HCPortal - work in progress report 2022

Eugen Antal and Pavol Zajac

Slovak University of Technology in Bratislava, Slovakia

Introduction

The **Portal** of **H**istorical **C**iphers (HCPortal) is an online portal consisting of several web pages and tools. Some of them are logically divided into modules. Each module represents a specific topic related to historical cryptology.

This work was partially supported by grant VEGA 2/0072/20.

Parts of the portal

In the first years of development, a series of modules and web pages were released: *Home page* (entry point of the portal), *Database of cryptograms*, *ManuLab Qt and API* (software product for statistical analysis), *Tools and web pages* (links to external projects), *Glossary* (glossary for historical cryptology, including codes and nomenclator terminology).

The content of the portal was gradually expanded. The UI of the HCPortal was redesigned in 2022. When designing new components, we focused exclusively on online accessible applications. We are presenting three new modules focusing on teaching and promoting cryptology.

- **Education** - contains a demonstration of selected classical ciphers and their respective cryptanalytic techniques. Each technique is accompanied by a visualization.
- **Nomenclator**
  - **CipherCreator** - an online tool designed to create, use, and share nomenclator keys.
  - **Database of cipher keys** - an online database containing digitized nomenclator keys with a public API.
- **Virtual museum** - represents a virtual museum of historical ciphers, built on a virtual reality framework.

We also released the **ManuLab Online** application, which is the online version of the original **ManuLab Qt** application implemented in Angular.

Portal of Historical Ciphers

To browse the content of the portal, please visit: https://hcportal.eu/.

Education module

The *Education* module is a collection of interactive tools with graphical visualization of the data designed for a better understanding of attacks on selected classical ciphers.
At the moment, the *Education* module contains:

- Brute-force attack on *Caesar Cipher*
- Hill-Climbing attack on *Simple Substitution Cipher*
- Friedman test and brute-force attack on *Vigenère Cipher*

Each demonstrated attack is divided into logical steps. For visualization, we attach special *cards* to each of these steps.

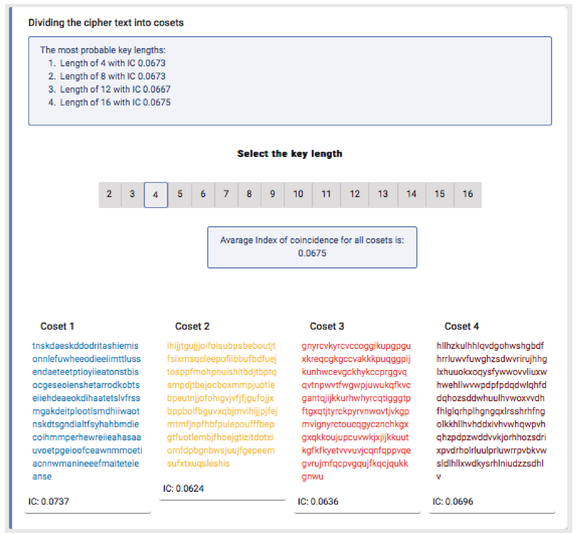

Figure 1:Education module - Vigenère cipher ciphertext divided to r cosets

Nomenclator module

The *Nomenclator* module is currently hosting two projects related to nomenclators. The first project, called *CipherCreator*, is a tool that allows the user to create custom nomenclator keys, while the second (unnamed) project focuses on the management of historical nomenclator keys.

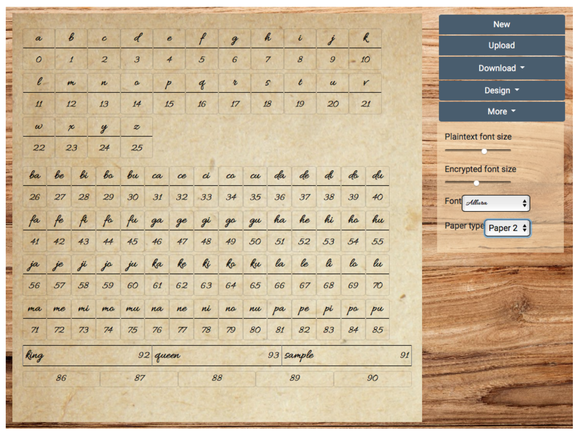

Figure 2:Nomenclator module - CipherCreator nomenclator key with font and paper settings

Virtual museum module

The *Virtual Museum* module is based on the virtual reality concept. In this way, we can present the materials collected in HCPortal in a familiar „museum" style. We use a virtual reality engine for web browsers. In this way, materials can be displayed online, even if the user does not have a VR device. The goal is to promote public interest in ciphers using modern technologies.

Figure 3:Virtual museum of historical ciphers

ManuLab Online

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

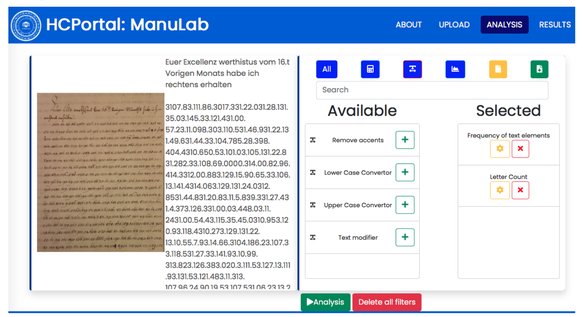

Figure 4:ManuLab Online

Technologies and access

The front-end of this portal was designed to provide a responsive and modern UI/UX. We used technologies as: Angular, TypeScript, A-Frame, MySQL, PHP, JavaScript, HTML, CSS.
We support free access to information. Our databases and tools are open-source and accessible without the need for registration. The major part of the portal's back-end is also available as a public API.