Szakmai beszámoló, K- 101544

A kutatás tartalmi eredményei

A pályázatban ígért három terület mindegyikén sikerült jelentős eredményt elérni.

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. 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. Közép-európai kutatóutak során összehasonlítottam ezt a forráscsoportot a lengyel, cseh és az osztrák levéltárakban fennmaradt anyaggal.

A forrásanyag meglepően gazdagnak bizonyult mind mennyiségében, mind diverzitásában. Amint az elkészült publikációim és megtartott előadásaim (egy megjelent monográfia magyar nyelven, ennek elkészült de még nem publikált angol nyelvű változata, kilenc cikk hazai és nemzetközi folyóiratokban és hét konferencia előadás nemzetközi fórumokon) részletesen dokumentálják, 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, számos társadalmi réteg használta mindennapi élete során.

Ahogy a felhasználók sem voltak szükségképpen politikusok, úgy a sifrírozás célja sem volt szükségképpen politikai: a magánélet, a szerelmi kapcsolat, az intim barátság, a szégyen, a mértéken felüli alkoholfogyasztás, a katonai gyengeség, a félelem, a családi konfliktusok, az erkölcsi kihágások, a térítés részletei, a vallásos meggyőződés, a tudományos recept vagy a talizmánmágia titkosítására egyaránt adódnak példák. Ahogyan pedig 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 kutatásom 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.

A kutatás kézzelfogható eredményei

Megjelent és megjelenés alatt álló könyvek

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

Use of ciphers and codes in early modern Hungary: secrecy and the social history of cryptography (az előző tétel angol nyelvű, kész fordítása, amelyet célszerűbbnek tűnik tanulmányok formájában publikálni folyóiratokban, mint egységes könyvként) A kötet tartalomjegyzékét a beszámoló függeléke tartalmazza.

The Rohonc Code: tracing a historical riddle (korábbi könyvemnek, a Jaffa kiadónál 2011-ben megjelent Rohonci kódnak az angol nyelvű fordítása, lezárt kézirat, benyújtva a MacMillan kiadónak és két literary agentnek) A kötet tartalomjegyzékét a beszámoló függeléke tartalmazza.

Láng Benedek, Lehofer Anna, Hegedűs Gyula, eds.: **Történelmi titkosírások megfejtése (új dokumentumok a Wesselényi szervezkedés történetéből)**, nyolc titkosított levél, megfejtésük, esetlegesen fennmaradt kulcsuk, a megfejtés módszertanának magyarázatával. Szerkesztés alatt, kiadóhoz benyújtás ideje: 2016. A kötet tartalomjegyzékét a beszámoló függeléke tartalmazza.

Az utolsó három tétel kéziratait igény szerint szívesen a bíráló rendelkezésére bocsátom.

Megjelent tanulmányok

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

Az ördög kézjegye, In: „Serpentarius viginti quatuor stellis decoratus" ed.: Ekler Péter, Budapest: OSZK, 2015. 24-25.

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

Zrínyi Miklós és a rejtjelezés, *Irodalmi magazin,* 2014/4, 13-15.

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.

Konferenciaelőadások

2015. Oct. 26. "Beyond the Da Vinci code and the Voynich manuscript: ciphers as historical sources", Yale University, History Department

2015. Oct. 22. "Use of the techniques of cryptology in real life situations (17th-18th century Central Europe)" *2015 Cryptologic History Symposium*, October 22 & 23, Johns Hopkins University Applied Physics Laboratory Kossiakoff Center, Laurel, Maryland, organized by the National Cryptologic Museum Foundation (NCMF)

2015. June 2. "„Csonkaságaiban kiegészíteni a haza történelmét:" történelmi hamisítások a 19. században" (Complementing national history, forgeries in the 19th century) Hamisítások és leleplezések, (Forgeries and debunking) Committee for the History of Science and Technology, Hungarian Academy of Sciences.

2014. June 10. "Encrypted Forms of Magic Knowledge: The rhetoric of secrecy" Scripted Forms of Magic Knowledge – Grimoires in the Matrix of Western Cultures, Israel Institute for Advanced Studies (IIAS) at The Hebrew University of Jerusalem, Israel

2013. Oct. 18. "Shame, sex and alcohol: ciphers in the context of everyday practices of secrecy in the early modern times," *2013 Cryptologic History Symposium*, October 17 & 18, Johns Hopkins University Applied Physics Laboratory Kossiakoff Center, Laurel, Maryland, organized by the National Cryptologic Museum Foundation (NCMF)

2013. June 26. „Latest trends in the history of cryptography," Collegium de Lyon, Ecole Normale supérieure de Lyon

2013. Apr. 20. „A social history of cryptography and secrecy in East-Central Europe - 1450-1700" *Eurias Annual Meeting,* Swedish Collegium of Advanced Study, Uppsala, April, 19-20th 2013.

2013. Feb. 26. "Les chiffres français dans la diplomatie hongroise" Chaire tournante, Isntitut Hongrois – Collegium Hungaricum, Paris

A kutatás során fejlesztett számítógépes programok

1. http://dev.philos.bme.hu/decipherng

Történelmi titkosírások megfejtésére fejlesztett szoftver. A program legfontosabb eszköze a kódfejtők köreiben jól ismert szó-mintázat módszer. Más, közkézen forgó kódfejtő programokhoz képest a szoftver előnye, hogy felhasználója könnyen és praktikusan bele tudja táplálni azt a nyílt szöveget, amelynek statisztikájával a szómintázataival a rejtjelszöveg szimbólumait össze kívánja hasonlítani. A szoftver másik előnye, hogy bár monoalfabetikus titkosírások megfejtésére készült, bármennyi karaktert képes kezelni, és ezért egy homofonikus titkosírás megfejtéséhez is segítséget nyújthat. A homofonikus titkosírások, bár jelentősen komolyabb kihívásokkal szembesítik a kódfejtőt, bizonyos részeikben – különösen, ha a kódoló megelégedett kevés homofon használatával – lényegében monoalfabetikusak. A titkosírásfejtő szoftver képes lehet arra, hogy egy-egy jellegzetes szómintázatot felismerjen, és ezzel a kódfejtő számára betörési pontot kínáljon.

A felhasználó mindenekelőtt beletáplálja rejtjelszöveget (a rejtjelszöveg számokból áll, minden szám után pont áll, egy, két, három és többjegyű számok egyaránt kezelhetők a program számára). Ezek után a felhasználó betáplálja azt a nyílt szöveget, amelyről azt gondolja a kódszöveghez időben, térben és nyelvhasználatban a lehető legközelebb van. Természetesen olyan file-t is lehet használni, amely több nyelven tartalmaz szövegeket. Amennyiben a felhasználó tudja, vagy sejti, mi lehet a rejtjelszöveg nyelve, hasonló nyelvű nyílt szöveget használ. Mind a rejtjelszöveg mind a nyílt szöveg esetében igaz, hogy minél hosszabb a szöveg, annál több remény van sikeres kódfejtésre.

A program kiszámolja, és összehasonlítja mindkét szöveg jellemző frekvencia statisztikáit (szimbolumokra, bigrammokra, trigrammokra, stb), majd végigvizsgálja a szövegek szómintázatait (minthogy a rejtjelszövegben nincsenek szóhatárok, sem ott sem a nyílt szövegben nem tekinti a szóhatárokat, "végigtolja" a mintázat vizsgálatot a space-ek nélkül vet szövegen). A folyamat néhány másodperctől néhány percig tart. A szómintázat azonosítás eredményeként a például a "little" (egy meglepően ritka szerkezetű szó) "ABCCAD", az "emperor" "ABCADED", less, és így tovább. Az alapgondolat az, hogy a minél ritkább mintázatú szavak kiugorjanak.

A lehetséges mintaegyezéseket a program abból a szempontból is vizsgálja, hogy mennyire gyakori karaktereket tartalmaznak az első, második, stb. pozíciójukban. Ebből az értékből indexszámot generálva súlyozza, mennyire valószínű, hogy egy-egy pattern egyezés valódi megoldást rejt, hiszen természetesen több szó is tartozhat ugyanahhoz a szó mintázathoz.

A program minden szóhoz kiszámolja, mennyire jól illeszkedik egy adott rejtjelszimbólumának relatív gyakorisága, a nyílt szöveg azonos mintájú szavának azonos pozíciójában álló betűjének relatív frekvenciájához. Minél kisebb ez az érték, annál valószínűbb, hogy a mintázatok egyezése valódi azonosságra utal.

Milyen jellegű helyzetben használható a szoftver? Míg a titkosítási technika gyakran rendkívül egyszerű, a nyelvi feladat annyira összetett lehet (felismerni egy különös, még a 17. században sem létezett, mert a rejtjel céljára megváltoztatott magyar nyelvet), hogy a számítógépes támogatás nélkül rendkívül nehéz volna felismerni, melyik nyelvről van szó. A szoftver tehát olyan helyzetek kezelésére készült, amelyekben nem a kriptográfiai eszköz kifinomultsága, hanem a nyelvi helyzet komplexitása okozza a problémát.

Igény szerint a bíráló rendelkezésére bocsátom a belépési jelszót (mint ahogy a korábbi, nem publikus beszámolóimban ezt már megtettem).

2. http://sharky.naplopok.hu/rohonci

A szoftver a Rohonci kódex karaktereinek digitális változatát, fontjait telepíti, valamint a kódex teljes átiratát, lekódolt változatát tartalmazza. A mellékelt szótárban szabadon lehet jelentést tulajdonítani az egyes kódszavaknak. Igény szerint a bíráló rendelkezésére bocsátom a belépési jelszót (mint ahogy a korábbi, nem publikus beszámolóimban et már megtettem), de a program egyelőre nem hozzáférhető a szélesebb közönség számára, mert olyan kutatási adatokat tartalmaz, amelyeket a kódex megfejtői, Király Levente Zoltán és Tokai Gábor addig nem kívánnak közkincssé tenni, amíg a megfejtésről szóló publikációjuk a *Cryptologia* c. folyóiratban meg nem jelenik.

További perspektívák

A kutatás tapasztalatai alapján összeállítottam egy ambíciózus ERC Consolidator Grant pályázatot lényegében hasonló tematikával és módszertannal, mint az OTKÁt, de egész Európára vonatkoztatva. Bár a pályázat nem lett sikeres, az összeállítás során megalapozott kutatási kapcsolatháló Európa szinte minden, történelmi titkosíráskutatásban aktív kutatójával igen gyümölcsözőnek bizonyult. A szakmai kapcsolatok számos forráscserében manifesztálódnak, valamint újabban egy tervezett COST pályázat benyújtásában is összpontosulnak. A COST pályázat (Historical Cryptology - HICRYPT) benyújtója az Uppsalai Egyetem tanszékvezetője, a számítógépes nyelvész Megyesi Beáta, célja pedig, hogy a hasonló területen dolgozó európai kutatók – történészek, informatikusok, számítógépes nyelvészek,

levéltárosok – rendszeres rendezvényeken találkozhassanak, valamint, hogy európai szinten megalapítsuk a lokális szinten már jól működő « történeti kriptológia » diszciplináját.

Függelék

Use of ciphers and codes in early modern Hungary: secrecy and the social history of cryptography

Contents

The Rohonc Code: tracing a historical riddle

Contents

Láng Benedek, Lehofer Anna, Hegedűs Gyula, eds.: **Történelmi titkosírások megfejtése (új dokumentumok a Wesselényi szervezkedés történetéből)**

Tartalom