szi az alkímiából a fémeket, legfontosabb motívumként, az alkímia alapgondolataként a halhatatlanság megvalósítására tett kísérletet tünteti ki, és a továbbiakban az ősi művészet „szellemi vagy szakrális származását" kutatja. Az alkimista szövegek eszköztárának, metaforáinak és analógiáinak forrását – sőt: magyarázatát – pedig az ősi egyiptomi mitológiában és (ezzel összefüggésben vagy ettől függetlenül?) a késő ókori hellenizált Alexandriában találja meg.

Az alkímia hagyománya mindig is egyiptomi eredettel büszkélkedett, még ha erre a vélt származásra kevés konkrét bizonyíték található is. Farkas Attila Márton munkáját olvashatjuk úgy, mint az egyiptomi-görög eredet részletes kifejtését. Azonban kérdés, mennyiben tekinthető kizárólagos magyarázatnak, amikor modern alkimista szövegekre és a XVI–XVII. századi képi ábrázolásokra az egyiptomi istenvilágban talál párhuzamot. Ne felejtsük el, hogy az alkímia számos, rendkívül általános metaforával dolgozik (elmúlás, pusztulás, feltámadás, nemzés, születés, gyilkosság, a test feldarabolása stb.), amire minden bizonnyal az eszkimó hiedelemvilág is bőséggel kínál analógiát. De fogadjuk el az érvelés kedvéért, hogy az alkímiából szabadon elhagyható a vegyészet és az aranycsinálás, hogy a könyv elemzései megállják a helyüket, és valóban Egyiptom hoz fényt a kora újkori allegóriák homályába. Ebben az esetben sem értem, hogy miközben szabadon utazunk fel s alá a Kr. u. III. és a XVI. század között, miért nem állhatunk meg egy percre az arab és a középkori alkímiánál. Nem értek egyet azzal, hogy az alkímia nélkülözné a történelmi dimenziót, hogy Alexandriában mindjárt a végleges formájában alakult volna ki (15. vagy 42. old.), és időtlenül, a későbbi korok tudományára, vallásos meggyőződéseire és művészetére ügyet sem vetve hagyományozódott volna tovább. Csak jelzésképp említem, hogy az alkímia műfajainak, terminológiájának, fogalmainak jelentős része a kora középkori arab tudomány öröksége, ekkor váltja fel az arisztotelészi négy elem koncepciót a Mercurius–Sulphur ellentétpár, melyre a fémek összetételét vissza lehet vezetni. Az eredetileg görög szövegek kiegészülnek az arab korpusszal (Rasis, Jabir, Avicenna etc.), majd a XII. századtól a délolasz és spanyol fordítóiskolákban a keresztény Nyugat számára is hozzáférhetővé és továbbgondolhatóvá válnak. Az alkímiai szimbolizmus termékeny kölcsönhatásra lép a középkor vallási koncepcióival, és csak ekkor – az érett középkor századaiban – jelennek meg a görög és arab hagyományban ismeretlen illusztrációk, allegorikus ábrázolások.

A kén és a higany mellé egészen későn, Paracelsusnál társul harmadikként a só (de még ha a legendás Basileus Valentinus valóban létezett is, akkor is csak a XV. században), módszertanilag tehát problematikus egyiptomi magyarázatot (a mumifikálást) kínálni a sónak az Opus Magnum létrejöttében játszott szerepére (34. old.). Csodálkozva láttam, hogy noha a szerző tisztában van azzal, hogy a hagyományban sokszor tűnnek fel autoritásként mitologikus, de legalábbis nem alkimistaként működő szereplők, és Hermészben nem kell szükségképpen történeti személyt tisztelnünk, sem Platónban alkimistát, a „zsidó Mária" (24. old.) és Kleopátra (35. old.) mintha történelmi realitással rendelkező, hellenizmus kori alkimistákként jelennének meg.

Az egyes korok jellemzései és az egyéb ítéletek sokszor elnagyoltak és történetietlenek (a késő antik világot világvégeérzés gyűri maga alá – 31. old. –, a középkori alkímiát nem tudták kikezdeni a mindent letaroló nagy vallások – 41. old.), máskor vállon veregetők (Descartes a naiv lelkek közé sorolható, mert a rózsakeresztesek tagja kívánt lenni, és nem értette, hogy itt szimbolikus dologról van szó – 45. old.). Hogy Newton és Leibniz rózsakeresztesek lettek volna (48. old.), nem könnyű bizton állítani, minthogy mindmáig nem tudjuk, vajon ez a titkos társaság valóban is létezett-e. Ha viszont a szerző e két filozófus híres mágikus érdeklődésére gondol (Newton esetében az alkímiára, Leibniznél pedig a kombinatorikus művészetre), nyitott kapukat dönget, mert erről a művelt olvasónak már régen tudomása van.

Egyszóval, Farkas Attila Márton számos érzékeny elemzést közöl az alkímia hagyományának szimbólumrendszeréről, de könyve inkább népszerűsítő, mint tudományos, leírásai sokszor megmaradnak a legendás anekdoták felsorolásának szintjén, hivatkozásai esetlegesek, tárgyalásmódja pedig ahistorikus.

Lezárásképp érdemes egy szót ejteni a kissé kinyilatkoztató elbeszélői hangról. Olvasóként nem tudtam szabadulni a gyanútól, hogy a szerző az igazság birtokában van, és ezt maga is jól tudja. Amit a könyvben bemutat, az az alkímia „valódi lényege", a királyi művészet „igazi gyökerei", szemben mindazzal, amit a korábbi, előítéletek ballasztjával csetlőbotló szakirodalom csinált.

Természetesen tudom, hogy abban az esetben, ha a szerző beavatást nyert az ősi hagyomány igazságába, kritikám nem ér semmit: a történelemtudomány szempontjait a kinyilatkoztatott igazsággal szemben nem lehet relevánsan felvetni. De Farkas Attila Márton örvendetesen elhatárolódott az obskúrus, beavatott értelmezésektől, ezért joggal értékelhetjük könyvét az alkímia nemzetközi szakirodalmának tükrében.

LÁNG BENEDEK

Simon Singh: Kódkönyv

A REJTJELEZÉS ÉS REJTJELFEJTÉS TÖRTÉNETE

Fordította: Szentgyörgyi József. Park Könyvkiadó, Budapest, 2001. 399 old., 2900 Ft

Simon Singh műve rendkívül élvezetes módon megírt, népszerűsítő könyv, melynek legfontosabb erénye, hogy a közérthetőség határainak számottevő átlépése nélkül képes pontatlanságtól mentesen tárgyalni a titkos kommunikáció kérdéskörét. Annak ellenére ugyanis, hogy a téma számtalan ponton kötődik a humán tudományok, sőt a mindennapi élet világához, a kriptográfiai algoritmusok, a rejtjelezés, illetve kódfejtés

módszereinek, gyakorlatának megértése némi agytornát, kisebb-nagyobb matematikai kalandozást mindenképpen feltételez az érdeklődő olvasó részéről. Singh ezt a problémát – mely a nagyközönséget általában elriasztja a kémtörténeteken túlmutató művektől – elegáns módon oldja meg: regényes, történeti érdekességek közé beékelve adagolja az algoritmusok fejtörést igénylő „gyakorlatait", amelyek után jólesik a következő izgalmas történettel folytatni az olvasást.

Az indiai származású brit fizikus, Simon Singh a BBC tudományos osztályán pruducerként és rendezőként valóban magas színvonalú sorozatok készítésével szerzett gyakorlatot a természettudományok népszerűsítésében, sőt első könyve, a *Nagy Fermat-sejtés* is egy általa rendezett BBC dokumentumfilmen alapul. A könyv a Pierre de Fermat, XVII. századi francia matematikus által megfogalmazott briliáns rejtvény megoldásának – ami végül 1995-ben egy brit tudósnak sikerült – tudománytörténetét dolgozza fel, s Nagy-Britanniában az első matematikai tárgyú bestsellerként tartják számon. A tisztán matematikai kérdést körbejáró műhöz képest a *Kódkönyv* megírása feltehetőleg könnyebb feladat volt, hiszen a téma jóval szélesebb asszociációs mezőben tárgyalható, a fentiekben említett megkerülhetetlen agytornáztatás ellenére is. A mű Singhnek valóban meghozta a világhírt; a *Kódkönyv*ből tévésorozat is készült, abból pedig – a *Fermat-sejtés*hez hasonlóan – *The Science of Secrecy* címmel egy újabb könyv, amely a *Kódkönyv* afféle „könnyített" változata, nagyobb illusztrációs anyaggal, több sztorival. (Simon Singh hivatalos weboldalát érdemes felkeresni, ahol a *Kódkönyv*ről, egyéb műveiről s a kriptográfiáról találhatók háttéranyagok: http://www.simonsingh.com/)

A *Kódkönyv* nem vádolható felszínességgel, bár sok minden hiányzik belőle: nem összefoglaló igénnyel írt tudományos munka, hanem intellektuális kalandokra csábító, népszerűsítő mű. A végén található irodalomjegyzék és webcímek gyűjteménye jó kiindulópont a téma iránt bővebben érdeklődő olvasó számára. Azt pedig, hogy a *Kódkönyv* mennyire képes gyakorlati tapasztalatok átadására is, bizonyítja a függelékben található rejtvénygyűjtemény, melynek a figyelmes olvasó legalább egy részét könnyedén meg tudja oldani a gyakorlati útmutatások alapján. (A teljes feladatsor megfejtése azonban nem könnyű feladat, a komoly pénzjutalommal járó nemzetközi versengés a könyv megjelenésétől számítva egy teljes évig tartott. Nem is csoda, hiszen az utolsó két feladvány éppen a ma is széles körben használatos 512 bites RSA kódolás. A rejtvényekről és a kódfejtő versenyről részletes információk találhatók Singh weboldalán.)

Singh könyve a történeti szálat nagyjából következetesen követve mutatja be a kriptológiai eljárások fejlődését, az ettől való eltérések oka a szellemes bestsellerszerkezet, amely minden „nehezebb" szövegrészt kerettörténetekkel tesz könnyebben emészthetővé.

A kezdetektől a XV. századig húzódó időszakot tárgyaló első fejezetet például Mária skót királynő esete keretezi, aki a börtönből való kiszabadítására és megkoronázására szövetkező híveivel megfejthetetlennek vélt titkosírással tartotta a kapcsolatot. Vesztét a kód megfejtése okozta. Egyik titkosírással írt levelébe néhány sort belehamisítva csalták ki a bizonyítékot tőle s gyanútlan híveitől: mindkét fél fehéren-feketén leírta szándékait, mivel biztosak voltak benne, hogy üzeneteik a kívülállók számára megfejthetetlenek.

Ez az első fejezet kicsiben az egész könyv szerkezetét szemlélteti: Mária hányatott életének történelmi novellájával egybefűzve Singh bemutatja a fontosabb ókori kriptográfiai és szteganográfiai eljárásokat, Julius Caesar behelyettesítéses (monoalfabetikus) kódját, az arab „találmányt", az egyszerű betűgyakoriságon alapuló kriptoanalízist, melyet egy kódszöveg megfejtésén keresztül be is mutat, szól a nyugati reneszánsz híresebb titoknokairól, a szóbehelyettesítéses kódról, s végül a skót királynő kivégzéséhez vezető történet segítségével bizonyítja a Caesar-féle módszeren alapuló monoalfabetikus kódok gyengeségét. Mindez 42 oldalt vesz igénybe, azaz elismerésre méltóan haték-kony „edutainment": túlzás volna azt állítani, hogy történelmi kalandregényhez hasonlóan könnyű olvasmány, de semmivel sem kíván több szellemi erőfeszítést az olvasótól, mint egy Edgar Allan Poe-novella, például a titkosírást és annak kriptoanalízisét is ismertető *Aranybogár*. A tömörség természetesen meggátolja Singh-et abban, hogy minden fontos történeti, gyakorlati részletet ismertessen, ám a megértéshez fontos kérdésekre mindenhol kitér, sehol sem pontatlan, s a fontosabb tényeket is, legalább utalások szintjén, érinti.

Továbbhaladva az időben, Albertitől kezdve bemutatja a poli-, illetve homoalfabetikus kódolás történetét, a sokáig „feltörhetetlennek" tekintett Vigenère-sifre-t, s hogy Charles Babbage – akinek életéről, találmányairól jól összeállított, rövid, könnyed, de informatív életrajzot közöl – hogyan fejtette meg 1854 körül; megemlíti a titkosírások irodalmi vonatkozásait Jules Verne és Poe műveiben, illetve *A táncoló emberkék* című Holmes-történetben. A könyv második kerettörténete egy elásott kincs helyét tartalmazó kódolt dokumentum, a „Beale-papírok" esete, mely egy kevéssé ismert s máig feltöretlen titkosírás történetének részletes és regényes leírása. Singh igyekszik szokatlan, kevéssé ismert sztorikat felhasználni a könyv színesítésére – a Beale-rejtély anyagának összegyűjtéséhez a helyszínen, Virginiában végzett kutatásokat, a tárgykör szakértőivel konzultálva.

A gépesített titkosítás kezdeteinek vázlatos ismertetése után a két világháború regénybe illő kriptológiai eseteivel, különösen pedig a brit hírszerzéssel foglalkozik alaposabban, mely a Zimmermann-távirat megfejtésével elérte, hogy az amerikaiak belépjenek az első világháborúba, a másodikat pedig jelentősen megrövidítette a német és japán üzenetváltások megfejtésével. A második világháború minden kriptológiával foglalkozó mű kedvenc terepe, felkínálva a titkos kommunikáció s az üzeneteket elfogni igyekvő, minden bokorban rejtett információt sejtő cenzorok szórakoztató történeteinek rendkívül széles repertoárját. Singh ezen anekdotagazdag periódust tárgyalva elismerésre méltó önmérsékletet tanúsít, tartóz-

kodik a mosolyogtató esetek bemutatásától, s a náci kódok, kiemelten az Enigma történetének, feltörésének részletes leírására koncentrál. A laikus számára is érthetően magyarázza el az Enigma működési elvét, s a különböző, továbbfejlesztett Enigma-variánsok feltörési kísérletein át vezeti végig az olvasót az összetettebb kriptoanalízis logikáján, módszerein. A lengyel kódfejtők, különösen Marian Rejewsky kezdeti sikereitől Alan Turing (http://www.turing.org.uk/turing/) megoldásáig végigkíséri a „Turing-bombák" történetét, megemlíti a legerősebb német kód, a Lorentz feltöréséhez használt Colossust, mely talán a világ első programozható elektronikus számítógépe volt. A háború után a brit hírszerzés összes gépét szétszerelték, a dokumentációkat jelentős részben (a Colossus esetében teljes egészében) megsemmisítették, a németektől zsákmányolt Enigmákat pedig búcsúajándékként szétosztották a korábbi brit gyarmatok államapparátusában, kényelmes betekintést engedve az azokat lelkesen alkalmazó kormányok titkos üzenetváltásaiba. Ennek a szórakoztató ténynek volt köszönhető, hogy a Bletchley parkban berendezett kódfejtőközpontban történtekről (a Blechley park hivatalos oldala: http://www.bletchley-park.org.uk/), a háború kimenetele szempontjából döntő sikerekről egészen a hetvenes évekig nem szivárgott ki érdemi információ. A hetvenes években az univerzális számítógépek elterjedésével anakronisztikussá vált a titkok további őrizgetése; ettől kezdve könyvek, publikációk özöne indult útjára a történelem talán egyetlen olyan háborújának hírszerzéseiről, melyben az egyik háborús fél folyamatosan olvasgatta a másik üzenetváltásait, s matematikusokat alkalmazott olyan „hadmozdulat-algoritmusok" kidolgozására, amelyek „fehérzajszerűen" alkalmazzák csupán a megszerzett információt, elaltatva ezzel az ellenség esetleges gyanakvását.

A Blechley parki titkok kipattanásáig a második világháborús kriptológiáról csupán az amerikaiak jóval szerényebb, unalmasabb sikerei-kudarcai voltak ismertek, melyeket Singh jobbára mellőz is könyvében. Kitér azonban a navahó „kódbeszélők" esetére (1968-ig szintén titoknak számított), mely a maroknyi populáció által beszélt nyelven kommunikáló indián rádiósok alkalmazásával teljességgel feltörhetetlen titkos kommunikációs csatornát biztosított az amerikai hadsereg számára. A bájos történetet Singh szellemes fordulatra használja fel: a „nyelvi korláton" alapuló kóddal vezeti át az olvasót a régészet s az elfelejtett nyelvek megfejtésének világába. A *Kódkönyv* terjedelméhez képest meglepő alapossággal kalauzol el az archeológia és a kriptoanalízis közös történetében, az egyiptomi hieroglifáktól a lineáris B-ig, Athanasius Kirchertől John Chadwick és Michael Ventris sikeréig, részletesen ismertetve a megfejtésre irányuló erőfeszítések gondolatmeneteit.

A *Kódkönyv* utolsó harmada már a számítógépes kriptológia történetét tárgyalja. A közérthetőség határterületeire csupán ritkán kalandozva Singh bemutatja a digitális formában továbbított szövegek rendszerét, s azok kódolási mechanizmusait: a hetvenes évek kezdeti kódjaitól egészen a napjainkban használatos algoritmusokig érthetően magyarázza el működésüket. Kitér az újításokat „feltaláló" kriptográfus egyéniségekre is, s rámutat a szabad kódolást gátolni igyekvő titkosszolgálati-politikai szempontokra. Bölcs óvatosságot tanúsít a „szabad titkolódzás" kérdésének megítélésében, Phil Zimmermann s a Pretty Good Privacy (a PGP-ről szóló amerikai oldal a http://www.pgp.com, a nemzetközi http://www.pgpI.org/, a magam részéről az utóbbit javaslom) nevű kódolórendszer történetét elmesélve szemlélteti a gondolat- és cselekvésszabadságban hívő egyének s a bűnszövetkezetek, terroristák titkos üzenetváltásaitól rettegő intézmények küzdelmét. A politikusok és a fantáziadús újságírók által időről időre felröppentett gyagyaság-rémeket leszámítva is tény ugyanis, hogy kábítószer-terjesztő hálózatok s bizonyára a terrorszervezetek is használják a digitálisan kódolt kommunikációt ügyleteik intézésére, de az is, hogy az egyén személyiségi jogait, a magánszféra védelmét egyre inkább csak a megbízható kódok garantálják. A történelem legnagyobb részében a magánélet szentségét a megfigyelés technikai nehézkessége biztosította, a parabolamikrofonok, lézeres interferométerek, műholdas megfigyelőrendszerek világában azonban az egyetlen védekező eszköz a megfelelően erős kriptográfia maradt, mely legalább kismértékben megizzasztja a leselkedőket a kilesett információ megfejtésekor. Nem is igazán az a probléma, hogy „szabad-e" kódolva kommunikálni, ezt amúgy sem sikerült – eddig – betiltani, hanem az, hogy az ismert hatalmas lehallgatórendszerek működéséről nagyon keveset tudunk, s hogy ezeknek „szabad-e" működniük. Annak ellenére, hogy politikusok, katonatisztek időről időre tagadják az egyetemes megfigyelőrendszerek létezését, afelől mindenki nyugodt lehet, hogy mindennapjaink privát történéseiről tudtunkon kívül gyűjtött hatalmas mennyiségű kép, lehallgatott telefon/fax/elektronikus levél stb. található intelligens elemző szoftverek olvasónaplóiban. (Kiindulópontként csupán néhány ízelítő a megfigyelőrendszerekből:

http://www.echelonwatch.org/
http://serendipity.magnet.ch/hermetic/crypto/echelon/echelon.htm
http://www.thecodex.com/
http://mediafilter.org/
http://www.greenpages.com.au/baird/default.htm
http://www.privacyinternational.org/
http://www.orwelltoday.com/ surveillance.shtml
http://www.counterpane.com/.)

A kriptoanalízis, a kép- és hangfelismerő programok fejlődése, illetve az adatgyűjtés/tárolás egyszerűsödése ugyanis oda vezetett, hogy hatékonyabb magukat a dokumentumokat elemezni, mint forrásukról, címzettjükről megállapítani, hogy érdemes-e megfigyelni őket. Singh bölcs hallgatása az egyetemes megfigyelésről tehát meglehetősen bosszantó, de sajnos érthető: ez nem a népszerűsítő tudomány terepe, bár itt kutatni volna mit, de lehetetlen. Meg aztán az ember harci kedve alábbhagy, amint belegondol, hogy a polgárjogi aktivisták legfőbb szövetségesei a kettős

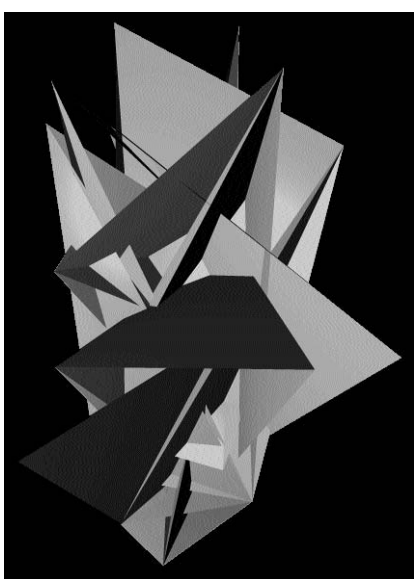
játékot űző nagyvállalatok, amelyek az erős kriptográfiától az elektronikus kereskedelem fellendülését, az eladások növekedését várják, másrészről viszont az adatgyűjtögetés/elemzés lelkes, bár nem nyilvános hívei és támogatói.

A *Kódkönyv* utolsó, nyolcadik fejezete a „technika természetfelettijével", az egyelőre csupán a fantázia világában létező kvantumszámítógépekkel (The Centre for Quantum Computation: http://www.qubit.org/) s az azok működésével megvalósuló „kvantumkriptográfiával" foglalkozik. Annak ellenére, hogy manapság sokat hallani ilyesmiről, nem nagyon találkozni olyan „közérthető" művel, amely e szép csengésű fogalmak jelentését is megkísérelné felfedni. Singh az előző fejezetekhez hasonlóan frappáns módon magyarázza el a kvantumfizika alapgondolatait, a „Schrödinger macskája" néven ismeretes példázatot, azaz a szuperpozíció elvét. A híres négylábú a példázat szerint egy lezárt ládikában üldögél egy rendkívül törékeny ciánkapszula társaságában. A láda kinyitása nélkül nem szerezhetünk információt arról, hogy a macska életben van-e még, vagy eltörte a fiolát és elpusztult. A kvantumelmélet gondolkodásmódja szerint a cica ilyenkor szuperpozíciós állapotban van, egyszerre élő is meg halott is, mindkét állapotnak megfelel. A szuperpozíció addig áll fenn, amíg a macskát „szem elől vesztjük", a láda kinyitása, a leskelődés azonban „kikényszeríti", hogy a macska egyik vagy másik állapotban legyen, így a szuperpozíció azonnal megszűnik.

A kvantumszámítógép tehát egyszerre – és itt valóban egyidejűségről van szó – számtalan műveletet képes elvégezni, hiszen olyan elemekből áll, melyek a szuperpozíció elvén számtalan állapotot képesek egyszerre felvenni. Ha valaha elkészül, minden feladatsort egyszerre, szuperpozíciós állapotban végez el, így nem a napjainkban megszokott, gyakran „szédítőnek" megélt számítógépes sebességnövekedést, hanem valóban végtelen gyorsaságot, a kvantumkriptográfia pedig abszolút biztonságot jelent majd. Singh könyve utolsó mondataiban fel is teszi az ezzel kapcsolatos magától értetődő kérdést: „...engedi-e majd az állam ennek a módszernek a használatát? Hogyan szabályozza majd az állam a kvantumkriptográfiát olyképpen, hogy gazdagítsa általa az információ korát, de ne védje a bűnözőket?"

E kérdések valóban felmerülnek a kódolt üzenetváltások esetében, de vajon mi lesz a helyzet a megfigyelőrendszerek által kódolatlan formában gyűjtött információval? A kvantumszámítógépeken futó elemző szoftverek egyetlen pillanat alatt átvizsgálják majd az egész életünkről szóló dokumentumokat, képsorozatokat, hangfelvételeket, s ki tudja, még miket; gyakorlatilag mindazt, amit egyszerre beletáplálnak. Jobban tesszük tehát, ha eltanuljuk tőlük a szuperpozíció elvét, s alkotórészeinket végtelen sok állapot egyszerre való felvételére bírva egyetlen pillanat alatt kirosszalkodjuk magunkat. A szuperpozíció azonban csak olyankor létezik, amikor nem figyelhető meg: ahogy Schrödinger ládájának kinyitása is „kikényszeríti", hogy a macska egyik vagy másik állapotba kerüljön, úgy a szuperpozícióban felszabadultan randalírozók is elintézhetők egyetlen cenzor-szemvillantással.

SZEGEDY-MASZÁK ZOLTÁN



Szegedy-Maszák Zoltán
Csontváry Cryptogram: Ki festhet csataképet?
képernyőfotó, 1996