W. Somogyi Judit

Sifrírozási szabályok késő középkori rejtjelkulcsok tükrében

Bevezetés

A XIV. század második felétől kezdődően a nyugat-európai diplomáciai gyakorlatban egyre erőteljesebb igény jelentkezett arra, hogy az írott szövegek tartalma bizonyos esetekben csak a beavatottak számára legyen elérhető. A probléma megoldására felvetődött lehetőségek közül sikeresnek bizonyult az az eljárás, és terjedt el később széles körben, amelynek keretében az ábécé betűit – kezdetben csak egy részüket, később mindegyiket – rejtjelekkel (szimbolikus grafémákkal) helyettesítették, vagyis egy alfabetikus rendszerben írt szöveget egy másik, kizárólag ebből a célból kialakított kódrendszerbe ültettek át. A szöveget ebben a rejtjelezett (kódolt) formában juttatták el a címzettnek, aki szintén csak egy újabb művelet (dekódolás) elvégzése után ismerhette meg annak tartalmát.

Az itáliai diplomáciai praxisban a XVI. század végéig szinte minden jelentősebb hatalmi központban, amennyiben felhasználták a sifrírozás által kínált lehetőségeket, a kódolásra szánt dokumentum nyelvétől függetlenül az úgynevezett egyábécés (monoalfabetikus) rejtjelezési eljárások egyikét alkalmazták, azaz a sifrírozáshoz minden esetben csak egyetlen elemkészletből álló kódrendszert használtak. A század utolsó évtizedeiben új megoldásként jelent meg a többábécés (polialfabetikus) módszer – amely egyszerre több elemkészletet feltételez a kódoláshoz –, ez azonban még hosszú ideig nem tudott széles körben az elődje helyébe lépni. Itáliai gyűjteményekben a több évszázadot átölelő „egyábécés" időszakból számos rejtjelezéssel kapcsolatos forrás maradt fenn, amelyek különféle, egymással párhuzamosan létező vagy egymást dinamikusan követő kódrendszereket és azok gyakorlati alkalmazását dokumentálják.

A tanulmány célja az egyábécés sifrírozási eljárás elméleti megközelítése a kódrendszereket leíró és használatukat irányító szabályok alapján. Az alábbiakban röviden összehasonlítom a két írásrendszernek a tanulmány témája szempontjából számottevőnek ítélt főbb jellemzőit; felvázolom a sifrírozott formában történő üzenetküldés folyamatait, és megjelölöm a folyamatokban résztvevők szerepét. Ezt követően térek rá az egyábécés eljárást leíró és irányító, elsősorban kódkulcsokban megfigyelhető szabályok

tartalmi és formai jellemzőinek bemutatására. A „szabály" kifejezést a Magyar Értelmező Kéziszótár általános értelmezése szerint alkalmazom.[1]

A korpusz nagyobb hányadát észak-itáliai városok (Milano, Modena, Mantova, Venezia) állami levéltáraiban[2] őrzött és a Vestigia kutatói projekt keretében feltárt XV–XVI. századi kéziratos források alkotják, amelyek közül több dokumentum digitális fényképe megtalálható a projekt keretében létrehozott Infocus adatbázisban is (www.vestigia.hu). Az eredeti levéltári dokumentumokon kívül az elemzést néhány esetben korábban már publikált kulcsokra[3] is kiterjesztettem.

Az alfabetikus és a rejtjeles írásrendszerek főbb jellemzői

Az alfabetikus (a továbbiakban ALF alakban rövidítve) és a rejtjeles (a továbbiakban: SIF) írásrendszerek főbb jellemzőinek összehasonlító elemzése, néhány találkozási pont mellett számos eltérésre is rámutat. Formai szempontból, természetesen, kiemelkedő szerep jut a grafikai természetű különbségeknek, ezek azonban csak marginálisan kapcsolódnak a szabályok tartalmi kérdésköréhez, ezért részletesebb bemutatásukra a tanulmányban nem térek ki.

Az ALF írásrendszerek a nyelvi megnyilatkozások tartalmának rögzítése mellett a (hangzó) beszéd egyéb jellemzőinek vizuális megjelenítésére is törekednek. Az írásban – a fonémáknak grafémákkal (betűkkel) történő megfeleltetésén túlmenően – szóköz, különböző szerepű központozásjelek utalhatnak a hangzó szöveg szerkezetére, intonációs és pragmatikai jellemzőire, de egyéb grafikai eszközök (nagybetű, soremelés, új bekezdés stb.) is támogathatják és irányíthatják a nyelvi produktum feldolgozását és – a szövegalkotói szándéknak többé-kevésbé megfelelő – értelmezését.[4] Az ALF írásrendszerek konvención alapuló közösségi rendszerek; a nyelvek betűkészlete, az írásmódot irányító szabálygyűjtemény kodifikált és bárki számára szabadon hozzáférhető. A sifrírozó rendszerek célja a tartalom minél

[1] Szabály = 1. magatartást, cselekvést, ill. ennek módját, rendjét megszabó irányelv, rendelkezés; 2. vminek a rendjében, menetében stb. érvényesülő (tapasztalati úton felismert) törvényszerűség. *Magyar Értelmező Kéziszótár* (2003[2]), Budapest, Akadémiai Kiadó.

[2] A felsorolás sorrendjében: Archivio di Stato di Milano (ASMi), Archivio di Stato di Modena (ASMo), Archivio di Stato di Mantova (ASMn), Archivio di Stato di Venezia (ASVe). A dokumentumok jelzetét az adott levéltári gyakorlatnak megfelelően, egyszerűsített formában adom meg; a kódkulcsok címét (ha ez a dokumentumon szerepel) páros idézőjel között tüntetem fel.

[3] Aloys Meister (1902), *Die Anfängen der modernen diplomatischen Geheimschrift.* Paderborn, Schöningh; Aloys Meister (1906), *Die Geheimschrift im Dienste der Päpstlichen kurie von ihren Anfängen bis zum ende des XVI. Jahrhunderts*. Paderborn, Schöningh.

[4] Giorgio Raimondo Cardona (2009), *Antropologia della scrittura*, Torino, UTET. 75.

nagyobb mértékű elfedése. A vizsgált periódusban alkalmazott monoalfabetikus eljárást olyan, egyénileg kialakított, többnyire csak korlátozott tér- és időbeli keretek között használt struktúrák jellemezték, amelyek saját jelkészlettel és szabályokkal rendelkeztek, valamint a rendszert rögzítő kódkulcshoz csak meghatározott személyek férhettek.

Funkciójuk alapján a készletek grafikai elemei mindkét (ALF és SIF) rendszerben három csoportba sorolhatók: a) beszédhangot ábrázoló (azaz hangértékkel bíró, ennélfogva nyelvi tartalmat közvetítő) grafémák; b) a beszéd akusztikai jellemzőire vagy tagolására utaló (vagyis nyelvi tartalmat nem közvetítő, de annak rögzítését és feldolgozását segítő) grafémák; c) számot jelölő grafémák (számjegy). Az első két funkció esetében több eltérés mutatkozik a két rendszer között (a számjelölés kérdésével jelen tanulmány nem foglalkozik).

A beszédhangot ábrázoló ALF grafémák csupán egy fonéma grafikai megfelelőjeként szerepelnek, ennek következtében például a *páros* szó öt fonémáját öt betű (graféma) jelöli. A SIF rendszerekben ugyanez a szó többféle módon kerülhet rögzítésre, ugyanis egyetlen (hangértékkel rendelkező) SIF graféma referense nemcsak egy fonéma lehet, hanem egy fonémasor (dupla mássalhangzó, szótag, önálló szó) vagy fonéma sorozat (több szóból álló tulajdonnév) is. Ennek megfelelően a fenti *páros* szó sifrírozása monoalfabetikus rendszerben, a rejtjelek számát figyelembe véve, több módon is lehetséges (a példákban kiskötőjel választja el egymástól a SIF grafémák referensét jelölő ALF egységeket): öt grafémával (*p-á-r-o-s*); négy grafémával (*pá-r-o-s*; *p-á-ro-s*; *p-ár-o-s*; *p-á-r-os*); három grafémával (*pár-o-s*; *p-á-ros*; *pá-r-os*; *pá-ro-s*; *p-ár-os*); két grafémával (*pá-ros*; *pár-os*); egy grafémával (*páros*).

Sok SIF rendszerben előfordulnak homofónok is, ami ebben az esetben azt jelenti, hogy ugyanaz a fonéma több SIF grafémával is szabadon helyettesíthető. (Ehhez látszólag hasonló jelenség a magyar j/ly grafémák váltakozása a palatális likvida [λ] jelölésére, a két graféma szabad felcserélését azonban lexikális korlátok irányítják.)

Nyelvi tartalmat nem közvetítő grafémaként mindkét írásrendszerben vannak központozásjelek – bár a SIF rendszerekben ezek konvencionális funkciójuk szerinti használata meglehetősen ritka. Ezen kívül, a rejtjelezés biztonságának növelése érdekében, a SIF rendszerek túlnyomó többségében megfigyelhető jelentés nélküli, a kód feltörését nehezítő grafémák (úgynevezett vakbetűk vagy nullitások), valamint a kódolás közbeni esetleges nyelvváltásra figyelmeztető vagy a leírt szöveg érvényességére (vagy érvénytelenségére) utaló jelek alkalmazása is.

Az egyábécés eljárást alkalmazó információcsere keretében a rejtjelezéssel kapcsolatos folyamatok (a szöveg kódolása adott kódkulcs alapján, majd a kódolás feloldása) több személy együttműködését feltételezték. A közös

munka kereteit a kulcs készítője határozta meg. A kódoló (aki lehetett egyben a kulcs készítője is) tevékenysége meghatározó volt nemcsak a kriptogramm biztonsága, hanem az üzenet célba érése szempontjából is: kihasználta-e és milyen mértékben a kulcsban leírt rendszer lehetőségeit (például váltogatta-e a rendelkezésre álló homofónokat); képes volt-e eltávolodni a konvencionális írásszokásoktól (például használt-e szóközt, írásjelet); mennyit hibázott a kódolás során. A dekódoló már „kész anyagot" kapott: feladatai közé tartozott a dekódolás, a kódoló által elkövetett hibák (kihagyás, tévesztés stb.) kijavítása, a dekódolt szöveg „kiigazítása" (a kódolás során elhagyott elemek v. írásjellemzők visszaépítése).

A két írásrendszer nem teljesen ugyanazokat az elvárásokat támasztja alkalmazói felé; az eltérések közül szükségesnek vélem megemlíteni az úgynevezett distanciálási képességet,[5] amely az átalakítás sikerességének egyik fontos tényezője. Az ALF eljárásra épülő egyábécés rejtjelezési rendszerek készítőinek és használóinak, különös tekintettel a kódolókra, képesnek kellett lenniük arra, hogy „kívülről" is tudják szemlélni a nyelvet és annak (konvencionális) írott formáját, hiszen csak ennek eredményeként nyílt lehetőség a megfelelően biztonságos SIF rendszer kialakítására és alkalmazására. Egy időben meg kellett tudniuk tehát valósítani a nyelvben való „benne levést" (hiszen nem tudtak kilépni a konvencionális keretből) és a nyelvtől való „eltávolodást". Minél nagyobb mértékű volt a distanciálás, annál sikeresebb lehetett a rejtjeles üzenetváltás.

Sifrírozási szabályok

Az egyábécés eljárást leíró és irányító általános normák a vizsgált időszakban szinte kivétel nélkül íratlan szabályként működtek; a kulcsok összeállítói az esetek többségében csak a saját rendszerükre vonatkozó információkat rögzítették. Az eljárás kezdeti időszakában csak néhány rejtjelezésről szóló elméleti munka született, amelyek azonban egyáltalán nem, vagy csak szűk körben váltak ismertté. A sort (eddigi ismereteink szerint) Leon Battista Alberti 1466-ban írt *De componendis Cyfris* című latin nyelvű traktátusa nyitotta meg, amely azonban csak egy évszázaddal később került publikálásra.[6] Az írásmű középpontjában egyébként Alberti invenciója, a többábécés sifrírozási eljárás áll; az egyábécés módszerről szóló részekben nem esik szó az eljárás lényegét megfogalmazó, úgynevezett keretszabályokról.

[5] Tolcsvai Nagy Gábor (1998), *A nyelvi norma,* Budapest, Akadémiai Kiadó. (Nyelvtudományi Értekezések 144.) 16–17.

[6] Cosimo Bartoli, *Opuscoli morali di Leon Battista Alberti* című, 1568-ban Velencében nyomtatott kötetében (199–219).

A rejtjeles információcsere térhódítása a sifrírozás gyakorlatában általánosnak tekinthető szabályok körének bővülését is eredményezte. A XV. századtól kezdődően a kódstruktúrákra már jellemző volt, hogy az ábécé minden betűjét rejtjellel helyettesítették, de nagy eltérés mutatkozott abban, hogy a biztonsági elemek közül – homofónok, vakbetűk; nagyobb hangzó egységek (szótagok, szavak stb.) egyetlen SIF jellel történő helyettesítése; szövegrész utólagos érvénytelenítése – hányat, melyiket és hogyan alkalmaztak.[7] A kód feltörésének megnehezítése céljából a sifrírozás során gyakran tudatosan megsértették a korabeli írásmód normáit is. Erre a gyakorlatra utalnak Alberti említett traktátusából (1a) alatt idézett szavai,[8] valamint erre szólítanak fel az 1539 és 1542 között keletkezett, Giovanni Ricci Montepulciano nuncius számára készített kulcsban (1b),[9] valamint egy másik, szintén XVI. századi, Mantovában őrzött kulcsban (1c)[10] olvasható szabályok:

(1) a) „[…] gioverà ancor molto non tener conto della Ortografia”
(„nagy haszonnal jár, ha eltekintünk a helyesírás követésétől”)

b) „Scrivasi congiunto senza servare ortographia et pongasi la nulla al fine di ogni parola.”
(„Írjunk mindent egybe, a helyesírást mellőzve, és minden szó után illesszük be a nullitást.”)

c) „Le doppie non si mettono pero bisognera scriuere semplicemente tutte le parole.
Le nulle saranno […….] le quali si metterano nel principio della ziffra, et alle uolte alcune di infra litere nelle parole accio la zifra sia piu difficile da estrare intesa.”
(„Ne írjunk dupla mássalhangzót de írjunk minden szót egymás után. Ezeket a nullitásokat […….] a rejtjeles rész elejére kell tenni és olykor egyet-egyet a szavakban a betűk közé a kód feltörésének nehezítésére.”)

Minden kódkulcs önálló szabálygyűjteménynek tekinthető: a szabályok számát, tartalmát és formáját a kód összeállítója határozta meg. A kulcsokban az adott sémára és annak használatára, bizonyos esetekben annak bővítési lehetőségeire is vonatkozó normák mellett egyéb, az információcsere

[7] Az eltéréseket szemlélteti a mintegy félszáz XIV. és XV. századi kulcs tartalmi szempontú elemzését összegző írásom, lásd W. Somogyi Judit (2016), Caratteristiche strutturali di cifrari monoalfabetici italiani nei secoli XIV e XV. *Verbum* XVII/1–2, 195–217.

[8] Bartoli 1568:208.

[9] Meister 1906:176.

[10] ASMn AG 424 n. 39.

körülményeivel kapcsolatos adatok is helyet kaphattak. Ez utóbbiak jól elkülönültek a szabályoktól: többnyire a kulcs azonosítását is megkönnyítő címben, ritkábban a lap alján[11] olvasható a használat helye és ideje, vagy hogy kinek a számára készült.

A kifejtett szövegrészeket – a korabeli nyelvhasználati szokásoknak megfelelően[12] – sokáig latin nyelven fogalmazták meg, azokban az esetekben is, amikor a kulcs tartalma (például a tulajdonnevek alakja) alapján kikövetkeztethető, hogy az népnyelvi szöveg rejtjelezésére készült. Néhány kulcsban olvasható a kódolandó szöveg nyelvére vonatkozó utasítás is, például egy 1469-ben keletkezett, a modenai herceg titkárának (Uguccione de Abbazia) címzett és a Modenai Állami Levéltárban őrzött kulcs[13] címében ez olvasható:

(2) „Ziffra pape cum amico tam in vulgari quam latino sermone”
(„A pápa sifréje barátjával népnyelvi és latin szöveghez”)

A kulcsok információtartalma[14] igen változatos volt. A korpusz egyetlen kulcsa sem rögzít olyan explicit szabályt, amely a rendszert alkotó összes rejtjel mennyiségére vonatkozna (például: „ez a rendszer X számú rejtjelből áll”), és a biztonsági elemek számának és a rejtjelek funkció szerinti megoszlásának jelölésére sincs utalás a kulcsokban (például: „ez a rendszer X db biztonsági elemet tartalmaz; ebben a rendszerben Y db rejtjel helyettesíthet magánhangzót” stb.).

Egy adott rejtjel funkcióját többféle módon jelölhették meg. A hangértékkel bíró grafémák esetében az azonosítás általában csak mellérendelés (melléhelyezés) útján – az adott ALF graféma (vagy graféma sor) alá vagy mellé írt SIF elemmel – történt, vagyis a szabály kb. ebben a formában fogalmazható meg: „a *c* betűnek ez a T jel felel meg; a *ba* szótag helyett ezt a Z jelet írd; a *quando* szót ez a Z rejtjel helyettesíti stb.” [a példákban megadott helyettesítő elemek csak fiktív rejtjelek]. Ritka kivételnek számít az a kódkulcs, amelyet 1582. szeptember 3-án Veronából küldött Velencébe egy Giustiniano nevű követ,[15] és amelyben az első szabály explicit formában

[11] A korpusz jelentős részét az egy lapra, egy oldalra írt kulcsok alkotják, ugyanis a használat, a biztonságos megőrzés stb. érdekében feltehetően ez a megoldás bizonyult hatékonynak. Természetesen léteznek – a tartalomtól, az írásmódtól vagy a lap méretétől függően – egy lap mindkét oldalát, vagy akár több lapot is elfoglaló kulcsok.

[12] Claudio Marazzini (1998), *La lingua italiana. Profilo storico*. Bologna, il Mulino. 213–214.

[13] ASMo, Canc. ducale, Mappe II, n.2; Meister 1902: 36.

[14] A jelkészletek grafikai jellemzőit figyelmen kívül hagyva.

[15] ASVe, Cons. di Dieci, Cifre, b.3.

megadja a betűk és a rejtjelek közötti megfelelést is (a kulcsban a rejtjeleket egy- és kétjegyű számok alkotják):

(3) „Il soprascritto alfabetto da lettera A. fin Z. li numeri sotto cadauna lettera si intende per quella lettera. Le cinque vocali cioe A . E . I . O . U . come lettere che si frequentano ad usare piu delle altre hanno tre numeri per cadauna di esse per poterle mutare nel scriuere. Qui sotto saranno cinque numeri che non uogliono dir lettera alcuna, ma bisogna usarli nel scriuer perche sara piu dificile il lezer la Zifara, et sara piu sicura. Numeri che non uogliono dir lettera alcuna. n.o 1 . 18 . 25 . 31 . 44 .”

> („A fenti ábécénél A betűtől Z betűig a betűk alatti számok az adott betűt jelölik. Mind az öt magánhangzóhoz, vagyis A . E . I . O . U . betűkhöz, mivel a többinél gyakrabban fordulnak elő, három szám tartozik abból a célból, hogy változtatni lehessen az írásmódjukat. Lejjebb szerepel még öt szám, amelyek egyetlen betűnek sem felelnek meg, de alkalmazásuk szükséges az írásban, mert így nehezebb feltörni a sifrét, és az biztonságosabb lesz. Semmilyen betűt nem jelentő számok n.o 1 . 18 . 25 . 31 . 44 .”)

A kulcsokban szükségszerűen megnevezésre kerültek azok a rejtjelek, amelyeknek nem volt megfelelőjük az ALF rendszerben. A nulla értékű elemek megjelölése történhetett például (jelzős) főnévvel: *Nulla* vagy *Nulle* ‘nullitás vagy nullitások’, *Littere nihil importantes*’semmit nem jelentő betűk’; jelzőként: *Ni(c)hil importantes, Nihil relevantes, Nihil significantes* ‘semmit nem jelentők’; vagy – elsősorban a XIV. század végén és a XV. század első felében keletkezett kulcsokban – akár egész mondat formájában, például: *Infrascripte posite cum aliis zifferis nichil habent importare* ’az alábbi rejtjelek mások mellé téve nem jelentenek semmit’;[16] *Iste nihil important* ‘ezek semmit nem jelentenek’.[17] Hasonló módon fordulnak elő a kulcsokban az egyéb szerepkörben használatos, de a sifrírozásban ritkábban alkalmazott jelek is. Egy 1483. január 10-én keletkezett, Milánóban található kulcs[18] például érvénytelenítő jeleket tartalmaz:

[16] Gabriele De Lavinde 1379-ben összeállított kulcskönyvében a 2. kulcsban szereplő forma; ennek különböző változatai olvashatók még az 1., 5., 8., 12. számmal jelölt kulcsokban; Meister 1906:171–173.

[17] XV. századi, Luccában (dátummegjelölés nélkül) összeállított kulcsban („Alia cyfra cum prelibato domino episcopo”); Meister 1902:55.

[18] ASMi, PE, Cifre, Fasc. 2.

(4) „Quicquid positum fuerit inter hec signa […] nihil importabit.”
(„A két […] jel közötti rész semmit nem jelent.”)

Egy másik, 1442. november 7-én Pisában keletkezett kulcsban[19] szereplő hét szabály közül az utolsó három [5–7.] a latin rövidítésrendszerből megőrzött, a rövidítéskor kihagyott elemekre utaló úgynevezett „titulusokat”, valamint központozásjeleket nevez meg, és némelyiknek megadja a funkcióját is [az idézett részekben az eredeti rejtjeleket arab számokkal helyettesítettem]:

(5) [5] „Sono dipoi li tituli che sono tre .1. .2. .3. lo primo .1. significa .M. lo secondo .2. .N. lo terzo .3. si pone per tutte quelle lettere che si mettono doppie nelle dictione per piu brevita.”
(„Három titulus van .1. .2. .3., az első .1. jelentése .M., a második .2. .N. a harmadik .3. a dupla mássalhangzókat rövidíti az írásban.”)

[6] „Et per il segno della parentesi si nota questo.5. .6.”
(„A zárójelet ezek jelölik .5. .6.”)

[7] „Et li punti sono questi, cioe singula .7. mezopunto .8. il quale dinota anchora non esser finita la sententia ma con li rami la lega insieme. Et per punto fermo questo mettiamo .9. che divide la clausula et nel fine questo .10. che pone termino perfetto.”
(„A pontok ezek, vagyis egyszerű .7., középső .8. ami még nem jelöli a mondat végét, de összeköti a részeket. A mondat végére ez kerül .9. és a bekezdés végére ez .10. ami tökéletesen lezárja.”)[20]

A biztonsági elem szerepű rejtjelek (homofónok, nullitások stb.) alkalmazásának módjáról (melyiket, hányszor, a szövegben hol stb.) a kulcsokban igen változó mértékű útmutatás figyelhető meg. Részletezőbb leírások többnyire a XVI. századi kulcsokban olvashatók: a legtöbb a nullitások beillesztésének lehetőségeire utal, de többé-kevésbé csak irányadó jelleggel. A már idézett szabályok közül, például, a (1b) és (1c) alattiak konkrétabb használatot jelölnek meg, ezzel szemben a (3) alatti szabályban csak a rejtjelek funkciójáról esik szó, használati módjukról nem. Az utóbbi szabályban egyébként a homofónok esetében is hasonló eljárás figyelhető meg: csak a váltakozás lehetőségét említi, annak módját nem. A (6) alatt idézett,

[19] Meister 1902:58–59.

[20] A négy központozásjel az úgynevezett négyes rendszerre utal, vö. Keszler Borbála (1995), *A magyar írásjelhasználat története a XVII. század közepéig*, Akadémiai Kiadó, Budapest. (Nyelvtudományi értekezések 141. sz.) 15–16.

1570-ben összeállított kulcs[21] szabályai, ezzel szemben, egyértelműen kijelölik mindkét biztonsági elem használatát:

(6) „[…] nel principio et fine di quello che si scriue in Ziffra sempre si hanno da mettere tre carateri che seruano per nulle et che siano della istessa Ziffra. Le Vocali hanno due carateri et si deue usare hor luno hor laltro per uariare et per tanto maggiormente difficoltar il conoscere le Vocali"

(„a rejtjelezett rész elejére és végére mindig három nulla értékű, a kulcsban szereplő jelet kell írni. A magánhangzóknak két rejtjel felel meg, és egyszer az egyiket, egyszer a másikat kell használni, hogy minél nehezebb legyen felismerésük"'

Az eddigiekhez képest újszerű megoldásnak tekinthető a (7) alatt idézett útmutatás, amely egy 1468-ra datált kulcsban[22] olvasható: jóllehet csak homályosan utal a használat módjára, azt egy konkrét példával szemlélteti, amelyben a nyílt szöveg és annak nullitással bővített rejtjelezett változata szerepel [ez utóbbinak az idézetben a dőlt betűkkel, folyamatosan írott sor felel meg, amelyben a vastagon szedett betűk a beillesztett nullitásokra utalnak]. Az eljárás érdekessége, hogy a megadott példa nincs összhangban a szabályban előírt használattal, ugyanis az öt beillesztett nullitás közül csak a második és az ötödik áll szóhatáron, a többi szavakon belül található.

(7) „Nulle saranno .e. a. da inserir qualche uolta tra le parole come sarebbe cosi
Vi prego a non mancar di sollicitarlo *V**a**ipregoe**a**nonman**a**cardisolle**i**citarlo**a***"

(„Nullitás lesz .e. a. ezeket olykor a szavak közé kell illeszteni ilyen formán")
("Kérlek benneteket, hogy ne habozzatok sürgetni őt")

A korpuszban szereplő kulcsok némelyike olyan útmutatásokat tartalmaz, amelyek eltérnek az eddig ismertetett szabályoktól, ugyanis a rendszer egyes SIF elemeinek grafikai kiegészítésére, ezáltal a kérdéses rejtjel funkciójának módosítására vonatkoznak. A rejtjel grafikai kiegészítése általában egy (konvencionális) központozásjel vagy szám meghatározott helyzetben történő elhelyezését jelenti, aminek következtében megváltozik a rejtjel eredeti funkciója. A (8) alatt idézett szabályok különféle lehetőségeket példáznak: (8a) a hangértékkel bíró elemek semlegesítését,[23] (8b) a mással-

[21] ASMn AG 424 n. 412, „1570 Per Vinegia".
[22] ASMi, Sforz. b. 1597 n. 70 („Zifra col secretario").
[23] ASMn AG 424.

hangzók szótaggá bővítését,[24] (8c) egy adott szó (*imperatore*) jelentésének megváltoztatását, valamint a mássalhangzók megkettőzését:[25]

(8) a) „Tutti li numeri con una riga di sotto sono fatte nulle, et niente significano, come a dire 10 15 30 […] etc."
(„Minden aláhúzással jelölt szám nullitás lesz, és nem jelent semmit, mint például 10 15 30 […] stb.")

b) „I medesimi caratteri dell'alfabeto seruiranno per silabe quando auranno uno di questi cinque numeri sopra cioe .4. 7. 2. 1. 8. che faranno per .a. e. i. o. u. […]"
(„Az ábécé betűiből szótag lesz, ha a következő öt szám, azaz .4. 7. 2. 1. 8. közül, amelyek .a. e. i. o. u. helyett állnak, egyet föléjük írunk […].")

c) „Li nomi delle donne con l'accento circonflesso et quelli delli stati con l'acuto si scriverano come Imperatore A. Imperatrice Â. Imperio À. Le doppie si farano colla tratta di sotto in questo modo b X bb X […]"
(„a nők nevét íves ékezettel és az államokét éles ékezettel írjuk, mint Császár A. Császárnő Â Császárság À. A dupla mássalhangzókat aláhúzás jelöli, így b X bb X […]"

A funkcióbővítés sajátos lehetőségét tartalmazza egy XVI. századi kulcs,[26] amelyben – az eddig bemutatott rendszerektől eltérően – a rejtjelek nem fonémákat, hanem (CV szerkezetű) szótagokat helyettesítenek (minden szótag SIF megfelelője egy kétjegyű szám). A kulcs összeállítója egy adott rejtjel referensének módosítására tíz lehetőséget jelöl meg aszerint, hogy egy meghatározott pozícióba (például a rejtjel első számjegye fölé) egy meghatározott kiegészítő jel (pont, éles ékezet, vízszintes vonal) kerül. A rejtjel előírt kiegészítési lehetőségei, például a *ba* szótag esetében, annak következő alakmódosulásait eredményezi (a kulcsban leírt szabályok sorrendjében): *ab, a, bal, ban, bar, bra, bran, sbran, bla, blan.* A bővítési lehetőségek szemléltetésére a (9) alatt a kulcsból – terjedelmi okokból – csak néhány szabályt idézünk:

[24] ASMn AG 424 („Cifra col Panira a di 26 giugno 1531").
[25] ASMn AG 424.
[26] ASMn AG 423 „(Prima ziffra che prevede con sillabe senza lettere separate").

(9) [1] „Cadauna di queste copie de numeri con un ponto denanti rende la sillaba riuoltata che comincia da uocale. [2] et in quello dello h leua laspiratione di maniera che rimane la vocale pura.”

(„Minden kétjegyű szám elé írt pont megfordítja a szótagot, így az magánhangzóval kezdődik. [2] és a h-val kezdődő szótagnál leesik a mássalhangzó és csak a magánhangzó marad.”

[3] „Posto cadauna delle copie di numeri un punto sopra il primo carattere di numero aggiungi alla sillaba un .L.”

(„Minden kétjegyű szám első számjegye fölé írt pont hozzáad a szótaghoz egy L betűt.”)

[6] „L’accento accuto posto sopra il primo carattere interpone l’ R tra la prima lettera et la vocale.”

(„Az első számjegy fölé írt éles ékezet az első betű és a magánhangzó közé beilleszt egy R betűt.”

[8] „Occorrendo nanti cadauna lettera aggiungere lo S si ha sopra la copia di numeri da poner una virgoletta trauersata ponendoui anco il punto o accento, et ambedue secondo il bisogno.”

(„Ha a betűk elé S-t szükséges írni, a számok fölé vízszintes vonalat kell írni, szükség esetén még a pontot vagy az ékezetet is, vagy mindkettőt.”)

Az utolsó példában, (10) alatt, a kódolás folyamatára vonatkozó, egyben a hibázási lehetőség minimalizálását célzó ajánlást idézünk egy szintén XVI. századi kulcsból:[27]

(10) „Quando si haverà da scrivere in cifra si doverà prima stendere in carta tutto quello che si haverà da scrivere et tenerlo avanti quando si scrive per non fare errore.”

(„Rejtjelezéshez először írjuk le a teljes szöveget, és a kódolásnál legyen előttünk, hogy ne kövessünk el hibákat.”)

Összegzés

A tanulmány olyan kérdésekre összpontosított, amelyek korábban nem estek a kutatások látókörébe. Többek között rámutatott arra, hogy a kódkulcsokban rögzített implicit és explicit formájú szabályok, tartalmukat tekintve, az egyábécés eljárás több területét érintik: a) meghatározzák és leírják az adott rendszert; b) előírják egyes rejtjelek használati módját; c) irányítják az adott rendszer bővítési lehetőségét; d) a kód biztonságának növelését

[27] Meister 1906:298 („Cifra a Monsignor Costa […] data in Roma 11 Octobris 1583”).

célzó javaslatokat fogalmaznak meg az írásmódra vonatkozóan; e) irányítják a kódolás folyamatát.

A vizsgálat eredményeként megállapítható, hogy explicit szabályokat már a korai időszakban keletkezett kulcsok is tartalmaztak, de előfordulási arányuk jóval nagyobb volt a XVI. században. A szabályok megfogalmazásában jelentős eltérések mutatkoztak, elsősorban a rejtjelek használati módját előíró normák esetében, amelyek gyakran csak irányadó jelleggel bírtak. A példaként bemutatott használati, valamint az írásmódra és a kódolásra vonatkozó szabályok tartalmi és formai jellemzői, különös tekintettel azok modális értékére, felvetik annak a valószínűségét is, hogy a felsorolt szabályokat tartalmazó kulcsok nem a kulcs készítőjének használatára készültek.

Az elemzés a témával kapcsolatban újabb, például a szabályok gyakorlati alkalmazásához, érvényességéhez, szerepéhez a dekódolás folyamataiban stb. kapcsolódó kérdéseket is felszínre hozott, amelyek megválaszolása a téma további vizsgálatát feltételezi.