

Láng Benedek

Az emberek titkai

*A kora újkori magyarországi rejtjelezés társadalomtörténetének kutatási lehetőségei**

Mi a közös a széteső házasságban élő, rokonaival pereskedő magyar költő, az éle-téért rettegő szerb kém, a tudását féltékenyen őrző erdélyi pénznyomó, a törököt és Habsburgot egyaránt megvető magyar nemes, a konstantinápolyi követeivel levelező császár és az olaszokkal üzenetet váltó prímás érsek tevékenységében? Ezek a személyek a társadalmi ranglétra különféle fokain álltak. Bár mindannyian írástudók voltak, műveltségük nagyon is eltért egymástól, nemkülönben hatalmuk, illetve befolyásuk a politika menetére. Mégis, mindannyian ugyanah-hoz az eszközhöz nyúltak, amikor üzeneteiket megpróbálták megóvni a kíváncsi szemektől: titkosírások meglehetősen komplex rendszereihez.

TITKOK ÉS ÍRÁSOK

A titok mint társadalmi jelenség növekvő szakmai figyelem fókuszába került az elmúlt évtizedekben. A titkok átadása, a kommunikáció titkos útjai, a kódolás és a dekódolás technikái, más emberek, valamint a természet titkainak kifürkészése mind olyan témák, amelyek alapvető szerepe kisebb és nagyobb közösségek, szakmák, egyházak és családok stabilizációjában és működésében ma már tagad-hatatlan. Ez a szerep számos fontos publikációnak szolgált témájául. William Eamon a késő közép- és a kora újkori Európa titokirodalmának széles választékát és olvasóközönségét vizsgálta.¹ Pamela Long a bányászati traktátusok nyílt szöve-geivel állította szembe az alkímiai iratok titkolózását.² Agostino Paravicini Bag-liani szerkesztésében látott napvilágot a *Micrologus* sorozat egy tematikus kötete, mely a középkori titokfogalom különféle aspektusait járta körbe,³ míg egy másik szerkesztett kötet, ezúttal William Newman és Anthony Grafton műhelyéből,

* A tanulmány írásának idején előbb a Magyar Zoltán Posztdoktori Ösztöndíj, utóbb a Bolyai János Kutatási Ösztöndíj támogatását élveztem. A cikk alap gondolata Bobory Dóra, Gecser Ottó és Novák Veronika intellektuális segítségével nélkül soha nem állt volna össze értelmes kutatói tervvé, velük együtt dolgoztam ki ugyanis azt az ERC Starting Grant pályázatot, amelynek ez a téma a központi részét képezte. Az alábbi cikk egy több évre nyúló kutatási projekt első vázlatát tartalmazza.

¹ Eamon 1994.

² Long 2001.

³ Paravicini Bagliani (ed.) 2006.

a kora újkori alkímia és asztrológia területére koncentrált.⁴ Egy német tanulmánykötet szélesebbre nyitotta a perspektívát, és egyaránt tárgyalta a diplomácia titkosságát, a szexualitás intimitását, a titkok helyszíneit a művészetben.⁵ Karma Lochrie *Covert Operations* (Álcázott hadműveletek) című könyvében kimondottan a női titkokra, a pletykákra, a gyónásra és a szexualításra helyezte a hangsúlyt.⁶ Aleida és Jan Assmann sokszerzős monumentális kötetei kevésbé történeti irányultságúak, és több figyelmet szentelnek az irodalomnak és a kultúrtörténetnek, mindazonáltal jól mutatják a titokfogalmak feltárása iránt megnövekedett igényt a kortárs vezető kutatók köreiben.⁷ Számos további publikációt említhetnénk, amelyeknek talán nem szerepel a címükben, mégis e jelenség aspektusait vizsgálják.

Azonban ezeknek a titokkal kapcsolatos kutatásoknak és feldolgozásoknak van egy közös jellemzőjük: szinte egyáltalán nem emlékeznek meg a kriptográfia (titkosírás) és a kódfejtés jelenségéről, és ha olykor mégis, kizárólag a politikai titkosírások területére merészkednek.

A másik oldalról nézve a kérdést, természetesen maguknak a titkosírásoknak is kiterjedt szakirodalma van.⁸ Ezek a publikációk viszont elsősorban a titkosítási módszerekre koncentrálnak, és e módszereket a legkevésbé sem igyekeznek a felhasználásuk társadalmi kontextusában tárgyalni. Szinte kizárólag két kérdéskör kerül terítékre: ki milyen kifinomult titkosítási eljárásokat eszelt ki a kora újkori értelmiségiek közül (többek közt Johannes Trithemius, Giambattista Della Porta, Gustavus Selenus, Blaise Vigenère és John Falconere munkáit vizsgálva), valamint mely diplomáciai gyakorlatban hogyan használtak egy – az előbbi módszerektől tökéletesen különböző – siffrózási eljárást, azaz hogyan kódolták a titkos üzeneteket követutasításokban, kémjelentésekben, összeesküvések során általában a kora újkor olasz,⁹ spanyol,¹⁰ francia,¹¹ német¹² és lengyel¹³ diplomáciai levelezésében.

A kriptográfia bonyolult elméleti invencióit és a lényegesen egyszerűbb diplomáciai gyakorlatát nem számítva azonban a titkosírások alig kerülnek a kutatás homlokterébe, pedig nemesek, tudósok, orvosdoktorok, egyetemi professzorok és diákok, alkímisták, mérnökök és más „mindennapos” szereplői a társadalomnak szintén használtak titkosírásokat saját – nem diplomáciai – céljaikra.

⁴ Newman – Grafton 2001.

⁵ Engel et al. (Hrsg.) 2002.

⁶ Lochrie 1999.

⁷ Assmann – Assmann (Hrsg.) 1997, 1998, 1999.

⁸ A kiterjedt irodalomból itt csak a legfontosabbakat emelem ki: Kahn 1996, Wrixon 1998, Singh 2000, Strasser 1988. A *Cryptologia* folyóirat a hetvenes évek második fele óta kínál megjelenési lehetőséget a titkosírástörténeti tanulmányok számára.

⁹ Meister 1906 és 1902; Pasini 1873; Cecchetti 1868–69.

¹⁰ Devos 1950; Biauudet 1910; Speziali 1955.

¹¹ Devos – Seligman (éd.) 1967.

¹² Rockinger 1892; Stix 1936, 1937.

¹³ Karttunen 1911; Platania 1988.

Egyfelől tehát amíg a titok jelensége nem kevés társadalmilag érzékeny feldolgozást kapott, ezek alig érintik a titkosírásokat, másfelől pedig a titkosírások kutatása alig integráltatik a titokkutatások kontextusába, és szinte csak mint technológia és diplomáciai gyakorlat kerül bemutatásra, leválasztva szélesebb társadalmi környezetéről. Ez az elhanyagoltság még szembeszökőbb Közép-Európában, és így Magyarországon, amely történeti konfliktusainak és széttagoltságának köszönhetően különösen termékeny területe volt a titkosítási eljárásoknak (amint erre R. Várkonyi Ágnes többször is felhívta a figyelmet).¹⁴ Ez a jelenség azonban a kutatásban mégis meglehetősen elhanyagolt. Bár hasznos esettanulmányok születtek a régió kriptográfiai gyakorlatáról,¹⁵ sem módszeres összefoglaló, sem társadalmi szempontból érzékeny feldolgozás nem került eddig napvilágra, és a források jelentős része is megfejtetlenül, sőt egyáltalán feltáratlanul várja kutatóját.

A közép-európai régió, és benne a történelmi Magyarország területének feldolgozása a titkosírások társadalomtörténete szempontjából korántsem tűnik elhamarkodottnak. A cikk alábbi része e projektnek egy első összefoglalása, a források legkönnyebben hozzáférhető részének gyors bemutatása, ez a kutatás azonban egy többéves projekt keretében valósul meg, és egy monográfia elkészítését célozza. A kutatás két célt fogalmaz meg. Egyrészt a rejtjelezés gyakorlatának és recepciójának vizsgálatát különböző társadalmi kontextusokban (az egyháztól a szekulárisig, az udvaroktól a városi adminisztrációig, a diplomataktól a mesteremberekig) –, nem csupán a diplomáciában tehát (ahol a titkosítási módszerek kétségtelenül a legnagyobb számban és a leghatékonyabb formában tűntek fel), 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 esztétörténetébe, a különféle – magán- orvosi, vallásos, családi, politikai és tudományos – titkolózási gyakorlatokba, abba a kontextusba, ahova magától értetődően tartozik, még ha ezt az eddigi kutatás nem hangsúlyozta is megfelelő mértékben.

A megválaszolandó kérdések száma nem kicsi. Mi a kapcsolat a szándékos titkolózás különféle gyakorlatai és a rejtjelezés közt? Hogyan terjedtek a társadalomban a titkosírás különféle technikái? 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? 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 titkukat? Mi volt a céljuk: elrejtteni egy adott információt vagy éppen felhívni rá

¹⁴ Többek közt: R. Várkonyi 1999.

¹⁵ Az adott publikációkat lásd alább.

a figyelmet? 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 (még akkor is, sőt különösen akkor, ha mára az adott információ egyáltalán nem tűnik sem fontosnak, sem relevánsnak). És végül egy Le Goff-pa-rafrázissal élve: mi a közös az egyetemi diákban, a császár titkárában és a bányafelügyelőben – már ami a rejtjelezés gyakorlatát illeti?

TITKOSÍRÁSOK MAGYARORSZÁGON

A kora újkori magyar diplomácia és ezen belül a titkosírások használata semmivel nem volt lemaradva a nyugatiakhoz képest. I. Ferdinánd Bécsben, II. Rudolf Prágában, I. és II. Rákóczi György az Erdélyi Fejedelemségben, Thököly Imre Felső-Magyarországon ugyanazokat a típusú behelyettesítéseket használta, amikor követekkel, megbízottaikkal vagy tábornokaikkal leveleztek, mint nyugat-európai kollégáik. Igaz ez nemcsak az uralkodókra, hanem azokra a politikusokra is, akik beleszóltak az országos politikába, így Zrínyi Miklósrá, Teleki Mihályra, Bercsényi Miklósrá vagy Lippay György és Pázmány Péter érsekekre.¹⁶

A leggyakrabban használt módszer az úgynevezett homofonikus behelyettesítés volt. Egy homofonikus rendszer rejtjelkulcsa elfér egy-két oldalon. Általában három-négy különböző jelet vagy számot feleltetnek meg az ábécé betűinek, gyakoribb betűknek általában többet, hogy a rendszer ellenálljon a titkosírásfajtók legkedvesebb módszerének, a betűgyakorosság-vizsgálatnak. Semmit nem jelentő karaktereket, nullításokat kevernek a jelek közé, hogy összezavarják a dekódolót. Külön jeleket használnak a kettős karaktereknek, sőt gyakran minden elképzelhető szótag is kap egy saját karaktert. Végül pedig speciális jeleket, kódszavakat, úgynevezett nomenklátorokat kapnak a leggyakoribb szavak, történeti szereplők és földrajzi helyek is.

Korszakunkat, az 1400 és az 1700 közötti időszakot éppen az emeli ki a történelem homogén folyásából a titkosírások tekintetében, hogy a rejtjelezés gyakorló felismerték, a monoalfabetikus – egy ábécén alapuló – titkosírások elavultak, túlságosan kiszolgáltatottak a betűgyakorosság-elemzésnek, ugyanakkor a több ábécét alkalmazó, úgynevezett polialfabetikus titkosírások bonyolultságuk okán még nem terjedtek el a diplomáciában. Ennek az átmeneti időszaknak a legkedvesebb titkosítási eszköze a homofonikus titkosírás.

¹⁶ Révay 1978: 57–155. Ezen kívül Vadai István és Vámos Hanna kutatásait lehet említeni, amelyeknek eredményei megjelenés alatt vannak. Vadai és Vámos számos megfejtetlenül maradt történeti titkosírást tört fel az utóbbi időben. Lásd: Régi magyar titkosírások, előadás az MTA Irodalomtudományi Intézetének Reneszánsz Osztályán, 2010. október 27-én.

1. kép

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	z	g	z
и	й	иꝛ	+	ю	л	п	ш	я	л	л	ꝛ	ꝛ	п	с	р	q	z	р	ѳ	ѳ	ѳ	ѳ
и	o	o	т	o	∞	8	8	α	ε	ε	÷	x	†	†	p	p̄	p̄	p̄				
-			‡				#															

Qua² que qui quo ѳ che come nuy vuy non per la m^a V. la S. V.

Nihil importantes	ñ	ñ	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
ab	ce	eb	eg	ib	b	ob	γ	vb	l													
ac	e	ec	e	ic	b	oc	γ	vc	l													
ad	γ	ed	e	id	b	od	γ	vd	l													
af	c3	ef	aa	if	b+	of	γ+	vf	b													
ag	c̄	eg	ā	ig	b	og	γ	vg	ij													
al	ca	el	ab	il	γ	ol	γ+	vl	j													
am	ce	em	ac	im	b3	om	γ	vm	la													
an	ci	en	ad	in	ba	on	γa	vn	le													
ap	co	ep	ā	ip	be	op	γe	vp	lo													
ar	cu	er	e+	ir	bi	or	γe	vr	lo													
as	es	es	a+	is	bo	os	γi	vs	lo													
at	et	et	āā	it	bo-	ot	γo	vt	lo													
ax	e+	ex	āā	ix	bu	ox	γo+	vx	ju													

Papa	3	Firentini	3 ^o	S. Roberto da San	
Colegio di cardinali	3 ^r	Duca de Calabria	3 ^u	Sever ^o	3 ⁴
Imperatore	3 ^r	Hippolita duchesse		Senesi	3 ⁴
Re di Franza	3 ^t	de Calabria	3 ^r	Bolognesi	3 ^r
Re darayona	3 ⁴	Duca de Modena	3 ^r	Duca Johanne	3 ⁴
Re de Inglaterra	3 ^a	Marchese de Mantoa	3 ⁿ	Re Renato	3 ⁴
Duca de Bregogna	3 ^e	Marchese de Mon-		Zenonesi	3 ⁴
Duca de Savoya	3 ⁱ	ferra	3 ^a	Nave	3 ^t
Duca de Milano	3 ^o	Conte de Urbino	3 ^a	Galee	3 ^r
Venetiani	3 ^{o-}	S. Alexandro	3 ⁱ	Duca de Bari	3 ³
				Filippo monsignore	3 ³

Homofonikus titkosírás 1448-ból, a Milánói herceg levelezéséből.

A rendszer nem tartalmazza kettős betűk jeleit, viszont gyakoribb kötőszóknak külön karaktereket feleltet meg¹⁷

¹⁷ Meister 1902: 30.

Pázmány Péter római levelezésében követett módszere különösen szép példája a homofonikus titkosírásoknak.¹⁸ C. H. Motman, az érsek itáliai információforrása üzeneteiben kettős számkombinációkat (számbigrammokat, mint például a 24) használt a nyílt szöveg betűinek kódolásához (rendszerint két bigrammot feleltetett meg egy betűnek, de a magánhangzók hármát is kaptak, mint egy jobb homofonikus kódábécében). Egy mássalhangzóból és egy számból álló kombinációkat használt szótagok kódolására (minthogy olasz nyelvről beszélünk, ezek mindig egy mássalhangzóból és egy magánhangzóból álltak). Valamint három számjegyből álló trigrammokkal jelölte a kódszavakat, ezek működtek tehát nomenklatorként. E kombinációk általában növekvő számsorban vagy betűrendben kerültek megfeleltetésre a betűknek, szótagoknak vagy kódszavaknak, a rendszer tehát igen szisztematikusan lett felépítve. Ez a struktúra – amely a rendszert könnyen használhatóvá, ugyanakkor sérülékennyé is teszi – azonban csak akkor szolgál a kódfejtő segítségére, ha már kellően előrehaladt a kódfejtésben ahhoz, hogy felismerje.

Pázmánynak ez a titkosírása, amelyet Tusor Péter történész Máté Imre kódfejtővel, az Országos Rejtjelfelügyelet nyugalmazott igazgatójával együtt fejtett meg, két további szempontból is jelentős. Egyrészt jól mutatja, milyen szintű és fontosságú diplomáciai források várnak még arra, hogy a kutatók elolvassák őket. Nem jelentéktelen forrásokról van szó: ezeket az üzeneteket valamikor a feladójuk olyan fontosnak tartotta, hogy titkosította őket, minden bizonnyal tehát olyan információkat tartalmaznak, amelyek nem fordulnak elő bármely más, a korszakból fennmaradt levélben. Másrészt pedig az is jellemző Pázmány levelében, hogy a rejtjelét egy történész és egy matematikus kódfejtő *együttműködése* útján sikerült feltörni. A homofonikus titkosírások jellegükénél fogva kényszerítenek ki effajta kooperációt. Míg ugyanis a betű és a szótagjelek azonosítása komoly matematikai, nyelvstatisztikai és logikai következtetéseket igényel, addig a földrajzi területeket és politikai szereplőket jelentő nomenklatorokat sokszor csak a történeti kontextus alapos ismerete révén lehet felfejteni.

Titkosírásokat nemcsak az országos szintű diplomácia használt, hanem a Magyarország történetében vissza-visszatérő Habsburg-ellenes szervezkedések, összeesküvések, szabadságharcok szereplői is.¹⁹ Wesselényi Ferenc összeesküvésének *sub rosa* egyezségei,²⁰ a Thököly-szabadságharc levelezése²¹ vagy II. Rákóczi Ferenc katonai döntései esetében élet és halál kérdése volt, hogy az üzenet ne jusson az udvar tudomására. Csak Rákóczi környezetéből mintegy száz, tökéletesen korszerű rejtjelkulcs (azaz közel száz *különböző* titkosírásrendszer) maradt fenn.²² Volt, hogy maga a titkosírás címzettje kérte Rákóczit, kevésbé buzgón titkosítson, mert leveleit a kulcs birtokában is nehezére esik dekódolni.

¹⁸ Tusor 2003.

¹⁹ Révay 1978: 124–151.

²⁰ R. Várkonyi 1987: 213–215.

²¹ MTA Mikrofilmtár, Mf 1606. A mikrofilmről Vadai Istvántól szereztem tudomást.

²² Révay 1974. A titkosírás-táblázatok másolatai: MTA Kézirattár, Ms 4951/5.

De nemcsak a hivatalos diplomácia és a nyílt ellenállás, hanem a politikai természetű nemesi levelezés is kiaknázta a rejtjelezésben rejlő lehetőségeket. A 16. század második felében és a 17. században a magyar nemesek egymás közt már leggyakrabban magyarul leveleztek. Zrínyi Miklós, Kemény Zsigmond, Barcsay Ákos, Apafi Mihály, Teleki Mihály és további főurak magyar leveleiben pedig nem volt ritka, hogy egy-egy szó, mondatrész vagy teljes mondat homofonikus rendszerben rejtjelezve került leírásra.²³ A titkosítás elsősorban személynevek és a politikailag kényesebb információk elrejtésére szolgált. Érdekes, hogy a titkosított szavak kiválóan tanúskodnak arról, hogy a Habsburggal és a törökökkel szemben is egyaránt gyanakvó, sőt ellenséges nemesaink éppen kinek a boszszújától tartottak jobban. Kemény János, későbbi erdélyi fejedelem például Barcsai Ákosnak írt levelében következetesen rejtjelezte az igen gyakran használt „pogány” szót mint a törökök kissé offenzív megnevezését.²⁴

A rejtjelezés technológiája igen árulkodó a történeti szereplők titokfogalmával, félelmeivel kapcsolatban. Zrínyi Miklós II. Rákóczi Györgyhez intézett hosszú levelében, az úgynevezett „nádori emlékiratban” olyan együttműködést kínál az erdélyi fejedelemnek, amelynek kitudódása mind a Habsburgok, mind a törökök előtt életveszélyes lett volna. Ebben az esetben akkor sem lennének meglepve, ha az egész levél titkosítva volna, és nem csak egy-egy politikai szereplő megnevezése volna elrejtve.²⁵ Ráadásul a levélnek nem is a legkritikusabb részei vannak kódolva, míg olyan, családi természetű részletek viszont igen, amelyeket bármely kortárs hamar megtudhatott. A titkosítás elemzése itt nemcsak a 17. századi titokfogalom rekonstrukciójára alkalmazható, hanem azt a célt is szolgálhatja, hogy a forrással kapcsolatos kételyeket megerősítse. A nádori emlékirat hitelességét ugyanis több *különböző* történeti érv alapján, nem utolsósorban a szokatlan módon használt titkosítás miatt R. Várkonyi Ágnes már 2000 körül kétségbe vonta, és arra a következtetésre jutott, hogy a szöveget nagy valószínűséggel Thaly Kálmán illesztette össze és részben hamisította.²⁶ Tisztább a helyzet I. Apafi Mihálynak Teleki Mihályhoz intézett levelében, ami tulajdonképpen egy követutastítás: rendes diplomáciai tartalomhoz illő módon gyakorlatilag az egész levél titkosítva van.²⁷

Egy másik, rövidebb, Zrínyitől Rákóczinak küldött levélben nehezen tudjuk elképzelni, hogy egy politikában jártas kortárs ne tudta volna azonosítani a nyílt szöveg magyar nyelvű kontextusa alapján, melyik kód áll a „közások”, a „magyarok”, az „udvar” és az „erdélyi fejedelem” helyett. Nem is beszélve arról, hogy a Zrínyi által az erdélyi fejedelemnek küldött levelekben használt titkosítás viszonylag kezdetleges volt a korszakban megszokottakhoz képest: ugyan

²³ Hargittay (szerk.) 1981: II, többek közt: 123, 146, 253, 258, 363. Köszönöm Almási Gábornak, hogy felhívta a figyelmem e forrásokra.

²⁴ Hargittay (szerk.) 1981: II. 258.

²⁵ Hargittay (szerk.) 1981: II. 123. Eredetileg: Thaly 1868.

²⁶ R. Várkonyi 2000, különösen: 291.

²⁷ Hargittay (szerk.) 1981: II. 363–364.

több szám felelt meg egy-egy betűnek, ezek azonban pusztán növekvő sorrendben voltak megfeleltetve az ábécének, és így viszonylag könnyen azonosítani lehetett őket akár pusztán próbálgatással is.²⁸ Itt inkább arra gyanakodhatunk, hogy a cél a hírvivők kizárása volt a kommunikációból, vagy pedig az, hogy egy esetleges felségárulási perben – ami hamar bekövetkezett, bár azt Zrínyi Miklós már nem érte meg – a bizonyíték ne legyen egyértelmű. Ki tudja?

Nehéz kérdések másutt is adódnak. Kemény János egy 1657-es, II. Rákóczi Györgynek írt levelében attól óvja (hiába) az éppen lemondott fejedelmet, hogy visszatérjen az elhagyott fejedelmi trónra.²⁹ A levél egy része titkosítva van, de ez a rész szinte semmi olyat nem tartalmaz, amit a levél többi részéből ne sejtjenék amúgy is. Mi lehetett az az aggodalom, amely ennek a szövegnek a rejtjelezésére készítette Keményt?

E problémák megértésére addig kell várnunk, míg feltérképezzük a 17. század titokfogalmának a miénktől alaposan eltérő területeit, amíg megválaszoljuk, hogy miért jelentett valaki számára egy adott információ titkot. Szintén kérdés, amit tudomásom szerint még senki nem vizsgált módszeresen, hogy hogyan cseréltek jelkulcsot az egyes nemesi családok: minden két család vagy politikai tényező viszonylatában külön kulcs volt használatban, vagy egy közös módszert osztottak meg többen? Bármelyik is a helyzet, milyen gyakran érezték szükségét, hogy e kulcsokat (amelyek, mint láttuk, egy kétoldalnyi táblázatot rendszerint nem haladtak meg) mint elavultat lecseréljék?

A titkosítás-történet különösen izgalmas fejezetét képviseli a közép-európai kémkedés. A kémek, titkos levelezők és összekötők titkos rendszere behálózta a török hódoltság, a Habsburg irányítás alatt lévő Magyar Királyság és az Erdélyi Fejedelemség területét is, a kémek beszerző szerződésének pedig gyakran részét képezte a kódoló módszer rögzítése is.³⁰ Azt gondolnánk, a szakma veszélyes volta miatt alig maradt fenn információ arról, kik is voltak ezek a titkos ügynökök (*Geheimagent, secretarius explorator*), de szerencsére nagyon is jól azonosítható személyek, sőt olykor teljes családok nevezhetők meg, ahol e különleges mesterség apáról fiúra öröklődött. Ezek az emberek pedig korántsem tartoztak a társadalom politikai elitjéhez: olyan orvosok, kereskedők, katonák, követségi tolmácsok voltak, akik közel voltak a tűzhöz, polgári foglalkozásukból adódóan sok emberrel találkoztak, és gyakori utazásaik nem keltettek feltűnést (míg mondjuk egy földműves túlságosan kiterjedt megbeszélései, levelezése és helyváltoztatása hamar gyanút ébresztett volna). A kémek gyakran az európai és a török kultúra határmezsgyéjén élők közül kerültek ki, leggyakrabban délszlávok, szerbek, bosnyákok voltak, máskor örmények, szefárd doktorok vagy törökökhöz szökött keresztény renegátok. Leveleik a bécsi *Haus-, Hof-, und Staatsarchiv* Hungarica és Turcica gyűjteményében, az Osztrák Állami Könyvtár

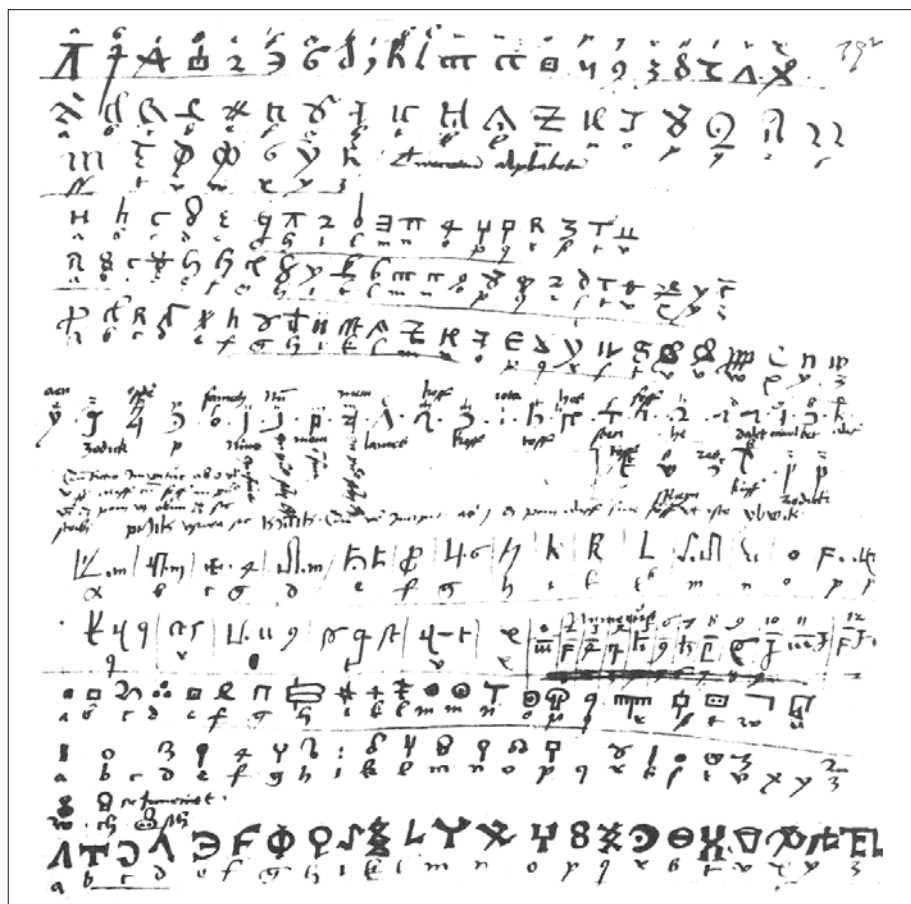
²⁸ A kétes hitelességű nádori emlékiraton kívül Zrínyi titkosító kulcsát lásd: Zrínyi 1958: 466, 477–479, 494.

²⁹ Hargittay (szerk.) 1981: II. 253–254.

³⁰ Kerekes 2007; 2003; 2010; Petercsák – Berecz (szerk.) 1999.

kézíráttárában és az Esztergomi Főszékesegyházi Könyvtárban maradtak fenn számos vastag kötetben, de több nemesi család levéltára is őriz kémjelentéseket. E levelekből a történész rendkívül részletes, életteli képet alkothat a kémek félelmeiről, műveltségéről, háttéréről, fizetésének nagyságáról, az őket fenyegető veszélyekről, de a rajtuk keresztül érkező információk természetéről is, valamint arról, hogy mindezt milyen komolyan vette a Habsburg udvar, mennyire sietősen dekódolta leveleiket az Udvari Haditanács.³¹ Minthogy e kémek nemritkán egyszerre kétfelé dolgoztak, más szóval kettősügynökök voltak, minden okunk megvan azt feltételezni, hogy valamiféle tudásátadásnak is csatornái lehettek a török (arab) és a Habsburg (nyugati) rejtjelezési technikák közt.

2. kép



Rejtjelábécék egy krakkói diák kézikönyvében³²

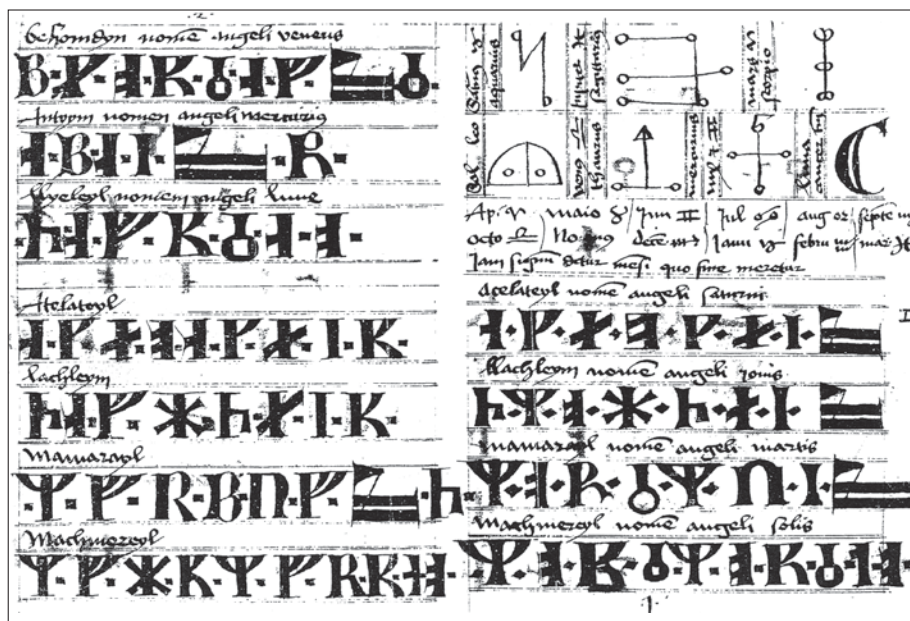
³¹ Kerekes 2007.

³² BAV Pal. Lat. 1375, fol. 19r. Lásd bővebben: Láng 2008: 132.

A kémeknél kevésbé veszélyes szakmát űző foglalkozásokban is dokumentálható a titkosírások használata, így az egyetemi diákok, a kézművesek és iparosok, sőt a költő Balassi Bálint életében is. Ami az egyetemi diákokat illeti, kézikönyveikben bőséggel maradtak fenn rejtjelábécék és rejtjelezett üzenetek a késő 15. és a kora 16. századból. Az alábbi példák nem Magyarország területéről valók, hanem a magyar diákok által is intenzíven látogatott Krakkói Egyetemről. Az egyik itt tanult német diák, Johannes Virdung de Hassfurt kódexében például egy teljes oldalon sorol fel különféle kódábécéket. Ezek azonban kivétel nélkül monoalfabetikus ábécék.³³

A krakkói diákok köreiben több példányban is forgott a *Rúnák könyve*, amelyben skandináv rúnabetűkkel szednek bolygószellemneveket. A rúnákkal (azaz tulajdonképpen egy egy ábécét használó egyszerű behelyettesítéssel) megírt talizmánok a felhasználó kezében különféle jó- és rosszindulatú mágikus célokra voltak alkalmasak.³⁴ Más, hasonló tartalmú szövegekben is előfordult, hogy szellemek neveit speciális jelekkel, egy angyali vagy démoni ábécé karaktereivel nevezték meg.

3. kép

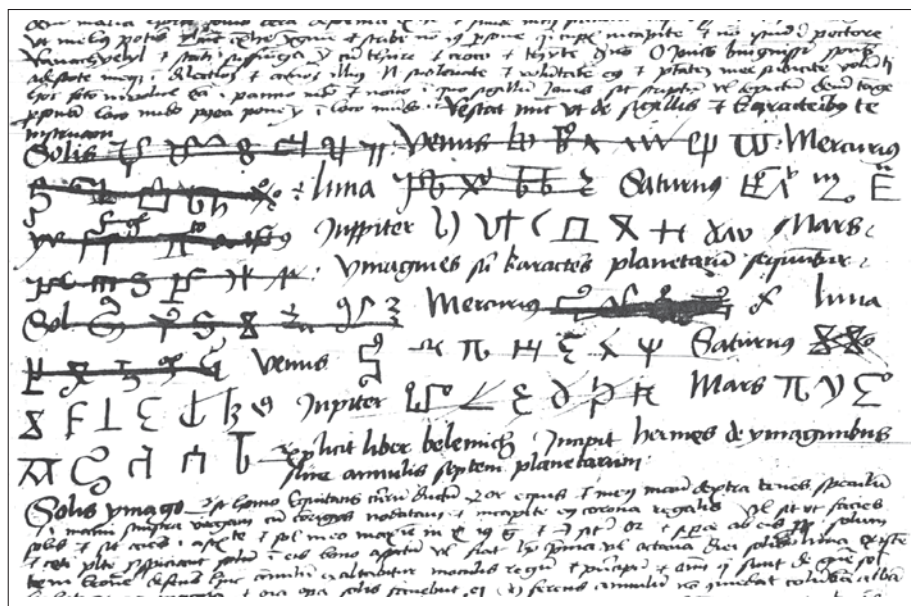


Egy oldal a Krakkóban másolt *Rúnák könyve* című szövegből³⁵

³³ Láng 2008: 3. és 9. fejezet.

³⁴ SLB N. 100, fol. 198r–200v; BAV, Pal. lat. 1439, f. 346r–347v.

³⁵ SLB N. 100, f. 198r, lásd: Láng 2008: 109–115.



Karakteres planetarum, azaz bolygó(szellem)e(k) karakterei
egy krakkói egyetemi kézükönyvben³⁶

Két közös vonása van ezeknek az ábécéknek. Egyrészt mindegyik megmarad egy viszonylag egyszerű szinten, és egyik sem lép túl a megszokott monoalfabetikus (egy ábécét használó) rendszeren, pedig ekkorra, a 15. és a 16. század fordulójára már viszonylag megszokottak voltak a nomenklátorokkal kiegészített homofonikus rejtjelek. Másrészt pedig mindegyik valamilyen mágikus szövegrészletet kódol le, és leggyakrabban a bolygószellemek neveivel működő talizmánmágia keretein belül marad. A rejtjelezés ebben az esetben a legkevésbé sem tűnik a rejtőzködés eszközének. Nemcsak azért nem, mert könnyen megfejthető ábécéről van szó, hanem azért sem, mert a latin szövegek egyéb, nem kódolt részeiből pontosan látható, hogy miről szól a szöveg, a titkosírás egyáltalán nem teszi hozzáférhetetlenné a tartalmat. Minden jel arra utal inkább, hogy a különös karakterek a szellemi szféra mágikus tartalmát voltak hivatottak megidézni vagy megnevezni, és paradox módon nem annyira elrejtették a szöveg rituális tartalmát, mint inkább felhívták rá a figyelmet. Rejtélyes megjelenésükkel mintegy reklámozták őket. A speciális betűk használatának célja tehát ebben az esetben nem annyira a kriptográfia igényeinek kielégítése, a rejtjelábécé karakterei inkább a mágikus nyelvhasználat eszközeként, a spirituális világgal való kommunikáció csatornájaként szolgálnak.

³⁶ BAV Pal. lat. 1375 f. 270v, lásd: Láng 2008: 117.

Rejtjelek használatával a tudomány és a kézművesek, iparosok világában is találkozunk. A nyugati tudományban többek közt Galileo Galilei használt titkosírást tudományos sejtéseinek dokumentálására abban a korban, amikor még a szabadalmi hivatal nem létezett, hogy tanúsítsa, ki, mit, mikor fedezett fel.³⁷ Kódolt szövegben írt Robert Boyle is, amikor nem szerette volna, ha alkímiai kísérleteinek eredményei kitudódnának,³⁸ és a reneszánsz mérnök, Giovanni Fontana (1395?–1455) több művében is használt behelyettesítéses titkosírást komplex hadigépezetei és technikai szerkezetei leírásához.³⁹ Magyar környezetből egyelőre csak a kevésbé ismert Kolozsvári Cementes Jánost, a 16. századi ötvöst tudjuk említeni, aki a kolozsvári pénzverdében mint „cementes”, azaz nemesfém-finomító és -felügyelő dolgozott. Százhusz oldalas magyar nyelvű naplójában időnként titkosírással kódolta – bányászati, kohászati, gyógyszerészeti, pénzverői és alkímiai – mondanivalóját, leggyakrabban csak egyes szavakat, de például rögtön a könyv elején magát a címét is.⁴⁰ A titkosírás rekonstruált rendszere azonban nem olyan fejlett, mint a diplomáciai és általában a nemesi levelezésben használt homofonikus rejtjelezés, hanem a késő középkori diákokhoz hasonlóan Cementes az egyszerű és könnyen feltörhető monoalfabetikus módszert használja.

Végül pedig érdemes külön szólni a várúr, költő, katona és nagy csábító Balassi Bálint titkosírásáról is. Balassi többszörös örökösödési perben állt rokonaival, összeférhetetlen személyisége és botrányai miatt számos város folytatott ellene eljárást, és szerelmi ügyei sem csökkentették elrendezendő problémáinak számát. Viszontagságos és konfliktusokkal teli életében sokat kényszerült magánéleti és anyagi titkokról levelezni, az egyik ilyen levelében pedig – mint a magyar nemesek politikai levelezésükben – részleges titkosítást használt, csak bizonyos szavakat, leggyakrabban személyneveket rejtjelezett. A módszer azonban egyszerűbb volt, mint Zrínyi, Kemény vagy Pázmány homofonikus kódjában: monoalfabetikus módszert használt, és még e kategórián belül is egy egyszerű eljárást: az ábécé első felének betűit megfeleltette az ábécé második fele betűinek, és fordítva. Hogy ezzel a módszerrel kit akart megtéveszteni, nem tudjuk, de végül is nem valószínű, hogy a bécsi udvar legjobb kódfejtői érdeklődtek volna örökösödési és szerelmi titkai iránt, a kotnyeles postások és orrukat mindenbe beleütő rokonok megtévesztésére pedig bizonyára ez is elég volt.⁴¹

Hasonlóképpen egyszerű, könnyen feltörhető (bár az utókor által sokáig nem azonosított) titkosírásról van tudomásunk Illésházy István 1605-ben feleségéhez, Pálffy Katalinhoz intézett magánleveléből, valamint a Kuun kódexnek egy

³⁷ Biagoli 2006.

³⁸ Principe 1992.

³⁹ Thorndike 1923–58: IV. 150–182; Birkenmajer 1932. *Bellicorum Instrumentorum Liber* (BSB Cod. Icon. 242), *Secretum de thesauro experientorum ymaginationis hominum* (BnF Cod. Lat. Nouv. Acq. 635).

⁴⁰ A Cementes Jánosról szóló információkért Bobory Dóranak mondok köszönetet. Lásd Herzfelder 1896; Zolnai 1896; Szathmáry 1896: 111–129.

⁴¹ Révay 1978: 69–73; Eckhardt (szerk.) 1951; Révay 1974: 41–46.

Nagy Miklós nevű szerző által 1621-ben írt szövegrészletéből.⁴² A közös ebben a két forrásban az, hogy a nyílt szöveg mássalhangzóit kódolatlanul hagyják, és kizárólag a magánhangzókat titkosítják, azokat is jól felismerhető rend szerint. E források jelentőségét nem a követett módszer kifinomultsága adja, hanem az a – Balassi levele, a diákok kódexei és más források által is illusztrált – tény, hogy a professzionális diplomáciától igen távol eső területeken is használták a kora újkorban titkosírást.

Összefoglalva tehát, a kora újkori Magyarországon a titkosírás korántsem kizárólag a központi diplomácia eszköze volt, számos társadalmi réteg használta mindennapi élete során. Az egyetlen szelekciós szempontot az jelentette, hogy értelemszerűen írástudók privilégiuma kellett hogy legyen. A korszak egyik meghatározó történésze, R. Várkonyi Ágnes benyomása szerint a térségből különösen nagy mennyiségben maradtak fenn titkosírások.⁴³ Hogy ez mennyire igaz a kor más területeivel (például Lengyelországgal vagy a német fejedelemségekkel) összehasonlításban, egyelőre nyitott kérdés, amit módszeres kutatásnak kell tisztáznia.

A vizsgálatba vont háromszáz éves periódusban megfigyelhető bizonyos fejlődés. A politika fokozatosan elhagyta a monoalfabetikus titkosírásrendszereket, és előbb egyszerűbb, majd – Rákóczi korára – komplexebb homofonikus kulcsokat vezetett be. Ezzel párhuzamosan az egyszerűbb rejtjelezési technikák megjelentek a társadalom egyéb 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. A titkosírások elterjedése és mindennaposá 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 titkok tudóiként és továbbítóiként.

FORRÁSOK

Bayerische Staatsbibliothek, München (BSB)

Cod. Icon. 242, Giovanni Fontana: *Bellicorum Instrumentorum*.

Biblioteca Apostolica Vaticana, Città del Vaticano (BAV)

Palatinus latinus gyűjtemény, 1375.

Palatinus latinus gyűjtemény, 1439.

Bibliothèque nationale de France, Paris (BnF)

Cod. Lat. Nouv. Acq. 635. Giovanni Fontana: *Liber Secretum de thesauro experimentorum ymaginationis hominum*.

⁴² Vadai 1991.

⁴³ R. Várkonyi 1999.

MTA Kézirattár

Ms 4951/5. A Rákóczi szabadságharc titkosírásainak táblázatai.

MTA Mikrofilmtár

Mf 1606. A Thököly szabadságharc körüli iratok.

Sächsische Landesbibliothek, Dresden (SLB)

N. 100, fol. 198r–200v.

HIVATKOZOTT IRODALOM

- Assmann, Aleida – Assmann, Jan (Hrsg.) 1997: *Geheimnis und Öffentlichkeit (Schleier und Schwelle I)*. München.
- Assmann, Aleida – Assmann, Jan (Hrsg.) 1998: *Geheimnis und Offenbarung (Schleier und Schwelle II)*. München.
- Assmann, Aleida – Assmann, Jan (Hrsg.) 1999: *Geheimnis und Neugierde (Schleier und Schwelle III)*. München.
- Biagoli, Mario 2006: *Galileo's Instruments of Credit: Telescopes, Images, Secrecy*. Chicago.
- Biaudet, Henry 1910: *Un chiffre diplomatique du XVI^e siècle: Étude sur le code. Nunz. Polonia 27. A. des archives secrètes du Saint-Siège*. Helsinki.
- Birkenmajer, Alexander 1932: Zur Lebensgeschichte und wissenschaftlichen Tätigkeit von Giovanni Fontana (1395?–1455?). *Isis* (17.) 1. 34–54.
- Cecchetti, Bartolomeo 1868–69: Le scritture occulte nella diplomazia veneziana. *Atti del Regio Istituto Veneto* (14.) 1186–1211.
- Devos, J. P. 1950: *Les chiffres de Philippe II (1555–1598) et du Despacho Universal durant le XVII^e siècle*. Bruxelles.
- Devos, J. P. – Seligman, H. (éd.) 1967: *L'Art de déchiffrer: Traité de déchiffrement du XVII^e siècle de la Secrétairerie d'État et de Guerre Espagnole*. Louvain.
- Eamon, William 1994: *Science and the Secrets of Nature: Books of Secrets in Medieval and Early Modern Culture*. Princeton.
- Eckhardt Sándor (szerk.) 1951: *Balassi Bálint összes művei*. Budapest.
- Engel, Gisela et al. (Hrsg.) 2002: *Das Geheimnis am Beginn der europäischen Moderne*. Frankfurt am Main.
- Hargittay Emil (szerk.) 1981: *Régi Magyar Levelestár*. Budapest.
- Herzfelder Armand Dezső 1896: Kolozsvári Czementes János könyve. *Magyar Könyvszemle* (20.) 3. 276–301, (20.) 4. 351–373.
- Kahn, David 1996: *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York.
- Karttunen, Liisi 1911: *Chiffres diplomatiques des nonces de Pologne vers la fin du XVI^e siècle: Extraits des archives des princes Chigi à Rome*. Helsinki.
- Kerekes Dóra 2003: Hírszerzés a XVI–XVII században. *Irodalomismeret* 13. 63–70.
- Kerekes Dóra 2007: Kémek Konstantinápolyban: A Habsburg információszervezete és működése a magyarországi visszafoglaló háborúk idején (1683–1699). *Századok* (141.) 1217–1258.

- Kerekes Dóra 2010: *Diplomaták és kémek Konstantinápolyban*. Budapest.
- Láng, Benedek 2008: *Unlocked Books. Manuscripts of Learned Magic in the Medieval Libraries of Central Europe*. Pennsylvania.
- Lochrie, Karma 1999: *Covert Operations: The Medieval Uses of Secrecy*. Philadelphia.
- Long, Pamela O. 2001: *Openness, Secrecy, Authorship: Technical Arts and the Culture of Knowledge from Antiquity to the Renaissance*. Baltimore.
- Meister, Aloys 1902: *Die Anfänge der modernen diplomatischen Geheimschrift*. Paderborn.
- Meister, Aloys 1906: *Die Geheimschrift im dienste der päpstlichen kurie von ihren anfängen bis zum ende des 16. Jahrhunderts*. Paderborn.
- Newman, William – Grafton, Anthony (eds.) 2001: *Secrets of Nature: Astrology and Alchemy in Early Modern Europe*. Cambridge.
- Paravicini Bagliani, Agostino (ed.) 2006: *Il Segreto / The Secret. Micrologus 14*. Firenze.
- Pasini, Luigi 1873: Delle scritture in cifra usate dalla Repubblica Veneta. In: *Il Regio Archivio Generale di Venezia*. Venezia, 291–328.
- Petercsák Tivadar – Berecz Mátyás (szerk.) 1999: *Információáramlás a magyar és török végvári rendszerben*. Eger.
- Platania, Gaetano 1988: La Polonia nelle carte del cardinale Carlo Barberieni Protettore del regno. *Accademie e Biblioteche d'Italia* (56.) 2. 38–60.
- Principe, Lawrence M. 1992: Robert Boyle's Alchemical Secrecy: Codes, Ciphers and Concealments. *Ambix* (39.) 63–74.
- R. Várkonyi Ágnes 1987: *A rejtőzködő murányi Vénusz*. Budapest.
- R. Várkonyi Ágnes 1999: A tájékoztatás hatalma. In: Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és török végvári rendszerben*. Eger, 9–31.
- R. Várkonyi Ágnes 2000: Az elveszett idő: Zrínyi Miklós nádori emlékirata? *Hadtörténeti Közlemények* (113.) 2. 269–328.
- Révay Zoltán 1974: *II. Rákóczi Ferenc és korának rejtjelezése (XVIII. század)*. Budapest.
- Révay Zoltán 1978: *Titkosírások. Fejezetek a rejtjelezés történetéből*. Budapest.
- Rockinger, Ludwig von 1892: Über eine bayerische Sammlung von Schlüsseln zu Geheimschriften des sechzehnten Jahrhunderts. *Archivalische Zeitschrift* (3.) 21–96.
- Singh, Simon 2000: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. London.
- Speziali, Pierre 1955: Aspects de la cryptographie au XVI^e siècle. *Bibliothèque d'humanisme et Renaissance* (17.) 188–206.
- Stix, Franz 1936–1937: Die Geheimschriftenschlüssel der Kabinettskanzlei des Kaiser. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Philologisch-Historische Klasse*. Neue Folge, Fachgruppe II, 207–226, 61–70.
- Strasser, Gerhard 1988: *Lingua Universalis: Kryptologie und Theorie der Universal Sprachen im 16. und 17. Jahrhundert*. Wiesbaden.
- Szathmáry László 1986: *Magyar alkémisták*. Budapest.
- Thaly Kálmán 1868: Gr. Zrínyi Miklós emlékirata II. Rákóczi György fejedelemhez, 1653. *Századok* (2.) 9. 633–648.
- Thorndike, Lynn 1923–58: *History of Magic and Experimental Science*. New York.
- Tusor Péter 2003: Pázmány bíboros olasz rejtjelkulcsa: C. H. Motmann, Residente d'Ungheria: A római magyar agenzia történetéhez. *Hadtörténelmi közlemények* (116.) 2. 535–581.

- Vadai István 1991: Két XVII. századi titkosírás megfejtése. In: Ötvös Péter (szerk.): *Pálffy Kata leveleskönyve: iratok Illésházy István bujdosásának történetéhez (1602–1606)*. Szeged, 183–189.
- Wrixon, Fred B. 1998: *Codes, Ciphers and other Cryptic and Clandestine Communication*. New York.
- Zolnai Gyula 1896: Jegyzetek Czementes János könyvéhez. *Magyar Könyvszemle* (20.) 4. 373–377.
- Zrínyi Miklós 1958: *Összes művei II. Levelek*. (Szerk.: Csapodi Csaba – Klaniczay Tibor.) Budapest.