HCPortal Overview

Eugen Antal
Slovak University of
Technology in Bratislava
Slovakia
eugen.antal@stuba.sk

Pavol Zajac
Slovak University of
Technology in Bratislava
Slovakia
pavol.zajac@stuba.sk

Abstract

HCPortal is a portal consisting of several web pages and tools focusing on historical cryptology. The heart of the project is a comprehensive database of cryptograms accessible for everybody. The front-end of this portal was designed to provide a responsive and modern UI/UX. We used technologies built for the modern web. The major part of the portal's back-end is also available as a public API.

1 Introduction

The **Portal** of **H**istorical **C**iphers (HCPortal) is a gateway to the world of historical ciphers. You can find a comprehensive database of cryptograms, framework for document analysis, glossary and many more.

This project was created by researchers and students from the Slovak University of Technology in Bratislava in cooperation with other crypto history enthusiasts.

2 The Portal

The HCPortal consists of several parts. The portal's home page serves as an entry point, connecting these parts together. While the portal has started only recently, we have already prepared:

- **Home page** - entry point of the portal with navigation and information centre.
- **Database of cryptograms** - database with a public API, also contains visualization (front-end) and advanced search.
- **ManuLab** and **ManuLab online** - software product for statistical analysis, with a public API and example web page.
- **Tools and web pages** - links to external projects.
- **Glossary** - glossary for historical cryptology.

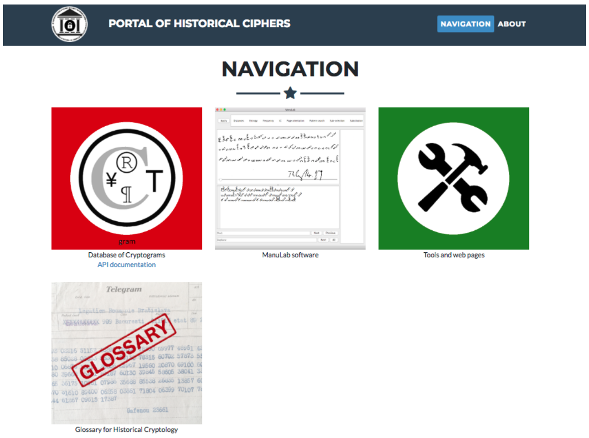


Figure 1: The main navigation screen.

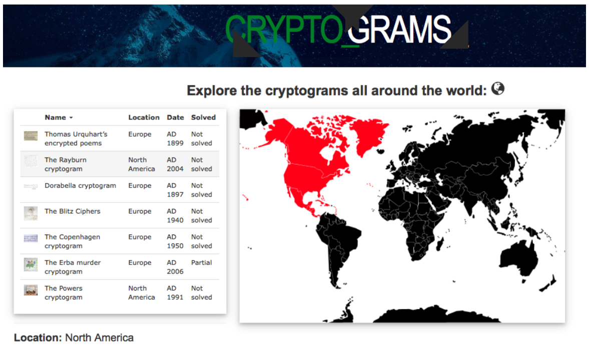
The portal's entry point is available at: https://hcportal.eu/.

3 Database of Cryptograms

We are carefully collecting[1] the most important information about known cryptograms, which are stored in a relational database. Cryptogram descriptions are also available through a web-service (public API). The front-end (web) contains cipher detail visualization and full-text search. We have also implemented an advanced search, where it is possible to find cryptograms based on location, language, sender and other parameters.

[1] The cryptograms are collected (and are planned) mainly from (Klausis Krypto Kolumne, 2019), (Crypto Cellar Research, 2019), (Breaking German Navy Ciphers, 2019), The Slovak National Archive and The Military History Archive of Slovakia, all with permissions.

The API documentation is available at:
`https://www.cryptograms.hcportal.eu/api/apidoc/index.html`
and accessible from:
`https://cryptograms.hcportal.eu`.



	Name ▾	Location	Date	Solved
	Thomas Urquhart's encrypted poems	Europe	AD 1899	Not solved
	The Rayburn cryptogram	North America	AD 2004	Not solved
	Dorabella cryptogram	Europe	AD 1897	Not solved
	The Blitz Ciphers	Europe	AD 1940	Not solved
	The Copenhagen cryptogram	Europe	AD 1950	Not solved
	The Erba murder cryptogram	Europe	AD 2006	Partial
	The Powers cryptogram	North America	AD 1991	Not solved

Location: North America

Figure 2: Cryptograms - home screen.

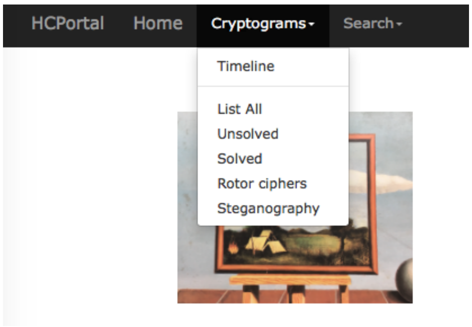
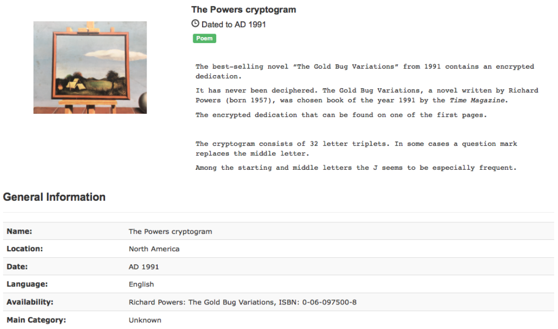


Figure 3: Cryptograms - main menu.



The Powers cryptogram

Dated to AD 1991

The best-selling novel "The Gold Bug Variations" from 1991 contains an encrypted dedication.

It has never been deciphered. The Gold Bug Variations, a novel written by Richard Powers (born 1957), was chosen book of the year 1991 by the *Time Magazine*.

The encrypted dedication that can be found on one of the first pages.

The cryptogram consists of 32 letter triplets. In some cases a question mark replaces the middle letter.

Among the starting and middle letters the J seems to be especially frequent.

General Information

Name:	The Powers cryptogram
Location:	North America
Date:	AD 1991
Language:	English
Availability:	Richard Powers: The Gold Bug Variations, ISBN: 0-06-097500-8
Main Category:	Unknown

Figure 4: Cryptograms - cryptogram detail.

4 ManuLab

ManuLab is a software product for statistical analysis of encrypted historical manuscripts. The document analysis is performed via a chain of *filters* (main building elements). A filter represents

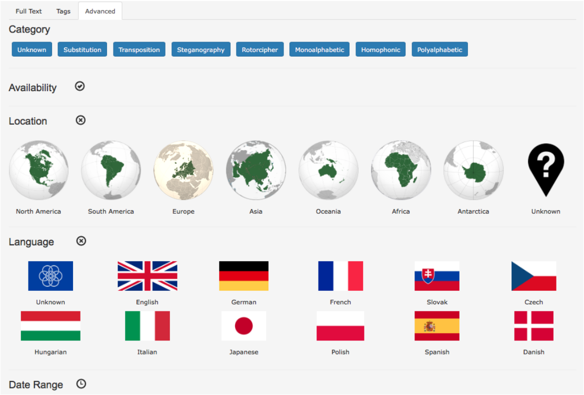


Figure 5: Cryptograms - advanced search options.

any operation realizable on a document transcription divided into a set of pages.

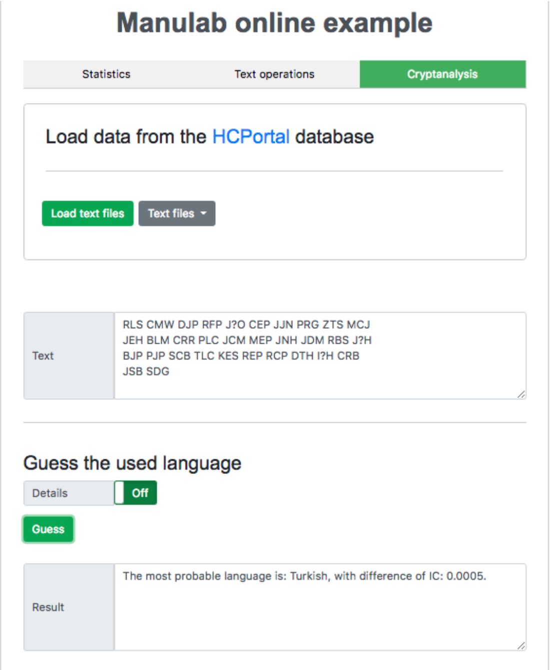
The implemented filters allow to change the reading direction, select sub-pages, or a subsection from the document, and calculate several statistics like the index of coincidence, Shannon's entropy, *n*-gram frequency, etc.

Later on, we have decided to create a more general framework independent from the operating systems, and ported the main functionality of the existing application to the web. **ManuLab online** is the online version of the ManuLab application, accessible via PHP scripts.

Furthermore we integrated the existing database of cryptograms directly to the example web page. The users can directly download and analyse text attachment of any cryptogram from the database.

The functionality was extended with cryptanalysis functions like language guess, anagram detection or Sukhotin's vowel detection method.

The source code is available online at the following GIT repository:
`https://bitbucket.org/jugin/manulab.git`.
The API documentation is available at:
`https://manulab.hcportal.eu/apidoc`
and an example web page (demonstrating the API) is available at:
`https://manulab.hcportal.eu/example`.



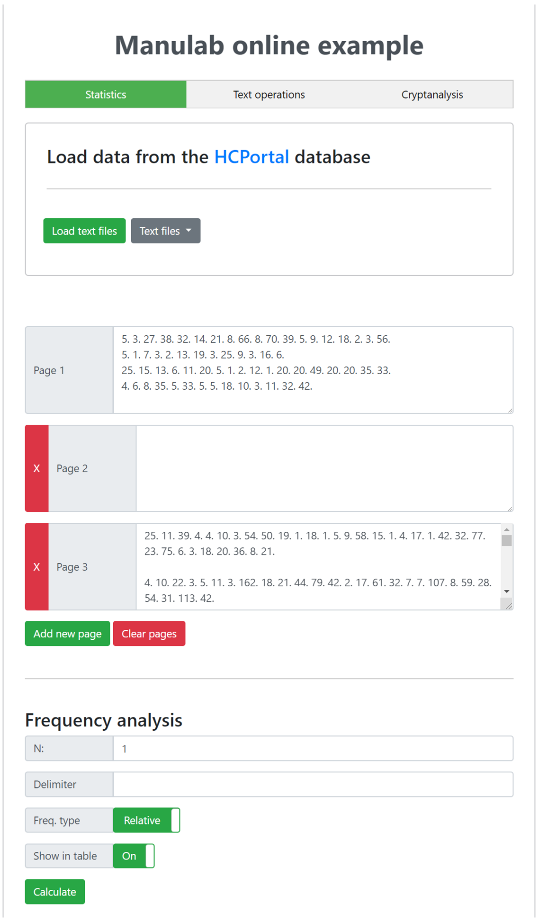
Text: RLS CMW DJP RFP J?O CEP JJN PRG ZTS MCJ
JEH BLM CRR PLC JCM MEP JNH JDM RBS J?H
BJP PJP SCB TLC KES REP RCP DTH I?H CRB
JSB SDG

Guess the used language

Details: Off

Result: The most probable language is: Turkish, with difference of IC: 0.0005.

Figure 6: Manulab online API example.



Page 1: 5. 3. 27. 38. 32. 14. 21. 8. 66. 8. 70. 39. 5. 9. 12. 18. 2. 3. 56.
5. 1. 7. 3. 2. 13. 19. 3. 25. 9. 3. 16. 6.
25. 15. 13. 6. 11. 20. 5. 1. 2. 12. 1. 20. 20. 49. 20. 20. 35. 33.
4. 6. 8. 35. 5. 33. 5. 5. 18. 10. 3. 11. 32. 42.

Page 2:

Page 3: 25. 11. 39. 4. 4. 10. 3. 54. 50. 19. 1. 18. 1. 5. 9. 58. 15. 1. 4. 17. 1. 42. 32. 77. 23. 75. 6. 3. 18. 20. 36. 8. 21.

4. 10. 22. 3. 5. 11. 3. 162. 18. 21. 44. 79. 42. 2. 17. 61. 32. 7. 7. 107. 8. 59. 28. 54. 31. 113. 42.

Frequency analysis

N: 1

Delimiter:

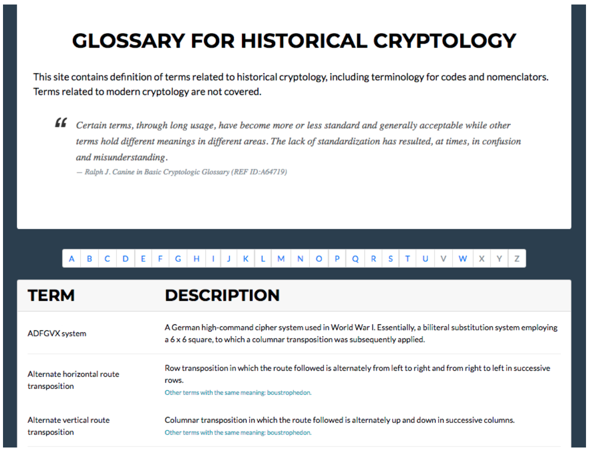
Freq. type: Relative

Show in table: On

Figure 7: Manulab online API example - multiple input pages.

5 Glossary

This site contains definitions of terms related to historical cryptology, including terminology for codes and nomenclators. Terms related to modern cryptology are not covered. The used terms are mainly from the declassified Friedman's collection - Basic Cryptologic Glossary (REF ID:A64719) and from (Klausis Krypto Kolumne, 2019). We are currently collecting visual examples (pictures) of selected terms to extend this glossary.



GLOSSARY FOR HISTORICAL CRYPTOLOGY

This site contains definition of terms related to historical cryptology, including terminology for codes and nomenclators. Terms related to modern cryptology are not covered.

> *Certain terms, through long usage, have become more or less standard and generally acceptable while other terms hold different meanings in different areas. The lack of standardization has resulted, at times, in confusion and misunderstanding.*
>
> *— Ralph J. Canine in Basic Cryptologic Glossary (REF ID:A64719)*

TERM	DESCRIPTION
ADFGVX system	A German high-command cipher system used in World War I. Essentially, a biliteral substitution system employing a 6 x 6 square, to which a columnar transposition was subsequently applied.
Alternate horizontal route transposition	Row transposition in which the route followed is alternately from left to right and from right to left in successive rows. Other terms with the same meaning: boustrophedon.
Alternate vertical route transposition	Columnar transposition in which the route followed is alternately up and down in successive columns. Other terms with the same meaning: boustrophedon.

Figure 8: Glossary.

Acknowledgments

This work was partially supported by grants VEGA 1/0159/17 and VEGA 2/0072/20.

References

Klaus Schmeh. *Klausis Krypto Kolumne* http://scienceblogs.de/klausis-krypto-kolumne

Frode Weierud. *Crypto Cellar Research* http://cryptocellar.org/

Michael Hrenberg. *Breaking German Navy Ciphers* https://enigma.hoerenberg.com/

Satoshi Tomokiyo. *Cryptiana* http://cryptiana.web.fc2.com/code/crypto.htm