HCPortal: Ten Years of Development

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 an online portal focusing on historical cryptology. It has now been in active development for ten years. During the development, many new changes and additional modules were added. We present the current state of the portal, with a focus on an overview of the main modules and their user interface specifics.

1 Introduction

The Portal of Historical Ciphers (HCPortal) is an online portal consisting of several web pages and tools, each related to historical cryptology (Antal and Zajac, 2020). The first version of the portal was developed in 2016, focusing on two aspects at that time: creating a collection of historical ciphers, alongside tools for analysing these ciphers (Antal and Zajac, 2018). The content of the portal was gradually expanded, featuring a modern Angular application for browsing the database of cryptograms since 2017. The main goal was to publish accessible data for enthusiasts and researchers to support their work and to promote the research in the area of historical cryptography.

In 2019, a new education aspect was introduced, focusing on various cryptanalytic techniques (Antal and Zajac, 2021). The database of cryptograms was expanded with a new separated database in 2020, and gradually upgraded in the following years. In 2021, a virtual museum and a special online tool (which can be used to create custom nomenclator ciphers) were integrated into the portal.

The user interface of the HCPortal was redesigned in 2022 (see Figure 1). When designing new components, the contributors focused exclusively on online accessible applications and modern web technologies such as Angular, React, Laravel, etc. In the same year, a new version of the

Figure 1: HCPortal - main portal page.

portal was introduced with a special focus on the following three aspects:

- education,
- promotion of historical cryptology,
- source of historical data (databases and annotated datasets).

The education module was redesigned to better support education goals and interactive teaching methods. Old, separate databases were integrated, and access to data was updated to facilitate easier access.

In 2024, an additional database of cryptologists was added as well. In 2025, a new web application was added for storing and sharing datasets used for various machine learning tasks, related to historical encrypted manuscripts and cipher keys.

In the rest of the article, we describe the current state of the portal with respect to selected areas of the portal's use. We point out how the specific parts of the portal support researchers, educators, and enthusiasts in the area of historical cryptology.

2 Related Work

Presently, numerous websites and online tools are accessible on the internet that specialize in historical cryptology. Notably, over the past decade, a substantial number of digital resources have emerged, providing support for research in this field and facilitating data access.

Enthusiasts can find various information about codes and unsolved cryptograms on various blogs and websites (Cryptiana, 2026; Crypto Cellar Research, 2026; Cipherbrain, 2022).

Websites such as dCode (2026), Cryptii (2026), CrypTool (2026) offer implementations of different classical ciphers. These and similar sources provide students and enthusiasts with an opportunity to interact with the cipher algorithm and learn basic encryption and decryption steps.

Online museums (Crypto Museum, 2026) and simulators (Virtual Colossus, 2026) provide detailed information about historical ciphers and cipher machines, shedding light on their operation and significance.

Databases of historical cryptograms, cipher keys, datasets, and other materials are equally important. These databases are primarily used in research projects focused on analyzing and decrypting historical ciphers (Megyesi et al., 2020; Antal and Zajac, 2020). They also enable a comprehensive study of historical ciphers, contributing to a deeper understanding of their significance.

We aim to position HCPortal as a bridge between various cryptology resources. We integrate all the above-mentioned aspects under a single umbrella with a unified design, while providing links to additional specialized resources.

3 Using HCPortal for Education

One of the main aspects of the portal is to support education goals and interactive teaching methods[1] on the topic of historical cryptology. For this reason a special *Education*[2] module was created. At the current state, it is divided into two main parts: cryptography and cryptanalysis.

The cryptanalysis part consists of a collection of interactive tools with graphical visualization of the data, designed for a better understanding of attacks on selected classical ciphers. Each demonstrated attack is divided into logical steps. At the moment, it contains five attacks on substitution ciphers:

- Brute-force attack on Caesar Cipher;
- Hill-Climbing attack on simple substitution cipher;
- Friedman test and brute-force attack on Vigenère cipher;
- Friedman test and brute-force attack on an *Autokey cipher*, including the Autokey to Vigenère transformation (see Figure 2);
- Manual and (semi) automated dictionary attack on substitution cipher based on word patterns.

For the transposition ciphers, three attacks are implemented:

- Brute-force attack on Scytale;
- The "moving strips" manual attack on columnar transposition;
- Multiple anagramming method.

[1] The primary goal for the inclusion of the *Education* module to HCPortal was to support an online education in our course Classical Ciphers taught at the Slovak University of Technology in Bratislava. However, we have designed the tools in such a way, that they can be used by other students and the general public (Antal and Zajac, 2021).

[2] https://edu.hcportal.eu

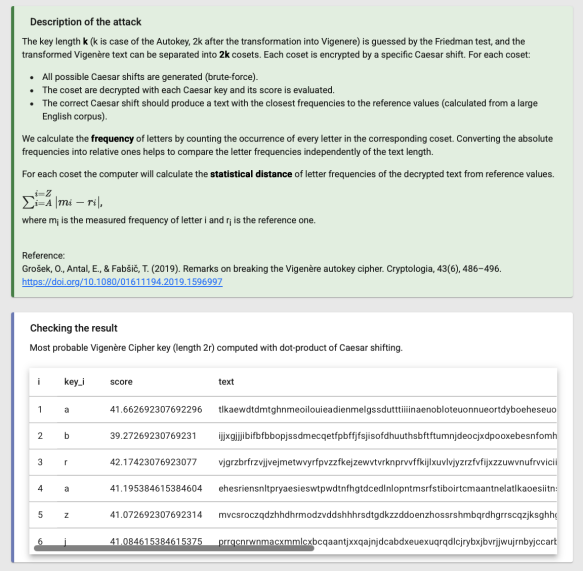

Figure 2: Education module - part of the attack on an Autokey cipher.

The cryptanalysis process is supported with a separate web application called *ManuLab online*[3]. ManuLab online is a software product for statistical analysis of encrypted historical manuscripts. It's the successor of the previous ManuLab Qt application (Antal and Zajac, 2018). The software is designed to display pairs of input files - an image file of ciphertext with the corresponding transcription (see Figure 3). Several functions (called filters) are implemented, which can be chained in the analysis process. The main filters are: frequency analysis of n-grams, Index of Coincidence, Shannon's Entropy, pattern search, text element distances, text modifications, anagram detection, vowel detection, and language guessing methods.

Figure 3: ManuLab Online - example.

In the cryptography part of the education module, general information and a classification of historical ciphers can be found. We present three types of classification based on various criteria for a better understanding of how historical ciphers work. In addition, the visitor can try the encryption and decryption process using various real cipher[4] implementations (see Figure 5), and try some helper methods[5] which are used in our course.

In addition to the real cipher implementation of the education module, a separate web application was created, where custom nomenclator keys can be created by the users (see Figure 4). This module is called *Cipher Creator*[6]. The cipher keys created with this application have both textual (JSON format) and graphical (PDF format) representations, and the website allows the user to encrypt and decrypt custom text messages with the generated nomenclator keys.

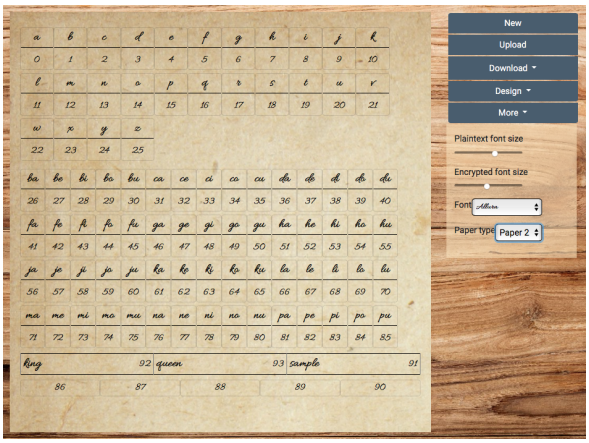

Figure 4: Cipher Creator module - custom cipher key.

A special glossary is accessible[7] from the main portal page, covering definitions of terms related to historical cryptology based on William F. Friedman's Basic Cryptologic Glossary and a discussion from Klaus Schmeh's former Cipherbrain blog (Cipherbrain, 2022).

[3]https://manulab.hcportal.eu

[4]Currently, the real ciphers part cover two Japanese ciphers, the Condenser PBJ cipher machine, and four ciphers from that were used in movies or TV series.

[5]The Bellaso's method of creating numeric permutations from passphrases, and various string-to-pattern conversion methods.

[6]https://ciphercreator.hcportal.eu

[7]https://hcportal.eu/glossary.html

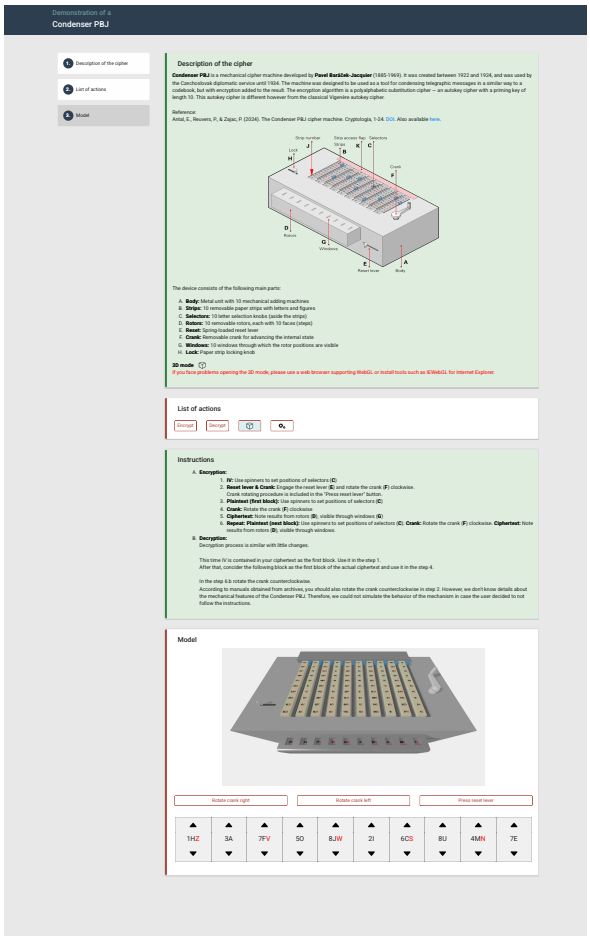

Figure 5: Education module - implementation of the Condenser PBJ cipher machine with a 3D model.

4 Promotion of Historical Cryptology

The second main aspect of the portal is to increase interest in historical ciphers among the general public. By using modern information technologies, a special *Virtual Museum*[8] was created based on the virtual reality (VR) concept.

The museum presents general information about the history of cryptology in a familiar "museum" style. A virtual reality engine for a web browser was used. In this way, materials can be displayed online, even if the user does not have a VR device (Antal and Zajac, 2021). The museum core consists of a static exhibition, which covers a timeline of ciphers and information about ciphers, steganography, cryptanalysis, unsolved cryptograms, and cipher machines (see Figures 6 and 7). In addition, a registered user can create dynamic exhibitions on various topics. These exhibitions allow us to present the following data types: text, image, video, and PDF files.

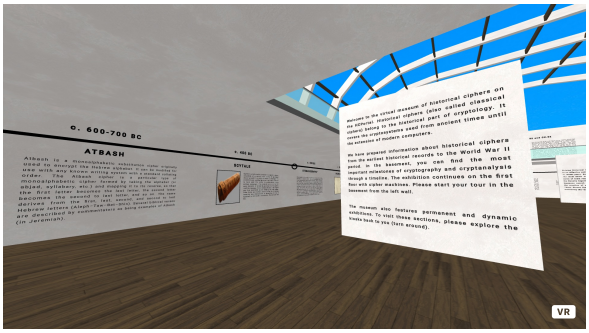

Figure 6: HCPortal - Virtual Museum.

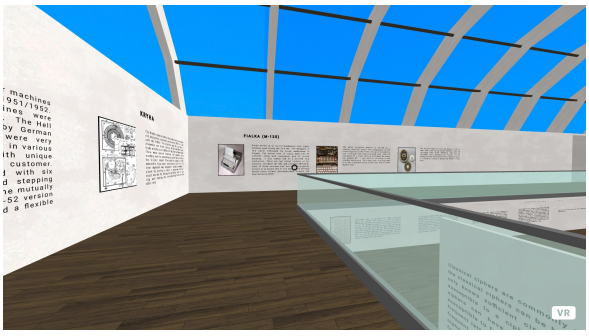

Figure 7: HCPortal - Virtual Museum - cipher machines section.

5 Historical Data Sources

The third important aspect of the portal is to provide a wide range of historical data for researchers and the general public. We collected, processed, and published different databases to support a wide range of research tasks. Contrary to other known databases of materials related to historical cryptology, all our data is publicly available for everyone without a need for registration or other types of special access [9].

For researchers who investigate the history of cryptology and analyse the development of cipher systems, two special databases are available:

- Database of cryptograms and cipher keys[10];
- Database of cryptologists[11].

[8] https://www.museum.hcportal.eu

[9] All the materials from archives and the owners are used with permission or have a public domain license.

[10] https://crypto.hcportal.eu/

[11] https://cryptologists.hcportal.eu

Currently, the database of cryptograms and cipher keys contains 1875 records of cryptograms and 319 records of cipher keys. The database contains, among others, a notable large collection of 988 cryptographic postcards, including Tobias Schrödel's collection (Tobias Schrödel, 2021). The records are supplemented with various metadata and tags (see Figure 8) to allow detailed browsing of the database. We have implemented a modern web interface to browse the database and provide statistics of the records (see Figure 9). Additionally, a timeline of the records is also available in the browsing interface.

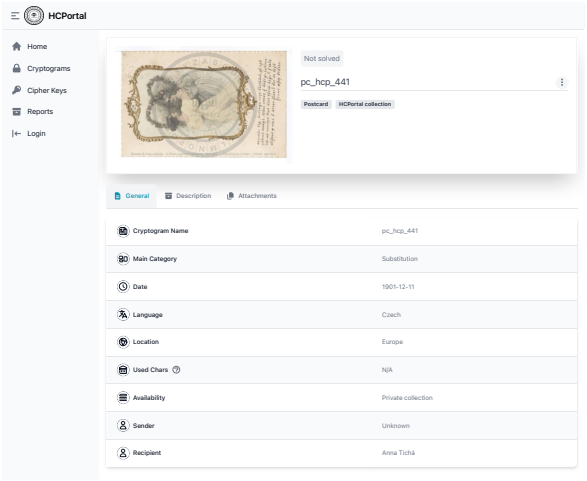

Figure 8: Database of cryptograms and cipher keys - example of a cryptogram record and its metadata.

The database of cryptologists contains 222 records at the moment from various public sources. The records are supplemented with various metadata and tags (see Figures 10 and 11) to allow detailed browsing of the database.

Both system provides content management system for registered users. The records are reviewed by an administrator, and only approved records will be visible in the public database.

For researchers who are working on various computer vision and machine learning tasks related to historical ciphers, a special repository of annotated datasets is available - the *Dataset Builder*[12]. Currently, the database contains 143377 instances of annotations divided into 172 classes (see Figures 12 and 13) (Antal et al., 2026).

This platform provides a wide range of functionality: dataset visualization, view of statisti-

[12]https://builder.hcportal.eu

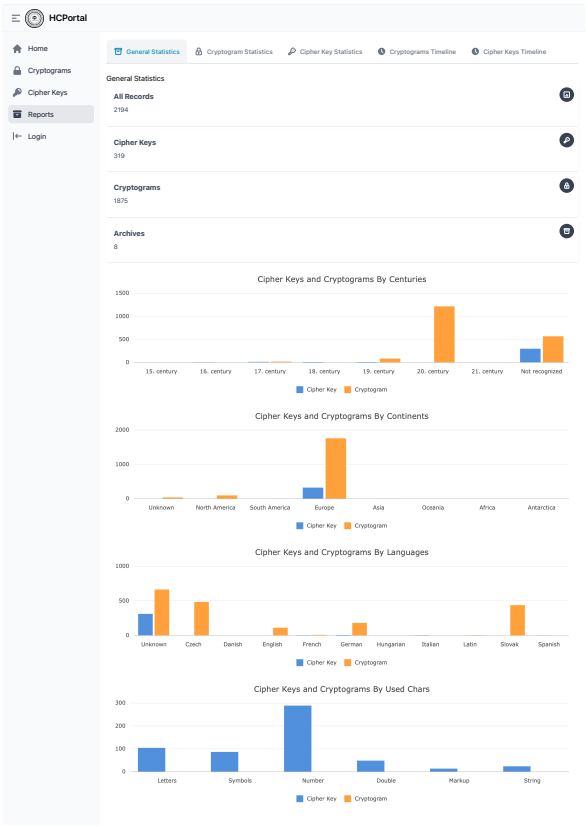

Figure 9: Database of cryptograms and cipher keys - statistics.

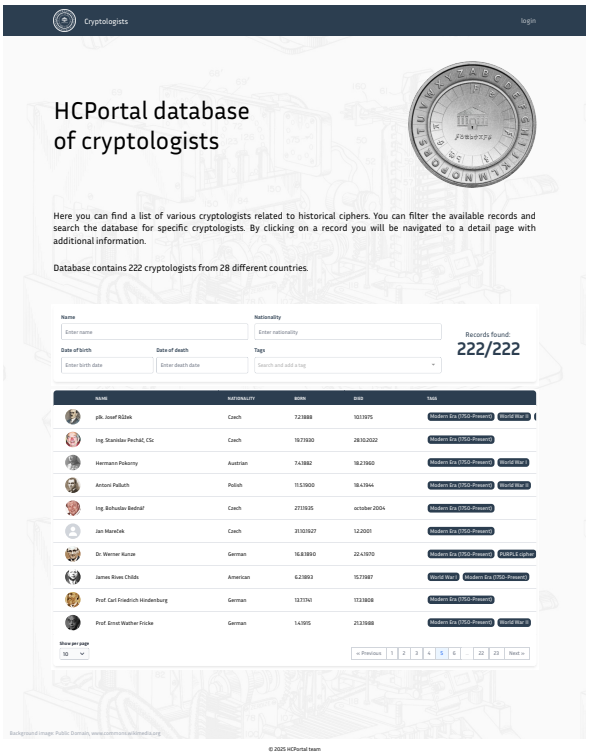

Figure 10: Database of cryptologists.

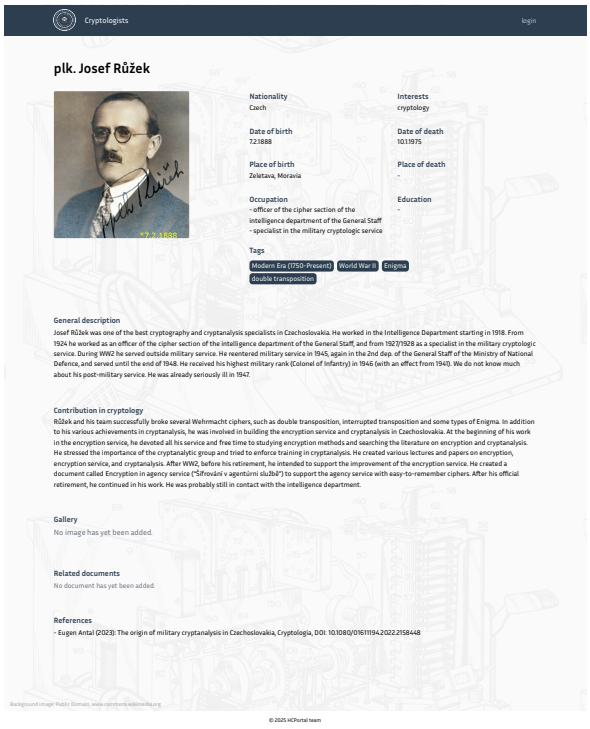

Figure 11: Database of cryptologists - example of a record and its metadata.

cal summaries, and customizable dataset generation (see Figure 14). The users can interactively select the annotation type (polygons and bounding boxes), symbol categories (currently, glyphs or digits are available), define dataset splits, specify target classes, choose individual samples with annotations, and balance the number of annotations across classes. Therefore, they can build a custom dataset that perfectly suits their needs. The datasets can be exported in several widely used annotation formats, including YOLO, COCO, Pascal VOC, and Labelme.

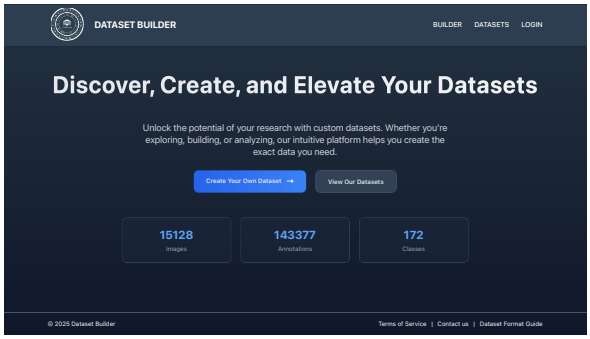

Figure 12: Dataset Builder.

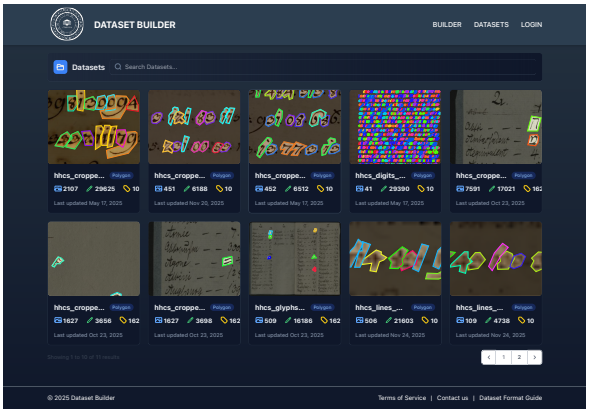

Figure 13: Dataset Builder.

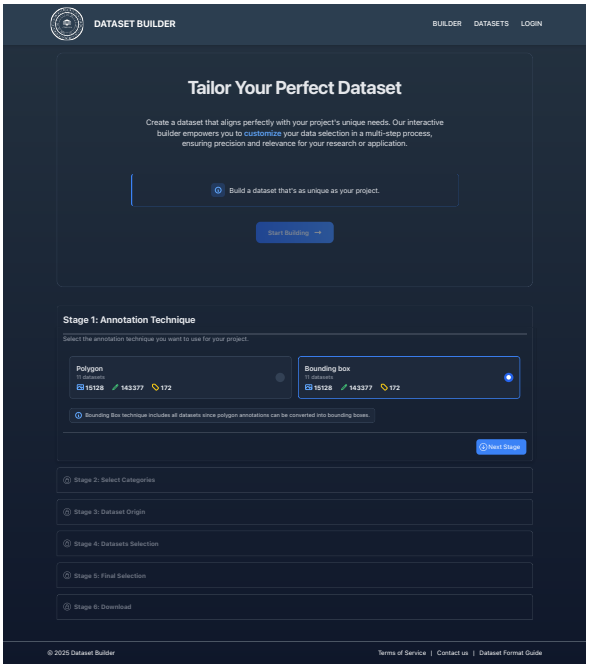

Figure 14: Dataset Builder.

6 Conclusions

There exists a wide range of resources for historical cryptography, including direct and indirect sources of data (such as online archives), online museums and collections, as well as education resources (CrypTool, 2026; Crypto Museum, 2026; dCode, 2026; Megyesi et al., 2020; Virtual Colossus, 2026). The current version of HCPortal represents a middle ground that combines different aspects into a single portal. Our collection of data and tools can support both research and education in the area of historical cryptography.

Acknowledgments

This work was supported by grant VEGA 2/0054/24.

References

Eugen Antal and Pavol Zajac. 2018. ManuLab System Demonstration. In *Proceedings of the 1st International Conference on Historical Cryptology, HistoCrypt 2018*, pages 125–128. Linköping University Electronic Press.

Eugen Antal and Pavol Zajac. 2020. HCPortal Overview. In *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, pages 18–20. Linköping University Electronic Press.

Eugen Antal and Pavol Zajac. 2021. HCPortal Modules for Teaching and Promoting Cryptology. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 1–11. Linköping University Electronic Press.

Eugen Antal, Pavol Marák and Filip Mikuš. 2026. HHCS: A Dataset of Cipher Symbol Annotations From Handwritten Historical Encrypted Documents for Machine Learning Tasks. In *IEEE Access*, vol. 14, pages 9226–9240, DOI: 10.1109/ACCESS.2026.3654267.

CrypTool Contributors. 2026. *CrypTool Portal*. `https://www.cryptool.org/en/`

dCode Contributors. 2026. *dCode - The ultimate collection of tools for games, math, and puzzles*. `https://www.dcode.fr/en`

Fränz Friederes. 2026. *Cryptii*. `https://cryptii.com`

Martin Gillow. 2026. *Virtual Colossus*. `https://virtualcolossus.co.uk`

Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker and Michelle Waldispühl. 2020. Decryption of historical manuscripts: the DECRYPT project. *Cryptologia*, 44(6), pages 545–559. Taylor & Francis.

Paul Reuvers and Marc Simons. 2026. *Crypto Museum*. `https://www.cryptomuseum.com/`

Klaus Schmeh. 2022. *Cipherbrain*. `http://scienceblogs.de/klausis-krypto-kolumne`

Tobias Schrödel. 2021. Cryptographic postcards. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 131–136. Linköping University Electronic Press.

Satoshi Tomokiyo. 2026. *Cryptiana* `http://cryptiana.web.fc2.com/code/crypto.htm`

Frode Weierud. 2026. *Crypto Cellar Research* `http://cryptocellar.org/`