Láng Benedek

MTA Doktori pályázat,
Filozófiai és Történettudományok Osztálya

Titkosírás a kora újkori Magyarországon (1500–1711)

Tézisfüzet

BUDAPEST
2016

I. A doktori műben tárgyalt kérdéskör tudománytörténeti előzményei és a doktori mű célkitűzései

Az elmúlt évtizedekben a titok mint társadalmi jelenség növekvő szakmai figyelem fókuszába került. A titkok átadása, a kommunikáció titkos útjai, a diplomáciai információ elrejtése, a tudományos titkolózás eszközei, a technológiai eredmények visszatartása, a magánélet titkai, a rejtélyek ábrázolása a művészetben, más emberek valamint a természet titkainak kifürkészése mind olyan témák, amelyek alapvető szerepe politikai egységek, kisebb és nagyobb közösségek, szakmák, egyházak és családok működésében tagadhatatlan.

Ez a szerep számos fontos publikáció témájává vált. William Eamon,[1] Agostino Paravicini-Bagliani,[2] William Newman és Anthony Grafton,[3] Karma Lochrie,[4] Tanya Luhrmann,[5] Pamela Long,[6] Koen Vermeir,[7] Aleida és Jan Assmann,[8] szerkesztett kötetei, monográfiai és publikációi jól mutatják a titok-fogalmak feltárása iránt megnövekedett igényt a kortárs vezető kutatók köreiben.

A szakirodalom csakúgy, mint maga a témakör, igen gazdag, és közös jellemzőjeként elmondható, hogy komoly erőfeszítést tesz a titok jelenségének kontextualista bemutatására, a titkolózás társadalmi hátterének, vonatkozásainak és következményeinek feltárására. Azonban ezeknek a titokkal kapcsolatos kutatásoknak és feldolgozásoknak van még egy közös jellemzőjük: szinte egyáltalán nem emlékeznek meg a kriptográfia (titkosírástan) és a kódfejtés jelenségéről, és ha

[1] William Eamon, *Science and the Secrets of Nature: Books of Secrets in Medieval and Early Modern Culture* (Princeton: Princeton University Press, 1994).
[2] *Il Segreto / The Secret*, ed. A. Paravacini Bagliani, *Micrologus*, vol. XIV (Florence: SISMEL, 2006).
[3] *Secrets of Nature: Astrology and Alchemy in Early Modern Europe*, ed. William Newman and Anthony Grafton (Cambridge, MA: The MIT Press, 2001).
[4] Karma Lochrie, *Covert Operations: The Medieval Uses of Secrecy* (Philadelphia: University of Pennsylvania Press, 1999).
[5] Tanya Luhrman, „The magic of secrecy," *Ethos* 17 (1989): 131–165.
[6] Pamela O. Long, *Openness, Secrecy, Authorship: Technical Arts and the Culture of Knowledge from Antiquity to the Renaissance* (Baltimore: The Johns Hopkins University Press, 2001).
[7] Koen Vermeir, „Openness versus secrecy? Historical and historiographical remarks." *The British Journal for the History of Science*, 45 (2012): 165-188.
[8] Aleida Assmann and Jan Assmann, eds. *Geheimnis und Öffentlichkeit (Schleier und Schwelle I,* Munich: Fink, 1997); *Geheimnis und Offenbarung (Schleier und Schwelle II,* Munich: Fink, 1998); *Geheimnis und Neugierde (Schleier und Schwelle III,* Munich: Fink,1999).

olykor mégis, kizárólag a kriptográfiai módszerek és a politikai titkosírások területeire merészkednek. A titkosírás elhanyagolása azért is meglepő, mert nehéz lenne tagadni azt, amit Dejanirah Couto így fogalmazott meg a kora újkori oszmán birodalomban folyó kémkedésről szóló kiváló cikkében: "kriptográfia nélkül, a titkolózásnak hiányzik az anyagi formája vagy olvashatósága" (without cryptography, secrecy lacks material form or readability).[9] A titkosírások kontextusa a titkolózás, feldolgozásának helye és kontextusa pedig a secrecy irodalomban volna.

A másik oldalról nézve a kérdést, természetesen magának a titkosírás használatnak is kiterjedt szakirodalma van. A huszadik század Alois Meister két rendkívül alapos és gazdagon dokumentált kötetével kezdődött, amelyekben a szerző a rejtjelezés történetének európai kezdeteit vizsgálta, az itáliai városok és a pápai udvar késő középkori és kora-újkori diplomáciájának titkosírásait.[10]

Bár a Meistert megelőző és követő évtizedekben számos hasznos cikk, forráskiadás és monográfia jelent meg, mégsem túlzás azt mondani, hogy a titkosírás-történet mint diszciplína csak David Kahn 1967-es vaskos monográfiájának, a *Codebreakers*-nek hatására született meg.[11] Kahn az akkor elérhető tudás alapján módszeresen végigtekintette a rejtjelezés történetét a kezdetektől a második világháborúig. Kahnnak alapvető szerepe volt a titkosírás-történet folyóiratának, a *Cryptológiá*nak a megalapításában, amely 1977 óta évente négy számban közöl fontos tanulmányokat, valamint nagy mennyiségben recenziókat titkosírás-történettel kapcsolatos szakkönyvekről.[12] Kahn szintén meghatározó alakja a szakma két évenként megrendezett találkozóinak, a Marylandben az NSA szervezte nagy titkosírás-történeti kongresszusnak. A folyóirattal, konferenciával és számos publikációval rendelkező szakma megerősödött, a forrásanyag rendszeresen ad

[9] Dejanirah Couto, "Spying in the Ottoman Empire: Sixteenth-Century Encrypted Correspondence," in Francisco Bethencourt and Florike Egmond, eds. *Cultural Exchange in Early Modern Europe (Volume III) - Correspondence and Cultural Exchange in Europe, 1400–1700* (Cambridge: Cambridge University Press, 2007) 274-312, a hivatkozott mondat: 278.
[10] Aloys Meister, *Die Anfänge der modernen diplomatischen Geheimschrift* (Paderborn: Ferdinand Schöningh, 1902); idem, *Die Geheimschrift im Dienste der päpstlichen Kurie von ihren Anfängen bis zum Ende des 16. Jahrhunderts* (Paderborn: Ferdinand Schöningh, 1906).
[11] David Kahn, *The Codebreakers. The Story of Secret Writing* (London: Weidenfeld and Nicolson, 1967); bővített kiadás: *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1996).
[12] http://www.tandfonline.com/toc/ucry20/current

munícióthoz további áttekintéseknek és monográfiáknak,[13] amelyek közül a legsikeresebb és legnagyobb hatású Simon Singh magyarul is megjelent *Kódkönyv*e volt.[14]

E publikációk jelentős részére igaz azonban (nem csak a kora-újkort illetőleg, bár most elsősorban azt vizsgáljuk), hogy elsősorban a titkosítási módszerekre koncentrálnak, és e módszereket ritkán igyekeznek a felhasználásuk társadalmi kontextusában tárgyalni. Szinte kizárólag két kérdéskör kerül terítékre. Az egyik azoknak a titkosítási és kódfejtési eljárásoknak a bemutatása és összehasonlítása, amelyet jelentős 15–17. századi szerzők, Leon Battista Alberti, Johannes Trithemius, Giambattista Della Porta, François Viète, Gustavus Selenus, Blaise Vigenère, vagy Athanasius Kircher fedeztek fel vagy fejlesztettek. A másik pedig különféle országok és városok diplomáciai gyakorlata, azaz hogy hogyan kódoltak titkos üzeneteket követutasításokban, kémjelentésekben vagy összeesküvések során a kora-újkor diplomáciai levelezésében.

A kriptográfia bonyolult elméleti invencióit, és a lényegesen egyszerűbb diplomáciai gyakorlatát nem számítva azonban a titkosírások használata csak elvétve kerül a kriptográfia monográfiák tematikájába, pedig nemesek, tudósok, orvosdoktorok, egyetemi professzorok és diákok, alkimisták, mérnökök, és a társadalom más „mindennapos" szereplői szintén használtak titkosírásokat saját, nem diplomáciai, céljaikra.

Általánosságban elmondható, hogy a kriptográfia történeti szakirodalom – mint a tudománytörténet egyik területe – túlságosan internalista. Internalistának hívjuk azt a történeti megközelítést, amely egy adott tudomány múltjában elsősorban az „intellektuális" tartalmat keresi, azoknak a fogalmaknak, elméleteknek és módszereknek a születését és fejlődését dokumentálja, amelyek a ma használatban lévő elméletek és módszerek elődei. Ezzel szemben az úgynevezett „externalista" történetírás feladatának tekinti az adott tudományterület társadalmi, gazdasági és intézményes vonatkozásainak vizsgálatát is. Azt a társas környezetet kutatja, amelyben az illető technológia használatba került, és amely gyakran hatást gyakorol

[13] Edmond Lerville, *Les Cahiers secrets de la cryptographie* (Párizs: Rocher, 1972); L. Sacco, *Manuel de Cryptographie* (Paris: Payot, 1951); Gerhard Strasser, *Lingua Universalis: Kryptologie und Theorie der Universalsprachen im 16. und 17. Jahrhundert,* (Wolfenbütteler Forschungen, Vol. 38.) (Wiesbaden: Harrassowitz, 1988); Fred B. Wrixon, *Codes, Ciphers and other Cryptic and Clandestine Communication* (New York: Black Dog, 1998); Friedrich L. Bauer, *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie* (Berlin: Springer, 2000) angol kiadásban: *Decrypted Secrets. Methods and Maxims of Cryptology* (Berlin: Springer, 2002).

[14] Simon Singh, *Kódkönyv: a rejtjelezés és a rejtjelfejtés története* (Budapest: Park Kiadó, 2001).

magára a tudományos tartalomra is?[15] A kriptográfia történetének feldolgozásai néhány kevés, cikkterjedelmű kivételtől eltekintve, úgy tekintenek a rejtjelezésre, mint egy tudományos technológiára, és az alkalmazás társadalmi környezetével alig foglalkoznak.

Amíg tehát a titok jelensége nem kevés, társadalmilag érzékeny feldolgozást kapott, ezek alig érintik a titkosírásokat, másfelől pedig, a titkosírások kutatása alig integráltatik a titok kutatások kontextusába, és szinte csak mint technológia és diplomáciai gyakorlat kerül bemutatásra, leválasztva szélesebb társadalmi környezetéről.

Az eddigiekben részletezett elhanyagoltság még szembeszökőbb Magyarországon, amely pedig történeti konfliktusainak és széttagoltságának köszönhetően különösen termékeny talaja volt a titkosítási eljárásoknak – amint erre R. Várkonyi Ágnes többször is felhívta a figyelmet.[16] A jelenség a hazai kutatásban mégis meglehetősen elhanyagolt, annak ellenére, hogy több értékes kezdeményezés is történt a hazai szakirodalomban.

Mindjárt 1848-ban Ötvös Ágoston I. Rákóczi György korának titkosított levelezéséből adott ki egy igen reprezentatív válogatást – megfejtve.[17] Ötvös, aki eredetileg orvos volt, a gyulafehérvári Batthyány könyvtár gazdag gyűjteményéből válogatta a forrásit, és minden jel arra utal, a rejtjelezett levelek egy részét saját maga fejtette meg, és legalább hat különféle titkosíráskulcsot rekonstruált. Ötvös után – egy-két elszórt forráskiadást leszámítva – sokáig elnémult a hazai titkosírás-kutatás. Az 1970-es évekig kellett várni, amikor Révay Zoltán alezredes – feltehetően a katonai hírszerzésnél betöltött beosztásából fakadóan – érdeklődni kezdett a téma iránt, és előbb egy általános monográfiát írt a titkosírások történetéről (*Titkosírások: Fejezetek a rejtjelezés történetéből*),[18] majd egy – kis példányszámban kiadott, és azóta is nehezen fellelhető – szakkönyvet kimondottan a Rákóczi szabadságharc rejtjelezéséről.[19] Számos szakmai fenntartás ellenére Révay könyvei ma is hasznos

[15] Steven Shapin, „Discipline and Bounding: The History and Sociology of Science as Seen through the Externalism-Internalism Debate," *History of Science* 30 (1992), 333–369.
[16] Többek közt: R. Várkonyi Ágnes, „A tájékoztatás hatalma," in Petercsák Tivadar and Berecz Mátyás, eds. *Információáramlás a magyar és török végvári rendszerben* (Eger, 1999), 9-32.
[17] Ötvös Ágoston, *Rejtelmes levelek első Rákóczy György korából,* (Kolozsvár, 1848).
[18] Révay Zoltán, *Titkosírások. Fejezetek a rejtjelezés történetéből* (Budapest, Zrínyi Katonai Kiadó, 1978.)
[19] Révay Zoltán, *II. Rákóczi Ferenc és korának rejtjelezése (XVIII. század)* (Budapest: Magyar Néphadsereg Híradó Főnökség Kiadása, 1974).

kiindulópontjai lehetnek mindenkinek, aki a kora-újkori magyarországi rejtjelezéssel kíván foglalkozni.

A következő évtizedekben Rákóczi György, a Wesselényi szervezkedés, vagy Rákóczi Ferenc titkosírásai többször is szóba kerültek (leggyakrabban R. Várkonyi Ágnes tanulmányaiban),[20] kevés publikációban kaptak azonban főszerepet. Az egyik ilyen tanulmány Pázmány Péter és római információforrása, C. H. Motmann olasz nyelvű levelezését vizsgálja, amelynek igen komplex titkosírás kulcsát történelmi érvek és matematikai elemzés útján Tusor Péter történész és Máté Imre kódfejtő, az Országos Rejtjelfelügyelet nyugalmazott vezetője rekonstruálta.[21]

Elérkezve napjainkhoz Vadai István és Vámos Hanna kutatásait és kódtörését lehet említeni: megfejtetlenül maradt titkosírásokat adnak vissza a történettudománynak.[22] Eredményeik egy része még megjelenésre vár, a Pálóczi Horváth Ádám másolatában fennmaradt nagybajomi titkosírásos kézirat azonban, amelynek polialfabetikus kódját Vámos Hanna sikeresen megfejtette, jól mutatja milyen gazdag perspektívák nyílnak a történeti kódfejtés előtt.[23]

Végül pedig saját monográfiámat említem a sokáig gyanakvást keltő Rohonci kódexről,[24] amelynek megfejtése – Király Levente Zoltán és Tokai Gábor munkájának köszönhetően – hamarosan nyomtatásban is olvasható lesz.[25] Bár korántsem bizonyított, hogy a minden bizonnyal 16. századi kódex valóban kapcsolatban áll a magyar történelemmel, mint ahogyan az sem tűnik valószínűnek, hogy valódi titkosírással állunk szemben (ugyanis a mesterséges nyelvek kontextusa jobban magyarázza a 450 oldalas, teljes egészében kódnyelven írt imakönyvet), a monográfiámban a lehetséges történelmi párhuzamok bemutatásakor áttekintettem a

[20] Többek közt: R. Várkonyi Ágnes *A rejtőzködő murányi Vénusz* (Budapest: Helikon Könyvkiadó, 1987), 213-215.; *eadem*, „Az elveszett idő: Zrínyi Miklós nádori emlékirata?" *Hadtörténeti Közlemények* 113 (2000): 269-328, különösen: 291; eadem, „A tájékoztatás hatalma."
[21] Tusor Péter, "Pázmány bíboros olasz rejtjelkulcsa: C.H. Motmann 'Residente d'Ungheria': A római magyar agenzia történetéhez", *Hadtörténelmi közlemények* 116 (2003) 535-581;
[22] Vámos Hanna, Vadai István, „Kuruc titkosírások megfejtése," in Mercs István, ed., *Kuruc(kodó) irodalom: tanulmányok a kuruc kor irodalmáról és az irodalmi kurucokról*, (Nyíregyháza, Móricz Zsigmond Kulturális Egyesület, 2013), 216-228; Vámos Hanna, Vadai István, „Pázmány Péter és I. Rákóczy György titkosírása," in Ajkay Alinka, Bajáki Rita, eds., *Pázmány nyomában, tanulmányok Hargittay Emil tiszteletére*, (Vác: Mondat, 2013), 461-479.
[23] Vámos Hanna, „Leleplezett titok: Pálóczi Horváth Ádám titkos, szabadkőműves dokumentuma," in Csörsz Rumen István és Hegedüs Béla, eds., *Magyar Arión Tanulmányok Pálóczi Horváth Ádám műveiről* (Budapest: rec.iti, 2011), http://rec.iti.mta.hu/rec.iti
[24] Láng Benedek, *A rohonci kód* (Budapest: Jaffa, 2011).
[25] A megfejtők, Tokai Gábor és Király Levente Zoltán cikke megjelenés alatt áll.

hazai titkosírás történet forrásait és szakirodalmát, és bevezetőt kínáltam a történeti titkosírások megfejtésének módszereibe.

Amint láttuk tehát, hasznos esettanulmányok születtek a régió kriptográfiai gyakorlatáról, de sem módszeres összefoglaló, sem társadalmi szempontból érzékeny feldolgozás nem látott eddig napvilágot, és a valaha megfejtetlenül maradt források jelentős része máig olvasatlanul, sőt gyakran feltáratlanul várja a kutatóját. A történelmi Magyarország feldolgozása a titkosírások társadalomtörténete szempontjából korántsem tűnik elhamarkodottnak.

A mellékelt monográfia az első módszeres feldolgozás a kora-újkori Magyarország titkosírásainak történetéről. Olyan következtetéseket tartalmaz, amelyek a – rendkívül kiterjedt – forrásanyag szisztematikus gyűjtése és elemzése során fogalmazódtak meg. Könyvem egyik legfontosabb érve, hogy a 16. és 17. században jelentősen sokszínűbb volt a kriptográfiai módszereket használó személyek társadalmi és politikai helyzete, célja, kriptográfiai tudása és eszközhasználata, mint azt az eddigi – elsősorban a diplomáciai gyakorlatra koncentráló – szakirodalom mutatta. Ezzel szoros összefüggésben azt kívánom megmutatni, hogy éppen a titkosírás használók szélesebb társadalmi hátterét, eltérő attitűdjeit és sokszínű céljait tanulmányozva válik lehetségessé, hogy a rejtjelezés történetét visszaillesszük oda, ahova eredendően tartozik: a titkolózás (secrecy) kontextusába. Ha a kriptográfia történetét többnek tekintjük egy tudományos technológia puszta fejlődésénél, és rekonstruáljuk a helyét a társadalmi tevékenységek komplex rendszerében, akkor a tudománytörténet írásnak ezt a hagyományosan „internalista” módon művelt területét társadalomtörténeti kontextusba tudjuk helyezni.

A kutatás két célt fogalmaz meg. Egyrészt a rejtjelezés gyakorlatát és recepcióját vizsgálja különböző társadalmi kontextusokban, nem csupán a diplomáciában tehát – ahol a titkosítási módszerek kétségtelenül a legnagyobb számban és a leghatékonyabb formában kerültek alkalmazásra, – hanem a tudományos gyakorlatban, a vallási életben, a kézműves hagyományban, az egyetemi környezetben, az orvosok, a nemesek, az alkimisták, a mérnökök, a kémek, és az „átlagemberek” közt, mindazon területeken, ahol az eddigi kutatás elhanyagolta e kérdést. A másik célkitűzés pedig a titkosírások gyakorlatának integrálása a titok eszmetörténetébe, a különféle – magán, orvosi, vallásos, családi, politikai, és tudományos – titkolózás gyakorlatába, abba a kontextusba, ahova magától

értetődően tartozik, még ha ezt az eddigi kutatás nem hangsúlyozta is megfelelő mértékben.

A megválaszolandó kérdések száma jelentős. Először is érdemes módszeresen vizsgálni, hogy mi a kapcsolat a szándékos titkolózás különféle gyakorlatai és a rejtjelezés közt. Mi volt a titkosított információ tartalma? Politika, szexuális titok, magánélet, vagy tudományos tudás? Nemcsak az a kérdés, hogy meg tudjuk-e fejteni a kortársak által dekódolatlanul hagyott, és így máig rejtélyes szövegeket, hanem az is, hogy milyen típusú információtartalmat tartottak a történeti szereplők titkosítandónak. Ez akkor is releváns, sőt különösen akkor, ha mára az adott információ egyáltalán nem tűnik sem fontosnak, sem veszélyesnek. Egy forrás esetében érdemes tételesen összehasonlítani, melyek azok a tartalmak, amelyeket lekódoltak, és melyeket hagytak meg nyílt szövegben, bármely olvasó számára hozzáférhető módon. Ez a vizsgálat hozzásegít ahhoz, hogy a múlt szereplőinek a titkolózáshoz való attitűdjét megértsük.

Nem kevésbé fontos a tudásátadás útjainak feltérképezése. Hogyan terjedtek a társadalomban a titkosírás különféle technikái? Nyomtatott könyvek, kéziratok vagy személyes tudásátadás útján? Hol volt az alkalmazott rejtjel technikák forrása: a diplomáciai praxisban vagy Trithemius, Kircher, Della Porta kézikönyveiben? Mely módszerek érkeztek nyugatról, és melyek voltak a régió saját fejlesztései? Volt-e bármiféle tudásátadás a középkorban jelentősen fejlettebb arab, és a 16. században felzárkózó nyugat-európai rejtjelezési gyakorlatok közt, és ha igen, ez nem éppen Magyarországon ment-e végbe, ahol a nyugati és az oszmán kultúra konfrontálódott, és ahol kettősügynökök lehettek mind a két titkosítási hagyomány birtokában? Ha viszont nem ment végbe kelet-nyugati tudásátadás, mi lehetett ennek az oka?

Milyen mértékben terjedt a rejtjelezés és a kódfejtés gyakorlata a politikai szférán kívül. Összefügg-e bármilyen módon az alkalmazott titkosírások színvonala és kifinomultsága a társadalmi státusszal, a műveltséggel, a környező veszéllyel, vagy a rejtjelezőnek a diplomáciai gyakorlathoz való közelségével?

Mi volt a – sokszor polgári – felhasználók viszonya ahhoz a technológiához, amit használtak: értették-e, kihasználták-e a lehetőségeit? Mennyire bíztak abban, hogy a titkosított szövegek megőrzik titkaikat? Mi volt a céljuk: elrejteni egy adott információt vagy éppen felhívni rá a figyelmet? Mi az oka annak, hogy bizonyos naplókban bármely olvasó számára könnyen feltörhető módon rejtjelezték a titkokat?

Hogyan tudjuk pusztán a titkosíráskulcs elemzésével megállapítani, hogy az adott rejtjel politikai vagy magánéleti titkok elrejtésére szolgált-e? Hogyan lehet rekonstruálni pusztán rejtjeltáblák alapján, kik voltak az adott konfliktus főszereplői? Mitől függött, hogy grafikus jeleket vagy számokat alkalmaztak-e az adott titkosírásban?

Mennyire voltak tisztában a politikai és katonai konfliktusok résztvevői azzal, titkosított leveleiket esetleg megfejthetik? Hogyan észlelték a fennálló veszélyt – és ezt a veszélyészlelést hogyan tudjuk mi ma rekonstruálni? Milyen mértékben aknázták ki a rejtjelkulcs kínálta lehetőségeket, mennyire veszélyeztették időnként saját hanyagságukkal, értetlenségükkel az információáramlás biztonságát? Milyen tipikus hibákat követtek el, milyen félreértésekhez vezettek ezek a hibák? Tisztában voltak-e az ellenfél kódfejtési technológiájával? Tettek-e erőfeszítéseket, hogy egy titkosítási módszert a lelepleződéstől megvédjenek? Cserélték-e időben a kulcsokat? Egy adott politikai szereplő volt-e annyira óvatos, hogy különféle levelezőpartnereivel különféle kulcsokat használjon? Ki végezte a kódolást: a kancellária vezetője vagy maga a fejedelem? És ki végezte a kódfejtést? Tudjuk-e mi magunk rekonstruálni a források alapján, milyen módszerekkel dolgoztak a kódfejtők? Mennyire múlott a kódfejtés sikerén vagy kudarcán, hogy egy akció lelepleződött-e? Befolyásolta-e egy sikeres kódfejtés a történelem menetét?

Röviden (egy Jacques Le Goff parafrázissal élve): mi a közös a függetlenségért harcoló fejedelemben, a törökellenes harcot folytató nemesben, az egyetemi diákban, a császár titkárában, és a bányafelügyelőben – már ami a rejtjelezés gyakorlatát illeti?

II. A doktori műben tárgyalt kérdéskör(ök) forrásai és a feldolgozásuk során használt módszerek

Következtetéseimet a kora-újkori magyar történelem kínálta gazdag forrásanyag alapján vontam le. Bár pillanatnyilag – tudomásom szerint – nem áll rendelkezésre módszeres vizsgálat sem a kora újkori lengyel, sem a cseh, sem az osztrák Habsburg területekről, a magyar forrásanyagról is ez a monográfia az első, amely a – viszonylagos – teljesség igényével lép fel, a fennmaradt titkosírás kulcsok száma, és a sifrírozott levelek aránya a teljes forrásanyaghoz képest mindenképpen különlegesnek tűnik.

Míg a titkolózástörténet természetesen nem ismeri a politikai korszakhatárokat, a korban legfontosabb, úgynevezett homofonikus titkosírás elterjedése és használata meglehetősen jól kijelöli a kora-újkor első két évszázadát. Nagyjából a 16. század harmadik évtizedében váltják fel a monoalfabetikus módszereket (még ha ezek 1700-ra sem tűnnek el teljesen), és terjednek el az országgal kapcsolatos diplomáciai gyakorlatban, és nagyjából a 18. században adják át a helyüket komplexebb eljárásoknak. A magyarországi titkosírás-használat – mind mennyiségében, mind minőségében – a Rákóczi szabadságharccal ér a csúcsra, az ezt követő évtizedekben – részben a lecsendesedő politikai helyzet következtében is – alaposan lecsökken a fennmaradt rejtjelek száma, és jellegük is megváltozik. A forrásanyag tehát szinte maga jelölte ki az 1526-1711-es korszakhatárokat. Ezeket az évszámokat azzal a fenntartással követtem, hogy a Mátyás és Jagelló kor viszonylag kisebb számban fennmaradt forrásait végül nem zártam ki a vizsgálatból, így tulajdonképpen a kezdetein kezdtem a magyarországi rejtjelezés történetét. Másrészt pedig, amikor tanulságosnak tűnt, esetenként egy-egy Rákóczi szabadságharc utáni esetet is vizsgáltam, azonban az 1711 utáni időszakra nem tekinthető teljesnek a kutatásom.

A forrásanyag alaptulajdonsága a titkolózás esetében általában, a rejtjelezés esetében pedig különösen, hogy elszórva található, jelentős részt azonosítatlan és publikálatlan. Gyakran a katalógusok és levéltári segédletek sem emlékeznek meg arról, hogy egy levél pár bekezdése titkosírással készült.

Kivételt képez ez alól néhány rejtjeltábla gyűjtemény, amelyet valamikori gyűjtője éppen azért helyezett egy levéltári fasciculusba vagy fondba, vagy egy kézirattári jelzetre, hogy a hasonló típusú, jellemzően egy oldalas források egy helyen legyenek feltalálhatóak. Gévay Antal 19. századi másolatainak mappája az OSZK Kézirattárában a Magyarországgal kapcsolatos Habsburg diplomácia közel ötven 16. századi tábláját tartalmazza.[26] A bécsi Haus-, Hof-, und Staatsarchiv gyűjteményébe tartozó Staatskanzlei anyagok közt többé-kevésbé ábécérendben közel kétszáz hasonló kulcs található[27] (részben ezeket másolhatta Gévay), de e kivételesen gazdag gyűjteménynek csak egy része kapcsolatos a magyar történelmi szereplőkkel.[28] Teleki

[26] OSZK. Quart. Lat 2254.
[27] Fazekas Istvánnak és Pálffy Gézának mondok köszönetet, hogy erre az értékes anyagra felhívta a figyelmem.
[28] ÖStA HHStA Staatskanzlei Interiora Kt. 13-16. Chiffrenschlüssel.

Mihály tíz clavisát a Teleki család Marosvásárhelyi Levéltárának MOL-ban őrzött anyagai közt lelhetjük fel.[29] A Wesselényi szervezkedés felszámolásakor lefoglalt titkosírások (huszonkét kulcs és öt titkosírt levél) szintén Bécsben vannak összegyűjtve.[30] A Rákóczi szabadságharc titkosírástábláit három jelzet alatt találjuk, kettő ezek közül a fejedelem levéltárának emigrációba vitt részére, a Rákóczi-Aspremont levéltár MOL-ban őrzött – és az 1956-os, éppen a Rákóczi anyagot megtizedelő nagy pusztítástól szerencsére megkímélt – gyűjteményre vonatkozik,[31] a harmadik pedig Ráday Pál irataira a Ráday Levéltárban.[32] E három jelzet alatt körülbelül százharminc táblát találunk, de ezek közt nagy az átfedés, a valójában különböző táblák száma jelentősen kisebb. Kisebb – tíznél kevesebb kulcsot tartalmazó – gyűjtemények találhatók a Mednyánszky család levéltárában II. Rákóczi György és Mednyánszky Jónás levelezéséhez,[33] és Esterházy Pál levelei közt szintén a MOL-ban.[34]

A titkosírás kulcsoknak e koncentrált gyűjteményeit leszámítva azonban számos más táblára és magukra a levelekre az igaz, hogy csak igen nagy erőfeszítéssel, sokszor véletlenül, és gyakran más kutatók segítő tanácsait követve azonosíthatóak. A monográfia mellékletében található mintegy háromszáz rejtjelkulcs és több, mint ezerhatszáz levél szándékaim szerint nem csupán kiegészítései a tanulmányomnak, hanem a munka legfáradságosabb részének lenyomatai. Reményeim szerint a későbbi kutatás kiegészíti, javítja és haszonnal forgatja az általam összeállított repertóriumot.

Hogyan viszonyul az itt bemutatott forrásanyag a teljes fennmaradt forrásmennyiséghez? Ezt a kérdést az egyes kategóriákra lebontva lehet vizsgálni.

Teljességre törekedtem a titkosírástáblák esetében. Ez a forrástípus jellemző módon kéziratos, kézirattárakban vagy levéltárakban érhető el. Kevés került a kéziratos anyagból publikálásra,[35] miközben a nyomtatásban megjelent táblák egy része rekonstruált, azaz a cikk szerzője által megoldott rejtjelezett leveleken alapszik. Ezek a rekonstruált táblák is rendkívül értékesek, megjelenési helyüket minden esetben feltüntettem a repertórium megfelelő oszlopában. Nem lehetek biztos benne, hogy minden fennmaradt kulcsot megtaláltam, a kimutatás folyamatosan – bár

[29] MOL. P 1238 Teleki Mihály Gyűjtemény. Vegyes Iratok. Titkosírás kulcsok
[30] ÖStA HHStA Ung Act. Spec. Fasc. 327. Konv. D. Chiffres 1664-1668.
[31] Mol G 15 Caps. C. Fasc 43 és 44.
[32] Ráday Levéltár C64-4d2-25.
[33] MOL. P 497 Mednyánszky Család, 3. csomó.
[34] MOL. P 125 No. 119772.
[35] A legtöbb Révay Zoltán idézett publikációiban.

csökkenő sebességgel – nő, reményeim és levéltári benyomásaim szerint most a fennmaradt anyag nyolcvan százalékánál járhatok.

Szintén a teljességre törekedtem (feltehetően szintén nyolcvan százalékos sikerrel) a forráskiadványokban és feldolgozásokban megjelent rejtjelezett leveleket illetően. Ebben nagy segítségemre volt az, hogy az anyag – különösen a 19. századi forráskiadványok – jelentős része digitális formában hozzáférhető. Fontos hangsúlyozni, hogy a kiadott levelek jelentős része mára elveszett vagy lappang, a sokszor kétséges értékű forrástisztelettel készült szövegkiadásokból csak korlátozott módon vonhatók le következtetések. Mivel azonban a nyomtatott és digitalizált anyagon igen jól lehet mennyiségi vizsgálatokat folytatni a titkolózás mechanizmusaival kapcsolatban, és jól azonosíthatók a rejtjelezésre vonatkozó explicit állítások, korántsem tartózkodtam attól, hogy komolyan vegyem őket.

Végül pedig meg kell emlékezni a kéziratban fennmaradt rejtjelezett levelekről. Ezek nagy mennyiségét gyűjtöttem össze, elegendőt ahhoz, hogy következtetéseket vonjak le a forrástípusról és a vele kapcsolatos történelmi tendenciákról. De hogy az általam a repertóriumban feltüntetett több, mint ezerhatszáz levél mekkora hányadát képezi a levéltárakban megőrzött teljes mennyiségnek, felbecsülni sem merem. Van olyan hadi konfliktusból származó levéltári fasciculus, amelynek száz százaléka titkosított levél, ez azonban inkább kivételes, mint jellemző. Amikor egy országos politikában jelentős család levelezését kértem ki, átlagosan minden századik levél volt rejtjelezett. Más típusú levéltári forrásanyagnál elhanyagolható is lehet az arány.

Számos – főleg diplomáciai és magán levelezést tartalmazó – levéltári fond átvizsgálása után az a benyomás alakult ki bennem, hogy a fennmaradt iratmennyiségnek akár egy százalékát is részben vagy teljesen rejtjelezett levelek teszik ki. Amennyiben a benyomásom megalapozott, az anyag összegyűjtése több generációs munka, amelyhez reményeim szerint a saját kimutatásom legjobb esetben is csupán alapot biztosít. Az átvizsgálás során arra törekedtem, hogy a repertóriumba felvett kéziratmennyiség kellően szignifikáns legyen a következtetések levonásához, s hogy a későbbiekben előkerülő források csak pontosítani, de nem érdemben módosítani tudják mindazt, amit az alábbiakban leírok.

III. A doktori mű főbb eredményei

A kora-újkori magyarországi titkosírás-használatot közel háromszáz – jobbára kéziratos formában fennmaradt – rejtjelkulcs, és több, mint ezerhatszáz – körülbelül négyszáz kéziratos, a többi kiadott – sifrírozott levél alapján vizsgáltam, és a forrásokat részletes adataikkal más kutatók későbbi használata érdekében feltűntettem a doktori munka mellékletében. A kutatásba nagy számban vontam be olyan „külső" forrásokat és megjegyzéseket is, amelyek a titkosítás különféle formáival, különösen a rejtjelezéssel kapcsolatosak, de maguk nem rejtjelezettek.

A monográfiám fejezetei részletesen dokumentálják, hogy annak ellenére, hogy a fennmaradt forrásanyag jelentős része a politika (diplomácia, követjelentés, katonai levelezés, stb.) területére tartozik, a kriptográfia korántsem maradt kizárólag a központi diplomácia eszköze volt, számos társadalmi réteg használta mindennapi élete során. Nem volt szükségképpen a férfiak privilégiuma sem, több forrás is arra utal, hogy a politikával több-kevesebb kapcsolatban álló nők is kezeltek clavisokat. Az egyetlen szelekciós szempontot az jelentette, hogy értelemszerűen írástudók privilégiuma kellett, hogy legyen.

Ahogy a felhasználók sem voltak szükségképpen politikusok, úgy a sifrírozás célja sem volt szükségképpen politikai: a magánélet, a szerelmi kapcsolat, a túl intim barátság, a szégyen, a mértéken felüli alkoholfogyasztás, a katonai gyengeség, a félelem, a családi konfiktusok, az erkölcsi kihágások, a térítés részletei, a vallásos meggyőződés, a tudományos recept vagy a talizmánmágia titkosítására egyaránt adódnak példák. Ahogyan módszeresen végignéztük a titkosított és nem titkosított szövegrészek viszonyát, az eddiginél jelentősen részletesebb betekintést nyertünk a múlt szereplőinek titokfogalmába. Gyakran szembesültünk azzal, hogy számukra a titkosítandó és nem titkosítandó tudás határai másutt húzódnak, mint ahol nekünk visszatekintve logikusnak tűnne. A titkolózásnak (secrecy) és a magánszféra védelmének (privacy) fokozati kategóriáit azonosítottuk: a legritkább esetben volt valami teljesen elrejtve, a források inkább úgy viselkedtek, hogy maguktól csupán valamilyen fokú megértést tettek lehetővé, ennél behatóbb megértéshez pedig komolyabb erőfeszítésre volt szükség. Meglepően gyakorta találkoztunk olyan forrásokkal, amelyek bizonyos információkat kódoltak ugyan, a kód kulcsát azonban – egy másik oldalon – maguk kínálták fel az olvasónak. Amint a titok dekódolhatósága, úgy a titokhoz való hozzáférés is fokozatos volt, az egyik

közösségnek könnyebb, másiknak korlátozottabb hozzáférése nyílt az adott levélhez, kódexhez, naplóhoz, üzenethez. A titok mint tartalom és a titkolózás mint gyakorlat időnként elvált egymástól: a talizmánmágia kézikönyvei kevéssé rejtélyes szellemneveket titkosítottak, míg – ha a feltételezésünk helyes – a Rohonci kódexet senki nem kívánta szándékosan titkosítani, tartalma mégis titok lett.

A vizsgálat fontos részét képezte a kriptográfia technológiájának tudománytörténeti megközelítése. Amennyire a források engedték, feltérképeztem, hogyan viszonyultak a felhasználók az alkalmazott eszközhöz, mennyire értették alkalmazásának módját, védelmének szükségességét, hogyan cseréltek, és milyen gyakran váltottak titkosíráskulcsot. Némi meglepetést okozott, mennyire nem volt jellemző a kora-újkor Magyarországán – legalábbis a hozzáférhető források alapján – a homofonikus rejtjelek sikeres megfejtése. (Ez a monográfia egyik olyan területe, ahol könnyen el tudom képzelni, hogy a további kutatás módosítja az álláspontomat, és a most ismertnél szervezettebb és sikeresebb kódtörő iroda működését azonosítja.)

A vizsgálatba vont háromszáz éves periódusban megfigyeltünk bizonyos fejlődést. A politika fokozatosan elhagyta a monoalfabetikus titkosírás rendszereket, és előbb egyszerűbb, majd – Rákóczi korára – komplexebb homofonikus kulcsokat vezetett be. Hasonlóképpen maradtak el a grafikus jelekkel működő rendszerek, átadva helyüket a kezelhetőbb, számkódos behelyettesítéseknek. Ezzel párhuzamosan az egyszerűbb rejtjelezési technikák megjelentek a társadalom diplomáciától távolibb szintjein, különféle szakmák képviselőinek gyakorlatában is, itt azonban – talán a titok természete, talán a professzionális kódtörők hiánya miatt – a gyakorlat, úgy tűnik, végig megmaradt a monoalfabetikus szinten. Bár a korszak könyvtáraiban – ha nem is nagy mennyiségben, de – voltak hozzáférhető szakkönyvek, amelyek megtermékenyíthették volna a sifrírozási technikát, és amelyek a diplomáciai gyakorlattól távoli szereplők számára is hozzáférhetővé tettek szofisztikált módszereket, úgy tűnik e lehetőséggel nem sokan éltek. A kidolgozott sifrírozási módszerek egyedüli forrásának a politika tűnik maradni, minél távolabb kerülünk tőle, annál egyszerűbb módszereket találunk. (Ugyanakkor elképzelhető, hogy a további kutatás a mostaninál élénkebb tudásimportra fog utalni az oszmán-török kultúra irányából.)

A titkosírások elterjedése és mindennapossá válása közvetlen összefüggésben lehetett azzal a tendenciával, hogy a három részre szakadt Magyarországon a

társadalom széles rétegei találták magukat akarva-akaratlanul politikai ütközőzónában, és kényszerűen részt kellett venniük a tájékoztató hálózatban mint titkok tudói és továbbítói. Az 1711-es korszakhatárt követő időszakban – bár az írásbeliség éppen hogy növekszik – a politikai porond elnyugvásával és a katonai konfliktusok lecsengésével párhuzamosan visszaesik a titkosírás-használat.

Az elvégzett kutatásnak kettős haszna van. Egyrészt szövegközeli elemzés egy igen elterjedt forrástípusról, amely jellegéből adódóan a történelem számos kutatási területével kapcsolatban áll. Egy számítógépes szoftver segítségével valamint a megfelelő titkosíráskulcsokat azonosítva sikerült rekonstruálni több, korábban ismeretelen és titkosított volta miatt olvashatatlan levelet. Az adott eszközökkel további források rekonstruálása, és így a történettudomány számára hozzáférhetővé tétele várható. A munkám másrészt pedig általánosabb – társadalomtörténeti és kutatás-módszertani – következtetések levonására hatalmaz fel, így azon olvasók számára is releváns lehet, akiket a rejtjelezett levelek kevésbé, társadalomtörténeti fejlemények inkább érdekelnek.

IV. A doktori mű által tárgyalt kérdéskör(ök)ben a pályázó által korábban közzétett publikációi

Könyvek

Titkosírás a kora újkori Magyarországon: a titok és a rejtjelezés társadalomtörténete (1500–1711), (Budapest: Balassi kiadó, 2015) 340 old.

A Rohonci kód, Budapest: Jaffa, 2011, 227 old.

Unlocked Books, Manuscripts of Learned Magic in the Medieval Libraries of Central Europe, Penn State University Press, 2008. 334 p.

Cikkek

Ciphers in Magic: Techniques of Revelation and Concealment, *Magic, Ritual, and Witchcraft*, 2015/2, 125-141.

Shame, love and alcohol: Private ciphers in early modern Hungary, *Cryptologia* 39/3 (2015): 276-287.

Szerelem, alkohol és szégyen: titkosírások a magánéletben a kora újkori Magyarországon, Korall, 2014/2: 133-147

A rejtjelezés technológiájának használata Magyarországon az 1700 körüli években, *Aetas* 29 (2014/1): 86-111.

Héder Mihály, Láng Benedek, Lévai Szabolcs, **Filológiai okok egy monoalfabetikus titkosírásfejtő szoftver mellett: a program működése és tapasztalatai,** *Magyar Könyvszemle,* 129 (2013/4): 511-519.

Zrínyi Miklós titkosíráskulcsa, *Irodalomtörténeti Közlemények,* 117 (2013): 195-200.

A tudásátadás útjai a magyarországi kriptográfiai gyakorlatban *Századvég*, 67 (2013/4) ed.: Z. Karvalics László, 115-137.

Invented Middle Ages in 19th century Hungary: The forgeries of Samuel Literati Nemes, in Patrick Geary and Klaniczay Gábor, eds. *Manufacturing a Past for the Present: Forgery and Authenticity in Medievalist Texts and Objects in Nineteenth-Century Europe*. (Leiden: Brill, 2015). 129-143.

People's secrets: Towards a social history of Early Modern cryptography, *The Sixteenth Century Journal*, 45/2 (2014): 291-308.

Early modern ciphers as sources of history, *Perspectives, Journal: Réseau français, des Instituts d'études avancées* 8 (2012): 18-19.

Characters and Magic Signs in the Picatrix and other Medieval Magic Texts, *Acta Classica Universitatis Scientiarum Debreceniensis* 47 (2011): 69-77.

Az emberek titkai: A rejtjelezés társadalomtörténete Magyarországon, *Korall* 43 (2011): 174–189.

Why don't we decipher an outdated cipher system? The Codex of Rohonc, *Cryptologia,* 34 (2010): 115-144.

Miért nem fejtünk meg egy elavult titkosírást? – 2 (A „rohonci kódex": Megfejtési Kísérletek), *Magistrae Discipuli: Tanulmányok Madas Edit tiszteletére*. Szerk. Nemerkényi Előd. 193-199. Budapest: Argumentum Kiadó, 2009.

A világ felosztása – Mesterséges nyelvtervezetek Nyugat-Európában és Magyarországon, *Kommentár* 2009/5: 14-21.

Miért nem fejtünk meg egy elavult titkosírást? – 1 (A „rohonci kódex"), in *"Mielz valt mesure que ne fait estultie". A hatvanéves Horváth Iván tiszteletére*. Szerk. Bartók István et al., 141-147. Krónika Nova Kiadó, Budapest, 2008.