



THE VATICAN CHALLENGE – PART 5

Author: George Lasry

July 2019

The Secret Archives of the Vatican (ASV)

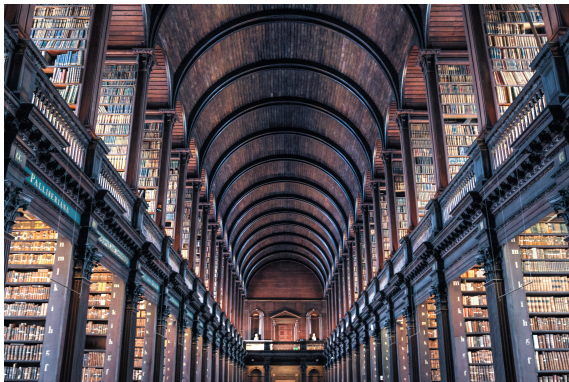


Figure: <https://www.pexels.com/photo/ancient-antique-architectural-design-architecture-442420/> licensed under Creative Commons Zero (CC0) license.

Introduction

The Vatican owns a large collection of hand-written historical manuscripts, letters and other writings, as well as printed books. Many of these writings are to be digitized and made available to the public. Some of these old historical manuscripts contain ciphertexts that have not been decrypted yet . . .

Challenge (1/6)

Enciphered messages were found in the Vatican Secret Archives (or ASV, in Latin: Archivum Secretum Vaticanum; Italian: Archivio Segreto Vaticano), Reference: ASV/i1025/SdS/Spain/IA/2. They are also included in the DECODE database [1].

The archive manuscript consists of multiple pages, with clear text and code digits mixed. A transcript is available in the additional file: ASV_i1025_SdS_Spain_IA-2.txt. Due to the preservation state of the manuscript, there might be multiple errors in the transcription.

Some notes in the archive: Lett. Orig. e cifre del card. Farnese al nunzio, 4 oct 1539-24 nov. 1548. ff. 7-123.

The key is unknown. The plaintext of the message is unknown.

Challenge (3/6)

Some observations and hypotheses (which might be correct or wrong):

- ▶ The language is probably Italian, as the vast majority of messages kept in the ASV are in Italian, and in this file, cleartext fragments are in Italian.
- ▶ The notation $\hat{}$ indicates some marking on top of the last digit. For example, 9^{\cdot} represents the digit 9 with a dot on top.
- ▶ Similarly, the notation _\cdot indicates some marking below the last digit. For example, 8_\cdot represents the digit 8 with a dot on the bottom.

Challenge (4/6)

- ▶ Most of the ciphers in the ASV are homophonic, that is, certain letters (or syllables) may be represented by more than one code, e.g. the letter *n* could be represented by both 45 and 75.
- ▶ Furthermore, in some cases, the homophones may have a different number of digits, e.g, the letter *m* could be represented by both 7 and 17.

Challenge (5/6)

- ▶ Some ASV ciphers are polyphonic, that is, a code (usually, a single digit) may have more than one meaning. For example, 4 could represent both the letters *g* and *t*.
- ▶ Most of the ciphers in the ASV have nulls, that is, a set of 1 or 2 digit codes that do not represent any letter, syllable or word. They are sometimes used to delimit words. It is not clear whether nulls are used in the challenge cryptogram, and how.

Challenge (6/6)

A useful source (in German) about the history of Vatican ciphers may be found in [2].

The answer to the challenge should include:

- ▶ The key.
- ▶ The plaintext.
- ▶ Optionally (for additional points): The method used to recover the key and plaintext.

References

1. Megyesi, B., Blomqvist, N., and Pettersson, E. 2019. The DECODE Database: Collection of Historical Ciphers and Keys. "In Proceedings of the 2nd International Conference on Historical Cryptology (HistoCrypt 2019)." NEALT Proceedings Series 37. June 23-25, 2019, Mons, Belgium. Published by Linköping Electronic Press (<http://www.ep.liu.se/ecp/contents.asp?issue=158>). This work is part of the DECRYPT project financed by the Swedish Research Council, grant 2018-06074.
2. Aloys Meister, "Die Geheimschrift im Dienste der päpstlichen Kurie von ihren Anfängen bis zum Ende des 16. Jahrhunderts", Paderborn 1906, available online <https://archive.org/details/diegeheimschrift00meis/page/n6>