

## A Habsburg-ellenes mozgalmak kuruc hadvezéreinek kódolási technikái

A kuruc mozgalom kezdetétől egészen annak végéig és később az emigráció éveiben is jelen volt a titkosírás, a rejtjelezés. Az 1670–1711-ig terjedő kuruc harcok időszakából három jelentős kuruc vezető emelkedett ki, akik hosszabb vagy éppen rövidebb ideig, de meghatározták a Habsburg-ellenállás menetét. A kezdeti, kibontakozási korszakban az Erdélybe menekült bujdosók Teleki Mihályt választották fővezérnek, aki az 1670-es években mint kuruc hadvezér, az erdélyi seregek parancsnoka, és fejedelmi tanácsos irányította az ellenállás politikáját. A hadi tanácsokkal és tisztekkel élénk levelezést folytatva megjelent a homofonikus behelyettesítő sifre<sup>1</sup> mellett a nomenklátor használata. Az egy ív terjedelmű lapon a felső sorba elkészítették, a nyílt ábécé alá írva a kódábécét, s ezt követte egy hosszú többnyire ábécérendbe, kezdőbetűk alá feltüntetett szóaljstrom. Ez volt a nomenklátor<sup>2</sup>, ami mindig az adott nyelvhez igazodott. Amennyiben a levél magyar nyelven íródott, akkor a kiegészítésben személynevek, hónapok nevei, városnevek – Lócse, Kassa, Tokaj, Kálló –, gyakori szavak – vár, sereg –, illetve egyéb földrajzi nevek – Tisza, Szamosköz – jelentek meg.

A nomenklátor alapján könnyebb az adott kódváltozat korbeli behatárolása is. Teleki Mihály iratai közt megtalálható a Wesselényi-összeesküvés alatt futó egyik kódábécé, amelyben csak a legismertebb résztvevőket említve – I. Rákóczi Ferenc: 181, 182, 183; Zrínyi Péter: 169, 170, 171; Palatinus: 151, 152, 153; Nádasdy: 154, 155, 156; Thököly István: 205, 206, 207, vagyis általában három számváltozat alatt jelöltek egy személyt – mellettük egyházi – pápa, püspök, érsek – és világi vezetők – francia, lengyel király – is megjelennek a nomenklátorban. Erre a klavistáblázatra jellemző, hogy minden három számot kap, a betűk kétjegyű számokat, a nomenklátor szóaljstromában szereplő szavak háromjegyű számokat.

Hogy a kódábécé és ezzel természetesen a nomenklátor listája is folyamatosan változott, ez magától értetődő és nagyon jól észrevehető például a személynevek változásában.

A Wesselényi-összeesküvést követően a kuruc mozgalom kibontakozásával megjelenik a fiatalabb generáció a névlajstromban – Wesselényi Pál és Thököly Imre – és a bányavárosok kifejezés, egy 1677. július 30-as klavisváltozaton. Ez a dátummegjelenés egy kivételes eset, mert szinte soha nem fordul elő, hogy dátumoznák a klavist. Az ív külső hajtásán volt szokás feltüntetni, hogy kinek a klavisa és kihez lett rendelve, de a dátumozás nem jellemző. Ez az 1677-es kódváltozat azért is nagyon kirívó eset az iratok sorában, mert a szóaljstrom végén praktikus használati tanácsokat is feltüntettek: „azonban nagyobb homályosításért, az rend szerint való ábécé betűiből is kell bele elegyíteni, az írásban megismert ilyen jegyeket is: + ≠ # ϕ”<sup>3</sup>

Itt ebben az esetben ezek a szimbólumok nullításoknak<sup>4</sup> számítanak, vagyis tartalmuk, jelentésük nincs. Viszont előfordult, hogy a szimbólumok tartalmat is nyertek. Található az iratok közt olyan eset is, amikor a kódábécében keverik a számokat és a szimbólumokat, tehát egy betűt szám és szimbólum egyaránt rejthet – például „U : 17, 13, 21, E, #”<sup>5</sup>

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	r	s	t	u	v	z	y
8	+	GD	≠	λ	Ϸ	70	VI	ϣ	Ϸ	10	p	Θ	25	ϕ	=	~	5	3	P	ξ	4

Ez a fajta behelyettesítéssel kód, amikor betűket vagy szimbólumokat használnak, illetve ezek keverékét: a monoalfabetikus behelyettesítéssel kód.<sup>6</sup> Teleki Mihály levelezésében ez volt az egyik legjellemzőbb, előfordult a csak szimbólummal jelölt betűk változata is.<sup>7</sup>

Teleki Mihály kódjaiban igen gyakori volt a nullítások alkalmazása. Ezeknek a száma általában tíz körüli volt – 9, 10, 13 darab nullítás – és mindig a nihil vagy nulla kifejezés alatt tüntették fel, a számok teljesen ad hoc jelleggel két vagy háromjegyűek, egymást követők, vagy egymástól független számsorok, melyeket közbeékeltek a kódolt szövegben.

A francia és lengyel kapcsolatokból adódóan természetesen elkerülhetetlen a közvetítő nyelv, a latin jelenléte a klavisok között. Számos klavis és sifre íródott latin nyelvre és ebben megjelenik a latin nyelvtan is. A magyar nyelvénél Teleki Mihály irataiban a ragokra és a kötőszavakra érzékeny volt a kódolás. A latin nyelvénél szintén megjelenik ez, a latin nyelv specifikumaival. A ragozásnál a nominatívus (alanyeset) maga a szó leírása volt, majd a genitívus ( - birtokos eset), datívus ( p részeshatározó eset), accusatívus ( Θ tárgy-eset), ablatívus ( + határozóeset) szimbólumot kap. Tehát a szót nem a latin nyelvtan szerint ragozva írták le, hanem az alapszó számkódolása után az eset szimbólumjele került. Megjelennek gyakori latin szavak – arma, castellanus –, kifejezések – quam, quod – és a gyakori szókezdések vagy szótagok – ce, cito, nam – a tulajdonnevek mellett. Ezeket is ábécé sorrendbe a kezdőbetű alá felsorolásszerű lajstromba rögzítették, sokkal részletesebben, mint a magyar kódokat. A szólaajstromban egy kezdőbetű alá általában 5-20 darab között mozgott a felsorolás száma. S egy-egy kifejezés, szó után pontozott sorvezetéssel, egymás alá vezették fel a számokat. Tehát egy sorban egy kifejezés és egy szám szerepelt szigorúan egymás alatt, az áttekinthetőség érdekében.<sup>8</sup> A következő kezdőbetűt vonallal választották el az előzőektől, így a végeredmény párhuzamos és függőleges vonalak által keretezett táblázat lett:

B. .... .58	D. .... .73
Ba. .... .59	Da. .... .74
Be. .... .60	De. .... .75
Bi. .... .61	Di. .... .76
Bo. .... .62	Do. .... .77
Bu. .... .63	Du. .... .78
Brevi. .... .64	Decem. .... .79
	Duo, dua. .... .80
C. .... .65	E. .... .81
Ca. .... .66	Enim. .... .82
Ce. .... .67	Est. .... .83
Ci. .... .68	Et. .... .84
Co. .... .69	...
Cu. .... .70	
Centum. .... .71	
Cum. .... .72	

Ezeket a változatokat használták az 1670-es években, és ahogy a bujdosómozgalomhoz csatlakozott Thököly Imre, kezdetben a Teleki Mihály által adott clavisformákat írta, tehát az alapokat, és a rejtjelezés ismeretét gyorsan elsajátította. 1680 után a Habsburg-ellenes mozgalom élére kerülve Thököly Imre alatt már a rejtjelezés technikája finomodott és fejlődött is. Bár ilyen részletes gyűjteménye nem maradt fenn a Thököly-levelezésben a kódolt leveleknek, az kivehető volt, hogy Thököly fennmaradt iratai közt a szimbólumhasználat nem volt jelen, vagy nem volt gyakori. Thököly kedvelt sifreformatuma a

homofonikus behelyettesítő sifre volt, a fennmaradt levelekben gyakoriságát tekintve ez jelenik meg. A Thököly-felkelés alatt tehát elsősorban a homofonikus behelyettesítő sifre volt használatban. A francia kapcsolat mindvégig jelen volt a korszak Habsburg-ellenes mozgalmában, és a latin nyelv használatánál már látszott, hogy közvetítő nyelvként kezdetben főleg ezt a nyelvet használták a sifrékben is. Nem egyértelmű, hogy mennyiben őrizték és vitték tovább Thököly tisztviselői, kurucai, a kuruc mozgalomban a Thököly-hagyományokat a kódolás használatában és mennyiben hatottak a Thökölytől látott kódolási módok mostohafia levelezésére.

II. Rákóczi Ferenc beleszületett a kuruc mozgalmakba és annak minden hozadékát átélte. Anyja mellett jelen volt Munkács ostrománál, mostohaapja mellett többször a katonai táborokban. Tudott a Thököly Imre és Zrínyi Ilona közötti titkos kódról is, amin azok ketten leveleztek egymással<sup>9</sup>, tehát már gyermekként is magába szívta a titkosírás fontosságát. Nyíló gyermeki értelmével pontosan érzékelte mostohaapja politikájában és levelezésében a rejtjelezés hasznosságát. Ezeken az alapokon haladva, és a francia kapcsolat erősödésével nem véletlen, hogy Rákóczi emigrációba vitt levelei közt a sifretáblázatok tobzódó tárházára lehet találni.

A Rákóczi-szabadságharchoz vezető úton, a Wesselényi-összeesküvéstől addig eltelt harminc-negyven év fejlődése bővítette és szélesítette a kódolási technikákat, hogy Rákóczi alatt, a már tapasztalt kuruc tisztek a régi thökölysták és a francia közvetítés hatására a kor legfejlettebb kódolástechnikái jelenjenek meg a kuruc mozgalmak utolsó fellobbanásánál.

A monoalfabetikus behelyettesítő kód, a homofónikus behelyettesítő sifre továbbra is jelen volt, azonban megjelentek olyan technikák, amelyek – ha használtak is – a korábbi évekről nem maradtak fenn.

A nomenklátorok szórajstromai kibővültek, már szinte fontosabb a szóbehelyettesítés számsora, mint a betűk kódolása. A kódszavak mennyisége egy-egy clavistáblázatban, a korábbi évtizedek százaz számkörén messze túllép, sűrűlva a félezer szó számkódolásának mennyiségét egy-egy klavisban.

A legnagyobb hátránya, hogy egy-egy ilyen táblázat elkészítése sokkal több időt vehetett igénybe, cseréje fáradtságosabb feladatnak számított. A Teleki és Thököly idejében jellemző mono- vagy homofónikus sifréket gyorsan papírra lehetett vinni, és szükség esetén havonta vagy akár sűrűbben is cserélni.

A Rákóczi-szabadságharcra mintha mindez lelassult volna, több idő jutott még vonalak és sifrekódok készítésére is.

A ráérős sifrekészítés remek példája<sup>10</sup>, hogy a gondosan, precíz, olvasható betűformálással készített táblázatot, színekkel – piros, zöld sáv – és kerettel készítették. A számok piros színnel, a betűk feketével, a vonalak zölddel készültek és a sifretáblázat üresen maradt részeit virágmotívumokkal rajzolták tele. Ez a példa természetesen francia munka, de jól érzékelhető, hogy itt nem a hadmozdulatok tervezésében készített sürgős sifrekészítés eredménye a táblázat, amikor kalamárisládában tárolt ív papírosra vitték fel rövid idő – egy-két óra alatt – a rejtjeleket, sokszor maguk a levélírók. Teleki Mihály gyűjteményében található ívről vágott papírosnyi változatok, amik a tervezést, vagy a gyors sifrekészítést sejtetik. Rákóczi emigrációs gyűjteményében csak üres táblázatok vonalazásai láthatók és csakis egy rejtjelezési technikára jellemző táblázatból.

Ez a híres Vigenére-tábla. A Vigenére-sifre nem egy, hanem huszonhat különféle kódábécét használ a nyílt szöveg rejtjelezésére. Egységbe öntöje az 1523-ban született Blaise de Vigenére volt. A Vigenére-tábla elkészítése a következő volt: a tábla kisbetűs legfelső sora a nyílt szöveg betűit tartalmazta. A nyílt ábécét huszonhat kódábécé követi, amelyek

mindegyikét egy hellyel eltolják az előzőhöz képest. A Vigenére-sifre alkalmazásakor az eredeti üzenet betűit a Vigenére-tábla más-más sora (más-más kódábécé) szerint sifírozzák, tehát a feladó az üzenet első betűjét a harmadik sor szerint is sifírozhatja, a másodikat a tizenkettedik szerint stb. Az üzenet desifírozásakor a címzettnek tudnia kell, hogy az egyes betűk sifírozásához a Vigenére-tábla melyik sorát használták, tehát a két félnek előzetesen meg kell állapodnia a sorok változtatásának sorrendjében. Ez kulcsszó alkalmazásával volt lehetséges.<sup>11</sup>

A kulcsszó ismeretében a desifírozáskor a nyílt szöveg fölé kellett írni a kulcsszót, egymás után a sor végi utolsó betűig. A kulcsszó betűje határozza meg, hogy a Vigenére-tábla mely sorát kell használni és ahol keresztezi a nyílt ábécé megfelelő betűjének sorát, az a betű lesz a desifírozott betű.<sup>12</sup>

Rákóczi emigrációs iratai közt található egy példa a *clavis musicalis* magyarországi jelenlétére is.<sup>13</sup> Ez a rejtjelezési mód nem lehetett sem túl gyakori sem túl kedvelt. A nyílt ábécét az öt vonalas kotta alá írták. A kotta vonalain pedig a zenei módosítójelek – szünet, kereszt – mellett a különböző hangok, más és más betűt jelentettek, ahogy a negyed és félértékű hangok is. A kottaképből szerepelt a pontozott negyed, pontozott félérték és triola is. Tehát a ritmus, és „hangzás” együttesen kódolt üzenetet tartalmazott. Hogy zeneileg mennyire felelt meg az igényeknek az így készült dallam, azt nem tudhatjuk. Az emigrációba vitt részben nem voltak kottapapírok, csak maga a *clavis*.

Ez a példa is jól mutatja, hogy a kódolás és rejtjelezés túllépett a nyelvi-nyelvtani, a matematikai-statisztikai feladatokon, és fejlődésében már a művészetek területére is eljutott. Közvetítéssel eljutottak a kódfejtés legújabb fejlesztései Magyarországra is.

Összefoglalva elmondható, hogy minden kornak megvolt a maga kedvelt és bevett kódolási – rejtjelfejtési gyakorlata. Az idők fejlődésével az egyre bonyolultabb, de ezáltal egyre nehezebb és egyre több időt igénylő kódolási technikák lettek népszerűbbek. Teleki Mihály korában a monoalfabetikus behelyettesítő kód volt népszerű, Thököly Imre a homofónikus behelyettesítő sifrét alkalmazta a legsűrűbben, II. Rákóczi Ferenc a Vigenére-sifre rendszerét kedvelte és használta. Sikerük vagy bukásuk nem a rejtjelezési technikán múlt.

## JEGYZETEK

- |   |  |    |  |
|---|--|----|--|
| 1 | Bővebben lásd Kardos Tímea: Thököly Imre és a homofónikus behelyettesítő sifre. Kódolás a kuruc fejedelem idejében. In. Valóság, 2012. 5. sz. 27–38. | 8  | MNL, OL, Családi levéltárak, Teleki Mihály gyűjtemény 34. d. Vegyes iratok P 1238. 18.                 |
| 2 | Simon Singh: Kódkönyv. Park Könyvkiadó, 2001. (Továbbiakban: Singh) 40.  | 9  | Lásd még. Kardos Tímea: Thököly Imre és Zrínyi Ilona levelezése 1686-ban. In. Honismeret, 2013. 4. sz. |
| 3 | MNL, OL, Családi levéltárak, Teleki Mihály gyűjtemény 34. d. Vegyes iratok P 1238. 3.  | 10 | MNL, OL, G 15 Emigrációba vitt rész Caps C. Fasc. 43. 20.  |
| 4 | Singh, 47.   | 11 | Singh, 58.   |
| 5 | MNL, OL, Családi levéltárak, Teleki Mihály gyűjtemény 34. d. Vegyes iratok P 1238. 17.   | 12 | Singh, 58.   |
| 6 | Singh, 25.   | 13 | MNL, OL, G15 Emigrációba vitt rész Caps C. Fasc. 43. 9.  |
| 7 | MNL, OL, Családi levéltárak, Teleki Mihály gyűjtemény 34. d. Vegyes iratok P 1238. 118.  |    |  |