

A KÓDFEJTÉS FÜGGŐSÉGHEZ VEZETHET

Vadai István és Vámos Hanna irodalomtörténészek a Bölcsészettudományi Karon. Az utóbbi időben egy olyan tudományterület foglalkoztatja őket, amely nagymértékben felkeltette a helyi és az országos sajtó érdeklődését. A két tudós a fejtés élménye, a végeredmény miatt kezdett el foglalkozni a titkosírásokkal, valamint abból a célból, hogy a kidolgozott módszereket más tudósok számára is elérhetővé tegyék. Vámos Hanna távollétében Vadai Istvánnal beszélgettünk a kezdetekről, módszerről, okokról és a jövőről.

Húsz éve foglalkozott először kódfejtéssel, majd hosszú szünet után újra felidézte ezt a tevékenységet kolléganőjével, Vámos Hannával. Mi volt a szünet oka és mi az újrakezdésé?

A pauza oka, hogy nem találkoztam megfejtetlen titkosírásokkal, tudniillik, az ember nem „megy szembe” ilyesmivel az utcán sétálva. Az ilyen szövegeket szisztematikusan kell keresni levéltárakban, könyvtárakban. Némelyik nyomtatásban is olvasható: 19. századi történéslapokat felütve például találunk közleményeket, levelezéseket II. Rákóczi György korából, és amit ott nem tudtak megfejteni, az számjellekkel szerepel a lapokban.

Húsz éve én két kisebb titkosírást megfejtettem, utána nem találkoztam titkosírásokkal. Négy éve egy konferencián két kolléga – Kasza Péter, aki az SZTE-n tanít és Szabó András budapesti irodalomtörténész – is megkeresett. Szabó András egy kódolt Wesselényi levelet, Kasza Péter pedig egy Brodarics levelet adott, amelyben négy sornyi kódolás szerepelt.

Mivel matematikus szakra jártam, mondtam, hogy majd én megfejtem, de egyedül nem ment volna, ugyanis mindkét szöveg latin nyelvű, tehát nagyon alapos latinnyelv-ismeret kellett hozzájuk. Hanna latin szakos, de ő nem volt gyakorlott titkosírás-fejtésben. Az első reakciója az volt, hogy „Á, ezt nem fogjuk tudni megfejteni!”. Én mondtam, hogy „ha az értelmezésben segítesz, akkor a rejtvényfejtő részével én megpróbálkozom”. Egyébként neki is nagyon racionális, logikus gondolatmenetei vannak, imád kombinálni. Ehhez pont ez kell. Két nap alatt „kivégeztük” mindkét szöveget.



Akkor megjött a kedvünk. Mivel Hanna történelem szakos, közösen készítettünk egy bibliográfiát arról, hogy hol vannak kiadva titkosírásos levelek, aztán jött az Országos Széchenyi Könyvtár, az Országos Levéltár, a Ráday Levéltár, a budapesti Egyetemi Könyvtár. Elkezdtünk gyűjteni, és gyűjtés közben további fejtések történtek. Most harmincnynél tartunk: ez ennyi különböző ügyet jelent. Tehát ha például egy Teleki levelezésben van 10 Teleki levél, de mindegyik ugyanazzal a kódrendszerrel készült, az egynek számít.

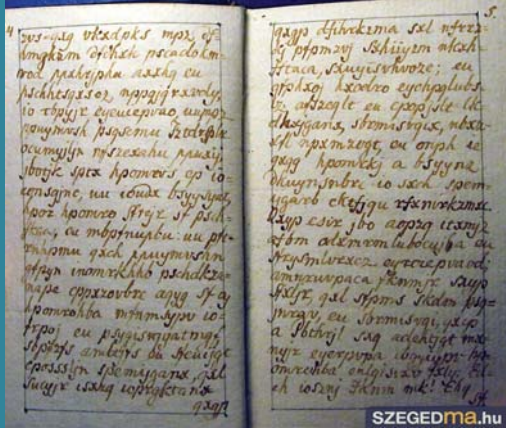
A harmincnolc irgalmatlanul nagy szám. Magyarországon eddig nagyon kevés sikeres fejtésről tudunk. Thaly Kálmán és Szilágyi Sándor a 19. században sikeresen megoldott egy-egy titkosírást. Gyürk Ottó és Gilicze Gábor a Gárdonyi Titkosnaplót. Van néhány ember, aki fejtett már titkosírást, egyet vagy kettőt, de aki kettőnél-háromnál többet, olyat nem ismerek.

Mi lepődtünk meg a legjobban, amikor észrevettük, hogy már 10 fölött járunk. Ezután megmutattuk a fejtéseket az Irodalomtudományi Intézetben. Ebben a listában már a nagybajomi szabadkőműves titkos irat is benne volt, ez kapott sajtónyilvánosságot.

21

21
MAG

Vadász



Alkalmas lehet ugyanazon kód több titkosírás megfejtésére?

Ilyen csak akkor történhet, ha mondjuk Pázmány Péter és I. Rákóczi György megállapodnak, hogy „Levelezzünk!”. Elküldi az egyik a másiknak a „kulcsot”. Ha ezt a kulcsot nem cserélik le, és többször ugyanazt használják, akkor előfordulhat, hogy két levélváltás is ugyanazzal a rendszerrel működik. De még két ember levelezésénél is bekövetkezik, hogy egy-két hónap vagy egy-két hét után úgy döntenek, lecserélik a kulcsot, mert észnél vannak és tudják, hogy feltörhető, elveszhet, megtalálhatják.

Ha Thököly Imrének a kuruc mozgalmak korában egy rajtaütés során menekülnie kellett, hátra kellett hagynia minden ingóságát, személyes dolgát, és az ellenfél megtalálta Thököly ezüst írókészletét,

benne a titkosírásos kulcsokkal, akkor abban a pillanatban ezek a kulcsok tovább nem voltak használhatók. II. Rákóczi Ferenc levéltárában 70 korabeli Rákóczi-kulcs van, számozva. Fejedelmi udvarokban ennek komplex rendszere volt, magánhasználatban pedig nagyon esetleges, hol ilyen, hol olyan. Vannak ördögien nehezek is, ilyenek például a nemzetközi diplomácia kulcsai.

Pálóczi Horváth Ádám szabadkőműves naplójában Ádámtól Aquinói Szent Tamásig sorol szabadkőműves nagymestereket. Természetesen egyik említett személy korában sem létezett még a szabadkőművesség. Mi lehetett a szerző célja a megírás-sal és a titkosítással?

A szabadkőművesek a saját nagymestereik geneológiáját, leszármazási rendjét szertartásos okokból tartják nyilván. Ez egy titkos rend és büszkék arra, hogy ősi eredetűek. A beavatásokban a mai napig hatalmas szerepe van Hirámnak. Az ő neve jelenik meg a szertartás során. Tehát Ádámtól Hirámgig és Hirámtól Tamásig. Hirám Salamon templomának az építőmestere, azaz kőműves, az első szabadkőműves.

Az a fajta Ádámgig visszanyúló, a középkori kereszténységet is magába foglaló névsor, melyet Pálóczi Horváth írt le, teljesen egyedi. Létezik egy hasonló tartalmú magyar nyelvű kézirat, amelyről azt gondolta a szakma, hogy ezt Pálóczi Horváth találta ki, az ő agyszüleményének tekintették. A titkosírás megszületése azt bizonyítja, hogy ez nem így volt, ő egy német Federspiel nevű hadnagytól kapta az eredeti kéziratot. Azért kapta, mert be akart lépni a szabadkőművesek közé. Miután beavatták, megfejtette, használta, átvette. Ez az írás valószínűleg azért titkos, mert a szabadkőművesek titkos társaságának szent titkait őrzi. Rituális okokból. A titkos tudásnak van egy efféle önmítosza.

Tervezik, hogy kiadnak egy gyűjteményt titkosírásokból valamint egy kódfejtéssel kapcsolatos könyvet. Elérhetővé teszik módszerüket a „nagyvilág” számára?

Nincs értelme ezt magunkban tartani. Ez a könyv kéziratban már szinte teljesen készen van. Javítgatjuk, igazítgatjuk, kiadót keresünk, lényegében összeállt. Ez afféle vegyestár, svédasztal. Az volt a célunk, hogy minél gazdagabb mintát mutassunk arra vonatkozólag, hogy milyenek a titkosírások, tudniillik, úgy lehet elindulni a fejtéssel, hogy látom a „mezőnyt”. Pontosan az a célja a könyvnek, hogy ne csak a metódust mutassa meg, hanem a fejtés egyes lépéseit részletesen, fejtés közben.

Nem féltett titok ez: az alapeljárásoknak, a nyelvstatisztikának, a magánhangzók elkülönítésének, a betörési pontok keresésének nemzetközi szakirodalma van. Ami miatt ez nem fog szélesebb körben működni az az, hogy a hétköznapi olvasó nem fog bemenni a Ráday Levéltárba kuruc kori eredeti kéziratok között bogarászni. Ha előkerül egy titkos kézirat, akkor úgyis az a fontos, hogy el lehessen olvasni, nem az, hogy én fejtsem meg.

Gondolkodnak-e azon hogy többet foglalkozzanak a kódfejtéssel tudományos körökben, hogy tanítsák az egyetemen?

Biztosan lenne rá érdeklődés. Néhány egyetemi órát tartottunk, néhány előadást a tanszéken, egyet az Eötvös Kollégiumban. A Pálóczi szakértők nagyra értékelték, hogy megfejtették a naplószöveget. Kasza Pétert, akinek Brodarics István a szakterülete, örömmel töltötte el, hogy Hanna felfedte a Brodarics szöveget.

Mindezekon kívül azonban történészek, irodalomtörténészek eddig nem kezelték a kódfejtést önálló témaként, nem igazán került ez előtérbe. Most a sikeres fejtések után arra várunk, hogy szorosabb szakmai együttműködés alakuljon ki, hogy ezzel a metódussal eddig tisztázatlan ügyek derüljenek ki. Tehát szakmai kapcsolatokat keresünk, történészekkel való közös munkát szorgalmazunk. Örülünk mindenféle konferencia-előadásnak, mert akkor létrejönnek ezek a kontaktok.

ofcma

MAGAZIN

Walter 22



Miért csinálja ezt az ember?

Mert ha rákapott az ízére, akkor függővé válik. A szakmai készségek szerencsés együttállása valósult meg esetünkben: matematika, irodalomtörténet, latin, történelem.

A titkosírások megfejtése olyasmi, mint az ejtőernyőzés: fölmeleg az emberben az adrenalin és addig nem hagyja nyugodni a kérdés, amíg meg nem oldja. Vannak nagy megoldatlan rejtélyek, nemzetközi és magyar vonatkozásúak is, amelyeken állandóan töri a fejét.

A bölcsész kutató tudja, hogy a saját szakmájához ugyanúgy kell logika, mint például a természettudományokhoz. Egy filozófus akkor filozófus, ha kombinatív, ha ravasz, ha széles körben tájékozott. Nem olyan nagy bűvésztüccs ez, demisztifikálnám a dolgot. Nem én vagyok a zseniálisan ördögös agyú titkosírás-fejtő vagy kódtörő, de nekem volt szemem arra, hogy ezzel érdemes próbálkozni. Látszólag a rejtély megfejthetetlenül nehéz, ha közelebb hajol az ember, akkor kiderül, hogy ezt meg lehet oldani. Ha ezt a könyvünk el tudja magyarázni, akkor lesz sikeres.

Módszertani kisokos

Tisztázni kell, hogy ha azt mondjuk ma hétköznapi beszélgetésben, hogy titkosírás, mindig arra gondolunk, hogy az ABC minden betűjének van egy jele. Ha ez lenne a titkosírás, akkor mindegyik nagyon könnyen megfejtendő lenne, ha elég hosszú a szöveg.

Petróczi Kata Szidónia, az első magyar költőnő kap egy levelet, amiben van egy 45 betűs titkos rész. Ez így nagyon nehéz, mert 45 betű nem elég a fejtéshez. Ha 300-400 van, akkor egy olyan típusú klasszikus titkosírás, hogy „egy betű egy jel”, egyszerű nyelvstatisztikával fejtethető.

A dolog ott válik nehezebbé, amikor egy betűnek több jele is lehet, a gyakoriaknak hét-nyolc is. Előfordulhat a jelek között semmit nem jelentő jel, a „nullitas”. Rákóczi fejedelmi udvarában használtak olyan kulcsot, amelyben van „Backspace” kód, azaz visszatörölő jel. Egy ilyen szöveget egyszerű statisztikával nem lehet feltörni. Vannak betűpárokat, szótagokat, szavakat jelölő rendszerek vagy olyanok, amelyek a jel helyzetétől függenek. Tehát ha az első helyen áll, akkor azt jelenti, hogy „a”, ha a másodikon, akkor azt, hogy „b”.

Először az összes körülményt tisztázni kell, hogy a szöveg milyen nyelvű, miről szól, ki írja kinek, mikor. Filológiai vagy művelődéstörténeti kérdéseket kell tisztázni. Utána azonnal következik, hogy hogyan lehet rejtjelezve. Mohács idején például csak néhány fajta titkosírás jöhet szóba, mert mást nem használtak még abban a korban. Ha Kossuth korában keletkezett a levél, akkor már bármilyen kód szóba jöhet, mert már mindent ismertek. Ha megvan a nyelve, akkor természetesen jön a statisztika, miből hány darab van, melyik a leggyakoribb jel, hogyan néz ki szöveg, tagolva van-e szavakra, látok-e vesszőket, szóközöket, stb.

Lényeges, hogy van-e a szövegnek felismerhető betörési pontja. Ez azt jelenti, hogy ki tudom találni, hogy mi van odaírva. Egy imádság utolsó szava például általában az, hogy *ámen*. Egy levél első két szava az, hogy *Kedves Barátom*. Ha csak részben van titkosítva a levél, akkor néha megkínál betörési ponttal. Kemény János erdélyi fejedelem egyik levelében szerepel egy kétbetűs szó titkosan, utána pedig közvetlenül az áll, hogy kezük se lábuk. Azonnal ki lehet találni, hogy a se szócska van előtte. Ha ilyen nincs, akkor ismétlődéseket kell keresni, mintázatokat. Minden kódtörő úgy dolgozik, hogy feltérképezi a kódokat, hogyan szerepelnek egymás mellett. Vannak matematikai algoritmusok, amelyekkel el lehet különíteni magánhangzókat és mássalhangzókat, pusztán azon az alapon, hogy melyik melyik mellett áll szívesen. Rendszert kell keresni és kombinálni.

Ez olyan, mint egy rejtvény, ami nem hagy nyugodni, amíg ki nem jön. Valójában nem nehezebb ennél. Egy picit tájékozódni kell a titkosírásos rendszerek ügyében, kicsit érteni kell a korhoz, a nyelvhez. Anélkül nem megy. Egy matematikus azért nem tud ilyet fejteni, mert nyelvtudás nélkül nem tud elolvasni egy kézírásos latin levelet, egy bölcsész pedig hiába tudja elolvasni, megáll ott, hogy „jaj, itt számok vannak!”.

**Fotók: <http://szegedma.hu/>
Online Újság a Táncsicsban**