Real Life Cryptology

Published by Amsterdam University Press

Real Life Cryptology: Ciphers and Secrets in Early Modern Hungary.
Amsterdam University Press, 2018.
Project MUSE. muse.jhu.edu/book/66424.

For additional information about this book
https://muse.jhu.edu/book/66424
9. **Summary**

This research on the cipher use of early modern Hungary was based on nearly three hundred code keys that survived mostly in manuscripts, and more than sixteen-hundred ciphered letters, about four hundred in manuscripts, the rest published. Considerable amount of “external” sources and comments connected to various forms of cryptology was also taken into account.

A historian of the period emphasized the particularly great number of surviving ciphers from the Hungarian region.¹ How far this is true as compared to other countries of the region (such as Poland, the German states, France or Spain) is still an open question that systematic research has to confirm. This much-needed large-scale comparative analysis would include a methodical study of the nomenclature collections, a typology of the enciphered letters, and a collection of comments on cipher use and on the practice of secrecy. It could be a study of similar structure with similar research questions as this present work, except on a greater scale, covering all of the European sources. Only after that is completed can one satisfactorily place the Hungarian sources and evaluate their richness.

What are the main conclusions of the present work, and how successfully could this research answer the initial research questions?

Despite the fact that the majority of the surviving sources are from the field of politics (diplomacy, envoy’s reports, military correspondence, etc.), cryptography extended beyond central diplomacy to be used by various social layers on a day-to-day basis. It was not necessarily a privilege of men, several sources testify that women connected to politics in this way or another used claves too. Apparently, the only criterion for cipher use was literacy.

Just as the users were not all politicians, the purpose of ciphering was not necessarily political either: private life, love affairs, extremely intimate relationships, shame, excessive drinking, military weakness, fear, family feuds, moral sins, details of missionary work, religious conviction, scientific recipes, magic of the talisman were all topics that cried for enciphering. A close examination of the relation of cipher and plain texts provides a deeper understanding of the secrecy concept of the people in the past. What they deemed worthy of encrypting today sometimes seems to lack any sense. Levels of secrecy and privacy can be identified: hardly anything

---

¹ Várkonyi, “A tájékoztatás hatalma.”
was ever completely encrypted, most encrypted sources made some sense to the reader without a clavis too, and only a more concrete understanding required more elaborate tools of decrypting. Some sources encode certain information, only to give away the code key in the same source (as in the diaries of Haller, Szaniszló or Cementes, or the talisman scripts of Krakow). As the level of decoding was gradual, so was access to the secret: one community had more direct access to a particular letter, codex, diary or message than the other. Secret as content and secrecy as practice sometimes parted: the handbooks of the magic of talisman encrypted the not-so-mysterious names of spirits, while the Rohonc codex was not meant to be encrypted (or so we assume), yet its content is not accessible to us now.

An important facet of the this research focused on the history of cryptographic technology. As the sources allowed to, there was an attempt to map up, how much the cipher users understood the way it worked, whether they realized how important it was to protect the key, how they exchanged claves and how often they replaced them. It was astonishingly difficult in early modern Hungary to decipher a homophonic code, at least this is what the available sources indicate. One area of the monograph where it could be challenged is this: future research should identify a more organized and more successful codebreaking office related to the Vienna Court.

In the three-hundred-year-long period under study, certain trends might be highlighted. Central diplomacy abandoned the monoalphabetic ciphers and gradually turned to more complex homophonic methods. By the end of the period, not only letters of the alphabet, but also syllables had separate signs or numbers in the ciphers, while nullities and code words were more and more extensively used. Parallel to this development, simpler enciphering techniques appeared on lower levels of society in the practice of various professions. The further we descend from diplomatic routines, the more dominant monoalphabetic ciphers become. This was probably due to the lack of professional code breakers on the given level, to the less vital nature of the secret to be protected, and not least that complex homophonic methods were not known and available to everyone. The libraries of the period did carry the reference books that could even have strengthened the ciphering techniques of people outside the spheres of politics, yet hardly anyone used these resources, it looks. Politics may have been the unique source of advanced ciphering methods – the further we get away from it, the simpler methods we find. Future research may find more evidence of knowledge transferred from the Turkish-Ottoman culture, however, there is no sign at the moment that such investigations would yield any result,
particularly because the Turks themselves do not seem to have been aware of their rich Arabic heritage in the field of cryptography.

Various types of everyday users became part of the history of ciphers. The widespread use of ciphers and their growing popularity must have been related to the fact that in the three-partite Hungary, partly occupied by the Turks, partly living under Austrian direction, and partly balancing between the two in Transylvania, a particularly large portion of the population was living in the frontier zone and participated (or was forced to participate) in the network of information flow as possessors and transmitters of secrets. The depth they submerged into cryptography and the aims for which they used ciphers indicate a great variability in their attitudes to secrecy.

While many conclusions of local significance might be drawn (and have been drawn) from this large-scale research – regarding technology usage, knowledge transfer, etc. – where I find it most fruitful are the two following claims: 1) histories of cryptography should combine internalistic and externalistic approaches, and 2) investigations into ciphers should take into account the secrecy studies of the same periods, if we really want to understand how this technology was used in real life.