Status of CrypTool 2

Munich, October 31st 2019

Dr. Nils Kopal

CrypTool 2 Project

kopal@cryptool.org

CrypTool Meeting 20+ Years

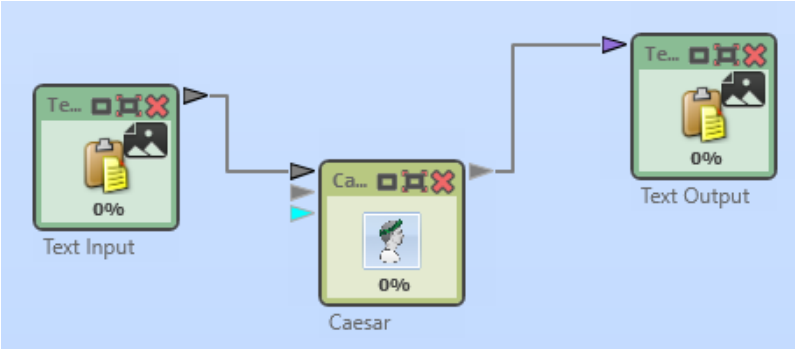
Content

1. What is CrypTool 2?
2. Highlights
3. Future Plans

1. What is CrypTool 2?

1. What is CrypTool 2

- **„Graphical programming language“**
  - over **170 components** for cryptography/cryptanalysis
  - over **220 templates** for cryptography/cryptanalysis



- **Classical and modern cryptography**
  - Caesar, substitution, transposition, ADFGVX, Enigma, M209, etc.
  - AES, RC2, RC4, DES, Diffie-Hellman, RSA, SHA-1, Keccak (SHA-3), etc.
- **Cryptanalysis of classical and modern ciphers/protocols**
  - Vigenère analyzer, keysearcher (brute-force attacks on symmetric modern ciphers), factorization, Enigma analysis, etc.

1. What is CrypTool 2

- **CT2 current version: 2.1**
  - next release in December (Christmas update)
- **Different types of builds**
  - Nightly builds every night ☺
  - Betas and releases 1-3 times a year
- **Two installation types**
  - Installation via executable (NSIS installer)
  - ZIP-installation via unpacking
- **Automatic updates**
  - Both installation types support auto-updates

1. What is CrypTool 2

- **Three Languages: English, German, and Russian**
  - Main application, components, help, templates, Wizard
  - Russian done by automatic translation ☺

- **.NET Version: 4.7.2**

Microsoft® .NET

- **We use Visual Studio 2019 (Community Edition)**

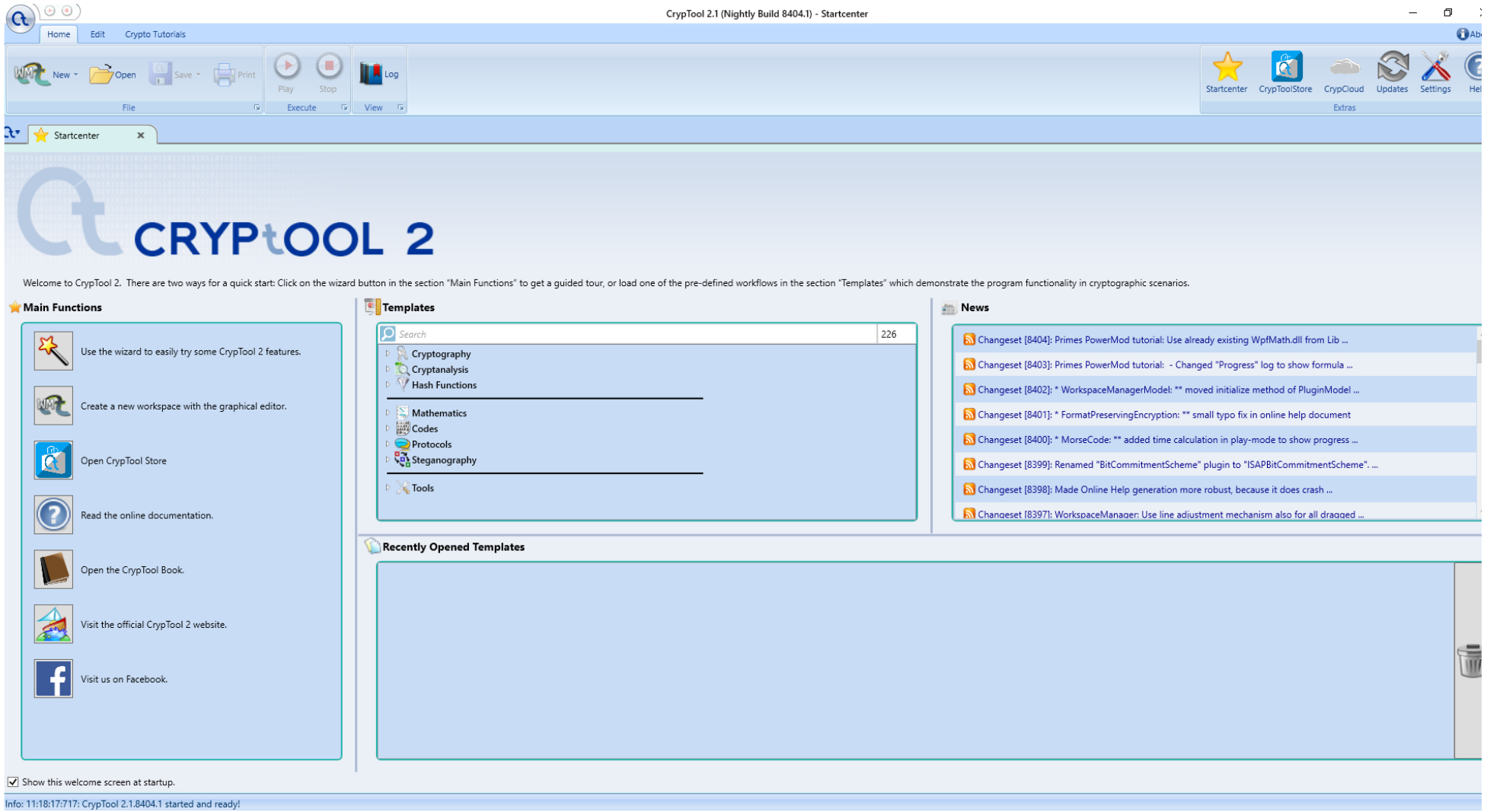
1. What is CrypTool 2

Some challenges we faced and solved in the last year(s)

- **Update of Visual Studio to new version (from 2010 to 2019)**
  - **Pro:** newest version ☺
  - **Contra:** update of build server takes a lot of time and is difficult
- **Change from x86 to x64 target**
  - **Pro:** more memory!! ☺
  - **Contra:** update all libraries and components to x64
- **Update of all C++ libs to newest Visual C++ redistributables**
  - **Pro:** no need for parallel installations of different redistributables
  - **Contra:** update of all libraries and components to the newest version

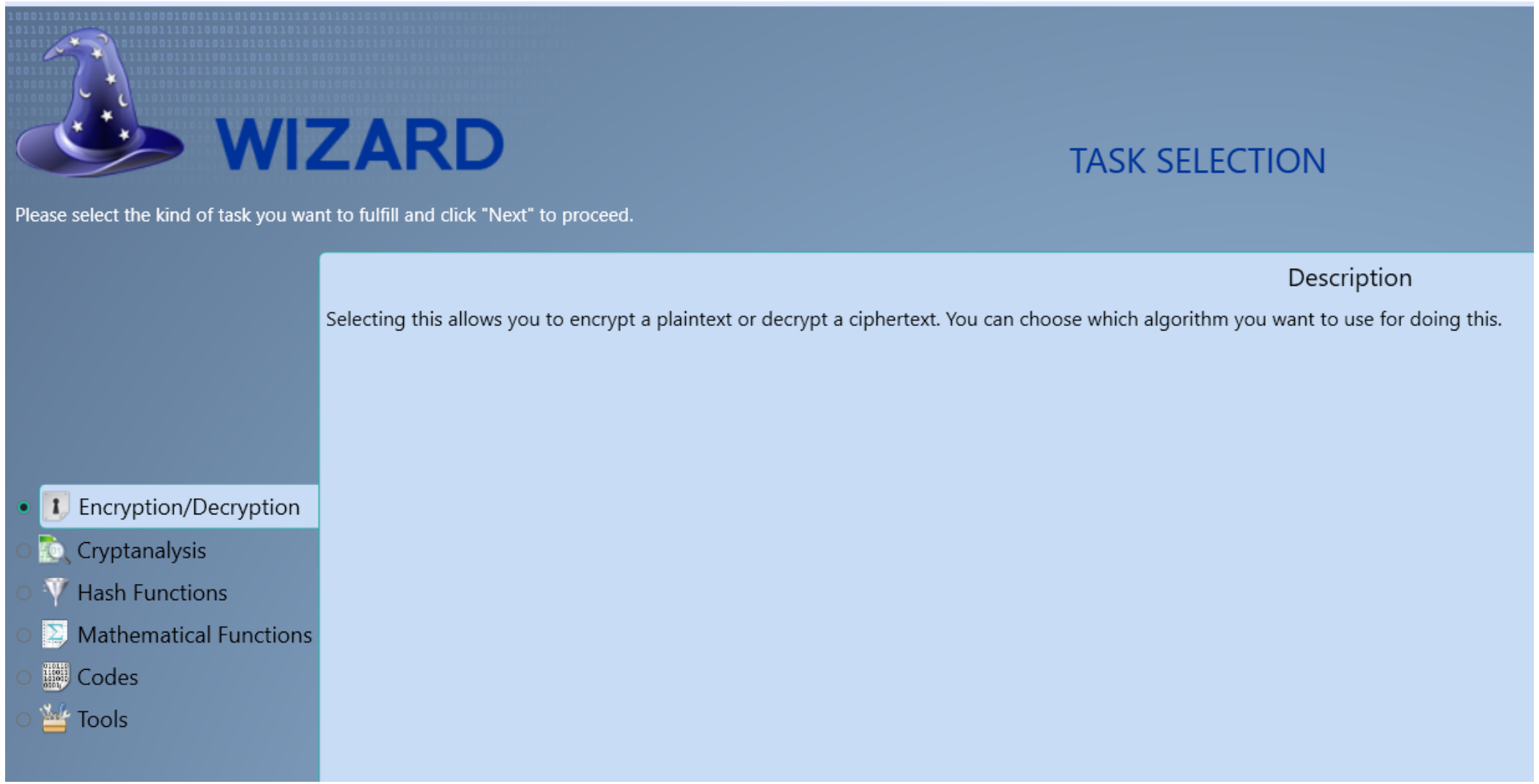
1. What is CrypTool 2

1. The Startcenter – the entrance into the application



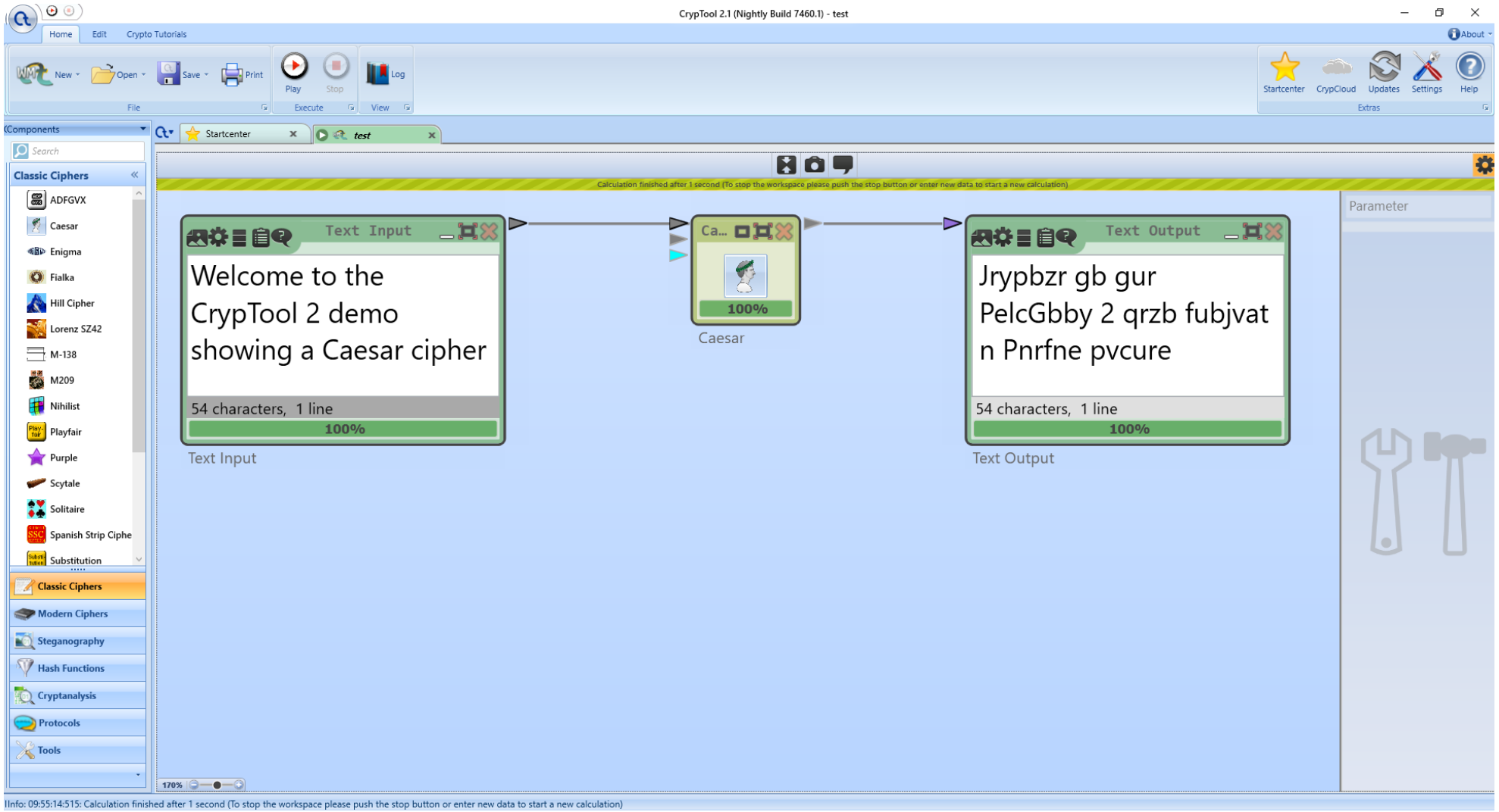
1. What is CrypTool 2

2. The Wizard – for beginners



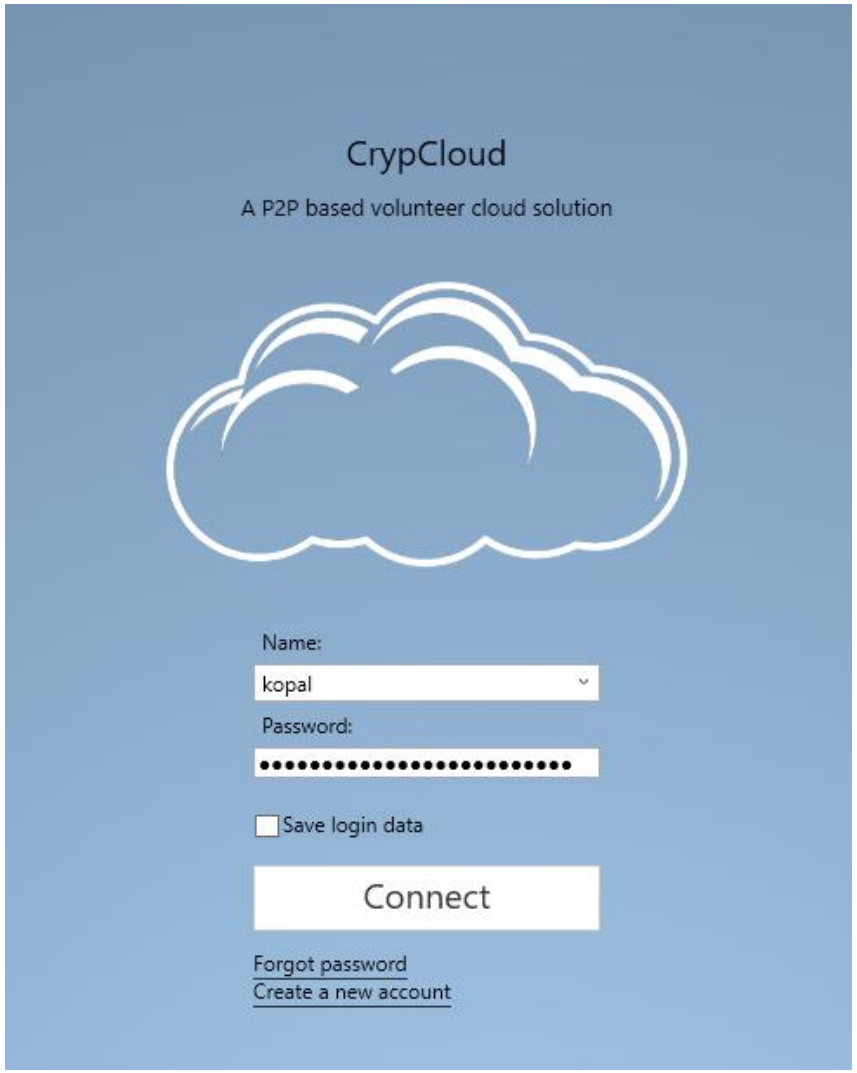
1. What is CrypTool 2

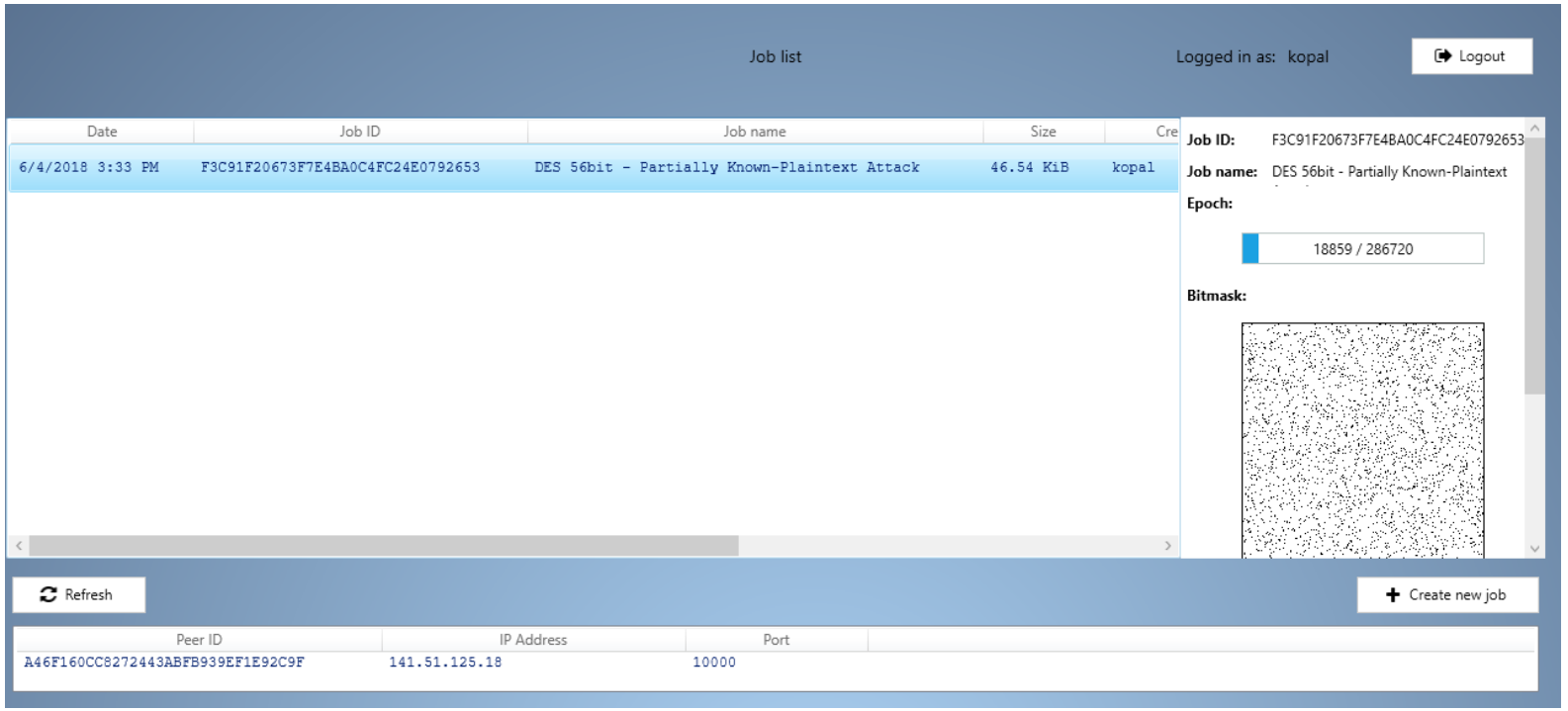
3. The Workspace Manager – implements the graphical programming language

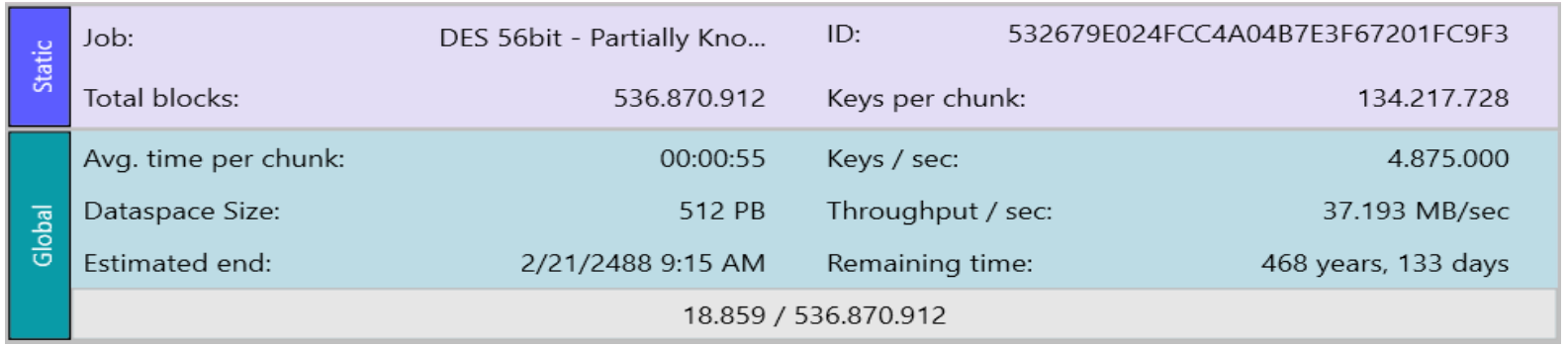


1. What is CrypTool 2

4. The CrypCloud – allows distributed cryptanalysis in the „cloud“







1. What is CrypTool 2

5. The CrypTool Store – allows to easily publish components

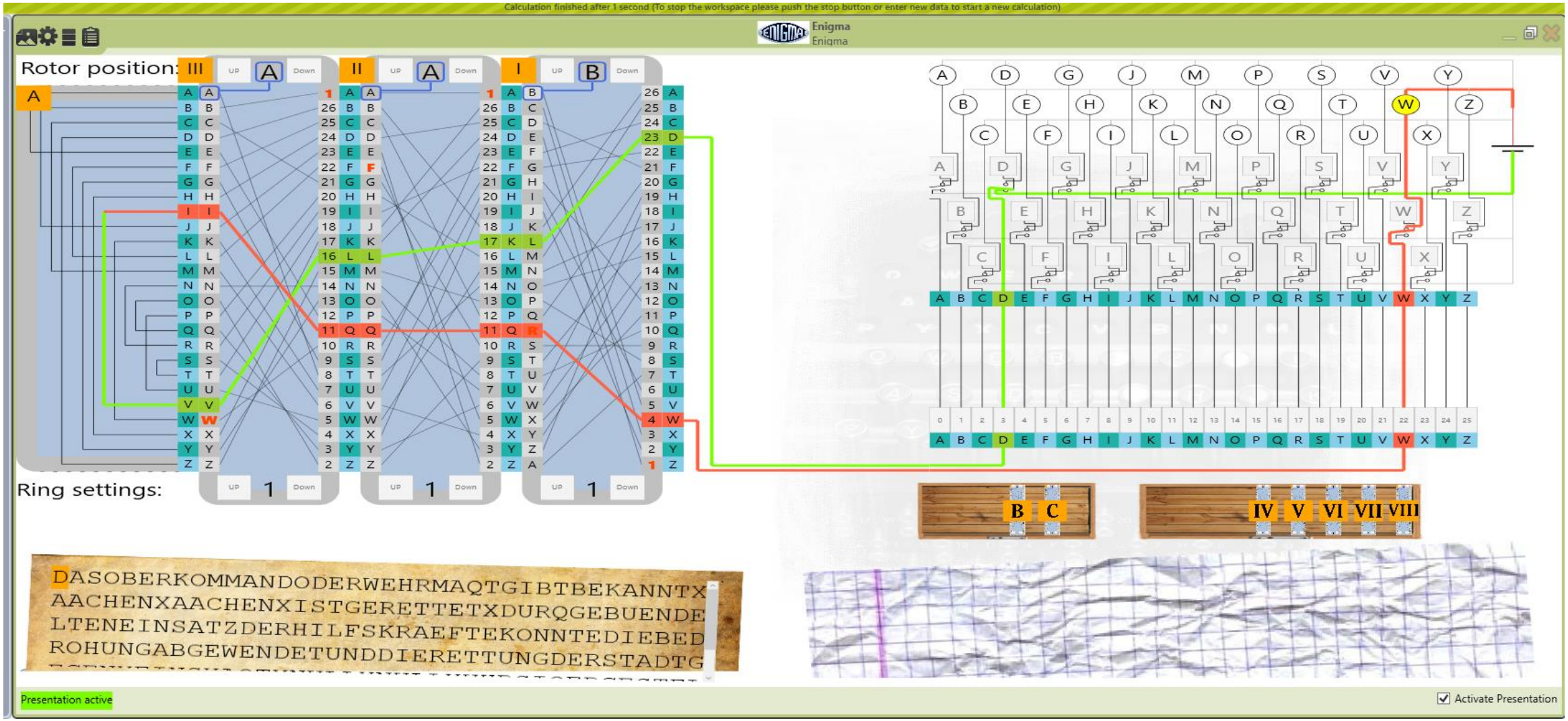
1. What is CrypTool 2

6. The Online Help – contains information about each component (en/de/ru)

2. Highlights

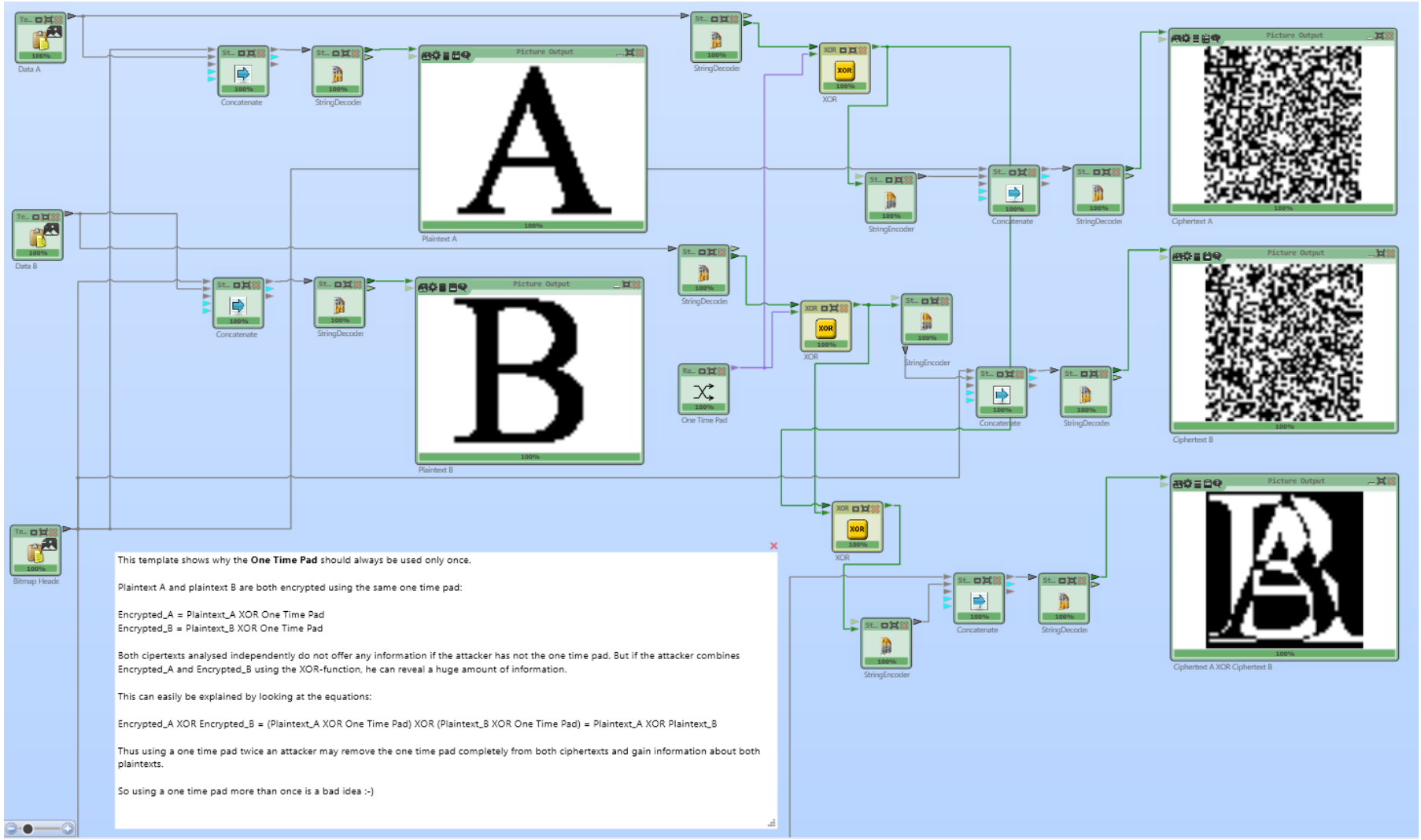
2. Highlights

1. Enigma visualization of internal workings



2. Highlights

2. One-time pad misusage (same key used twice)

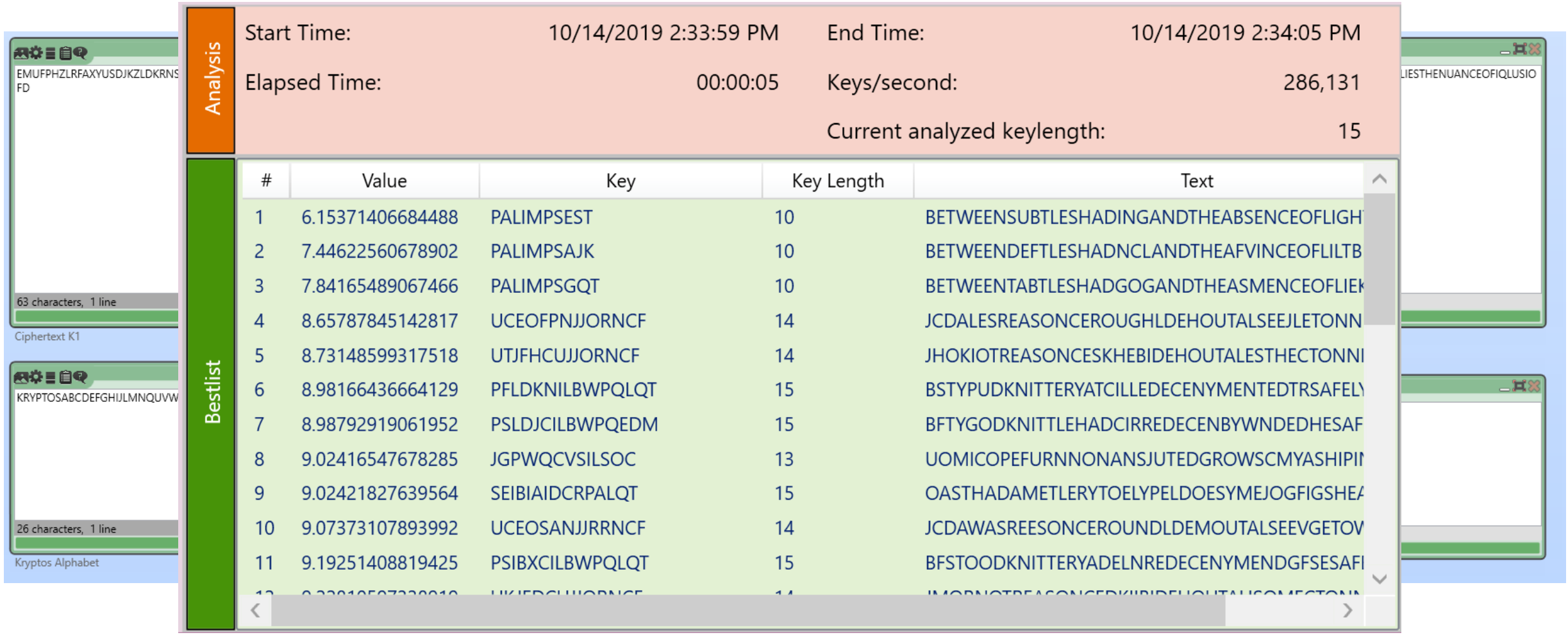


2. Highlights

3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2

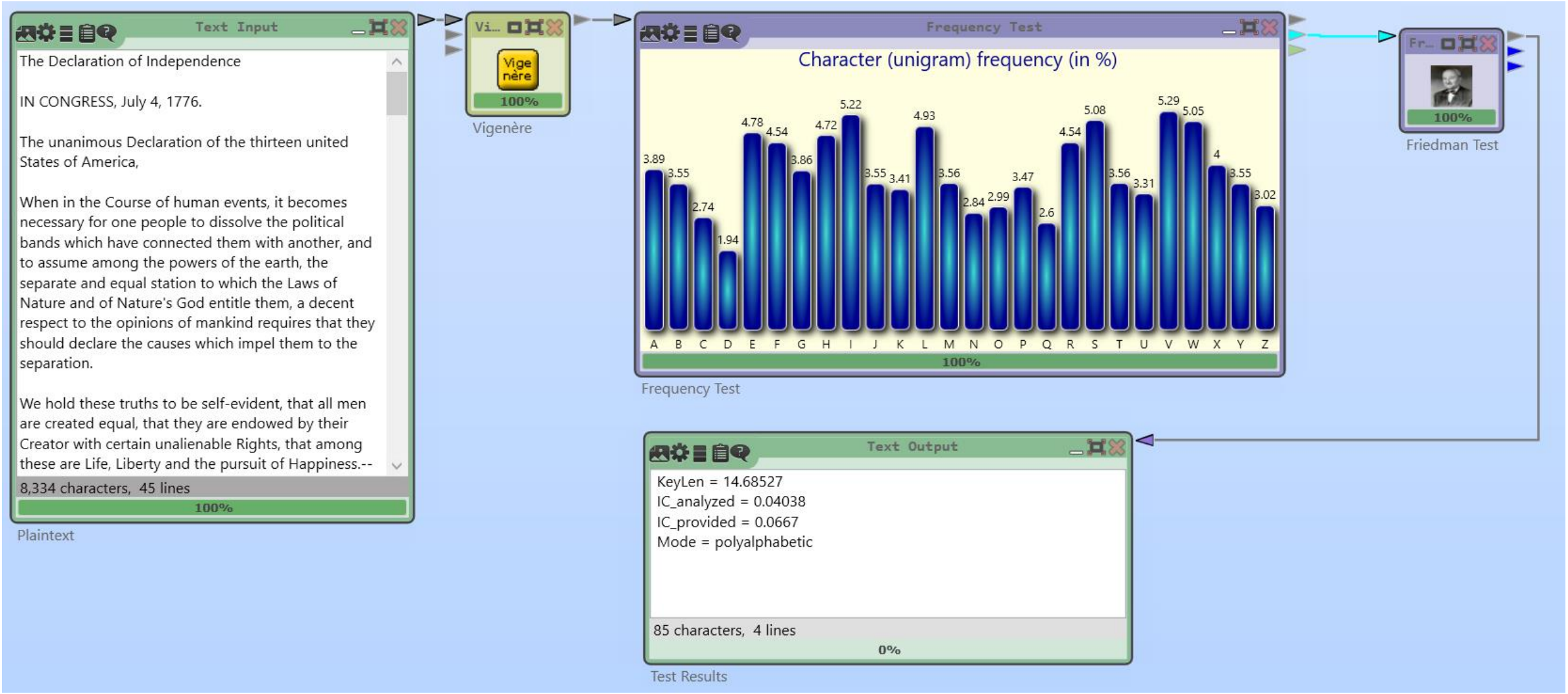
2. Highlights

3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2



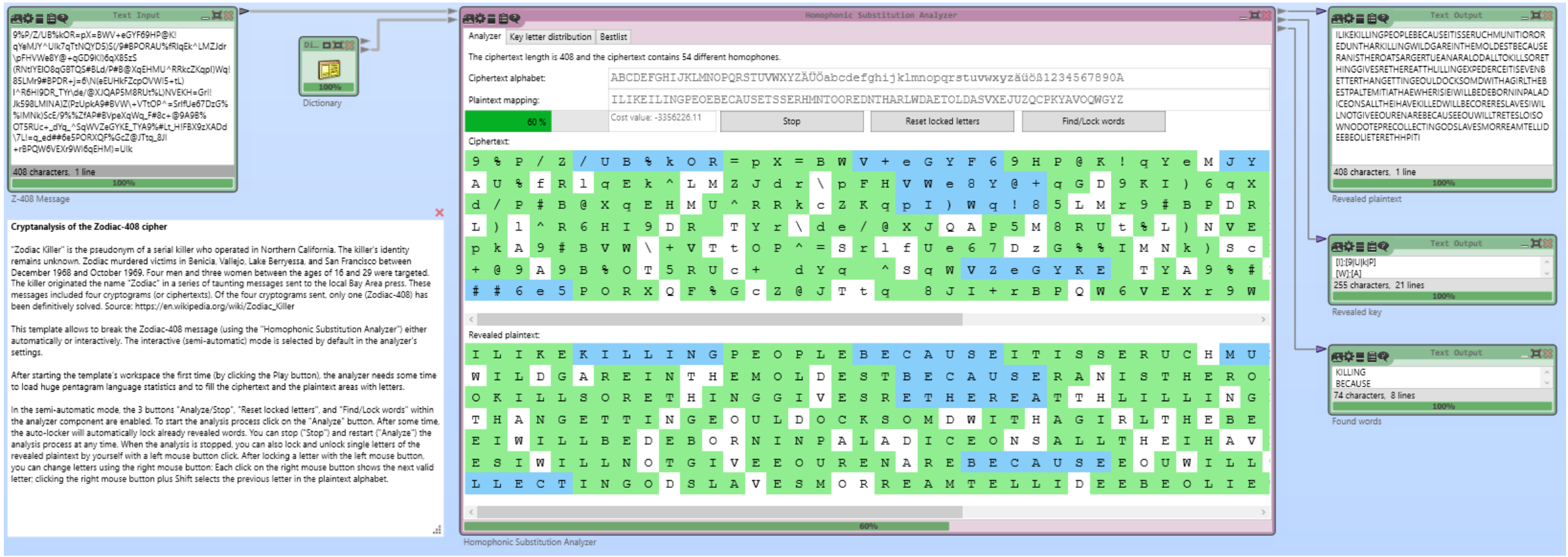
2. Highlights

4. Letter frequency analysis and Friedman test



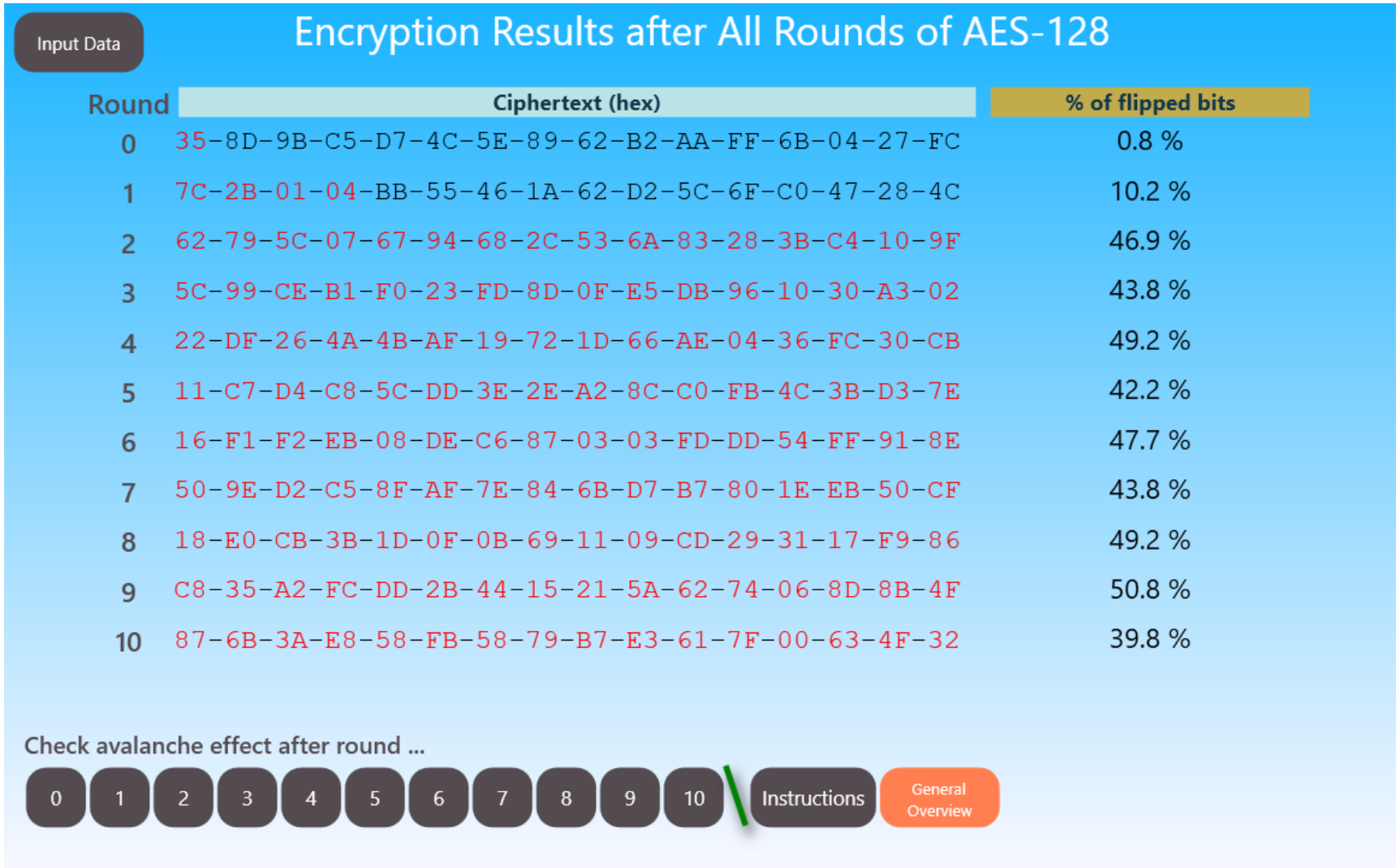
2. Highlights

5. Homophonic Substitution Analyzer – breaking of the Zodiac-408 letter



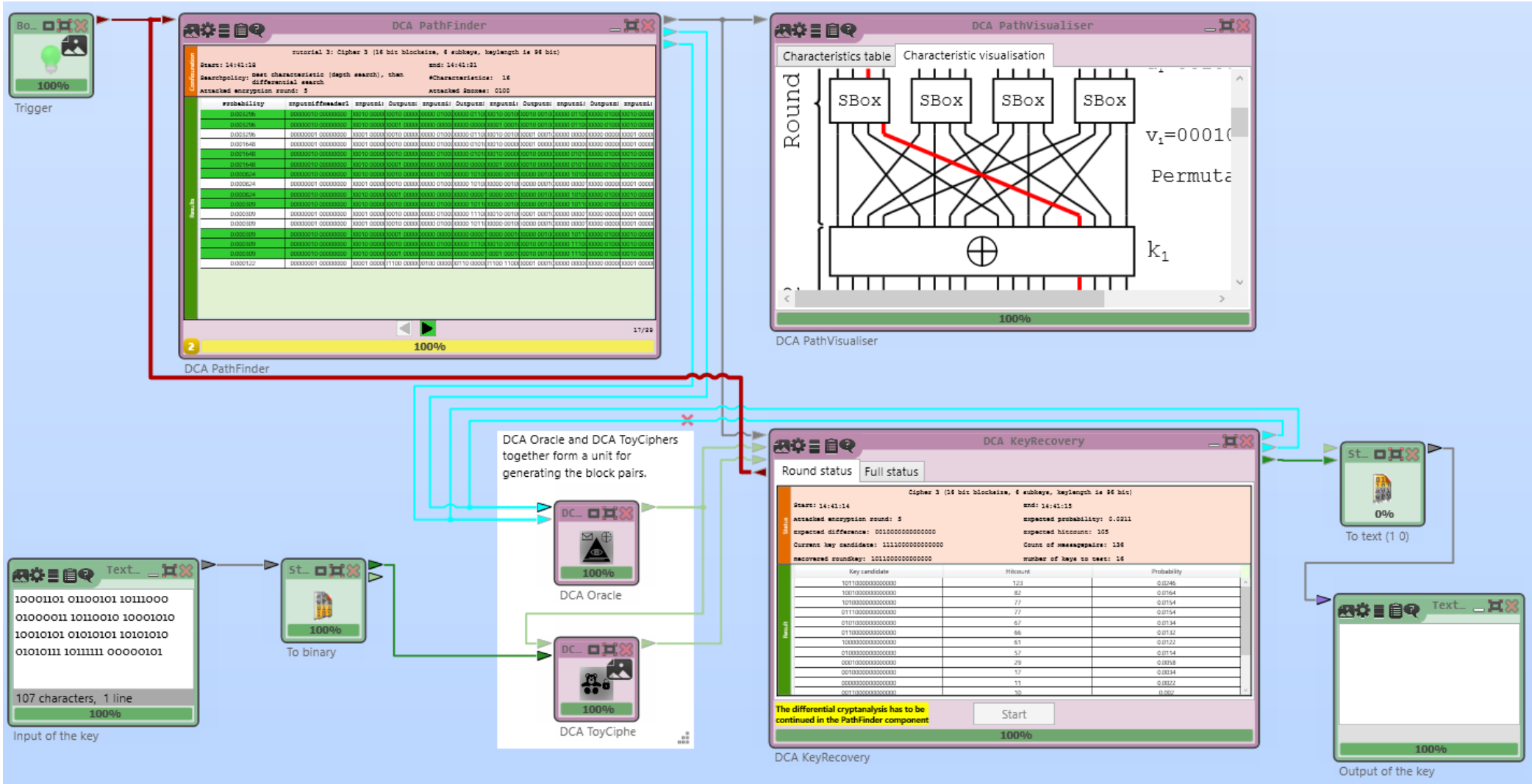
2. Highlights

6. Avalanche effect visualization (AES)



2. Highlights

7. Differential cryptanalysis

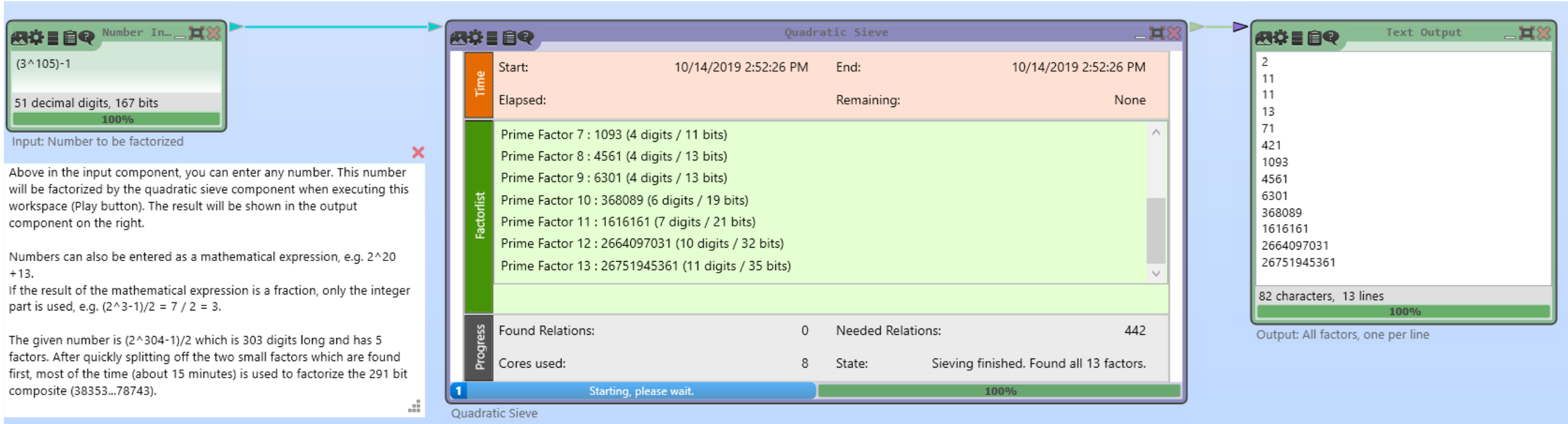


2. Highlights

8. Image hashing (robust hash functions)

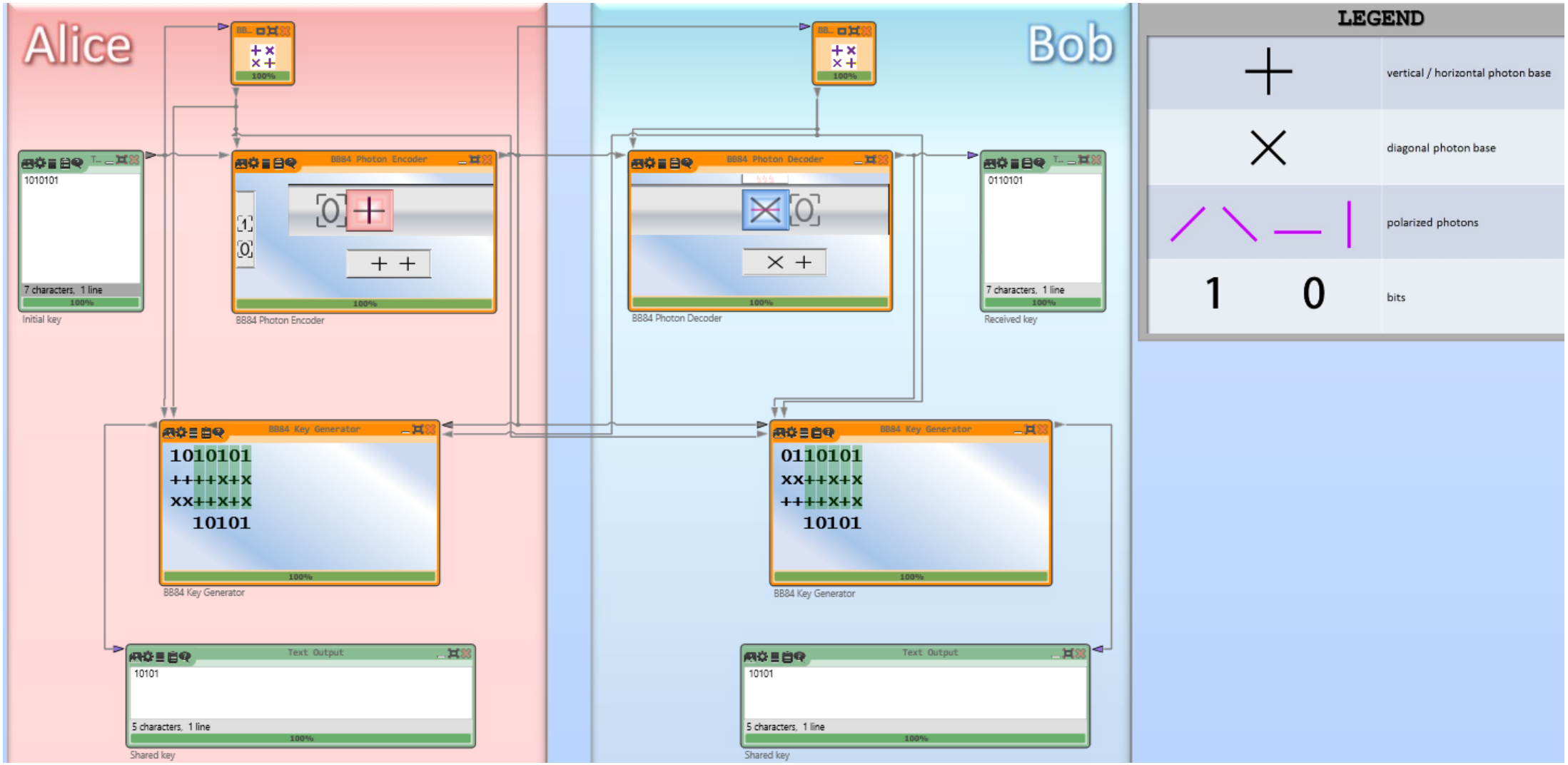
2. Highlights

9. Factorization of big numbers with the quadratic sieve



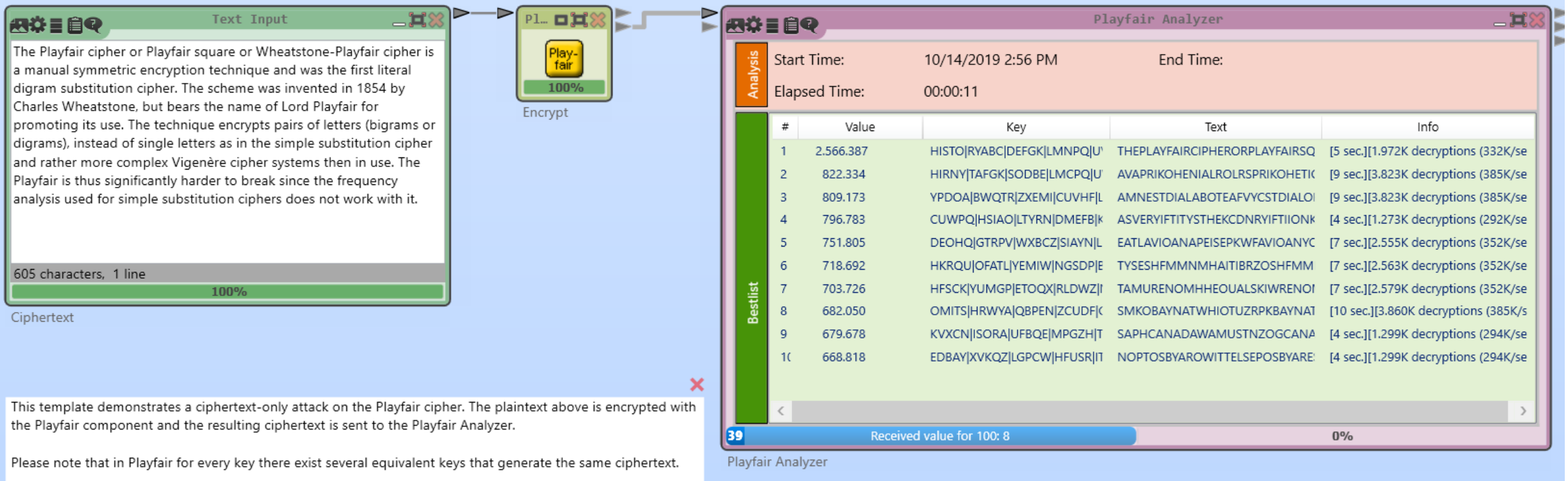
2. Highlights

10. Visualization of the BB84 quantum key exchange protocol



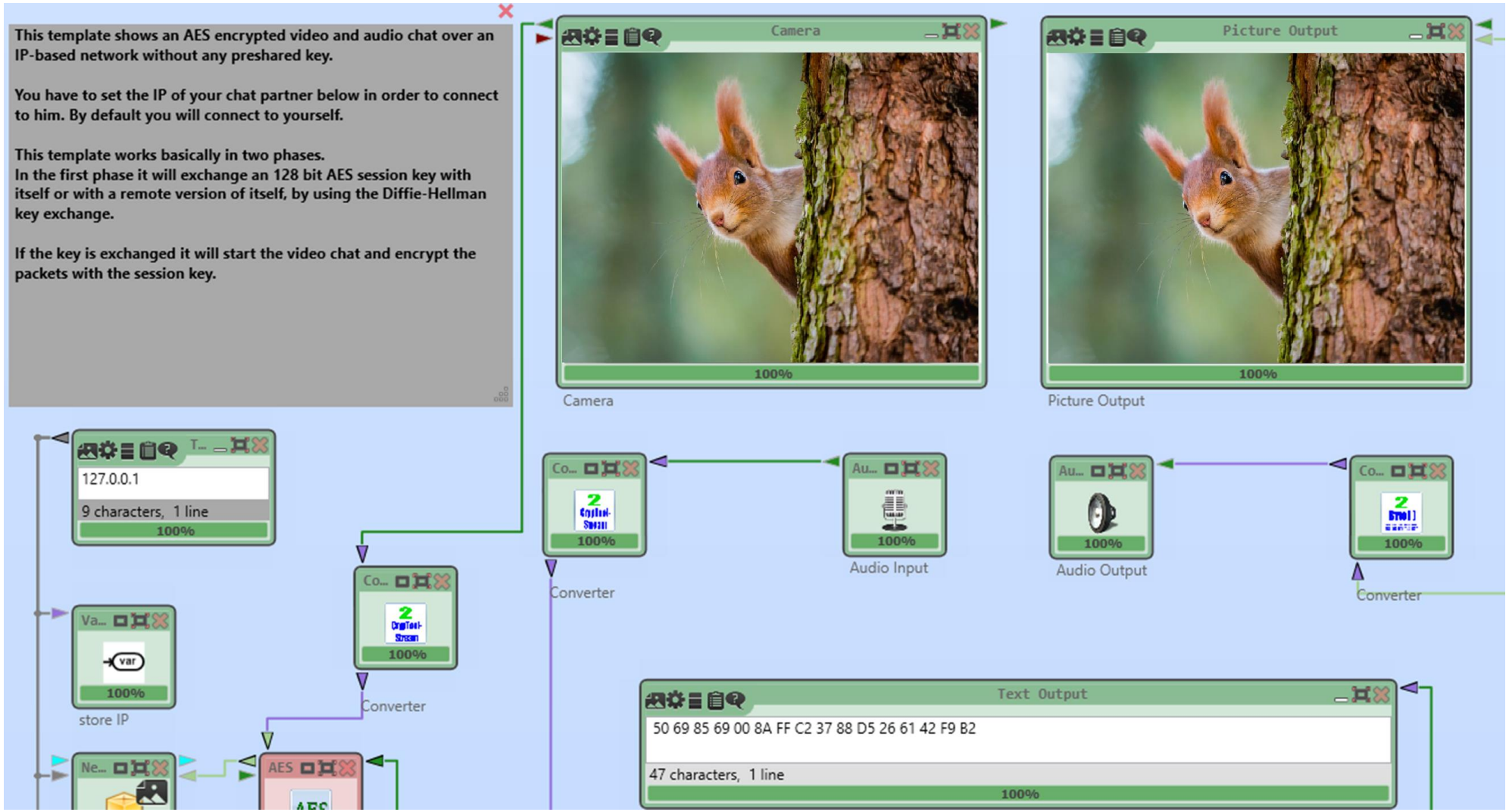
2. Highlights

11. Cryptanalysis of (short) Playfair ciphers (using an external cryptanalysis program written by Lasry)



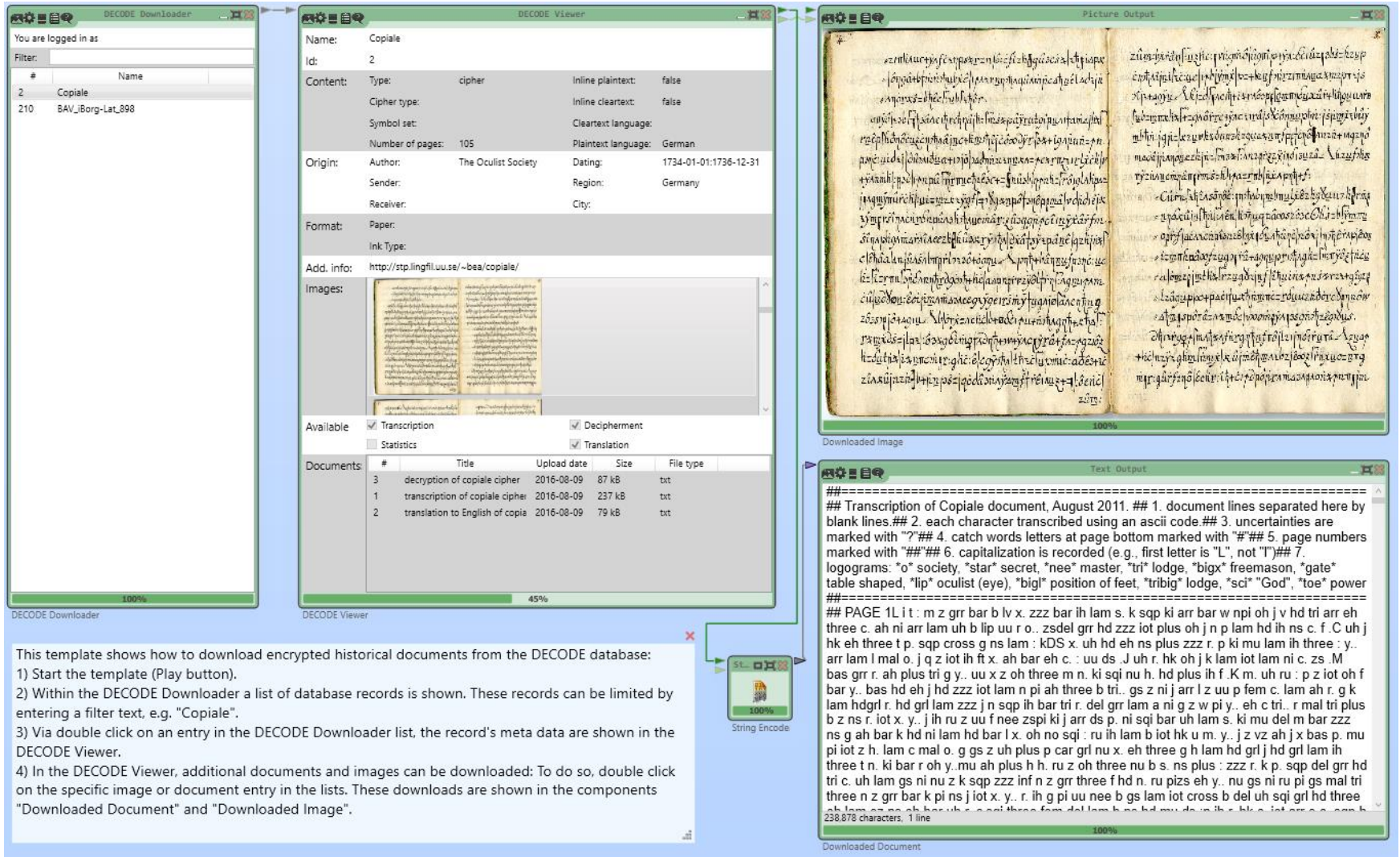
2. Highlights

12. AES-encrypted video chat (with Diffie-Hellman)



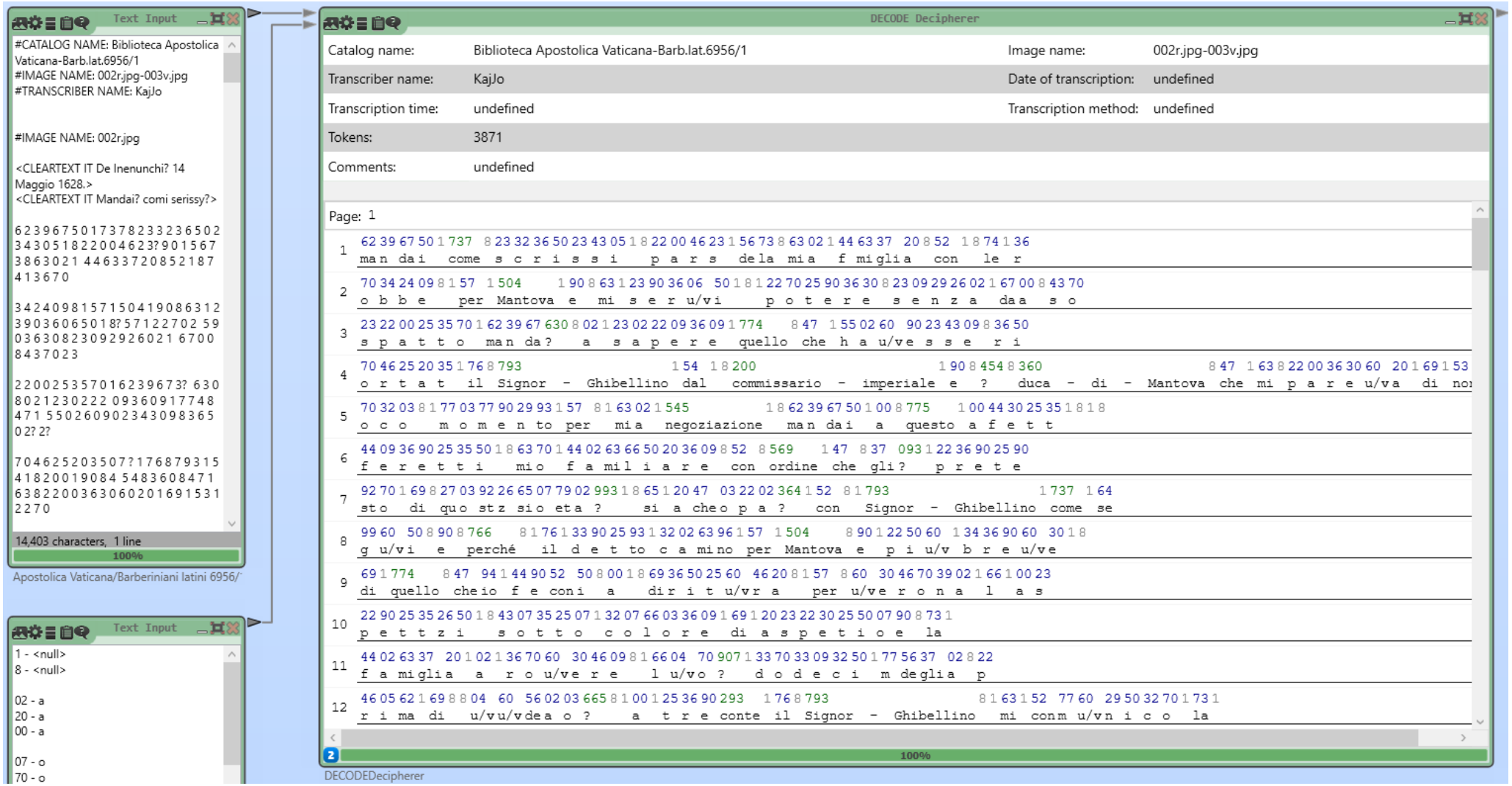
2. Highlights

13. Connection to the DECODE database for downloading original historic ciphers



2. Highlights

14. DECODE Decipherer in CT2 – decryption of historic ciphers



3. Future Plans

3. Future Plans

- **Make CT2 more attractive for users and developers**
  - **„Achievement system“ (inspired by computer games)**
- **Establish CT2 more in research and teaching**
- **Continue implementing current developments of cryptology**
  - Classic/historic cipher analysis: **DECRYPT project**
  - Modern cryptology/cryptanalysis, e.g. **post-quantum cryptography**
  - Cryptanalysis **framework of choice** (for symmetric ciphers)
- **Implement a rich set of YouTube videos for users/developers**
  - Create content for the CrypTool 2 **YouTube** channel
- **Wishes? What do you think/want?**

Questions and discussion

Thank you very much for your attention!

Do you have questions?