Benedek Láng

Real Life Cryptology

Ciphers and Secrets in Early Modern Hungary

Amsterdam
University
Press

ATLANTIS
PRESS

Real Life Cryptology

Real Life Cryptology

Ciphers and Secrets in Early Modern Hungary

Benedek Láng

Translated from Hungarian by Teodóra Király and Benedek Láng

Atlantis Press | Amsterdam University Press

Originally published as: ‘Titkosírás a kora újkori Magyarországon’ 2015, ISBN 9789635069514, Balassi Kiadó, Budapest

Cover design: Coördesign, Leiden
Lay-out: Newgen / Konvertus

ISBN	978 94 6298 554 4
e-ISBN	978 90 4853 669 6
DOI	10.5117/9789462985544
NUR	685

Table of contents

Abbreviations

AR	*Archivum Rákóczianum, II Rákóczi Ferenc levéltára* (Rákóczi Archives) (Budapest: MTA Tört Biz. Kiad. 1873–1935) vols. 1–12.
ÖStA HHStA	Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv, Vienna
MNL OL	Magyar Nemzeti Levéltár, Országos Levéltar, Budapest (Hungarian National Archives, Budapest)
MTT	*Magyar Történelmi Tár* (Hungarian Historical Records), (Pest, Magyar Tudományos Akadémia, 1855–1934)
OSZK	Országos Széchényi Könyvtár (National Széchényi Library)
Teleki	*Teleki Mihály Levelezése* (Correspondence of Mihály Teleki) (Budapest: Magyar Történelmi Társulat, 1905–1926), vols. 1–8.

Note on terminology

In theory, cryptology is a discipline composed of two fields, cryptography, that is secret writing, and cryptanalysis, that is codebreaking (cryptanalysis is a modern term forged by William Friedman). In the period under study, no such methodical distinction was used, ciphering, encryption, "translating", "working with chiffres" and many other terms are applied somewhat inconclusively in the sources. Therefore, throughout the book, differentiation between cryptology and cryptography will be neither systematic nor analytic. Whenever I refer to the practice of ciphering in general, I will use cryptography, unless I want to particularly emphasize that besides encryption, codebreaking is also included in the activity, because then I will use cryptology.

All other terms – open text, plain text, monoalphabetic, homophonic, and polyalphabetic ciphers, frequency analysis, probable word method, entropy, etc. – will be explained in the book at their first occurrences.

Note on names

In the early modern times, person names were used inconclusively: sometimes in the language of the country of origin of a given person (which is not necessarily identical with his or her nation), sometimes in Latin, and – particularly in the countries under the Habsburg crown – sometimes in German. I made an attempt at using those name versions in each case that were the most frequently used in the sources and in the secondary literature for a given historical actor. These were most often those variations that refer to the country of birth. I did not wish to follow those scholars, who anglicize the Hungarian, German, Italian and other names, which have never been used in English (and write Francis Rákóczi, instead of Ferenc Rákóczi). I only anglicized emperors' names, such as Charles V or Ferdinand I, when these are the most widespread versions in the secondary literature.

1. Introduction

What do the following people have in common: the Hungarian poet whose private life is in crisis while he is in litigation with his family; the Serbian secret agent whose life is in danger while he is sending crucial information to the imperial court; the Transylvanian master of the mint who is eager to protect his technical knowledge; the Hungarian magnate who despises both the Turkish and the Habsburg powers; the Emperor in Vienna who corresponds with his ambassador in Constantinople; and the Archbishop who is writing to his Italian delegate? These people stood on various levels of social hierarchy. Though they were all literate, their education and cultural backgrounds differed, as did their political power and influence on history. Yet, they all applied the same means when trying to protect their messages from prying eyes: the technology of ciphering.

Even though they and their secret writings have long been known, this monograph is the first systematic work on the history of ciphers of early modern Hungary. Its conclusions have been formed through the systematic collection and analysis of sources that come in remarkably high numbers. The most important argument of this book, as stated in the lines above, is that the social and political background, the intentions, the cryptographic skill and choice of tools of those using cryptographic methods in the sixteenth and seventeenth centuries show a much more significant variation than the traditional scholarship – concentrating primarily on the practice of diplomacy – had shown. The second argument – closely related to the first one – is that studying the variety of attitudes of this wider social environment of cryptography and the many ways people made use of enciphering methods is an approach that will help reintegrate the history of ciphers in the growing scholarship on secrecy. In other words, studying cryptography not only as a scientific technology, but rather as a complex system of social practices, will enrich the traditional "internalistic" approach to this branch of the history of science and will situate it in the context of social history.

The source material used as a sample to demonstrate these arguments comes from early modern Hungary that – because of its history particularly rich in conflicts in this period – provides ample resources for such an examination. I do not wish to claim that no other region could have provided this richness of resources to such research, as I will show in detail later. The assumption that Hungarian history is more abundant in secret writings than other countries is in itself to be examined and presently I would refrain from taking sides in this matter. It is argued that a similar demonstration might be carried out relying on the source material of other regions as well, and the conclusions aim to bear general relevance to the history of secrecy.

The research discussed here has yielded two results. First of all, it is a text-based analysis of a very common type of source which is inherently connected to a number of research areas within the discipline of history. Furthermore, it enables us to draw general implications connected to social history and research methodology, thus becoming relevant even for those readers who are interested in socio-historical developments rather than in coded letters.

In the following chapters I will first review the literature on the topic to prove that this study fills a niche, and then, having summarized the international developments in the historiography of secret writing, I will discuss the Hungarian contributions. Subsequently, through the analysis of sources, some of which was printed, some of which only exist in the archives in manuscript form, I will reach more general conclusions, which I will use to adequately support my two main statements above. Thus, this book starts out from the technical and source-centered aspects to reach finally more general socio-historical conclusions.