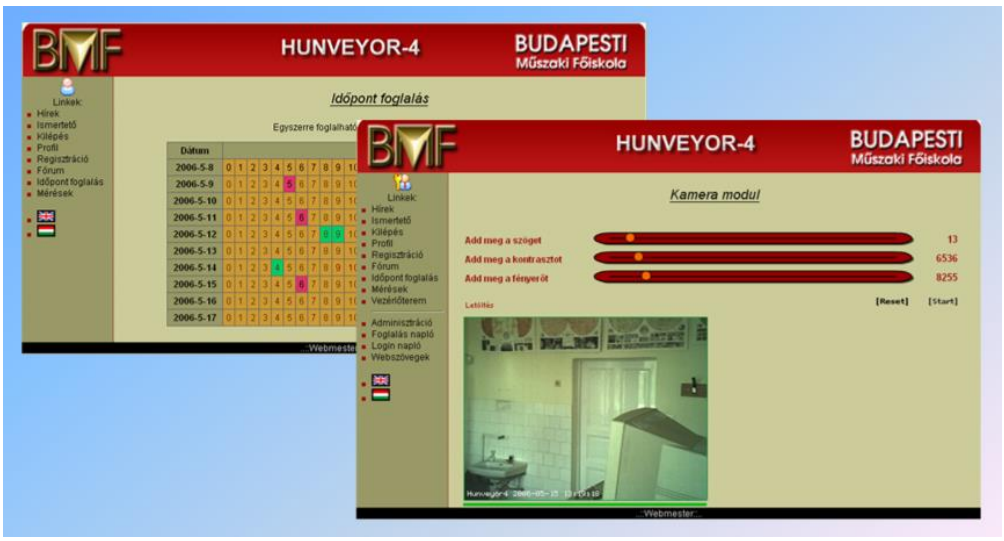
A későbbiekben felmerült az igény, hogy egy elektromos és közvetlen kábeles hálózati elérése nélküli, valódi terepen is működőképes verzió álljon elő. Így készült el a HUNVEYOR-4b, melynek főbb jellemzői:

- új, kisebb teljesítmény igényű, aktív hűtést nem igénylő alaplap
- kisebb erőforrásigény
- merevlemez helyett Compact Flash memória (CF kártya)
- nincs webszerver és adatbázis
- egyedi, XML/RPC alapú kommunikációs protokoll a szerverrel
- egyetlen, 12 V tápfeszültségről, napelemmel töltött akkumulátorról is képes működni
- rádiós (Wireless Lan) kommunikáció
- IIC-re felfűzött mérőeszközök
- jobbra-balra és fel-le is nézni képes sztereo webkamera
- napelem mozgató mechanika (Napraforgó modul)
- rádióvezérlésű kiskocsi (HUSzAR – Hungarian Surface Analyser Rower)
- a szabad téri működtetés érdekében kék védőburkolat



5. ábra A HUNVEYOR-4b blokkdiagramja, valamint az alaplap, a tápegység és a CF kártya

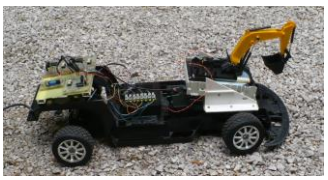
6. ábra A HUNVEYOR-4b a „szerelő csarnokban”



7. ábra A HUNVEYOR-4b felhasználói felületei
(erőforrás-foglalás és a kamera modul)

VI. A HUNVEYOR-4 MŰSZEREI

A teljesség igénye nélkül, csupán ízelítőként bemutatok néhány, többségében a diákok által készített eszközt és mérőműszert.

”Szélkakas” szélsebesség, szélirány és hőmérséklet mérés 	gáz, légnedvesség, légnyomás megvilágítás erősség spektrális intenzitás, villámdetektor 
a három rezgés-érzékelő egyike, burkolat nélkül 	LED-spektrométer 
a sztereo kamera modul 	HUSzAR a kiskocsi 
a gamma sugárzás detektor 	WLAN access point 
a vételi parabola 	a NAPRAFORGÓ modul 

1. táblázat A HUNVEYOR-4 néhány eszköze és mérőműszere

8. ábra A HUNVEYOR-4 harci díszben

VII. TEREPGYAKORLATOK

A terepgyakorlatok célja a HUNVEYOR-4 terepre való szállíthatóságának és rázásállóságának ellenőrzése, valamint annak megállapítása volt, hogy milyen típusú méréseket lehetséges, illetve célszerű az egyes kiválasztott analóg környezetekben elvégezni. Ezen mérésekhez az aktuálisan meglevő műszerezettség mennyiben alkalmas, és milyen további eszközökre és fejlesztésekre lenne igény a jövőbeli környezet-vizsgálatokhoz.

A terepgyakorlatok során az alábbi hat hazai helyszínt jártuk be:

Kiskunsági Nemzeti Park, Fülöpháza - futóhomok

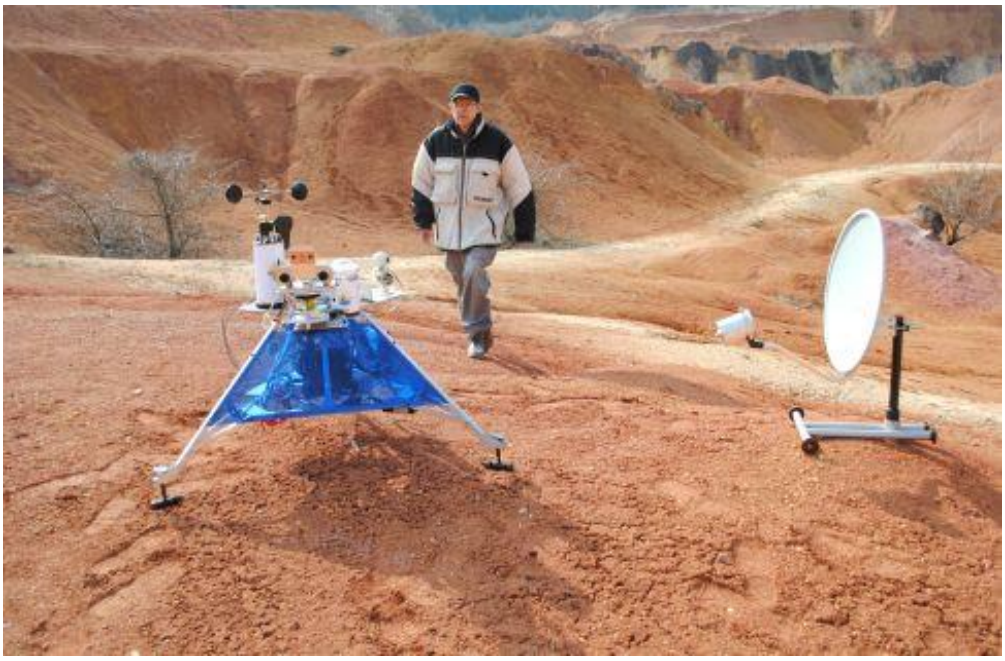
Gánt, bauxitbánya – víz és sárfolyások

Nógrád – a jégkorszakban simára csiszolt sokszöglapú ún. „éles kavicsok”

Bér – savanyú andezit

Szentbékkálla – köpenyzárványokkal tűzdelt vulkáni tufa

Hegyestű – bázikus bazalt



9. ábra Terepgyakorlaton a gánti bauxitbányában. A képen a szerző.

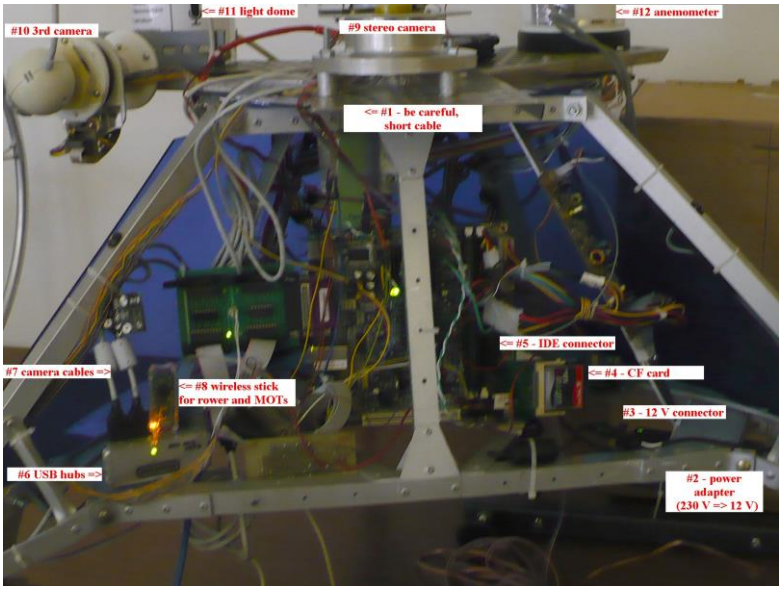
A WLAN (rádiós) összeköttetés hatótávolságát Székesfehérvár határában vizsgáltuk. A vételi oldalon parabola, a szonda oldalán egyszerű botantenna alkalmazásával 4,8 km-ről még kapcsolatot tudtunk teremteni.

10. ábra A WLAN összeköttetés ellenőrzése a terepen

Az Innsbrucki Egyetem és az Österreichische Weltraum Forum (ÖWF) 2013. februárjára egy nemzetközi terepgyakorlatot hirdetett meg [2],

melyre a szakmai pályázatunk alapján a HUNVEYOR-4 meghívást kapott. A helyszíne Marokkó, a Szahara nyugati része volt, ugyanis a terep és februárban az ott várható időjárási és hőmérsékleti viszonyok nagyban hasonlítanak a Mars nyári éghajlatához. További részletekre vonatkozóan ld. [3,4]. A HUNVEYOR-4, bár nem probléma nélkül, de sikeresen teljesítette a küldetését.

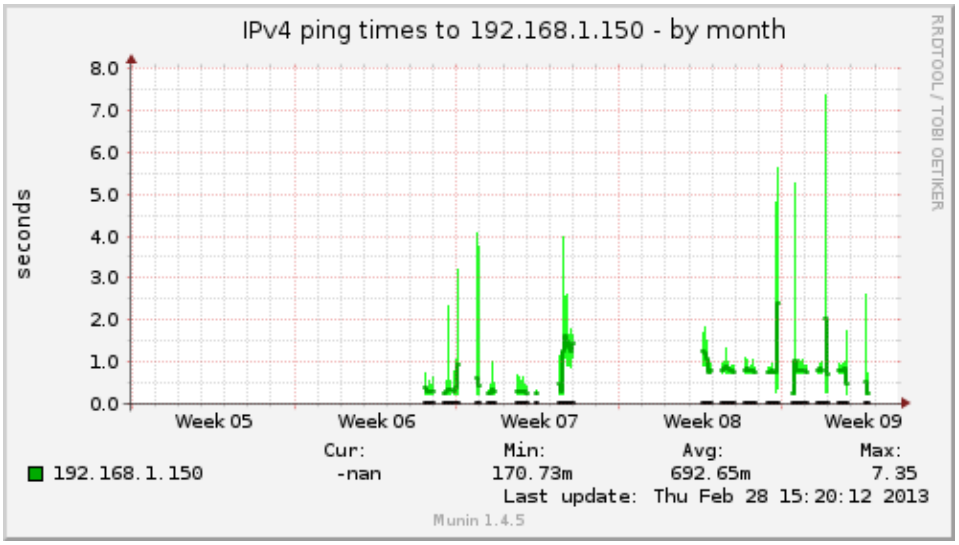
11. ábra A felhívás és a marokkói marsi analóg terepgyakorlat helyszíne



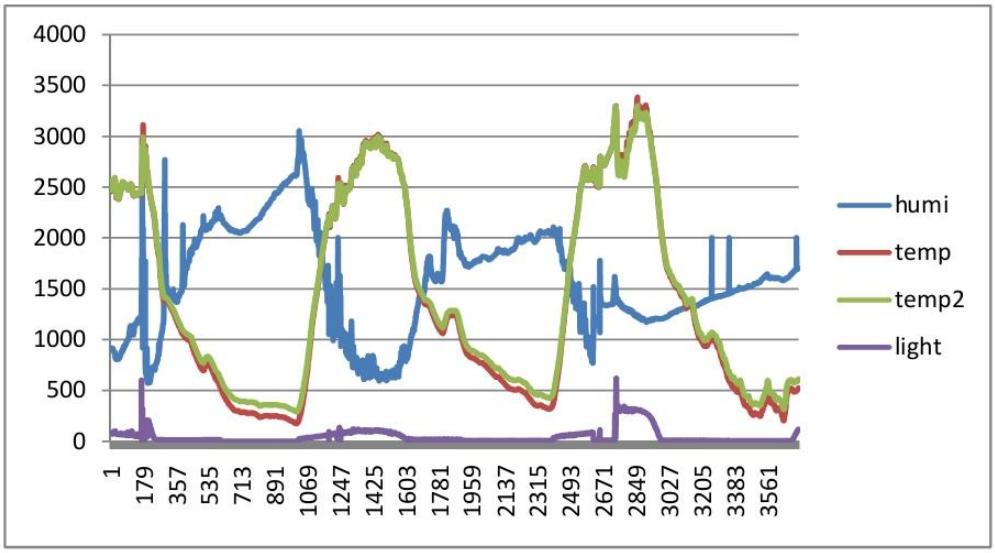
12. ábra A HUNVEYOR-4 burkolat alatti zsúfoltsága

13. ábra A HUNVEYOR-4 a marokkói marsi analóg terepgyakorlaton

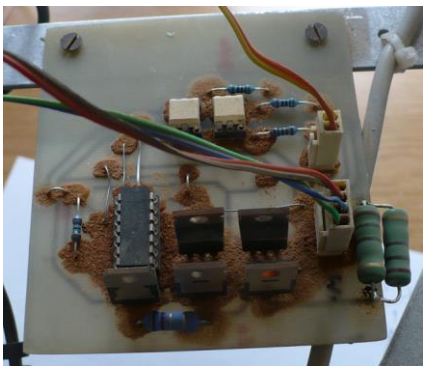
A szonda működését itthonról, interneten keresztül ellenőriztük, s a mért adatokat is azon keresztül hívtuk le. Az alábbi ábrákon a kapcsolat ellenőrzése, valamint egy méréssorozat eredménye látható.



14. ábra PING-statisztika a marokkói marsi analóg terepgyakorlatról



15. ábra A marokkói marsi analóg terepgyakorlat során a hőmérséklet, páratartalom és a fényviszonyok alakulásáról felvett adatsor

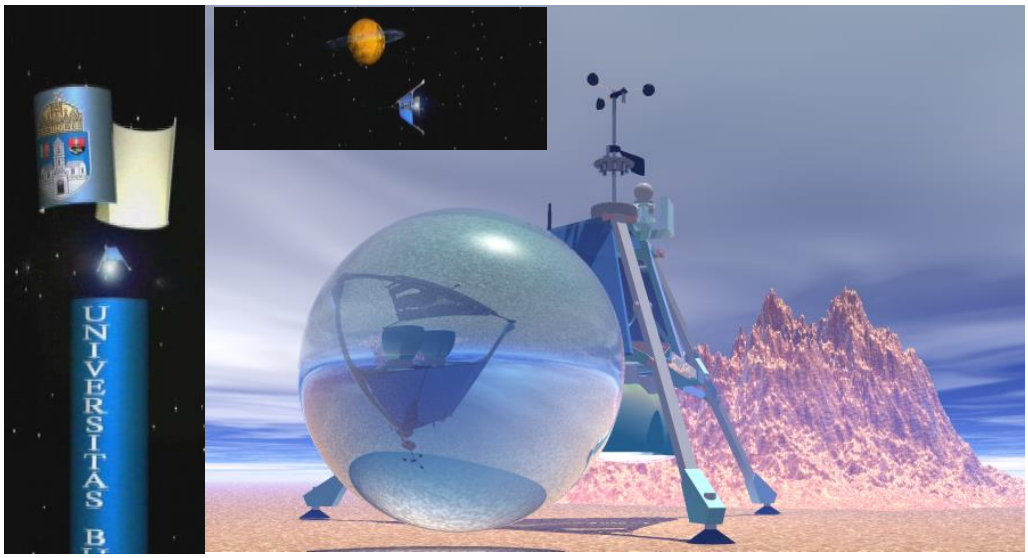


16. ábra A mágnesen (bal oldali kép) a sivatagi porból befogott vasszemcsék láthatók az elektronikán pedig rengeteg porszemcse gyűlt össze, valószínűleg elektrosztatikus feltöltődés következtében.

VIII. A HUNVEYOR PROJEKT KOMPLEXITÁSA

Mint az már az előzőekből is kitűnik, a HUNVEYOR projekt sokrétű, összetett, számos részfeladat megoldását igénylő vállalkozás. Tartalmaz mechanikus alkotóelemek készítését, mint a vázszerkezet, manipulátorok, pozícionálók stb. Az elektronika részéről elektromos (hardware) elemek tervezését, építését, érzékelők, detektorok fejlesztését, valamint NYÁK tervezést, szerelést, bemérést. Természetesen a katalógus böngészés, építőelemek kiválasztása és beszerzése is a megoldandó feladatok közé tartozik. További kihívást jelent az

építőelemekből a rendszer integrálása, interfészek definiálása, eszköz vezérlő programok, driverek és a magas szintű kapcsolódások megtervezése és elkészítése, különféle szimulációk végzése. A működést részben laboratóriumi körülmények között, majd terepi körülmények között végzendő, komplex, előre megtervezett mérési programok segítségével ellenőrizni kell, s az eredmények analizálása után szükség esetén módosításokat kell végrehajtani a rendszeren. Az alacsony szintű, közvetlenül a hardver elemek programozásán túl magas szintű programozásra is szükség van: az eszközök használatával történő adatgyűjtés, a mért értékek adatbázisba való rendezése, későbbi analizálása, feldolgozása, mások számára való hozzáférés biztosítása. Ide tartozik a web programozás számos eleme, beleértve a felhasználók regisztrációját, erőforrás igények kezelését, és így tovább. Külön vonalat jelent még animációk készítésének dús, fantáziát mozgató és igénylő lehetősége.



17. ábra Részletek egy animációból

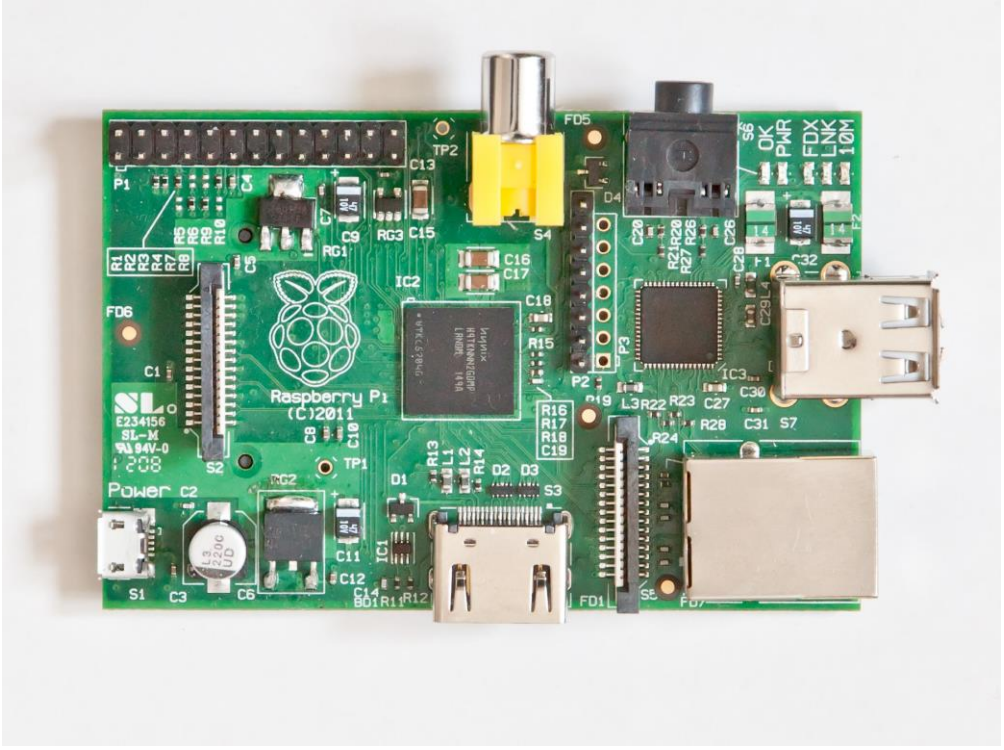
A projekt révén szoros munkakapcsolatban vagyunk az MTA X. és XI. Osztály Geonómiai Tudományos Bizottsága Meteoritikai és Planetológiai Albizottságával, valamint az ELTE Természettudományi Kar, Fizikai Intézet, Anyagfizika Tanszék, Kozmikus Anyagokat Vizsgáló Űrkutató Csoportjával.

IX. KONKLÚZIÓK, HOGYAN TOVÁBB?

A tapasztalat azt mutatja, hogy a HUNVEYOR projekt több mint egy évtizede folyik, és látványos sikereket tud felmutatni. Az oktatási

intézmények sajátossága azonban, hogy egy-egy diák csak viszonylag rövid ideig tud részt venni a munkában, tehát az építést hosszú távra kell tervezni. Idő közben a technikák és technológiák változnak és fejlődnek, ami az esetleg már meglevő részek újra tervezését vagy átstrukturálását vonhatja maga után. Tehát nem egy komplett, működő, befejezett űrszonda elkészítése a valódi cél, hanem maga az építési folyamat, annak ismeretszerzést, tanulást motiváló fenntartása. Ez a cél az elmúlt időszakban megvalósult, és remélhetően a jövőben is folytatódik. Eddig tíz diplomamunka és még több TDK dolgozat született a HUNVEYOR-4 építése kapcsán.

A jövőre nézve sem vagyunk fejlesztési tervek nélkül. A 12-es ábra tanúsága szerint a HUNVEYOR-4b eléggé zsúfolttá vált a sok, apránként fejlesztett modul hozzáadásával. A következő fejlesztési ciklusban egy robosztusabb megoldásra törekszünk. A technológia fejlődését követve a cél az, hogy áttérjünk Raspberry-PI alapú megoldásra, a HUNVEYOR-4c-re. Mivel ez a megoldás alapvetően különbözik a korábbitól, a feladatok bő tárházát nyújtja. A részletek ismertetése már túl messzire vezetne, de ebben a témában jelenleg két diplomamunka is készül.



18. ábra A Raspberry-PI

FORRÁSOK ÉS SZAKIRODALOM

A szerző alapvetően a HUNVEYOR-4 építése során felgyülemlett saját tapasztalatainak egy töredékét foglalta össze, és az általa vezetett projektről már számos publikációban beszámolt. Ezek felsorolásától e helyen eltekintek.

[1] SH atlasz, Űrtan, 13. o., szerkesztők: Almár I.-Both E.-Horváth A.-Szabó Gy., Springer Hungarica, Bp. 1966. ISBN 963 845582 9,

[2] Morocco 2013 Mars Analog Field Simulation, http://www.oewf.org/cms/mars2013.phtml

[3] MARS2013 Morocco Mars Analog Field Simulaton Recap, http://www.youtube.com/watch?v=VDfENbC_FOY

[4] This week on #simulateMars: MARS2013 Simulation Week 01, http://www.youtube.com/watch?v=kfRDkS9VRoQ

A részecskefizika rejtelmei

részecskék, gyorsítók, detektorok

Dr. Horváth Árpád
Óbudai Egyetem, Alba Regia Műszaki Kar
<horvath.arpad@amk.uni-obuda.hu>

I. BEVEZETÉS

Sötét és semmi voltak: én valék,
Kietlen, csendes, lény nem lakta Éj,
És a világot szültem gyermekűl.
Mindenható sugárral a világ
Fölkelt ölemből; megrázkódtatá
A semmiségnek pusztaságait,
S ezer fejekkel a nagy szörnyeteg,
A Mind, előállt. Hold és csillagok,
A menny csodái lőnek bujdosók
Kimérhetetlen léghatárokon.

Vörösmarty Mihály

Sok részecskét már rutinszerűen használunk. Ilyenek az elektronok, amelyek az elektromos készülékek, számítógépek működésében fontosak, vagy anti-részecskéje a pozitron, amelyet az orvoslásban használnak: a CT-berendezésekben.

Az anyagot alkotó részecskék világának leírásához a fizikusok *matematikai elméleteket* használnak. Ezeket az elméleteket igyekszem minél jobban szavakkal körülírni és hasonlatokkal szemléltetni, de érteni kell, hogy az elméletet a részecskerendszerek viselkedését leíró matematikai összefüggések alkotják. A mi agyunk a velünk közel azonos mérettartománybeli történéseken nevelkedett, fogalmai ebből a „hétköznapi világból" származnak. A részecskék világát a sokkal kisebb méretek és gyakran sokkal nagyobb sebességek jellemzik. Ez a világ a hétköznapi fogalomrendszerrel, közel sem írható le tökéletesen.

Akkor hogyan tudhatjuk meg, hogy egy fizikai elmélet helyes-e? Természetesen minden fizikai elméletben kell lennie olyan mennyiségeknek, amelyek mérhetőek. A *mérhető mennyiségek* esetén össze lehet vetni az elméletből kiszámolt értékeket a kísérletekben kapott eredményekkel. Ha ezek mindig egyeznek, akkor az elmélet jó.

A részecskék világában gyakran a mérés módja is eltér a hétköznapitól. A gyógyszerészek kétkarú mérlegen hasonlítják össze a tömegeket. Amennyiben a mérleg egyensúlyban van, a jobboldali serpenyőben lévő dolgok tömege megegyezik a baloldali serpenyőben lévőkével. Amennyiben az egyik oldalon levők össztömegét tudom, meg tudom mondani a másikakét is. Ez természetesen nem megy részecskék, mondjuk elektronok esetén. A tömegmérés eljárását módosítani lehet úgy, hogy a mérési eljárás más ugyan, de a mért érték minden esetben egyezzen, amikor mindkét eljárás használható. Így létrehozható olyan mérési eljárás, amellyel már az elektronok tömegét is megmérhetjük. Erre majd még visszatérek.

Ezekre a méréssel ellenőrizhető matematikai egyenletekre a fizikusoknak szükségük van ahhoz, hogy egy nyelvet beszéljenek, és az ismereteiket tömören tudják leírni.

A továbbiakban először a részecskék világának elméleti hátteréről és a megoldatlan rejtelmekről esik szó, azután arról, hogy milyen eszközök szükségesek ahhoz, hogy az elméletek igazolásához szükséges méréseket elvégezzük.

II. Rejtelmek, részecskék és kölcsönhatások

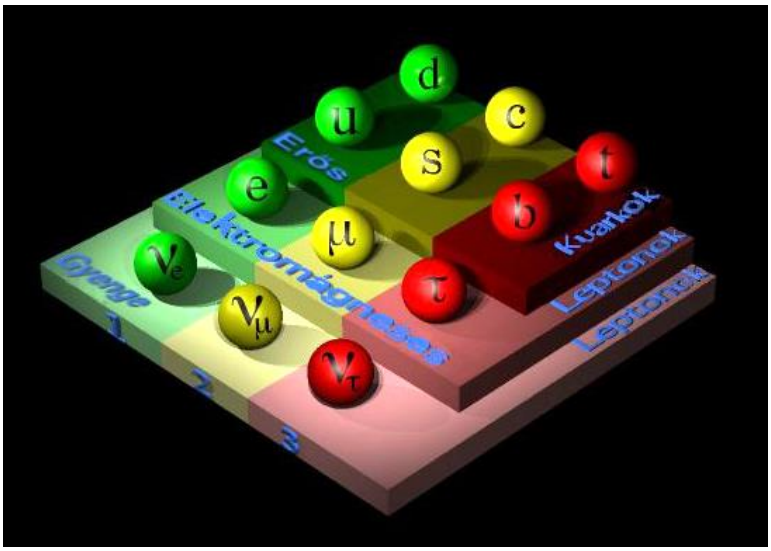
Előre vetítek pár rejtelmet példaként. A felsorolásban felbukkanó ismeretlen fogalmaktól ne ijedjünk meg, azokról hamarosan szó esik majd.

1. Miért van több részecske, mint antirészecske? ☹
2. Hogyan kapcsolódik a gravitáció a részecskefizikához? ☹
3. Miért ismétlődnek a részecskék, azaz miért alkotnak részecskecsaládokat? ☹
4. Hány részecskecsalád van? ☺

Egyelőre csak annyit vegyünk észre, hogy vannak olyan kérdések, amelyeket a jelenlegi elméletünkkel meg tudunk magyarázni, és olyanok is, amelyeket még nem. Az utóbbit szomorú fejecske jelöli az ábrán, a megoldott kérdést pedig vidám. Valójában annak, aki fizikusnak készül, megnyugtató lehet, hogy van még mit felfedeznie, annak a szomorú fejecskék jelenthetnek vigaszt.

Térjünk rá tehát a *részecskékre*. Már az ókori görögök felvetették, hogy a világ minden dolga valamilyen oszthatatlan részekből áll. Demokritosz ezeket atomoknak nevezte el, ami görögül oszthatatlant jelent. Mi ezek után a Demokritosz által elgondolt, oszthatatlan építőkövek után nyomozunk.

Amit mi *atomoknak* hívunk, arról később kiderült, hogy tovább oszthatóak. Az elektron „kering" valamilyen kis térrészre összezsúfolt pozitív töltésű rész, az *atommag* körül. Az atommagról szólt a Garai Géza Szabadegyetem egyik előadása. Abban szó esett arról, hogy neutronok és protonok alkotják az atommagot. Ezek a részecskék alapvető szerepet játszanak abban, hogy az atommag jelenségeit, és vele a Nap energiatermelését megértsük. A neutronról és a protonról is kiderült, hogy összetett részecskék. Az alkotórészeit *kvarkoknak* hívjuk.



1. ábra: Az anyag elemi részecskéi. Az egyes dobogók a kölcsönhatásokat jelképezik, amelyekben az egyes részecskék részt vesznek

Az eddig szereplő részecskék közül jelenleg a kvarkokat, az elektront és a pozitront oszthatatlan részecskéknek, más néven *elemi részecskéknek* gondoljuk. Az anyag részecskéinek elemi építőköveit az 1. ábrán láthatjuk. Az *elemi részecskék három családját* az ábrán egy-egy szám jelöli. Az első családban vannak az általunk eddig említett anyagok építőkövei. A protonok és neutronok, és így az atommag is u és d kvarkokból állnak. Az atommag körül kering az e-vel jelölt elektron. Az első családban láthatunk még egy részecskét, a neutrínót. Pontosabban a

három neutrínó közül azt, amelyik az elektronnal van szoros összefüggésben.

A második és harmadik család részecskéi hajdanán, midőn „ezer fejekkel a nagy szörnyeteg, A Mind, előállt", azaz az Ősrobbanást követő időszakban voltak nagy számban jelen. Ahogy a Világegyetem hűlt, a belőlük alkotott részecskék sorban elbomlottak olyanokká, amelyekben csak az első család részecskéi szerepelnek. A második és harmadik család egyébként teljesen olyan részecskékből áll mint az első, csak a benne szereplő részecskék tömege nagyobb. Az elektron nehezebb testvérei a μ-vel jelölt müon, és a τ-val jelölt tau-részecske. Ezeknek ugyanakkora az elektromos töltése, és a többi, később bemutatásra kerülő tulajdonsága, mint az elektronnak, csak a tömegük nehezebb. A többi sorban is, ahogy a nagyobb sorszámú család felé haladunk, egyre nagyobbak a tömegek, de az egyéb tulajdonságok nem változnak.

A táblázatban szereplő összes részecskét megfigyelték már. Felmerülhet a kérdés, hogy nem lehet több részecskecsalád? Nem, pontosan három van. Ezt kísérletileg határozták meg. Az ezután logikusan következő másik kérdésre viszont, hogy miért van három részecskecsalád, nem tudjuk a választ. Olyan mintha kaleidoszkópon keresztül látnánk a világot. Nem tudjuk, hogyan működik ez a kaleidoszkóp, mi játssza itt a tükrök szerepét.

De hol található a táblázatban az eleminek mondott pozitron? Az 1. ábrán tulajdonképpen minden gömb két részecskét jelöl. Minden itt látható gömbhöz tartozik egy részecske és egy *antirészecsk*e is. Az antirészecskék tömege, bomlásideje azonos a részecskéével, de a töltés jellegű mennyiségeik ellentétesek. Az egyes részecskék töltés jellegű mennyiségei láthatóak az 1. táblázatban. Az elektromos töltést az elemi töltésegység többszöröseként adjuk meg. Ez a töltés megfelel a proton töltésének. Érdekes módon a kvarkok nem egész töltéssel rendelkeznek.

1. táblázat: Az elemi részecskék tulajdonságai

Részecske	elektromos töltés (*e*)	bariontöltés	leptontöltés
u, c, t	2/3	1/3	0
d, s, b	−1/3	1/3	0
e^-,μ^-,τ^-	−1	0	1
ν_e,ν_μ,ν_τ	0	0	1

Az elektron és a pozitron megkülönböztetésére az e szimbólum fölött feltüntetjük a töltésüket. Az egyszeres elemi töltésű pozitron jele e^+, az elektroné, amely ellentétes töltésű e^-.

Egy részecske és egy antirészecske egymással találkozva megsemmisülnek, és sugárzás keletkezik.

Ha a protonban minden kvarkot antikvarkjára változtatok, az elektromos töltése is az ellentettjére változik. Ez az antiproton. Ha az antiproton köré pozitront helyezek, akkor olyat kapok, mint egy hidrogénatom, de pozitív elektronnal, és negatív atommaggal. Ilyet ténylegesen létrehoztak a kutatóintézetekben. Ezt nevezzük antihidrogénnek. Ugyanígy felépíthetem elméletben bármelyik antiatomot, létrehozhatok belőlük egy antielefántot, antibolygót, antigalaxist…

A korábban felsorolt rejtélyek között az első az, hogy miért nincs ugyanannyi antirészecske, mint részecske. Ha ugyanannyi lenne, akkor egymással találkozva megsemmisítették volna egymást, és nem lennének anyagi részecskék csak sugárzás. Vagy ha van anyag, akkor ugyanannyi antianyagnak is kellene lennie. Ha pedig nagyobb mennyiségű anyag és antianyag találkozik, akkor ott erős sugárzásnak kellene lennie, aminek a nyomát nem látjuk sehol. Az elméleteink szimmetrikusak a részecskékre és antirészecskékre nézve. Tehát azok szerint a Világegyetem keletkezésekor ugyanannyi részecskének és antirészecskének kellett volna keletkeznie. És ugyanolyan mértékben kellett volna fogyniuk, ahogy egymással találkoztak. Hogy milyen folyamat okozza azt, hogy több anyag maradt, mint antianyag, arra még nem válaszolt a tudomány.

Még nem beszéltünk a *kölcsönhatásokról*. Ezeket az 1. ábrán az egyes dobogók jelölik, amelyeken a részecskék találhatóak. A neutrínókra csak a *gyenge kölcsönhatás* hat. Ezért olyan kicsi a kölcsönhatásuk, hogy 100 neutrínóból mindössze nagyjából 50 nyelődne el, ha egy fényév vastagságú ólomfalon átbocsájtanánk.

Az összes elektromosan töltött részecskére hat az *elektromágneses kölcsönhatás*: a kvarkokra, az elektronokra és az elektron nehezebb testvéreire, beleértve ezek antirészecskéit is, például a pozitront. A mozgó töltött részecskék mozgásiránya eltérül a mágneses térben. Az *erős kölcsönhatás* csak a kvarkokra, és a belőlük felépített részecskékre, szakszóval *hadronokra*, hat. Emiatt van az, hogy az atommag nem esik szét, annak ellenére, hogy a benne lévő pozitív elektromos töltésű protonok taszítják egymást. Az erős kölcsönhatás ennek ellenére

összetartja az atommagot. A protonok ugyanis kvarkokból állnak, tehát közöttük is hat az erős kölcsönhatás.

A részecskefizika elméleti modellje, a *standard modell* ezeket a részecskéket foglalja egy elméleti keretbe. Ebben megtalálható a fenti három kölcsönhatás.

A standard modell szerint a kölcsönhatásokat is részecskék közvetítik. Mindegyik kölcsönhatáshoz egy vagy több részecske tartozik. Az 1. ábrán látható elemi részecskéken és a kölcsönhatások részecskéin kívül még egy részecskét tartalmaz a standard modell: a részecskék tömegéért felelős, rég megjósolt, és 2012-ben felfedezett Higgs-bozont, amelyért a 2014-as Nobel-díjat kiosztották azoknak, akik megjósolták.

A standard modell, olyan modell, amellyel a részecskék világában nagyon pontos jóslatokat tehetünk. Biztosan tudjuk, hogy mégsem teljes. Van ugyanis legalább három követelmény, amellyel minden elméletnek összhangban kell lennie:

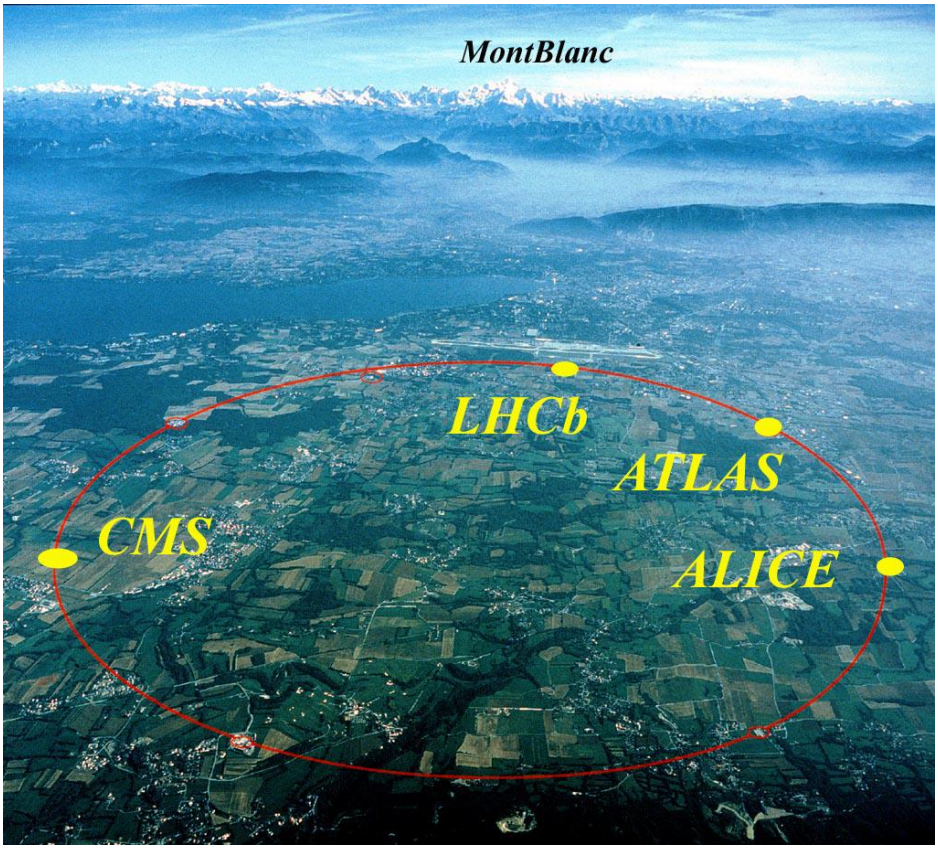
- relativitási elv: minden inerciarendszerben ugyanolyan egyenletek írják le a fizikai folyamatokat.
- kvantumosság: a részecskék hullámként viselkednek, nem határozható meg egyszerre tetszőleges pontossággal a helyük és a lendületük,
- van gravitáció: a tömeggel rendelkező testek vonzzák egymást.

A standard modell összhangban van az első kettővel, de a harmadikkal nem. Csak a már említett három kölcsönhatást tartalmazza, *a gravitációs kölcsönhatást* nem foglalja magában. Itt is van tehát teendőjük a fizikusoknak. A gravitációt is tartalmazó részecskefizikai modell megalkotása kemény diónak tűnik.

A fentiek közül a relativitási elvet önmagában sikerül összhangba hozni a gravitáció létezésével: ezt hívják általános relativitáselméletnek. Ez írja le, hogy a nagy tömegű testek közelében hogyan történnek a dolgok. De olyan elmélet, amely mindhárom követelménynek megfelel, még nincs.

III. KÍSÉRLETEK A RÉSZECSKEFIZIKÁBAN

A. A CERN és Genf



2 ábra: A CERN felülnézete. A nagy kör az LHC nevű gyorsítót jelöli, sárga felirattal a négy nagyobb kísérlet neveivel. Háttérben távolodva a genfi repülőtér, a Genfi tó csücske Genf városával és a Mont Blanc hegy látható

A részecskefizikai kísérletek összeállítása – főként annak magas technikai igényei, és magas költsége miatt – egyre inkább sok ország közös vállalkozásaként valósul meg. Az Európai Részecskefizikai Kutatóközpontot, a Genf mellett található CERN-t, a II. világháborút követő évtizedben hozták létre 12 európai ország részvételével. A tagság azóta további országokkal bővült, többnyire európaiakkal. Jelenleg 21 ország a tagja. A tagországokon kívül sok ország használja a CERN kísérleti eszközeit, akik a döntéshozatalba nem szólhatnak bele, hanem megfigyelő státuszban vannak (például USA, Japán, Oroszország), vagy másfajta kapcsolatban állnak a CERN-nel.

Magyarország 1992-ben csatlakozott hivatalosan, bár korábban is dolgoztak magyarok a CERN-ben.

Genf volt Kálvin János (1509–1564), a protestáns teológus életének legfontosabb tartózkodási helye, a reformáció egyik központja. A városban járva, a reformátorok falán megtalálhatjuk Bocskai István (1557–1606) szobrát is (3. ábra). Bocskai jelentős szerepet játszott a reformáció terjedésében, valamint a Habsburgok és a törökök közötti tizenöt éves háború lezárásában. A magyaroknak érdekes lehet, hogy a városban találhatunk Liszt Ferencről elnevezett teret is, és szobrot Erzsébet királynőről, azaz Sisiről is. Interneten rákeresve megtalálható, melyiküknek mi köze van Genfhez.

3.ábra: Bocskai a reformátorok falán

A továbbiakban a rövidség okán a kísérleti részecskefizikát a CERN példáján fogjuk bemutatni.

B. A részecskék gyorsítása és ütköztetése

A részecskék tulajdonságairól általában ütköztetésükkel tudhatunk meg többet. Minél nagyobb energiával ütköztetünk egymásnak részecskéket, annál nagyobb tömegű részecskéket is létre tudunk hozni, valamint annál finomabb részleteket tudunk tanulmányozni.

A részecskéket elektromos térrel tudjuk gyorsítani. A gyorsítók esetén az elért energiát nem is a középiskolában megszokott Joule egységben szokták mérni, hanem a gyorsító feszültségre utaló elektronvolt egységben. Egy elektron illetve proton, ha átjut 1000 Volt potenciálkülönbségen, akkor 1000 elektronvolt energiát nyer. Ezt a mennyiséget röviden 1 kiloelektronvoltnak nevezzük és 1 keV-vel

jelöljük. A most működő legnagyobb gyorsító a CERN-ben található LHC. Ebben 7 teraelektronvoltra (7 TeV) gyorsítanak fel protonokat, és azokat ütköztetik. A 7 TeV egység az 1 keV egység hétmilliárdszorosa.

A következő kérdésre adott válasz megvilágítja, hogy a részecskefizikában miért mindig energiát szoktunk megadni, miért nem sebességet.

Hányszor nagyobb a sebessége egy részecskének, ha 7 TeV az energiája, mintha 1 TeV lenne? A részecskék sebessége ebben az esetben fénysebesség közelében található, de azt természetesen soha nem éri el. Ebben az esetben már nem alkalmazható a kis sebességek esetén nagyon jó közelítést adó klasszikus mozgásienergia-képlet, az

$$E_{mozg} = \frac{1}{2}mv^2$$

Aszerint ugyanis a sebesség a hétszeres energianövekedés hatására $\sqrt{7} \approx 2{,}65$ szorosára változna. Itt már a speciális relativitáselmélet képleteit kell használni. Ennek a részleteit most nem tárgyalom. Nézzük meg, hogy mekkora a proton sebessége ilyen nagy energiákon.

1 TeV esetén	0,99999956c
7 TeV esetén	0,999999991c

Itt a sebességet a fénysebesség (c) többszörösében adtuk meg, ahol a szorzószám majdnem egy. A nagyobb energián természetesen a sebesség is nagyobb, de a százalékos növekedés jelentősen kisebb, mint a klasszikus képletből adódó több mint két és félszeres növekedés. Hogyan lehet egyáltalán ekkora energiára felgyorsítani? Hogyan tudunk 7 000 000 000 000 Volt feszültséget előállítani a gyorsításukra? A válasz az, hogy sehogyan, de ez nem is szükséges. A gyorsítás során körpályára tereljük a protonokat, és így képesek vagyunk minden körbefutás során viszonylag kicsit gyorsítva nagyon nagy energiára felgyorsítani azokat.

Ezeket a körkörös gyorsítókat *szinkrotronoknak* nevezzük. A CERN 27 kilométer kerületű szinkrotrona, a Nagy hadronütköztető gyűrű, angol rövidítésével LHC helyét a 2. ábrán piros kör jelöli. Ez a gyorsító valójában a földfelszín alatt található átlagosan nagyjából 100 méter mélyen. Ebben egymással szemben keringetnek sok-sok protont tartalmazó protoncsomagokat, és a gyorsító bizonyos helyein, a detektorokban összeütköztetik azokat. Ezek a detektorok nagy méretűek. A *CMS detektor*, amellyel több magyar fizikus is dolgozik, nagyjából kétszer annyi acélt tartalmaz, mint az Eiffel-torony. Az ütköztetés eredménye szanaszét repülő sokféle részecske lesz, amelyet a detektorok

„lefényképeznek”. De ez a felvétel a szétrepülő részecskék pontos útvonalát és leadott energiáját rögzíti, és nem csak síkban, hanem térben. Ezekből az adatokból hámozza ki a részecskefizikus kifinomult matematikai módszerekkel, hogy hogyan hat kölcsön a proton a protonnal. Sok ütközés vizsgálatából az is kideríthető volt, hogy létezik a Higgs-bozon.

Egy-egy ilyen óriási detektor egyben egy-egy kísérletet is jelent. Ezekben a kísérletekben sok száz fizikus vesz részt. Egyesek a detektorok építéséhez értenek jól, mások az ütközési folyamatokban lezajló fizikai jelenségekhez, illetve a mérési adatok kiértékeléséhez.

IV. Az adatok tárolása

A CMS kísérletben másodpercenként 40 millió proton-proton ütközés történik. Minden egyes ütközés után az elektronika eldönti, hogy az ütközés megjegyzésre érdemes-e. Amennyiben igen, akkor minden mért adatot tárol.

A rengeteg adat feldolgozására nem elegendő a CERN-ben megtalálható – amúgy elég komoly – számítógépes kapacitás. Az adatok feldolgozása a világszerte elhelyezkedő kutatóintézetek számítógépein zajlik. Ehhez a számítógépeket egy egész földre kiterjedő rendszerré kapcsolják össze. Az ilyen rendszereket nevezzük GRID-nek. A CERN GRID-je, az *LHC Computing GRID*, számos számítógépet és tárolóeszközt foglal magában.

A feldolgozandó adatoknak mindegyik helyen rendelkezésre kell állni. Az adatok tárolását adatközpontok szolgálják. A adatközpontok rendszere hierarchikusan épül fel. Van, ahol az összes adat rendelkezésre áll, van ahol csak egy-egy detektor által létrehozott adatok. 2013 óta Magyarországon, a Magyar Tudományos Akadémia Wigner Fizikai Kutatóközpontjában található a CERN legfelsőbb szintű adatközpontja.

V. Összefoglalás

A részecskefizikai kutatások az anyag legalapvetőbb építőköveinek tulajdonságait és kölcsönhatásait tárják fel. Egyáltalán nem befejezett tudomány, számos érdekes kérdés vár még megválaszolásra. A vizsgálatokhoz nagy méretű kísérleti berendezések és fejlett informatikai háttér szükséges, ezek megvalósításához pedig általában több állam összefogása. Magyarországnak méretéhez mérten komoly szerepe van a kutatásokban és az informatikai háttér biztosításában.

IRODALOM

A részecskefizikáról számos magyar és más nyelvű könyv, folyóirat, internetes oldal hozzáférhető. Az angolul tudók a CERN oldalán számos információt találnak közérthető formában is. Különösen az ATLAS és a CMS detektorok/kísérletek oldalait ajánlom.

[1] http://cern.ch

A fizika, de különösen a részecskefizika történetét ismerhetik meg az alábbi könyvből, amit egy Nobel-díjas fizikus írt:

[2] Leon Lederman, Dick Teresi: Az isteni a-tom, Mi a kérdés, ha a válasz a Világegyetem?, TypoTeX Kiadó, Budapest, 2010

Különösen középiskolások figyelmébe ajánlom a Részecskefizikai diákműhelyeket, amelyeken minden tavasszal 11-12-dikes diákok ismerkedhetnek a részecskefizikával. Mind a budapesti, mind a székesfehérvári helyszín oldala további hasznos információkat tartalmaz.

[3]http://www.rmki.kfki.hu/~jancso/Reszecskefizikai_Diakmuhely_RMKI
[4]http://arekold.amk.uni-obuda.hu/diakmuhely

A MÚLTBAN GYÖKEREZŐ JELEN
200 éve született Ybl Miklós 1814-1891

Dr. Lakner József c. egyetemi tanár
Óbudai Egyetem Alba Regia Műszaki Kar, Székesfehérvár
lakner.jozsef@arek.uni-obuda.hu

Absztrakt: **A cikk elemzi azt a politikai-társadalmi hátteret, amely meghatározó volt a 19. század második felének művészeti életére. Foglalkozik annak két legfontosabb művészeti irányzatával, a romantikával és a historizmussal, elsősorban azok építészeti vonatkozásaival, ezen belül is Ybl Miklósnak, mint a historizmus legnagyobb alakjának tevékenységével. Ismerteti a család székesfehérvári kötődéseit, a művész kapcsolatait a várossal és a megyével, valamint legfontosabb művein keresztül a kor művészetében betöltött szerepét. Befejezésképpen említést tesz napjainkra gyakorolt hatásáról, emlékének megőrzéséről.**

I. BEVEZETÉS: A KORSZAK

A korszak a 19. század, annak is inkább a második fele. A század a francia forradalom bukásával kezdődött, amely társadalmi visszarendeződést nagyfokú kiábrándultságot és a múlt felé fordulást eredményezett. Első fele a polgári demokratikus forradalmak és a modern nemzetállamok kialakulásának, míg az azt követő a második ipari forradalom korszaka volt. Társadalmi átrendeződés eredményeképpen a polgárság vezető szerephez jutott. A századra leginkább jellemző társadalmi mozgalom a liberalizmus és a nacionalizmus, míg a meghatározó szellemi és művészeti irányzat pedig a (nemzeti) *romantika* és a *realizmus* (az építészetben a *historizmus*).

Magyarországon a 19. század első fele a reformkor és a szabadságharc időszaka, míg a második felét a kiegyezés és az azt követő robbanásszerű gazdasági és társadalmi változások jellemezték, melynek eredményeképpen megszületett a magyar nemzet.

II. A ROMANTIKA

A romantika, mint művészeti irányzat, korban nehezen definiálható, a 18. század végétől a 19. század utolsó harmadáig, végéig tartott. Együtt élt

különböző irányzatokkal, kezdetben a késő barokkal és a rokokóval, majd a klasszicizmussal és a biedermeierrel, végül a realista és egyéb (historizmus) irányzatokkal. Magyarországon a reformkortól a 19. század végéig tartott.

A klasszikus kor újjáélesztésének egyik fontos irányzata a klasszicizmus volt. Mellette megnőtt az érdeklődés a közelebbi múlt, a középkor irányába, amely kiterjedt nemcsak az időbeli, hanem a térbeli távolságra is, nevezetesen a keleti kultúrákra, a Kelet építészetére. Romantika két jellegzetes főiránya bontakozott ki: a középkor építészetét, elsősorban az (angol) gótikát felelevenítő és a keletről ösztönzést merítő romantikus stílus.

A másik forrása a polgári társadalmak születésével együtt kifejlődő nemzeti tudat, amely felszította a népek saját történelmi múltja iránt az érdeklődést, ezért a romantika sok esetben nemzeti jelleget öltött *(nemzeti romantika)*.

Harmadik forrása a csalódás a felvilágosodás eszméit megtagadó forradalomban (és annak eszméiben), az emberek elvesztették a felvilágosodás optimizmusát, jellemző volt az illúzióvesztés, a kiábrándultság és a múltba fordulás.

A romantika a vele egy tőről sarjadó *klasszicizmus* ellenáramlata. Az általános érvényűvel szemben (klasszicizmus) a különlegest, az egyszerit, a sajátost és az egyedien természeteset hangsúlyozza. Jellemzője a művészi szubjektivitás, az irracionális, a misztikus és a transzcendentális iránti fogékonyság, elvágyódás a múltba és egzotikumba (kelet), a végletekben való gondolkodás, mint a jó-rossz, angyali-ördögi, világos-sötét ellentétje.

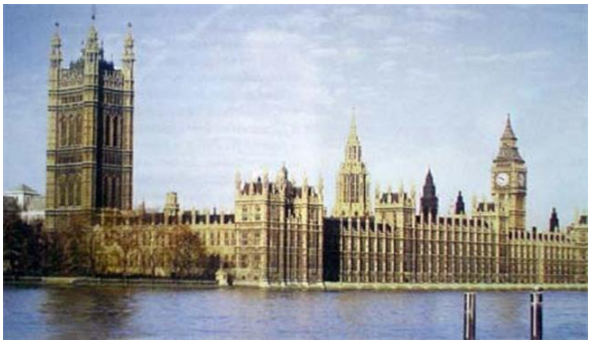
1. ábra. Géricault: Medúza tutaja

Inkább szellemi áramlat, ezért legtisztábban a festészetben (irodalomban) bontakozott ki (Goya, Delacroix, Turner). Ábrázolásukban a barokkhoz közelítenek: újra megjelenik az átlós elrendezés, a színesség, és a világos-sötét kontraszt (Géricault: Medúza tutaja)

III. A ROMANTIKA AZ ÉPÍTÉSZETBEN

Tulajdonképpen egységes romantikus stílusról nem beszélhetünk. Ami jellemzi, az a klasszicizmussal való szembehelyezkedés, a középkor építészeti elemeinek (román, bizánci, mór és az iszlám) felélesztése, felhasználása. Kezdetben klasszicista alapon szerveződött, a korai romantikára jellemző a klasszicista elrendezés romantikus elemek (félköríves, bélletes ablakok, pártázatok, függőleges osztáselemek, úgymint lizéniák, rizalítok, díszítő motívumok, stb.) felhasználásával bővült.

Az egyik irányzat a középkori építészet, elsősorban az (angol) gótika felelevenítése (London Parlament). Jellemzője a mérművek, a csúcsívek, bástyaszerű tornyok, a vertikális mellett egy horizontális tagoltság, a pártázat megjelenése. Többen ezt az irányzatot nem is a romantikához, hanem, mint első *neostílust*, a historizmushoz sorolják.



2. ábra. London Parlament

A másik irányzat a kelet építészetének, arab iszlám, mór (zsinagógaépítészet) stíluselemek beemelése (Ludvig Förster: Dohány utcai zsinagóga 1859).

A magyar építészetben 1840–1870 között jelenlévő, meghatározó stílusirányzat. Kronológiailag átmenetet képez a klasszicista építészet és a historizmus között. Mindhárom említett irányzat megtalálható: a korai romantika (pl. Ybl Mikós: Unger ház), a középkori építészet (Ybl: Fóti templom), benne az angol gótika (Brein Ferenc: Csősztorony,) és keleti hatás (a már említett Dohány utcai zsinagóga). Magyarországon ezen felül a politikai körülmények, illetve, elsősorban Feszl Frigyes (Pesti Vigadó) munkásságának köszönhetően, a romantika

3. ábra. Feszl Frigyes: Pesti Vigadó

nemzeti jelleget is öltött. A román és keleti mellett bőven tartalmaz magyar elemeket is.

IV. HISTORIZMUS

A *historizmus* (történetiség) az elmúlt korok stílusainak utánzása, újraélesztése a művészetben. Mint művészettörténeti korszak a 19. század második felében, elsősorban az építészetben jelentkezett.

A historizmus a romantikában gyökerezik. Az első neostílus, a neogótika még a romantikához tartozik. Az építészek, ahogy egyre újabb és újabb utakat kerestek, felelevenítették a reneszánsz, a román és a barokk stíluselemeit. A korai szakaszára a konkrét példák felhasználása (copywrite) és a stílustisztaság jellemző, majd a későbbiekben a stíluselemek már keveredtek (*eklektika*).

Maga a historizmus, ellentétben a festészet párhuzamos irányzataival (Barbizoni iskola, impresszionizmus), nem nevezhető progresszívnek. Ennek oka egyrészt az építészet sajátosságaiban (nehezebben mozdul, beruházás igényes, megrendelői elvárások, stb.), másrészt a közízlésben keresendők. A polgárság ugyan megszerezte a gazdasági és részben a politikai hatalmat, ízléskultúrája azonban még nem alakult ki, másolta a korábbiakat (arisztokrácia). A paradigmaváltáshoz általában három generáció kell, amely 60-80 évet jelenthet. Ez megfelel annak, hogy a polgárság saját (építészeti) kultúrája csak később alakult ki (szecesszió, a 20. század eleje, de leginkább a konstruktívizmus, a Bauhaus, a 30-as évek).

A historizmus Magyarországon a romantikával nagyjából párhuzamosan, az 1860-as évek elején jelentkezett. Az 1870-es évektől a fővárosi középületeknél gyakorlatilag a *neoreneszánsz* az „elvárt” stílus (Operaház), majd az 1880-as évektől a neogótika és a *neobarokk*, legkésőbb pedig a neoromán.

4. ábra. Ybl Miklós: Operaház

Az 1890-es évektől Magyarországon is jelentkező szecesszió együtt élt annak kései szakaszával. Az I. világháború után új erőre kapott, és egészen az 1940-es

évekig meghatározó volt, elsősorban az állami és az egyházi megbízók körében. A II. világháborút követően teljesen eltűnt? (Szocialista realizmus!).

V. HOGYAN KERÜL A KÉPBE YBL MIKLÓS?

Részletes elemzés helyett néhány újságcikket és egyéb forrást idéznék:

- Ybl Miklós a 19. század egyik legnagyobb magyar mestere, a historizmus európai jelentőségű képviselője (*Wikipédia*).
- Ybl Miklós építész, G. Semper és Ch. Garnier mellett a neoreneszánsz leghívatottabb képviselője (*Művészeti lexikon*).
- Ybl Miklósnak elismert erős oldala az, hogy műveiben a szépség mellett a gyakorlati célszerűség kívánalmaknak is mindenkor eleget tenni iparkodik, s tekintetbe veszi mindig a kor és a helyzet igényeit (*Vasárnapi Újság, 1865. március 26*).
- Ybl Miklós nevét nemcsak a Budán emelt szobor hirdeti, hanem maga Budapest is. Mert, hogy a régi Pestből, a szerény keleti városkából a mi dédelgetett Budapestünk lett, …abban a mi földinknek számottevő szerepe van. S tudnivaló, hogy a kerek Európában is kevés Budapesthez fogható város van… (*Székesfehérvár és Vidéke 1914. április 4*).

VI. AZ YBL CSALÁD

5. ábra. Kosteneuburg látképe

6. ábra. Ybl Miklós Márton az építész nagyapja

Az építész dédapja Jenő Vilmos a németországi Klosteneuburgban született, 1743-ban már pesti polgárként jegyezték.

Fia Miklós Márton 1746-ban Pesten született, de 1776-ban már Székesfehérvári polgár, a helyi Kereskedő Társaság tagja. Felesége Braun Mária.

Kisebbik fiúk Miklós, az építész apja, szintén kereskedő, a megyei választmány tagja, aktív közéleti ember. Felesége Eimann Anna.

7. ábra. Ybl Miklós szüleinek a sírja a székesfehérvári Csutora temetőben

Középső fiúk Miklós az építész, két fiútestvére volt. A család ezen ága Ybl fiával, Félixszel kihalt. Apja bátyjának unokája volt Ybl Ervin, a neves művészettörténész, aki az Ybl hagyatékot Székesfehérvárnak adományozta. A szülőknek több ingatlana is volt a városban, a szülőház a Fazekas (a mai Ybl Miklós) utcában állt, de az Ybl lakótelep építése során sajnálatos módon elbontásra került.

VII. YBL MIKLÓS ÉLETRAJZA

8. ábra. Ybl Miklós keresztelési anyakönyve

9. ábra. Marastoni Jakab festménye

1814-ben született Székesfehérváron. 1825-től a párizsi Császári és Királyi Polytechnikai Intézetben végezte tanulmányait.

1832-től Pollack Mihály, majd 1836-tól Koch Henrik építész irodájában dolgozott. 1840-ben Münchenbe ment, beiratkozott a Bajor Királyi Művészeti Akadémiára.

1841-ben Itáliában tett tanulmányutat. Hazatérésekor szembesült azzal a ténnyel,

hogy családjának anyagi gondjai vannak, ezért Pesten próbált szerencsét, ahol Helybeli Polgári Szabadalmas Építő Czéh Mesterei 1843-ban kebelbeli kőműves mesterré fogadták. 1841. Pollack Mihály fiával, Ágostonnal megnyitotta az Építészeti Intézetet.

1845-ben megbízást kapott Károlyi Istvántól, fóti kastélyának átépítésére, valamint a templom tervezésére. Károlyi uradalmi építésze lett.

1851-ben költözött vissza Pestre, feleségül vette Lafite Ida nevelőnőt.

1860-tól több fontos épület tervezett Pesten: Nemzeti Lovarda, Képviselőház (Ferenc József-rend lovagkereszt), Fővámház, stb.

1864-ben megszületett fia, Félix. 1873-ban az Operaház megtervezésére és az építésének irányítására, a Várkert Bazár megvalósítására kapott megbízást. Belépett a Közmunkatanácsba, 1882-ben megkapta a Lipót-rend lovagkeresztjét, 1885. június 21-én pedig a király a főrendiház tagjává nevezte ki.

10. ábra. Sírja a Kerepesi temetőben

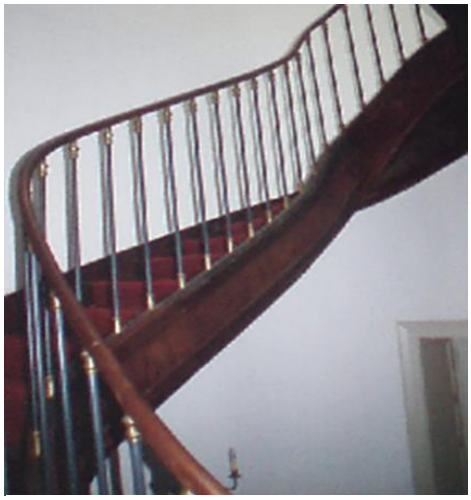
Folytatta a Hild József által tervezett Szent István bazilika építését is, majd a budai Vár újjáépítésén is dolgozott. Ezt a művét már nem tudta befejezni.

1891. január 22-én elhunyt.

VIII. KORAI MUNKÁK, FÓTI Ttemplom


11. ábra. A Fóti templom

Károlyi István 1844-ben határozta el és 1845-ben kérte fel Ybl Miklóst, hogy számára Fóton családi sírboltot és plébániatemplomot tervezzen. A templom 1855-ben lett kész. Formára angol gótikus stílus, de részleteiben román és bőven alkalmaz keleti elemeket is. Maga a templom kettős templom: az



12. ábra. A Fehérvárcsurgói kastély cselédlépcsője

alsó családi sírbolt, a felső a plébániatemplom.

Mint a Károlyi család főépítésze, a család megbízásából számos egyéb munkát is elvégzett. Közéjük tartozott a fóti- és a füzérradványi kastély átépítése, a fehérvárcsurgói kastély (kivitelező építész) cselédlépcsője, amit bizonyíthatóan ő tervezett.

Igen népszerű lett főúri körökben, számos kastély átépítésével (Lovasberény Cziráki, Várpalota Valdstein, Ikervár Batthyányi kastély), illetve tervezésével (Gerla Werkheim, Fegyvernek Szapáry kastély, stb.) bízták meg. Munkái igen változatosak, sok esetben alkalmazkodott a megrendelői igényekhez. Mindig magas színvonalon oldotta meg a feladatát (Károlyi kastély, Parádsasvár 1880-82), számára nem létezett kis és nagy feladat.

Polgári építkezései közül az Unger-ház (1852), Ybl első bérháza, a fóti templommal párhuzamosan épült a korai romantika minden jellegzetességét (klasszicista elrendezés, félköríves romanizáló bélletes ablakok, pártázat, függőleges lizéniák (oszlopnak kiképezve) magán viseli.

13. ábra. Székesfehérvár Zichy liget 4

További említésre méltó munkái e korai korszakából a Nemzeti lovarda, 1857-58 és a Balassa ház 1858.

Székesfehérváron négy épület van, a Zichy liget 4 és a Vörösmarty tér 6, 8, és 10, melyeknek a tervezésében, esetleg a kivitelezésében Ybl (valószínűleg) részt vett. Ezek 1860 körül épült kora romantikus lakóházak, a korai romantika minden említett jellegzetességeivel (ablakok rizalítok, stb.).

IX. A RENESZÁNSZ BŰVÖLETÉBEN

Ybl 1860-tól a neoreneszánsz felé fordult. A század utolsó harmadában a középületeknél ez volt a divatos irányzat Európa szerte. Első munkái a Budai Takarékpénztár (1860-62), és a Giest ház (1862), sajnos mindkettő lebontásra került .

1862-től a Nemzeti Múzeum körül egy palotanegyed kezdett kiépülni, mivel az arisztokrácia körében sikknek számított, hogy Bécs mellett Pesten is legyen palotájuk. Ebben a munkában Ybl is tevékenyen részt vett, az általa tervezett és fennmaradt épületek, a Dégenfeld és a Festetics paloták (1862), elsősorban az itáliai reneszánsz stíluslegyeit viselik magukon. Az Európa hírű palotanegyed épületei szintén részben lebontásra, részben átalakításra kerültek.

14. ábra. Dégenfeld palota

Az említett palotanegyed és Ybl egyik legkiemelkedőbb épülete Károlyi Lajos palotája (1863). Az egyemeletes, szabadon álló épület szokatlan, egyedülálló alkotás a XIX. századi magyar építészet történetében. Jellegzetes olasz reneszánsz kocsifelhajtója felett, sarkain egy francia reneszánsz kastély magas, keskeny, hasáb formájú tetőidomaival hangsúlyozott szint emelkedik. A sarokrizalitok ikerablakaiban merev tartású kariatidák állnak. A csaknem dísztelen - egyszerű ablakokkal ellátott - falfelületeket finom, de látványos építészeti elemek tagolják; nevezetesen a magas tetőidomok és ablakaik, a címer, a ballusztrád, stb.

15. ábra. Károlyi Lajos palotája

16. ábra. A Fővámpalota épülete

Középületei közül a Fővámpalota (a mai Közgázként ismert, 1870-74) a legfontosabb. Szerkezete, elrendezése is különleges, hosszoldali homlokzatból kiemelkedő középprizalitból és a sarkokon hozzákapcsolt két sarokpavilonból áll. A részletek itáliai, tömegalkotása és tagolása bécsi mintát követ. Az ünnepélyes külsőhöz hasonló belső tér társul (díszudvar, előcsarnok díszlépcső). A homlokzat erkélyeit szimbolikus alakok díszítik, a dunait antik istenek, vasút, gőzhajózás, festészet és szobrászat szimbólumai, az északit az erény allegóriák, a délit pedig magyar ősfoglalkozások alakjai. A két tér felé eső homlokzatokra a világtájakat jelképező domborművek kerültek.

A következő jelentősebb munkája a Várkert bazár, 1875-1883 épült neoreneszánsz stílusban, a Várkert Duna felőli lezárásaként. Eredetileg kereskedelmi funkciót töltött be, árkádsorai egykor üzletekkel voltak tele, 1895-ig a Történeti Arcképcsarnoknak, 1884-től műtermeknek (Stróbl Alajos) adott otthont. A II. világháború alatt súlyosan megrongálódott. 1961-84 között a Budai Ifjúsági Park működött benne. 2011-ben kezdődött a felújítás és a napokban fejeződött be. Az Ybl Miklós tervei szerint épült komplexumból 8988m^2 nagyságú épületegyüttest újítottak fel, a mélygarázzsal együtt 17722m^2 új területet építettek hozzá, 8734m^2 kertet és udvart alakítottak ki. Visszakapta eredeti funkcióját, összeköttetést teremt a Dunapart és a Vár között (mozgólépcső).

17. ábra. A Várkert bazár

1847 óta a Nemzeti Színház adott otthont a zenés drámai műfajnak. Az 1867-es kiegyezést követően, a város gyors fejlődése miatt egyre szűkebbnek bizonyult feladatai ellátására. 1872-ben létrejött az a bizottság, amely a felépítendő operaház helyét volt hivatva kijelölni. 1873-ban a belügyminiszter versenytárgyalást írt ki az épület megépítésére, ezt Ybl Miklós nyerte meg. Az építkezés 1875-től 1884-ig tartott. A Magyar Királyi Operaház ünnepélyes megnyitására szeptember 27-én került sor Ferenc József jelenlétében.

18. ábra. Az Operaház előcsarnoka

Palladio nyomán kialakított főhomlokzat a belső terei és főleg lépcsőháza a korabeli európai építészet kimagasló értékei.

A homlokzatot ballusztrádos főpárkány koronázza, tizenhat zeneszerző mészkő szobrával. A kocsifelhajtó két oldalán két zeneszerző, Erkel Ferenc és Liszt Ferenc nagyméretű szobrai (Stróbl Alajos) láthatók.

Az Operaház belső falfestéseinek megvalósításával Than Mórt és Lotz Károlyt bízták meg, akik a bécsi Staatoper mintájára átfogó programot gondoltak ki, amelynek központi mondanivalója a zene apotheozisa (többek között a nézőtér mennyezeti képe), allegorikus és filozófiai jelentéstartalma azonban sokkal átfogóbb és kigondoltabb, mint a példaképé (díszlépcső, nézőtér). További munkák Székely Bertalan (Székely Bertalan-terem, előcsarnok kilenc múzsa).

X. KÉSŐI MUNKÁK

A 19. sz. elején felmerült az igény, hogy a Lipótvárosnak saját plébániatemploma legyen. 1845-ben Hild József kapott megbízást a tervek elkészítésére, a klasszicista templom építése 1851-ben kezdődött. Hild 1867-ben bekövetkezett haláláig vezette a munkálatokat. Anyag- és kivitelezési hibák miatt a félig kész épület 1868-ban összeomlott, eltakarítás 1871-ig tartott.

19. ábra. A Bazilika (Lipótvárosi plébániatemplom)

Az építési tervek átdolgozására és a munkálatok vezetésére Ybl Miklóst kérték fel, aki neoreneszánsz stílusban dolgozta át a terveket és 1891-es haláláig ellátta a művezetői feladatokat. A díszítőmunkálatok és az épület belső végleges kialakítása 1905-re készült el Kauser József vezetésével.

Neoreneszánsz templom kevés van. A templomok kedvelt stílusa ebben a korban a neoromán és neogót voltak (ilyen stílusban készültek az újjáépítések is, Mátyás templom, pécsi székesegyház, stb.). Ybl is épített hasonlót, a Bakács-téri templom (1867-1879), Assisi Szent Ferenc tiszteletére (francia neoromán).

A Bazilika rendkívül gazdag képzőművészeti alkotásokban is. Az előcsarnokban Senyei Károly Szent István-domborműve, Székely Bertalan és Than Mór mozaikjai találhatók. A szentély fölötti kupola képeit (Úristen, Krisztus, próféták és evangélisták) Lotz Károly festette. A szentélyboltozat mozaikjai, a szentmise allegóriái Benczúr Gyula, valamint Szent István élete bronz domborműsorozat Mayer Ede munkái. A főoltár, szószék Kauser Józseftől való, a főoltár Szent István szobra Stróbl Alajos, oltárképe Benczúr Gyula, üvegablakok Roth Miksa művei. A templom orgonája pedig a korban elismert pécsi Angster József gyárának terméke.

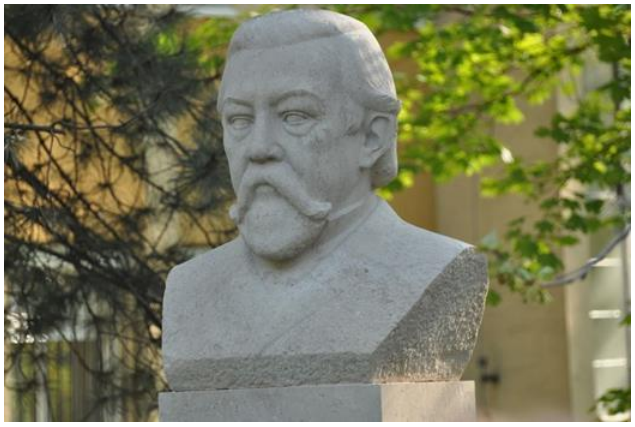
20. ábra. A Bakács-téri templom

Utolsó jelentősebb munkája a Királyi palota átépítése. A középkori palota (Zsigmond és Mátyás) a török idők alatt elpusztult. A még részben épen maradt épületeket elbontották, majd a romokra felépítették az első, kisméretű palotát. Az új, un. Mária-Terézia palota 1760 táján készült el. Kezdetben az Angol-kisasszonyok székháza, majd 1779-1789 között a Nagyszombatról Budára költözött egyetem otthona. Ezt követően a nádori

21. ábra. A Királyi palota Ybl Miklós által épített szárnya

család lakja.

A palota átépítését 1886 körül, előbb Ybl Miklós, majd halála után Hauszman Alajos tervei alapján kezdték el. Ybl eredeti terveiből a Krisztinavárosi-szárny (ma az OSZK) valósult meg.



22. ábra. Ybl Miklós székesfehérvári mellszobra

Hauszman a Mária Terézia-szárny tömegét megduplázta, a Duna felé eső homlokzatra, új neobarokk kupolát tervezett. Kisebb változtatásokkal, de az egész épületegyüttesen lemásolta a Mária Terézia-szárny homlokzati struktúráját. Az átépítés 1905-re készült el.

A II. világháború során súlyosan megrongálódott. Néhány részt lebontottak, a többit a 60-as években indokolatlan mértékben átépítették. A neobarokk belső teljesen eltűnt. Okok? A középkori részek bemutatása, az eklektika lebecsülése.

XI. Összefoglalás. Ybl Miklós jelentősége és emléke

A 19. század második fele volt az a kor, amikor Pest és még néhány vidéki nagyváros jelenlegi városképe kialakult. A magyar építőművészet

(a történelme során másodszor) szinkronba került az európaival és színvonalban is elérte azt.

Ybl kétségtelenül a legnagyobb magyar építész, közvetlen és közvetett hatása a kor művészetére, építészetére vitán felüli. Európai mércével is mérve a kor egyik legnagyobb építésze, a neoreneszánsz mestere, ezt a stílus irányzatot senki sem művelte olyan magas szinten, mint ő.

Tiszteletére alapították 1953-ban az évenként kiosztott építészeti Ybl Miklós Díjat. Szegeden, a Nemzeti Emlékcsarnokban őrzik portréját. Róla nevezték el a 2002-ben magyar csillagászok által felfedezett kisbolygót. 2014. január 22-én, halálának évfordulóján kezdődött Ybl-emlékév.

Szent István Egyetem Ybl Miklós Építészettudományi Kara viseli nevét. A Magyar Nemzeti Bank 2014-ben emlékérmet bocsátott ki.

Szülővárosa, Székesfehérvár is őrzi emlékét. Több iskolát is elneveztek róla, 1920-tól Ybl Miklós Főreáliskolát, majd Ybl Miklós Gimnázium és Ybl Általános Iskolát. Szülőháza helyén Ybl-lakótelep áll, szobrával. Unokaöccse, Ybl Ervin művészettörténész, Székesfehérvárnak ajándékozta a család gyűjteményét, amely a város egyik legpatinásabb épületében a Budenz házban nyert elhelyezést.

IRODALOM:

[1] Halász Csilla, Örfi József és Viczián Zsófia: *Ybl összes* (52 város 113 épület). Látóhatár Kiadó, Budapest 2014

[2] Lyka Károly: *Közönség és művészet a századvégen* (Magyar művészet 1867-1896). Corvina Kiadó, Budapest, 1982

[3] Lyka Károly: *Nemzeti romantika* (Magyar művészet 1850-1867). Corvina Kiadó, Budapest, 1982

[4] *Művészeti lexikon*. Akadémiai Kiadó, Budapest, 1965

[5] Ybl Ervin: Ybl Miklós, Budapest, 1956

[6]"YBL MIKLÓS építész – SZÉKESFEHÉRVÁR szülötte" című kiállítás a Fő utcán 2014 (nem publikált anyag)

Édesvizek ökológiájáról informatikus szemmel

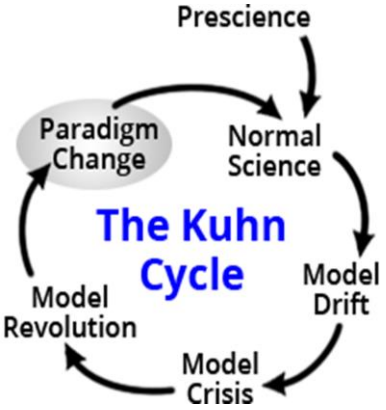
Milyen következtetésekre juthatunk tudományos adatbázisok felhasználásával?

Dr. Hajnal Éva
Óbudai Egyetem, Alba Regia Műszaki Kar (OE-AMK) Székesfehérvár,
hajnal.eva@amk.uni-obuda.hu

***Abstract*—Az írás bemutatja az ökológia alapkérdéseit, és az édesvízi ökológia néhány példáján keresztül érzékeltetni próbálja, hogy a tudomány az informatika eszközeit és lehetőségeit felhasználva milyen válaszokat adhat ezekre a kérdésekre. Miként használhatunk fel tudományos adatbázist a Balaton vízminőségének hosszú távú értékelésére, és hogyan állapítható meg adatbázisok segítségével egy élőhely, egy nagyobb régió, vagy esetleg az egész bioszféra fajgazdagsága.**

I. BEVEZETÉS

Jelen írásomban néhány példán szeretném bemutatni, hogy két tudományág, jelesül az informatika és az ökológia együttműködése milyen csodálatos új utakat és lehetőségeket teremt a felfedező elme számára. Mottóul választottam Phillip von Jolly elhíresült mondását: *"In this field, almost everything is already discovered, and all that remains is to fill a few unimportant holes."* Ő ezt (Ezen a területen már mindent felfedeztek, néhány lényegtelen hézag betömése van csak hátra) Max Plank-nak mondta 1878-ban arra a kérdésre, hogy érdemes-e elméleti fizikával foglalkozni. Véleménye teljesen tévesnek bizonyult, hiszen ez után jött még Einstein, a kvantumfizika, a részecskegyorsítók stb. Persze a tudomány változásában vannak nyugalmasabb, látszólag statikus időszakok - ezt az 1. ábrán a „normal science" és „model drift" részen látjuk - amelyeket egy modell krízis és modellváltás követ. Ezen időszakok a külső szemlélőnek rendkívül dinamikusnak, sok új felfedezéssel tarkítottnak tűnnek. A modell krízis és a modell váltás nagyon gyakran következménye egy



1. ábra
A tudomány kialakulása és fejlődése Kuhn tudományfilozófiai megközelítése szerint

alkalmazott új szemlélet, vagy technika alkalmazásának. A biológiában ilyen szemléletváltást hozott a matematikai statisztika módszereinek az alkalmazása, és mivel a biológiai mérések rendszerint igen nagy adattömeget szolgáltatnak, a következő lépés az adatbázisok és az informatikai módszerek felhasználása volt. Az ökológia elsősorban az egyed feletti szerveződési szintek, a populációk, társulások és az egész bioszféra, mint rendszer tudománya, így alapkérdései is ezeket a szerveződési szinteket érintik.

- Hány élőlény, hány faj van egy adott helyen, területen vagy a Földön? Mi ennek az oka és a következménye?
- Az egyes fajok populációi mekkorák, milyen a térbeli, időbeli változásuk? Mi ennek az oka és a következménye?

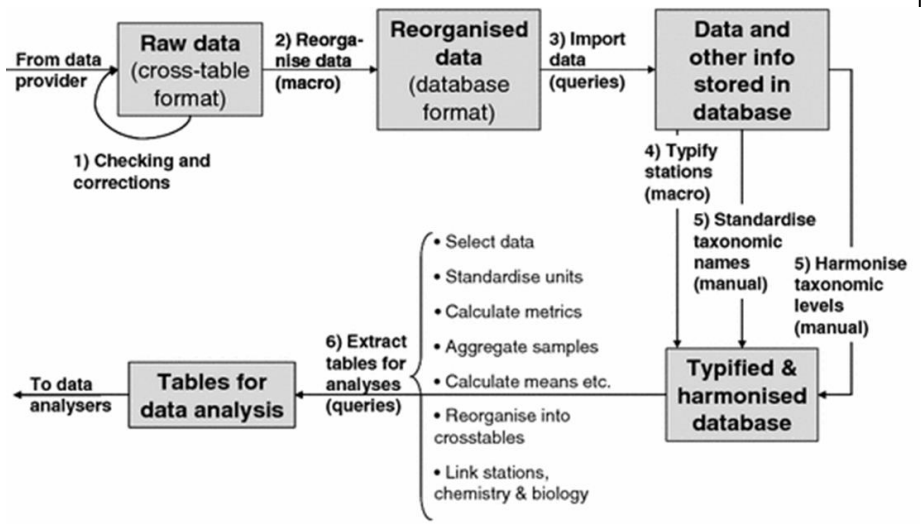
Az ökológiával határos alkalmazott tudomány a környezettudomány, mely mindezek gyakorlati vonatkozásait elemzi; alapkérdései:

- Milyen az egyes élőhelyek minősége, ökológiai értéke?
- Hogyan mérhetők, tarthatók meg, javíthatók ezek a jellemzők?

A jelen írásban 1-1 ökológiával és környezettudománnyal kapcsolatos problémakört mutatok be, közös jellemzőjük, hogy a vizsgálatukat nem lehetséges egy jól megtervezett tudományos adatbázis felhasználása nélkül megvalósítani.

II. TUDOMÁNYOS ADATBÁZISOK

Melyek a jellemzői egy tudományos adatbázisnak? Alapvetően persze ugyanazok, amelyek egy gondosan megtervezett egyéb adatbázisra is jellemzőek. Az általam ismert biológiai tudományos adatbázisok mindegyike relációs adatmodellen alapuló, normalizált adatbázis. Az üzleti alkalmazásoktól megkülönbözteti az adattárház jelleg, ami több vonásban is megmutatkozik. Az adatok sokszor különböző forrásokból származnak, nem egységes formátumúak, aminek az oka a mérőeszközök, mérési módszerek és a mérést végző személyek különbözősége. Az adatok időbélyeggel ellátottak. Jellemzően nemcsak az aktuális adatok tárolása a követelmény, hanem a témában felhalmozott tudás tárolását kell szem előtt tartani, mégpedig formájában és tartalmában is konzisztens módon, a szerzői jogokat és az adatok összehasonlíthatóságát kiemelt fontosságú szempontként kezelve. Így a tudományos adatbázisok tervezése és megvalósítása nem tekinthető rutin adatbázis kezelési feladatnak, mindenképpen önmagában is tudományos tevékenység, mely során (lásd 2. ábra) igen sok szakértői döntést kell meghozni, és az



2. ábra
A REBECCA nevű, európai tavakat érintő édesvízi ökológiai tárgyú tudományos adatbázis elkészítésének folyamata. Az adatokat jellemzően valamilyen táblázatkezelő alkalmazásból gyűjtik be, ezt követően történik az adatok átstrukturálása, és az adatbázisban történő tárolás. Ezután jórészt szakértői munkával történik meg az adatharmonizáció, ami ebben az esetben jelenti a nevezéktan egységesítését, és az adatok mérési pontosságának összehangolását. Az adatok vizsgálata, lekérdezése szintén nem egyszerű jelentéskészítéssel történik, hiszen szakértői döntést igényel a vizsgálatokba bevonható adatok kijelölése.

adatokkal kapcsolatos műveleteket legfeljebb fél-automatikus módon lehet elvégezni.

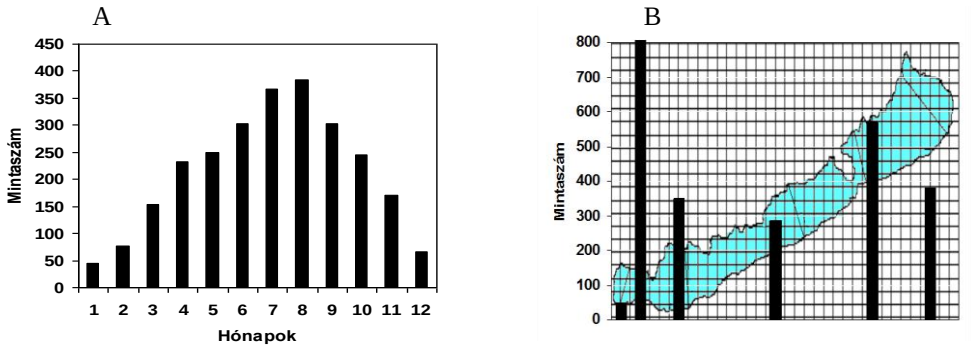
Néhány további kiragadott példa tudományos adatbázisokra, kiemelten az édesvízi ökológia témakörét érintve:

2005: Ecosurv Phare Project

Az Európai Unió vízzel kapcsolatos törvényét, a Víz Keretirányelvet 2000-ben szavazták meg. Ennek végrehajtásához nagymennyiségű tudományos vizsgálatra volt szükség. Erre indult ez a projekt, mely nem egyszerűen adatbázis építés, hanem állapot felmérés, ökológiai és releváns hidromorfológiai, fiziko-kémiai adatok gyűjtése volt minden magyarországi víztípusra, a Víz Keretirányelv (a későbbiekben VKI) szerinti 5 élőlénycsoportra (fitoplankton – vízben lebegő algák, fitobentosz – víz alatti kövek, növények élőbevonata, vízinövények, gerinctelen állatok, halak). Ezen belül fontos lépés volt a mintavételi helyek kijelölése (Magyarországon összesen 400 db, melyből 354 folyó, 46 tó) egy új szempontrendszer alapján. A korábbi monitoring-rendszerben kevésbé vizsgált kis- és közepes méretű vízfolyások, és a javasolt referencia-helyek, nemzetközi interkalibrációs helyek, a Natura 2000-es és Nemzeti Biomonitoring Rendszer (NbmR) helyek kerültek bele a vizsgálatba.

Almobal adatbázis

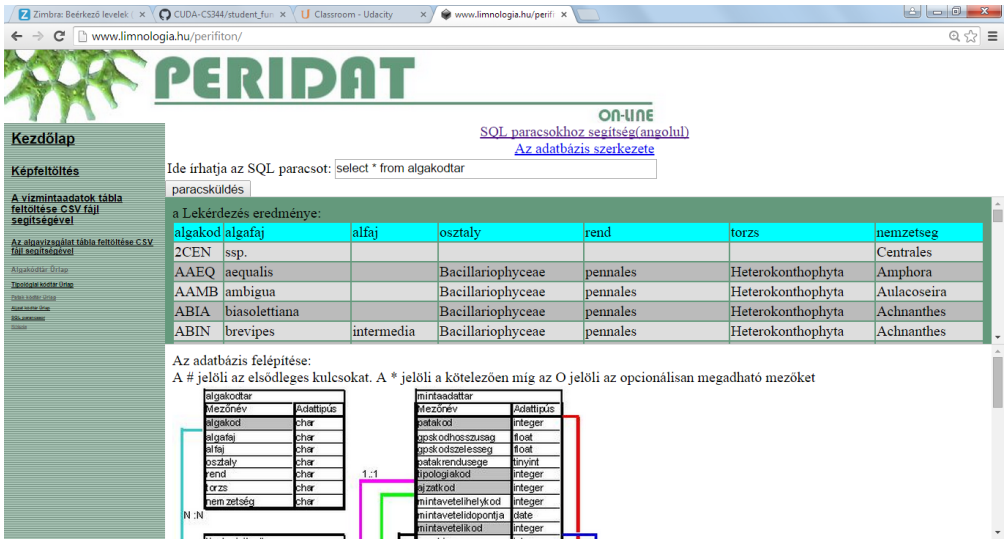
A szerző által elkészített tudományos igényű Balatoni fitoplankton adatbázis, amely történeti adatokat (papír alapú a Balatoni Limnológiai Kutatóintézet évkönyvei alapján 1933-1970 között 212 vízminta), a Pannon Egyetem Limnológia Tanszék jegyzőkönyveiben tárolt adatokat (elektronikus formában 1987-2006 között 1336 vízminta), a Dunántúli Környezetvédelmi Felügyelőség jegyzőkönyveiben tárolt adatokat (1980-1994 között 933 vízminta digitalizálva) és a Közép-Dunántúli Vízügyi Igazgatóság adatait tartalmazza (1998-2003 között 307 vízminta részben elektronikusan feldolgozva). Összességében az adatbázis 825 algafaj 77 179 adatrekordját tartalmazza az 1933 és 2006 közötti időszakból (3. ábra).



3. ábra
Az Almobal adatbázis adatsorainak hónapok (A) és mintavételi helyek (B) szerinti megoszlása. Egy vízmintában gyakran 80-100 algafaj is megtalálható. A szabványos módszer szerint 400 egyed meghatározása jelenti egy vízminta kiértékelését, így ebben az adatbázisban több tízezer órányi szakértői tevékenység eredménye van tárolva.

Peridat adatbázis

A szerző által készített on-line adatbázis vízfolyások adatainak tárolására, amely elsősorban közép-dunántúli patakok kovaalga flórájáról tartalmaz adatokat, vízkémiai és fizikai paraméterekkel kiegészítve (4. ábra). Az adatbázis tartalmaz adatokat a Torna-patak vörösiszap-katasztrófa előtti állapotáról, így a katasztrófa utáni regeneráció értékelésénél felhasználható.



4. ábra
A Peridat on-line adatbázis képernyőképe.

REBECCA adatbázis

Tudományos igényű adatbázis, amely az Európai Unió vízzel kapcsolatos törvényének, a Víz Keretirányelvnek a bevezetését próbálta tudományosan alátámasztani (2. ábra). Ehhez 5 000 tó különböző kémiai, fizikai, ökológiai adatait gyűjtötték össze 20 európai országból. A cél: Összefüggés keresés a kémiai stresszorok és az ökológiai válaszok között, a vizek tipizálása és a referencia állapot meghatározása volt. Az adatbázis tervezésnél különös gondot fordítottak az adatharmonizációra és a szerzői jogok tiszteletben tartására. Az adatok a szerző tulajdonjogát képezik. Ha a szerző elérhetővé teszi saját adatait, cserébe rendelkezhet a többi szerzőével is.

III. BALATON VÍZMINŐSÉGÉNEK HOSSZÚ TÁVÚ ELEMZÉSE A VÍZBEN LEBEGŐ ALGÁK ALAPJÁN

Magyarországon a Balaton vízminősége nemcsak nemzetgazdasági ügy, hanem turisztikai és természetvédelmi kérdés is, de mondhatjuk, hogy közügy, hiszen szinte mindenki érintett a kérdésben, és majdnem mindenki úgy gondolja, hogy ért is hozzá legalább egy kicsit. A Balaton tehát nemzeti kincsünk, és ez nemcsak szubjektív tény, hanem valóban a tó jellemzőit tekintve a világon egyedülálló. Kora 18-22 ezer évre becsülhető, felülete kereken 600 km^2, hossza 78 km, átlagos szélessége 7,7 km, átlagos mélysége 3,3 m, ami azt jelenti, hogy Közép-Európa egyik legnagyobb kiterjedésű tava, amely rendkívül sekély, így folyamatosan ki

van téve stresszhatásoknak (hőmérséklete viszonylag dinamikusan változik, vize folyamatosan átkeveredhet). Vize Ca-karbonátos, Mg-karbonátos, ami szintén eltér a tőlünk nyugatra és keletre található nagyobb tavakétól (5. ábra).

5. ábra
A Balaton vízgyűjtője (*forrás: MTA BLKI honlap*)

Kevesen tudják azt is, hogy a Balaton, mint a világon az egyik legrégebben és legalaposabban kutatott tó, rendkívüli tudományos értéket képvisel.

A tavak kutatásának tudománya, a limnológia körülbelül a XIX. század végétől datálható, mert 1892-1904 között jelent meg François-Alphonse Forel Genfi tóról írt monográfiája. Ebben tette közzé Forel a tudománnyal kapcsolatos alapdefiníciókat, de leírta a tavak hőrétegződését (legalul található egy 4°c-os réteg) és ennek néhány következményét is. Nem sokkal ezután - mondhatjuk, hogy szinte egyidőben - kezdte el Lóczy Lajos a Balaton tudományos vizsgálatát, első megfigyeléseit 1897-től tette közzé; ekkortól kezdve beszélhetünk a Balaton tudományos kutatásáról. A Balaton tanulmányozására 1925-től egy tudományos társaság is alakult, amely Klebelsberg Kunó minisztersége alatt reprezentatív, és jól használható kutatóintézetet kapott Tihanyban, a Balaton partján, ami a mai napig folyamatosan működve segíti a tókutatást. Így az 1930-as évektől kezdődően folyamatos adatsorok állnak a rendelkezésünkre, melyek szinte kiáltanak azért, hogy adatbázisba rendezzük őket, és statisztikai módszerekkel próbáljuk feldolgozni.

A következő, szinte filozofikus kérdés, hogy mit jelent a jó vízminőség? Elsőre egy laikusnak nem tűnhet nehéznek a kérdés, de ez csak addig van így, amíg nem kezdünk el gondolkodni a tartalmán. Jó. Mire is jó? Nyilván mást tart jónak a földművelő, a horgász, a fürdőző, vagyis a jó vagy rossz minőség függ a vízhasználattól. Sokkal értelmesebb, és objektívebb a víz állapotának jellemzőiről beszélni. Azonban, ha az igazságérzetünk megszólal, és önös érdekeinktől egy pillanatra eltekintünk, akkor érezzük, hogy biztosan lehet egy objektív mércét is találni a minőségre, amely valamiképpen azzal függ össze, hogy az ember mennyire változtatta meg

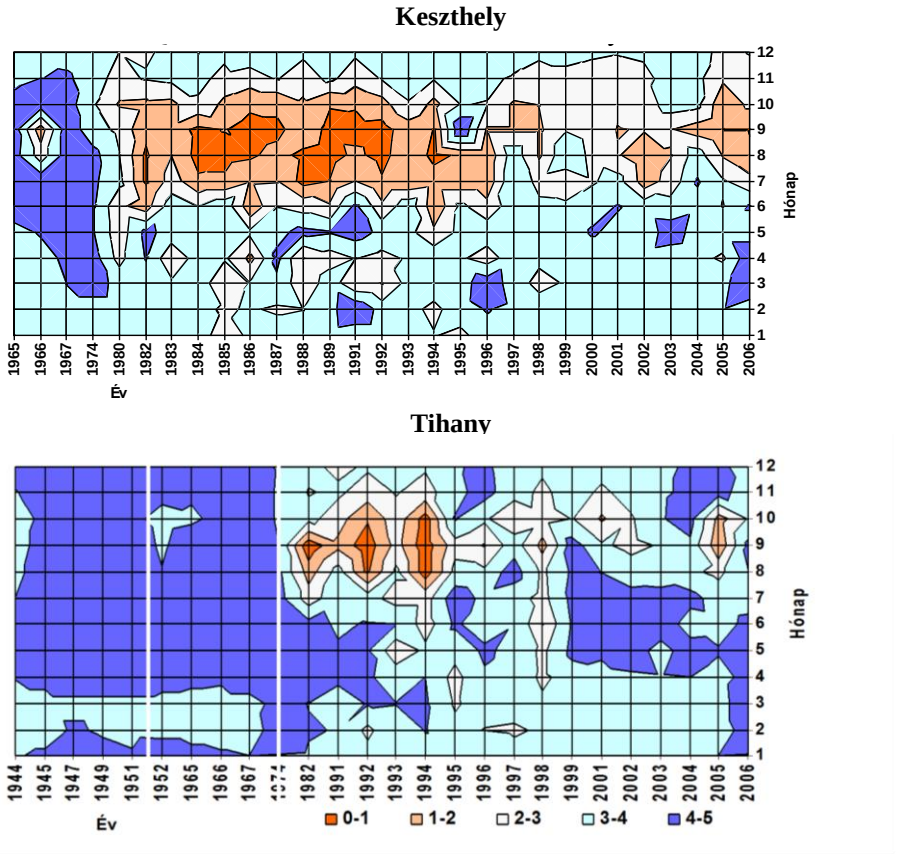
az adott vizet a tevékenységei során. És érezzük, hogy a legkevesebb bajt a bioszférában akkor okozhatjuk, hogyha a lehető legkisebb mértékben avatkozunk bele a természet folyamataiba. A természettudomány csodálatos eredményei ellenére is elmondhatjuk, hogy egy sor tevékenység következményét még nem tudjuk felmérni. Ezt a gondolatot az Európai Unió a Víz Keretirányelv nevű törvényben a következőképpen fogalmazta meg.

"A víz más termékektől eltérően nem kereskedelmi termék, hanem örökség, amit ennek megfelelően kell óvni, védeni és kezelni..."

Gyakorlati megoldásként pedig azt javasolták, hogy a vizeket típusokba kell sorolni, és ezután a vízminőséget az adott víztípus referenciaállapotához kell viszonyítani. Gyakorlati stratégiaként megfogalmazták, hogy az Európai Unió tagállamaiban 2015-ig jó állapotba kell hozni minden olyan felszíni és felszín alatti vizet, amelyek esetén ez egyáltalán lehetséges, és fenntarthatóvá kell tenni a jó állapotot. Az állapot meghatározáshoz pedig fizikai és kémiai paraméterek mérésén túl egy új elemet vezettek be. Alapelvként alkalmazták a biológiai indikáció jelenségét. Vagyis egy élőhely megfelelő állapotát, illetve annak megváltozását leggyakrabban a releváns élőlényfajok mennyiségének megváltozása jelzi, ilyen módon a közvetlenül nem mért jellemzőkről, és a tó globális állapotáról is lehet információt kapni. Az ökológiai állapot indikátorszervezetei a halak, makrogerinctelenek, makrofita, fitoplankton, fitobentosz. A Balaton esetében a nehéz kérdés a referencia állapot kijelölése, hiszen mint az előzőekben ismertettem, egyedülálló víztípusról van szó, így a referencia más tó nem lehet, csak a Balaton történeti adataiból lehet egy referencia-állapotot megfogalmazni. Szerencsére az adatok a rendelkezésre állnak. A feladat pedig a hosszú távú adatsorok értékelése. A következőkben a fitoplankton (vízben lebegő algák) alapú vizsgálatokat fogom bemutatni. A fitoplankton, mivel növény, a víz tápanyagait hasznosítva a levegő CO_2 felhasználásával, a napfény segítségével tudja életfolyamatait fenntartani,

6. ábra
Ceratium hirundinella, magyarul fecskemoszat a Balaton jellegzetes algafaja.

vagyis általánosságban a víz tápanyagtartalmáról, trofitásáról ad információt. A fitoplankton alapú értékeléshez lett bevezetve az ökológiai állapotindex, amely a víz fitoplankton összetétele alapján képlet segítségével számítható mennyiség, értéke 1 és 5 közötti szám (5 kiváló… 1 rossz vízminőség).



7. ábra
Az ökológiai állapotindex értékei évek és hónapok szerint Keszthelynél és Tihanynál. $Q = \sum_{i=1}^{N} p_i F_i$

Pi: az i. faj vagy az i. funkcionális csoport részesedése az összbiomasszából
N: fajok, vagy funkcionális csoportok száma
Fi: az i. funkcionális csoport vízminőségi besorolása (1..5)

Nézzük tehát az ökológiai állapotindex változásait hosszú távon, a tó keleti (Tihany) és nyugati medencéjében (Keszthely) a 7. ábra alapján!

Megállapíthatjuk, hogy a 40-es 60-as években lényegesen jobb volt a vízminőség, mint az azt követő időszakban. A tó kutatói ugyan már a 40-es években jelezték a tó romló vízminőségét, ez azonban a 70-es évekre vált mindenki számára evidenciává, és ekkortól kezdődött el a vízminőséget javító intézkedések megtervezése.

Az is látható, hogy a nyugati medencében lényegesen gyengébb volt a víz minősége, mint a keleti medencében, aminek két alapvető oka van. A Zala-folyó, ami a Balaton nyugati medencéjébe torkollik, hozza be a tó tápanyagterhelésének jelentős részét, a Balaton Tihanynál a legmélyebb, és ennek következtében a leghidegebb is, ami szintén kedvez a vízminőségnek.

Általában a 8-9. hónap a legrosszabb vízminőség szempontjából, aminek a közhiedelemmel ellentétben nem a megnövekedett fürdőzés, és emberi terhelés az oka, hanem a magasabb hőmérséklet kedvez az életfolyamatoknak, és így az algák is gyorsabban tudnak ilyenkor szaporodni. Meg kell említeni, hogy a nyári melegebb vízben el tudnak szaporodni olyan fonalas kékalgák is, amelyeknek a jelenléte ökológiai szempontból nem kedvező, ráadásul ezek a Balaton eredeti algaflórájából hiányzó jövevény fajok. A 6-7. hónapban általában már eléggé magas a vízhőmérséklet, de még nem állt rendelkezésre elegendő idő az algafajok elszaporodásához, így ilyenkor megfigyelhető egy „tisztavíz" fázis.

1980-as évektől kezdődően történtek intézkedések a vízminőség helyreállítására. Ide sorolható a Kis-Balaton Vízvédelmi Rendszer első ütemének átadása, Zalaegerszeg szennyvíztisztító telepének fejlesztése, a Balaton-körcsatorna átadása; ezek mind a Balaton tápanyagterhelésének csökkentését célozták. Az 1980-as években azonban ennek ellenére a víz minősége tovább romlott, ugyanis az üledékben felhalmozódott nagymennyiségű tápanyag hatása még évekig érezhető volt, több alkalommal figyeltek meg jelentős algaszaporulatot a vízben, ez az ún. vízvirágzás jelensége, amelyet legutoljára 1994-ben tapasztalhattunk.

A vízminőség a 90-es évek második felétől kezdett észrevehetően javulni, mostanra a 60-as 70-es évekre jellemző állapot visszaállt.

Az aszályos években (2002-2004) a vízszint csökkenése ellenére sem romlott a víz minősége.

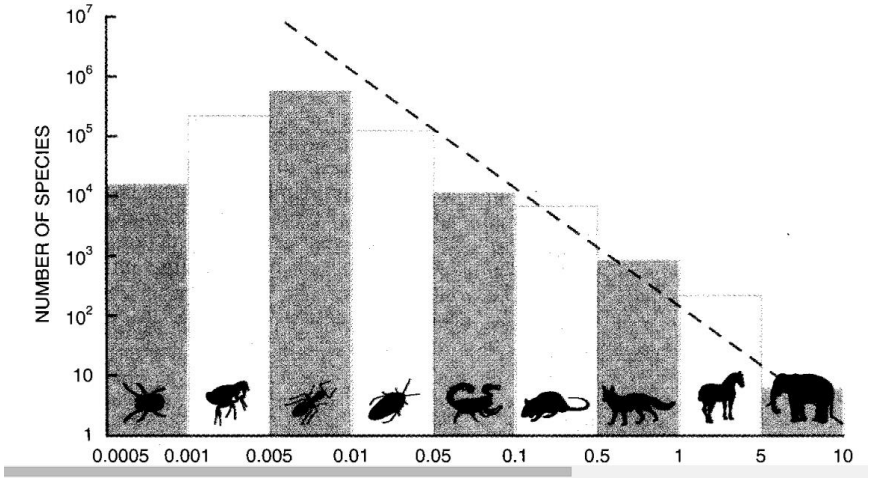
IV. HÁNY ÉLŐLÉNYFAJ ÉL A FÖLDÖN?

8. ábra
Az okapi (őserdei zsiráf) felfedezése 1900-ig váratott magára (*forrás: wikipedia.org/wiki/Okapi*)

Második fontos és érdekes kérdésem az élővilág sokféleségével függ össze, hiszen mindannyian csodálkozunk az elénk táruló gazdagságon. Ezek után már egy óvodás gyerek szintjén is fel lehet tenni a kérdést, hogy hány állatfaj él egy erdőben, vagy hányféle hal egy tóban. A tudós ugyanezt az érdekes kérdést kissé bonyolultabban is megfogalmazhatja: Hányféle fajt lehet egy habitát adott aszpektusában megfigyelni? Mekkora a bioszféra fajgazdagsága és ez történetileg hogyan változott? Itt már tekintetbe vesszük az időbeli és a térbeli léptékek változását, és felismerjük a rendszerekben rejlő dinamikát is, de ez a lényegen nem sokat változtat. A következő fontos kérdés, hogy a fajok vajon egyforma fontosak-e, vagy vannak fontosabbak és kevésbé fontosak, avagy a fajok hány százaléka fontos? Különösebb gond nélkül tolerálja-e a bioszféra a fajok egy, két vagy öt százalékának kipusztulását? Sajnos ugyanaz a helyzet ebben az esetben is, mint annyiszor a tudományban, hogy bonyolult kérdésekre tudunk válaszolni, és sokszor a legegyszerűbb alapkérdésekre nem, vagy csak részben. Ebben a tekintetben sincsen bizonyosságunk. Hasonlíthatjuk az élőlények szerepét a bioszférában a repülőgép szegecseihez. Ha a repülőgép szárnyában egy vagy kettő megsérül, abból még nem lesz baleset, de van egy határ, amit nem szabad átlépni. Más kutatók inkább úgy gondolják, hogy az élőlényfajok olyan szerepet tölthetnek be, mint az autón a lökhárító. Ha nincs lökhárítója egy autónak, az eléggé csúnya látvány, de a normál közlekedésben nem különösebben zavaró tényező. Azonban karambolnál már életeket menthet. Az élőlények sokfélesége egyfajta védőmechanizmust biztosít a környezet megváltozása esetére. Mégpedig oly módon, hogy ebben minden egyes élőlényfaj speciális szereppel bír, így bármelyik hiánya az adott életközösségre nézve végzetes lehet. Természetesen ez két szélsőséges álláspont, és a valóság biztosan a kettő között van valahol. De hogy pontosan hol, azt csak alapos kutatások után lehet megválaszolni. Pedig a kérdés égető, hiszen tudjuk, hogy naponta több száz fajt veszítünk el a bioszférából, mielőtt még egyáltalán megismertük volna ezeket. Hiba

az is, ha azt gondoljuk, hogy a fontosabb élőlényfajokat már biztos megtaláltuk, hiszen még a XX. században is találtunk olyan új fajokat, mint például az okapi (8. ábra), más néven őserdei zsiráf, de az 1990-es évek esőerdő kutatásai nyomán sikerült leírni több új emberszabású majomfajt is. Egyes kutatók a legnagyobb ökológiai katasztrófának az élőlényfajok kipusztulását tartják, sokkal nagyobb súlyúnak, mint egy-egy tengeri olajfúrótornyot, vagy tankhajót érintő katasztrófát vagy akár a cunamival együtt járó földrengést, ezek ugyanis lokális katasztrófák, míg az első a bioszféra egészét érinti.

Akkor tehát hány faj él a Földön? Ezt a kérdést tudományosan Linné vizsgálta először. Ő volt az, aki a rendszertan mai napig használatos ún. kettős nevezéktanát bevezette, és elkezdett ilyen típusú tudományos neveket adni az akkor ismert élőlényfajoknak. Könyvében Linné (1758) ~9000 növény- és állatfajt említ. Ez a szám dinamikusan növekedett, és napjainkra az írott és elektronikus forrásokban ~1,5 millió a leírt fajok száma. Természetes kérdés, hogy hányat nem találtunk meg eddig. Döbbenetes nagy a szám, a legszerényebb becslések szerint is 3 millió a



9. ábra
A testméret és a fajszám között összefüggés van. Mindkét mennyiséget logaritmikus tengelyen ábrázolva egy egyenessel köthetjük össze a mért értékeket. (forrás: *May, R. M. 1988. How many species are there on earth? Science 247: 1441-49.*)

fajok száma Raven (1983), mert a véleménye szerint a trópusokon kétszer annyi faj él, mint a mérsékelt övben.

Általános szakmai konszenzus szerint a Földön 10 és 50 millió között lehet az élőlényfajok száma, és eszerint legjobb esetben is a fajoknak csak 10 százalékát ismerjük még!

Milyen gondolatmenettel lehet mindezt megbecsülni? May (1988) azt a megfigyelést vette alapul, hogy kisebb élőlényekből többféle van, mint nagyokból. A mért értékeket grafikonon ábrázolta. Ezután meghúzva a legnagyobb és legkisebb élőlény mérethatárát, kiszámíthatjuk a görbe alatti területet. Becslése a testméret-abundancia összefüggés alapján 5 – 10 millió fajt adott ki úgy, hogy az alsó határt a baktériumok testméreténél húzta meg, azok már nem kerülhettek bele ebbe a becslésbe.

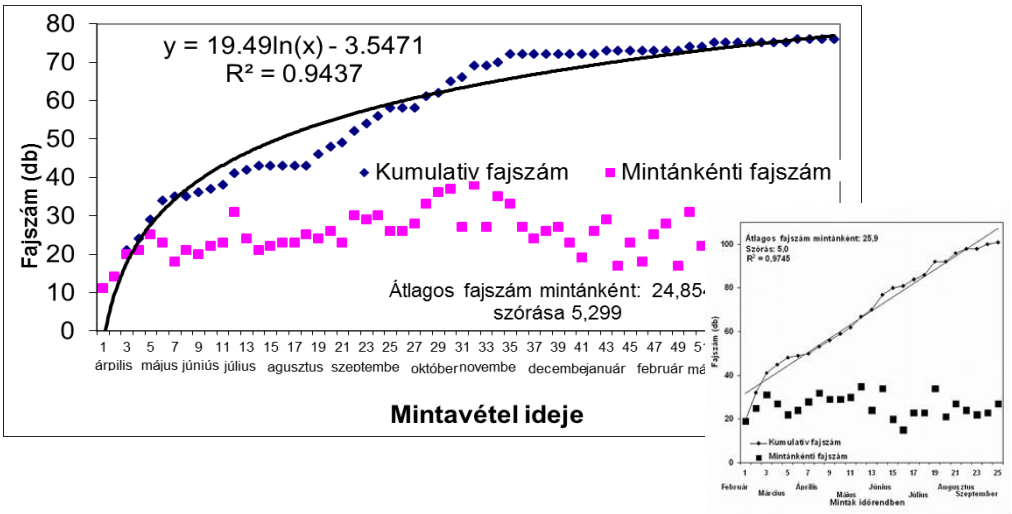
A kutató munkáját szakmai tudása sokszor behatárolja. Vannak tudósok, akik a pókok, mások a rágcsálók stb. szakértői, vannak olyan élőlénycsoportok, amelyeknek nincs jelenleg specialistája az egész világon, így ezen a területen egyáltalán nem halad előre a rendszertani kutatás. Erwin (1982) saját szakértelmét figyelembe vette az élőlényfajok számának megbecslésekor. Ő a bogarak specialistája volt, és egy kiterjedt kutatás segítségével egyetlen egy fáról (természetesen néhány ismétléssel) összegyűjtötte az összes bogarat, azokat meghatározta. Összesen 1100 fajt talált, amiből ~600 csak az adott fafajon megélő specialista faj volt. Ebből a számból a matematikai statisztika módszereit felhasználva megbecsülte az ízeltlábúak számát és végeredményben az összes faj számát is, ami 30-100 milliónak adódott.

Végezetül érdemes megtekinteni az 1. Táblázatot, amely a Földön és Magyarországon leírt élőlényfajok számát, különböző csoportok szerinti megoszlását mutatja be.

1. táblázat
A Földön és Magyarországon leírt élőlény fajok száma

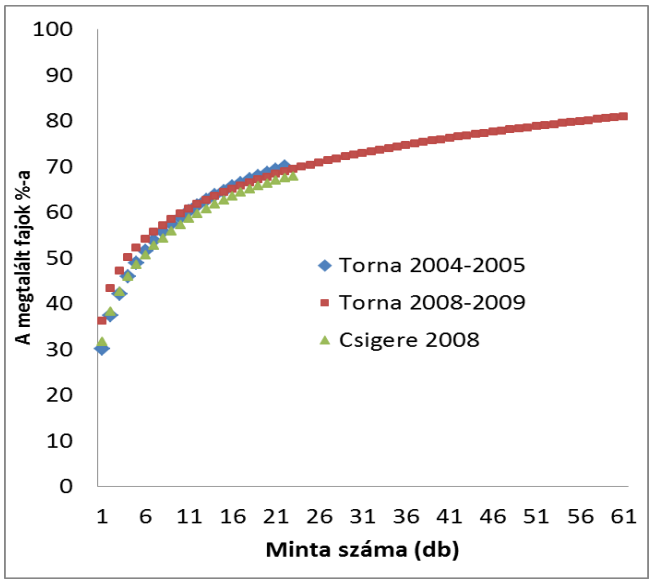
	Földön élő fajok száma	Hazai fajok száma
Algák	41 000	4 000
Gombák	65 000	2 500
Zuzmók	20 000	800
Harasztok	11 000	60
Edényes növények	250 000	2 200
Ízeltlábúak	900 000	35 000
Egyéb gerinctelenek	135 000	3 000
Gerincesek	42 000	560
Össz	**1 464 000**	**50 000**

V. HÁNY ÉLŐLÉNYFAJ ÉL EGY ADOTT ÉLŐHELYEN?



10. ábra
A Torna-patak és Csigere-patak 2008 évi kovaalga bevonat mintáinak vizsgálata során megtalált kumulatív fajszám.

Az előző kérdés fontos változata hogy hány faj él egy adott élőhelyen? Elsőre azt gondoljuk, hogy a kérdésre könnyű válaszolni, hiszen csak oda kell menni, és meg kell számolni. Sajnos azonban egy adott élőhely mérete eléggé nagy lehet, sok élőlénnyel, és egyszerre nem tudjuk az összeset átrostálni. Marad az a lehetőség, hogy mintát veszünk, viszont a minta sem biztos, hogy reprezentatív lesz. Így aztán minden mintavételkor újabb és újabb fajokat találunk, a fajlista hossza, amit kumulatív fajszámnak is nevezünk, a mintavételekkel egyre növekszik, és (ha közben az élőhely nem változik meg) egyszer csak telítésbe megy át. Ekkor elmondhatjuk, hogy megtaláltuk az összes fajt. Hány mintavétel után tehetünk efféle kijelentést? A Torna-pataknál és a Csigere-pataknál elvégzett vizsgálatban (10. ábra), a víz alatti kövek algabevonatából határoztak meg mintánként 400 egyedet, és még az 50. mintavételnél is bukkantak elő új fajok. A Csigere-pataknál az első 25 vizsgálatból szemmel még csak nem is érezzük, hogy hol lehet a grafikonon a plató, vagy egyáltalán van-e. Mikor gondolhatjuk szinte teljes bizonyossággal, hogy vannak még azonosítatlan fajok az adott élőhelyen? Akkor, ha vannak olyan fajok, amelyeket még csak egyszer találtunk meg. Ez az első mintavételnél mindegyikre igaz, de a második, harmadik stb mintavételeknél már csak a fajok egy része ilyen. Számukból úgynevezett



11. ábra
A mintavétel hatékonysága vízfolyások kovamoszatainak vizsgálatakor. Az első mintavételnél 400 egyed meghatározása után még csak a fajok 1/3-át találjuk meg, körülbelül 10 minta, összesen 4000 egyed meghatározása után ismerhetjük meg a fajlista felét.

becslőformulákkal meg lehet becsülni az összes fajszámot, mégpedig a mintavételek számával együtt növekvő pontossággal. Az élővilág változatosságára jellemző, hogy ez a szám a Torna-pataknál 88-nak, a Csigere-pataknál 123-nak adódott. Ez a két szám a statisztika felhasználásával, már néhány (5-10) mintavétel után ±5% pontossággal megbecsülhető volt, holott ekkor még csak a fajok körülbelül felét tudták megtalálni (11. ábra). Természetesen, hogyha sokáig járunk mintát venni, akkor közben egyes fajok megjelenhetnek, más fajok eltűnhetnek az adott élőhelyen, hiszen a fajlista a környezet változásait követve szintén dinamikusan megváltozik. Valóban nem léphetünk kétszer ugyanabba a folyóba. Éppen ezért érdemes a mintavételezést rövid időtávon megvalósítani vagy dinamikus modelleket bevezetni, amelyek a fajszám megváltozását is kezelni képesek.

VI. TANULSÁG

Az előzőekben két-három példán keresztül ízelítőt kaphattunk arról, hogy az adatbázisba rendezett adatok segítségével milyen típusú kérdésekre és hogyan lehet válaszolni. Beláthatjuk, hogy az adatbázisok alapvető módszertani feltételei a biológiai adatok tárolásának, és a matematikai

statisztika módszereivel kiegészítve hatékony eszközt adnak biológiai sejtéseink alátámasztásához.

Az adatbázisok az adatok különböző szempontú átrendezése, és kiválogatása révén új összefüggések megtalálásához is elvezetnek. Mindezt elmondhatjuk a harmadik évezred elején annak tudatában, hogy a jövőben reménykedhetünk a rendszerközpontú tudományok, közöttük az ökológia új forradalmában, az 1. ábra szerinti modell krízisben és újabb kifinomultabb modellek felállításában.

Források és szakirodalom

A témában igen kevés magyar nyelvű ismeretterjesztő irodalom érhető el. Ismereteinket leginkább nemzetközi tudományos folyóiratok cikkeire támaszkodva szerzhetjük be. Az alábbiakban néhány, mindenki számára elérhető forrást ajánlok az érdeklődőknek:

[1] Pásztor, E., Obornyi, B. Ökológia (Ecologie). Nemzeti tankönyvkiadó Budapest, 2007,

[2] Padisák, J. Általános limnológia ELTE Eötvös Kiadó Budapest, 2005

[3] http://vizeink.hu/index.php

[4] http://www.vizeink.hu/files/VGT_tajekoztato_20100618.pdf

[5] Üveges V, Andirkó V, Ács A, Bíró R, Drávecz E, Hajnal E, Havasi M, Hubai KE, Kacsala I, Kovács K, Kováts N, Kucserka T, Lengyel E, Matulka A, Selmeczy GB, Stenger-Kovács C, Szabó B, Teke G, Vass M, Padisák J A vörösiszap katasztrófa hatása a Torna-patak és a Marcal élővilágára, a regeneráció első időszaka ECONOMICA (SZOLNOK) 4:(12) pp. 95-139. (2011) http://tudomany.szolfportal.hu/downloadmanager/details/id/3000389/

Távcső helyett számítógép?

Dr. Nagy Rezső, főiskolai docens
Óbudai Egyetem, Alba Regia Műszaki Kar (OE-AMK)
és Terkán Lajos Bemutató Csillagvizsgáló, Székesfehérvár
nagy.rezso@amk.uni-obuda.hu

A címben feltett kérdésre a válasz természetesen az, hogy a csillagászok nem a távcsövek helyett használnak számítógépeket. Jelképük a távcső marad, noha sokkal régebb óta végeznek számításokat, mint távcsöves megfigyeléseket. Az előadásból kiderül, hogy mi mindenre használnak számítástechnikai eszközöket a csillagászatban, s hogy mit jelent a csillagvizsgáló a kutatók és a laikusok, köztük egy jól ismert magyar író és újságíró számára..

I. A TÁVCSŐ A CSILLAGÁSZOK JELKÉPE (DE CSAK PÁR SZÁZ ÉVE)

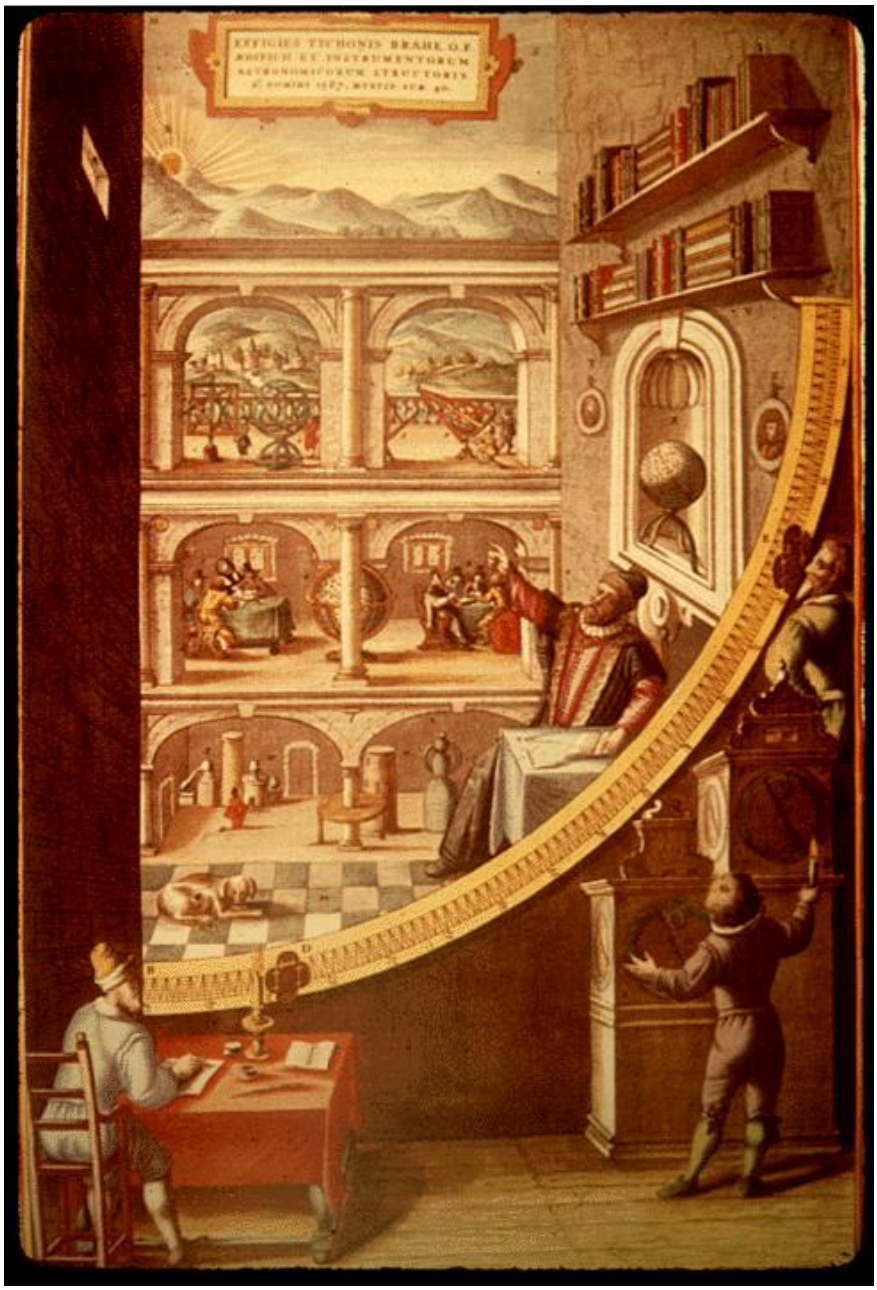
Ha valakit megkérnek, hogy rajzoljon le egy csillagászt, szinte biztos, hogy távcsővel fogja ábrázolni. Annak ellenére így van ez, hogy a csillagászok nem sokkal több, mint 400 éve használnak távcsöveket, míg maga a csillagászat több ezer évre tekinthet vissza.[1] Persze nem lehet megmondani, hogy pontosan mikor kezdődött a csillagászat tudománya, hiszen az égbolt – nem tudományos jellegű – megfigyelése egyidős lehet az emberiséggel. Mindenesetre sokezer éves kő-, ill. cseréptárgyakat is találtak, amelyek minden bizonnyal csillagászati témájú feljegyzéseket tartalmaznak.

A megfigyelések alapján számításokat is végeztek. Így például már több mint 4000 évvel ezelőtt is megkísérelték a nap- és holdfogyatkozások előrejelzését, 2500 évvel ezelőtt pedig ez már egészen pontosan működött (bár nem tudták, hogy valójában mi történik fizikailag). Több mint 2000 évvel ezelőtt Hipparchosz csillagpozíció-mérések és korábbi feljegyzések alapján nagy pontossággal kiszámította a precesszió[2] értékét.

A távcső előtti korszak végén működött az egyik legnagyobb észlelő csillagász, Tycho de Brahe. Hatalmas szögmérőkkel igen pontos

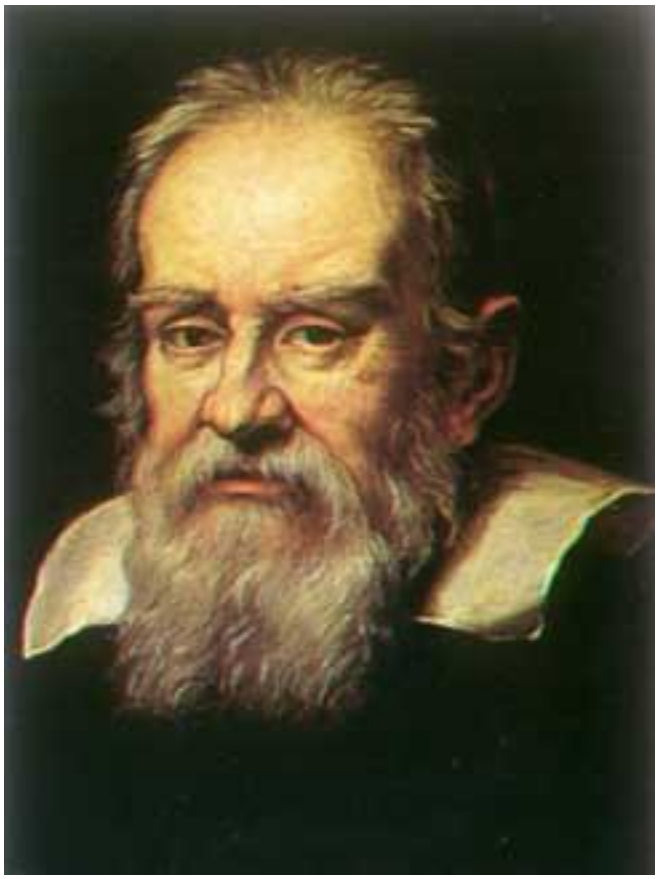
[1] Természetesen eleinte a tudományok nem különültek el a mai mértékben, de a tudományok első évezredeiben az egyik legfontosabb szakterület a mai csillagászatnak felelt meg.
[2] A Föld tengelye egy küppalást mentén kb. 26 ezer év alatt körbejár, ezért a tavaszpont (ahol a tavaszi napéjegyenlőség idején a Nap látható) „hátrál". A Nap rövidebb idő alatt jut el a tavaszpontból ismét a tavaszpontba, mint amennyi idő alatt 360°-ot megtesz a Nap körül.

méréseket végzett, a kiértékelésnél pedig figyelembe tudott venni olyan tényezőket, mint például a légkör torzító hatása. Mars-megfigyeléseinek pontossága lehetővé tette Kepler számára annak kiszámítását, hogy a Mars ellipszis alakú pályán kering a Nap körül.



1. ábra
Tycho de Brahe észlelés közben nagy kvadránsával és segítőivel

Galileo Galilei volt az, aki 1610-ben először publikált távcsöves megfigyelésekről szóló feljegyzéseket. Az előző évben több csillagász is végzett távcsöves megfigyeléseket, de nem publikálták. Mai szemmel furcsa, hogy akkoriban sok csillagász fel sem tételezte, hogy az égbolt távcsöves megfigyelése új információkkal szolgálhat.



2. ábra
Galileo Galilei (1564-1642)

A csillagászati műszerekről a sorozat más előadásában részletesen volt szó. Most csak annyit jegyezzünk meg, hogy a távcsövekre nem igaz az, ami a legtöbb műszaki eszközre (például a számítógépre), hogy tudniillik az évek során egyre kisebb méretben egyre nagyobb teljesítményt lehet megvalósítani. A nagy tudású távcsöveknek a fizika törvényei szerint nagyoknak kell lenniük.

II. A SZAKCSILLAGÁSZ TEVÉKENYSÉGEI A SZÁMÍTÓGÉP ALKALMAZÁSA ELŐTT

Évezredeken át a megfigyelések az égitestek pozícióinak mérésére és a fényességek becslésére szorítkoztak. A szögmérő eszközöknek nagyoknak kellett lenniük a megfelelő pontosság érdekében.

A XVII. századtól a csillagász távcsőbe nézett, amelynek szögnagyítása szükségtelenné teszi a hatalmas szögmérőket (persze láttuk, hogy maga a távcső viszont nagy). A távcsőben a közelebbi égitestekről kapott képet érdemes rögzíteni. Erre a távcső első két és fél évszázadában csak az a lehetőség kínálkozott, hogy a csillagász a látott képet lerajzolta. A fényesség-értékeket továbbra is becsléssel határozták meg.

A XIX. sz. második felétől fénymérő műszereket helyeztek a távcsövekre, és ezekhez hozzáigazították a hagyományos, becslésen alapuló fényesség-skálát. Hatalmas újdonság volt a színképelemzés megjelenése, amely lehetővé tette a csillagok és a csillagközi anyag összetételének megállapítását. A távcsőben megjelenő kép rögzítésére a XIX. sz. második és a XX. sz. első felében az ezüst-halogenides fényképezést alkalmazták.

Ezekben az évszázadokban a megfigyelésekhez sok (távcső) idő kellett, így mai szemmel kevés adat keletkezett. Igaz, számítógép nélkül lassú volt a feldolgozás, de nem keletkezett feldolgozhatatlan adatmennyiség.

Rengeteg számolni- és számítanivaló volt; a számítógép előtti korokban kialakult a csillagászat legtöbb szakterülete, így a szférikus csillagászat és az égi mechanika is.

A szférikus csillagászat a (képzeletbeli) éggömbön határozza meg az égitestek helyét a különböző égi koordinátarendszerekben. Műveléséhez elengedhetetlenek a szögfüggvények és a gömbháromszögtan. Ezeket még jóval a távcső feltalálása előtt kifejlesztették.

Az égi mechanika Kepler és Newton törvényei alapján az égitestek pályáit, mozgását, pozícióit számítja ki. Ez nem is lenne olyan bonyolult, ha csak két égitest létezne („kéttest-probléma"). A valóságban természetesen sok égitest van. A többtest-probléma azért olyan bonyolult, mert az égitestek egymáshoz viszonyított helyzete, távolsága, s emiatt a köztük fellépő gravitációs erő is állandóan változik.

Általános megoldást csak a két- és a háromtest-problámára ismerünk (utóbbi megoldása a gyakorlatban még számítógéppel sem használható, mert a Sundman-sor extrém lassan konvergál), így az égi mechanikában kifejlesztették a perturbációszámítást[3]. Ennek „legbarátságosabb"

[3] A perturbációt magyarul pályaháborgásnak nevezzük.

megközelítése az, hogy az égitestek mindig ellipszispályán mozognak, de mindig másik ellipszispályán, tehát a pályaelemek[4] állandóan változnak.

Számítógép nélkül kilátástalan lett volna iterációs megoldásokhoz folyamodni. Ezért az égi mechanikai problémák nagymértékben inspirálták a matematikai analízis fejlődését. Az analízisnek ezeket a módszereit később nagyon jól lehetett alkalmazni akár a villamosmérnöki tudományokban is.

Az égimechanikát úgy kell elképzelni, mint sokismeretlenes differenciálegyenlet-rendszerek megoldását a számításokat gyorsító, de elméletileg nehéz módszerekkel, sorfejtésekkel… Gondolom, kevesen irigylik a számítógép előtti korszak „számoló csillagászait".

Ennek ellenére nagyon sikeres volt az égi mechanika számítógépek előtti korszaka is. Talán a két legszenzációsabb siker a Halley-üstökös visszatérésének (1759.) kiszámítása, valamint a Neptunusz bolygó felfedezése (1846.) volt.

III. A CSILLAGÁSZAT A SZÁMÍTÁSTECHNIKA KORÁBAN (A XX. SZÁZAD 2. FELÉTŐL)

Az eddigiek alapján egyértelmű, hogy a számítógép nagy segítséget nyújthat az adatfeldolgozásban, az eredmények kiértékelésében, a „számoló" és az elméleti csillagászat minden területén. A továbbiakból azonban az is kiderül, hogy az észlelő csillagászat sem nélkülözheti ma már a számítástechnikát.

1975-ben kezdték alkalmazni a csillagászatban a digitális képfelvevő eszközöket. A CCD-képek rögzítéséhez és feldolgozásához számítógépet kell használni. Ugyanezt a megoldás célszerű alkalmazni a fotoelektromos észlelésekél is.

A csillagászatban rendkívül értékesek a régi megfigyelési eredmények, hiszen a legtöbb megfigyelhető folyamat nagyon sokáig tart. Már korábban is utaltunk a régi feljegyzések felhasználására. A csillagászati képfeldolgozásban is sikerrel kecsegtet, ha a régebbi, ezüsthalogenid-alapú képeket digitalizálják. 1995-ben fejezték be a Palomar Sky Survey[5] elnevezésű világméretű program felvételeinek digitalizálását.

A számítógép tehát a mérő- és képfelvevő eszközök vezérlését is végzi nem csupán az adatok gyűjtését, tárolását, feldolgozását. Természetesen

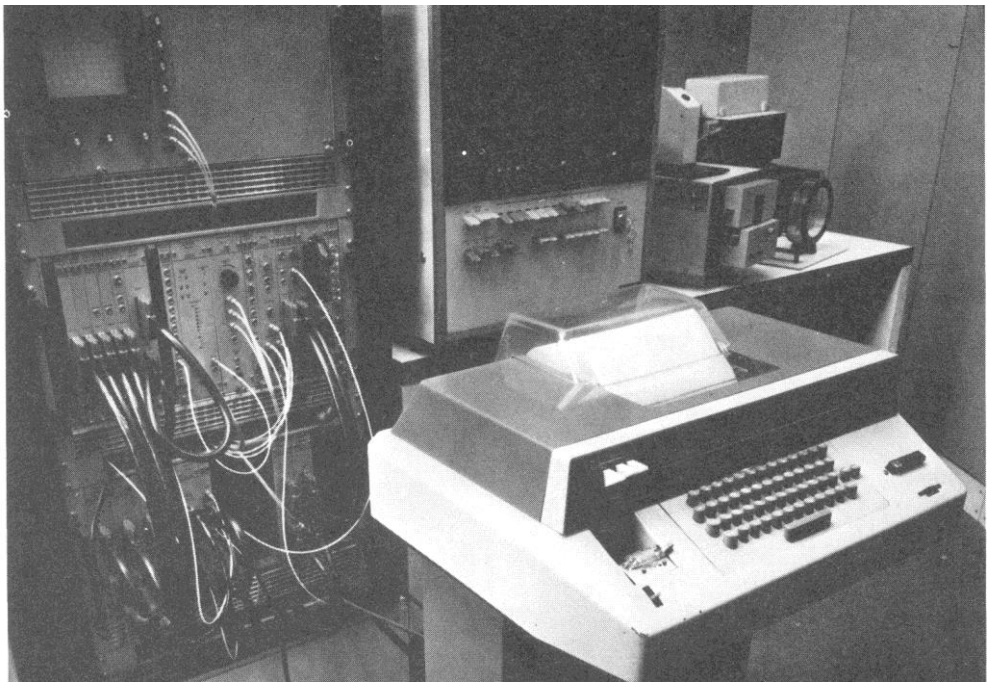
[4] A pályát meghatározó hat adat, melyek megadják pl. a pálya méretét, lapultságát, a pályasíknak a vonatkoztatási rendszer alapsíkjával bezárt szögét, stb.
[5] Először az 1950-es években készítettek az egész égboltot lefedő felvételsorozatot

akkor már végezheti magának a távcső beállításának, az egész megfigyelőrendszernek a vezérlését, távvezérlését, automatizálását is.

Hazánkban 1973-ban telepítettek és 1974-ben vettek használatba a piszkéstetői csillagvizsgálóban egy számítógépes rendszert, amelynek néhány jellemzőjét azért mutatjuk be, mert ma már technikatörténeti érdekességnek számít.

A 3. ábrán látható kép felső részének közepén van egy (a KFKI-ban készített) TPA/i kisszámítógép, mely 12 bites szavakat kezelt. Az operatív tár 16 k szó, a mágneslemez 256 k szó kapacitású volt. A képen a számítógéptől balra a CAMAC rendszerű real-time perifériavezérlés állványa, jobbra egy lyukszalagolvasó és egy lyukszalaglyukasztó látható. Az előtérben a terminálként használt teletype helyezkedik el.

A rendszert a pontos idő kezelésére, a pozíció és a fotoelektromos fotometria vezérlésére használták.



3. ábra
Az 1973-ban telepített számítógépes rendszer a piszkéstetői csillagvizsgálóban

A megfigyelő rendszer távvezérlése esetén az észlelő csillagásznak nem kell hosszú téli éjszakákon át a kupolában fagyoskodnia, s ha magashegyi

obszervatóriumban sikerül távcsőidőt kapnia, nem kell napokat eltölteni az alacsony légnyomáshoz való hozzászokással.

Lehetőség nyílhat komplett megfigyelési programok automatikus vezérlésére is: az időjárástól függően este a vezérlő szoftver kinyitja a kupolát, elindítja az égbolt aktuális állapotának megfelelő észlelési programot, elvégezteti a megfigyeléseket, eltárolja az eredményeket. Váratlan esemény hatására módosítja a programot, esetleg riasztja azt a személyt, aki a szükséges beavatkozásról dönthet.

A mai számítástechnika, információ- és infokommunikációs technológia – a többi tudományhoz hasonlóan – a csillagászatot is támogatja az anyaggyűjtésben, az eredmények dokumentálásában és publikálásában.

A számítógépes szimulációnak is fontos szerepe van sok tudományban, de a csillagászat bizonyos területein nélkülözhetetlen. A csillagászatban csak megfigyeléseket lehet végezni, kísérleteket nem[6]. A kutatás tárgyát képező objektumokat gyakran nem is tudjuk közelről megvizsgálni. Honnan tudhatjuk például, hogy mi van a Nap belsejében? Ha űrszondát küldenénk a Nap belsejébe, azonnal megsemmisülne. A megoldás: modelleket állítunk fel a Nap szerkezetére, fizikai ismereteinknek megfelelő szimulációkat futtatunk, majd megvizsgáljuk, hogy a szimuláció eredményeinek megfelelnek-e a megfigyelhető jelenségek. Ha nem, módosítani kell a modellt, és újra kell futtatni a szimulációt.

A drága műszerekkel felszerelt, nagyméretű távcsövekből álló automatizált megfigyelőrendszerek távcsőideje igen drága, viszont nagyon „termelékenyek": rövid idő alatt is hatalmas mennyiségű adatot (terabájtokat, petabájtokat) szolgáltatnak. Ennyi adatot számítógéppel sem egyszerű feldolgozni, az észlelési idő eltörpül a feldolgozási időhöz képest.

A csillagászok egyre nagyobb hányada szinte csak feldolgozással fog foglakozni. Persze az észlelő és a „számoló" csillagász személye régen is gyakran különvált. Láttuk, hogy pl. a kiváló észlelő Tycho de Brahe Mars-megfigyeléseit a kiváló matematikus, de nem túl jó szemű Kepler dolgozta fel (persze azért Kepler nevét egy távcsőtípus is viseli).

Egy másik, eddig nem említett probléma, hogy új eredmények általában különböző eredetű adatok együttes feldolgozásával születnek. Ezek az adatok különböző időpontokban, különböző eszközökkel (az

[6] 1957 óta kivétel ez alól az égimechanika, hiszen az űrtevékenység az égimechanika kísérleti ellenőrzésének is tekinthető

elektromágneses spektrum különböző tartományaiban) készülhettek, s a világ különböző pontjain találhatók.

Vajon tényleg probléma ez? Hiszen van világhálózat, az adatfeldolgozó csillagász töltse le a gépére az adatokat! Van azonban néhány kérdés, amelyekre a válaszok negatívak:

- Elfér-e a sok adat? Nem.
- Meddig aktuális a letöltött adathalmaz? Mire letöltjük, már nem.
- Tudok-e minden adatról? Nem.
- Azonos formátumban vannak-e az adatok? Valószínűleg nem.
- Elég nagy-e a gép számítási teljesítménye? Nem.

Megoldás: GRID (számítóhálózat[7]) kell!

A grid egy világhálózati infrastruktúra, amely **erőforrásokat** oszt meg. Nem tévesztendő össze a webbel, amely **információt** oszt meg! (Igaz, a grid is többnyire webes **felületen** működik.)

A grid által megosztható erőforrások: számítógépek, szuperszámítógépek, számítógép-fürtök (clusterek), adatbázisok, programok, különleges eszközök, berendezések, stb.

A szuperszámítógép jellemzői: több (sok) műveletvégző eszköz található egy gépben, speciális a felépítése, speciális belső összeköttetéseket tartalmaz, igen drága.

A fürt (cluster, klaszter) önálló, kommersz számítógépekből áll, amelyek kommersz hálózaton vannak összekötve és közös feladaton dolgoznak. Sokkal olcsóbb, mint egy szuperszámítógép.

A grid részeit a „közbülső réteg” (middleware) kapcsolja össze.

A grid infrastruktúrán többek között **virtuális obszervatórium**okat is kialakítottak, amelyeknek különböző csillagászati intézmények a tagjai. A virtuális obszervatórium a világhálózaton megosztja tagjainak csillagászati adatbázisait, a feldolgozó programokat, a feldolgozó számítógépeket, clustereket – így közvetve (nem valós időben) a csillagászati megfigyelőeszközöket is.

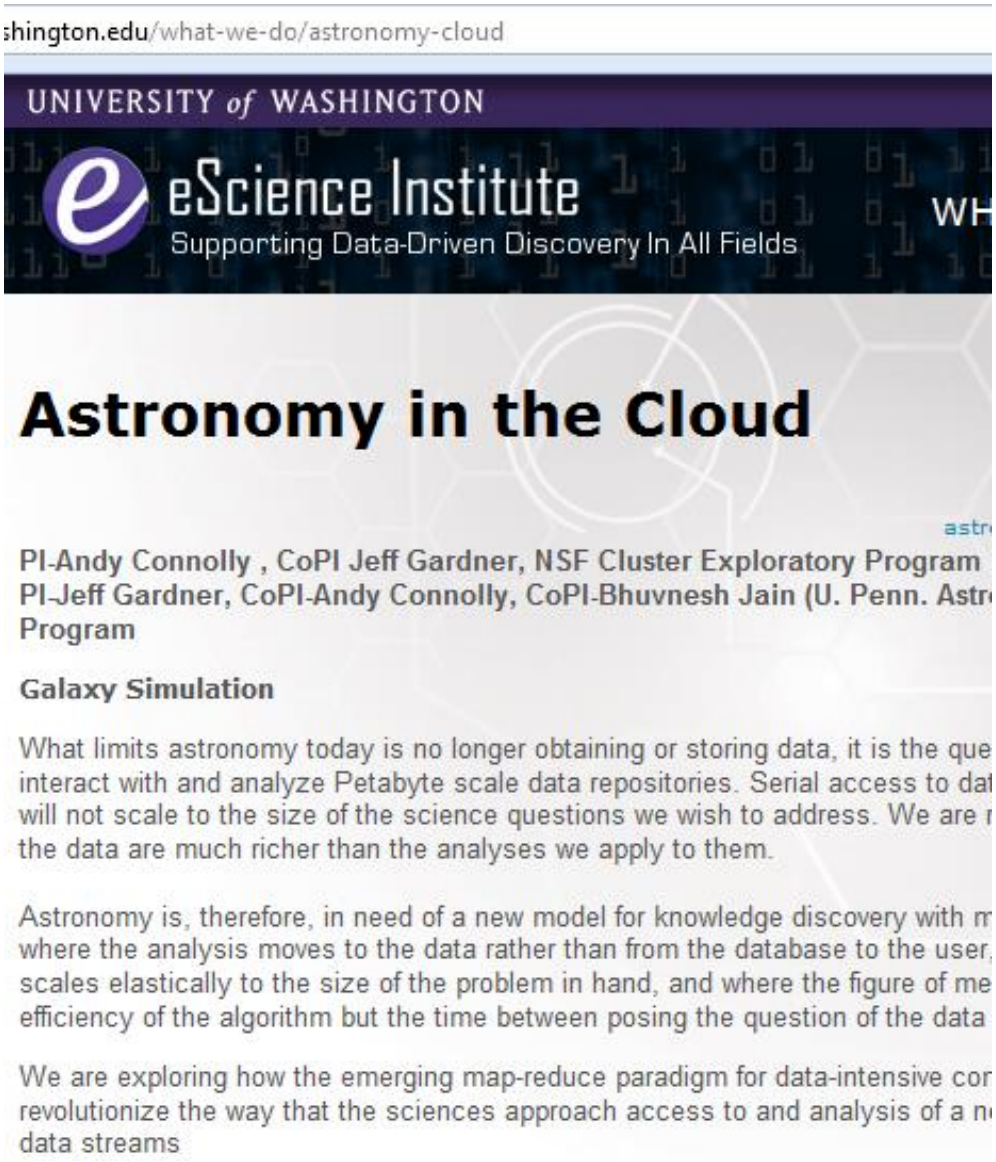
[7] A „számítóhálózat” szó a „számítógép” mintájára jött létre és nagyon találó, de sajnos nincs esélye, hogy elterjedjen – annyival hosszabb a „grid” szónál.

4. ábra
Egy virtuális obszervatórium weblapjának részlete (http://www.usvao.org/)

A virtuális obszervatórium a webes felületen bejelentkező csillagásznak segít megkeresni egy adott objektumra/objektumcsoportra vonatkozó megfigyeléseket és szűrni azokat, összeilleszteni a különböző megfigyeléseket, összehasonlítani az objektumokról a katalógusokban világszerte rendelkezésre álló információt, összehasonlítani a különböző időpontokban felvett megfigyelési adatokat. Ezzel leküzdi a berendezések említett korlátait.

Az utóbbi években előtérbe került felhő (cloud) technológia is kezd megjelenni a csillagászatban. A felhő-technológiát úgy közelíthetjük meg, hogy nagy számítási és tárolási teljesítményű virtuális számítógépeket

alakít ki a világhálózaton. Nagyon alkalmas lehet csillagászati szimulációs feladatok programjainak futtatására.



5. ábra
Webes cikk felhő-alapú galaxis-szimulációról
(http://escience.washington.edu/what-we-do/astronomy-cloud)

IV. A TÁVCSŐ, A CSILLAGÁSZAT ÉS A NAGYKÖZÖNSÉG

Mint írtam, a nagyközönség számára a csillagász, a csillagászat jelképe a távcső (az optikai távcső). Magam is tapasztalom a Terkán Lajos Bemutató Csillagvizsgálóban, ahogy a távcső közelében a látogatók érdeklődése megnyílik az égbolt és a világmindenség titkai iránt, és új élményekkel távoznak még akkor is, ha már nem először járnak ott.

6. ábra
Csoportkép a Terkán Lajos Bemutató Csillagvizsgálóban (Dr. Seebauer Márta felvétele)

Sehol nem olvastam ennek az élménynek és ismeretszerzésnek érzékletesebb leírását, mint Karinthy Frigyes Vigyázat, robbanunk! (Nyári éjszaka a sváb-hegyi csillagvizsgálóban) című cikkében, mely Az Est című lap 1933. augusztus 5-dikei számában jelent meg.

7. ábra
Karinthy Frigyes és Terkán Lajos

A természettudományok iránt érdeklődő híres írót az ország vezető csillagvizsgálójában Tass Antal igazgató és a székesfehérvári születésű Terkán Lajos[8] igazgatóhelyettes kalauzolta (akinek a neve a cikkben tévesen szerepel – lám, még a legnagyobbak is hibáznak néha).

A cikk tartalma azonban kárpótolja még a székesfehérvári olvasót is, íme néhány részlet belőle:

> *… a csillagászat az egyetlen emberi tudomány minden tudományok között, amit minden érdek, minden* ***hasznost is*** *mellékgondolat nélkül*[9] *fejleszt és feszeget és kutat az életnek talán legnemesebb, legcsodálatosabb megnyilvánulása: az emberi kíváncsiság.*
> *A legtisztább tudomány. Tudományok közt az, ami művészetek közt a költészet.*
>
> *- Most tessék itt alul benézni.*
> *A látótérben ott lebeg a Szaturnusz, sárgán és plasztikusan, kiemelkedve szinte hátteréből. Gyűrűje most ferdén, felülről látható - közelében Rhea, a tíz holdak egyike, világító pont.*

[8] Dr. Hudoba György: Terkán Lajos élete és munkássága ISBN 963 04 6187 0
[9] Ez persze nem egészen igaz, hiszen a csillagászatnak fontos szerepe van a naptár, az időmérés, a tájékozódás és az élet sok más területén – de a természettudományok többségétől valóban eltér.

Aztán Vega következik soron, ragyogó gyémánt, a mennybolt Kohinoórja - szinte vakít, ahogy szembekerülsz vele.

… két ikercsillag, egymás körül keringve - az egyik vörös, a másik kék - mindjárt vigasztalóbb látvány. Szinte kinyújtod érte a kezed - csak az tart vissza, hogy még ha odaérne is, nemigen találnád a helyén: negyven esztendővel ezelőtt lehetett ott, ahol most látod. Ennyi idő kell hozzá ugyanis, amíg a fénye eléri szemünket, a reflektor tükrein át.

A cikkben szó esik arról is, hogy a „spirálködök" valójában extragalaxisok, a Tejútrendszeren kívül vannak (ezt csak az 1920-as években sikerült eldönteni) és az akkor frissnek számító felfedezésről: arról, hogy a galaxishalmazok távolodnak (erre utal a „Vigyázat, robbanunk" cím).

Befejezésül nem tehetek jobbat: javaslom, hogy olvassa el mindenki Karinthy Frigyes teljes cikkét[10]!

NÉHÁNY AJÁNLOTT IRODALOM

[1] Csillagászat (szerk. Marik Miklós) Akadémiai Kiadó, Budapest 1989. ISBN 963 054657 4 (kifejezetten szakkönyv, nem ismeretterjesztő)

[2] A távcső világa (szerk. Kulin György és Róka Gedeon) Gondolat Kiadó. Budapest 1980. ISBN 963 280 817 7 (kicsit régi, de szinte nélkülözhetetlen)

[3]Dr. Hudoba György: Terkán Lajos élete és munkássága Székesfehérvár, 1996. ISBN 963 04 6187 0

[4] Karinthy Frigyes: Szavak pergőtüzében Szépirodalmi Könyvkiadó, 1984. ISBN 963 15 2450

[5] Az égi mechanika történetéről (Nagy Rezső szakdolgozata csillagászatból, 1989.)
http://arekold.amk.uni-obuda.hu/~rnagy/egmetor.zip

A számítástechnika alkalmazásával kapcsolatban az újabb és újabb fejleményeket a weben való böngészéssel találhatjuk meg.

[10] A „Szavak pergőtüzében" című gyűjteményes kötet 180. oldalán is megjelent a Szépirodalmi Könyvkiadónál 1984-ben. A weben több helyen is olvasható, pl: http://members.iif.hu/visontay/ponticulus/rovatok/megcsapottak/karinthy_svab.html, itt a honlap szerkesztője említi Terkán Lajost, de Terkán Antal néven. Egy másik webhely: http://mek.oszk.hu/05800/05815/05815.htm#34, itt nincs megjegyzés, viszont a megjelenés dátuma: ***1933. július 30.***