

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 CryptTool 2?

2. Highlights

3. Future Plans

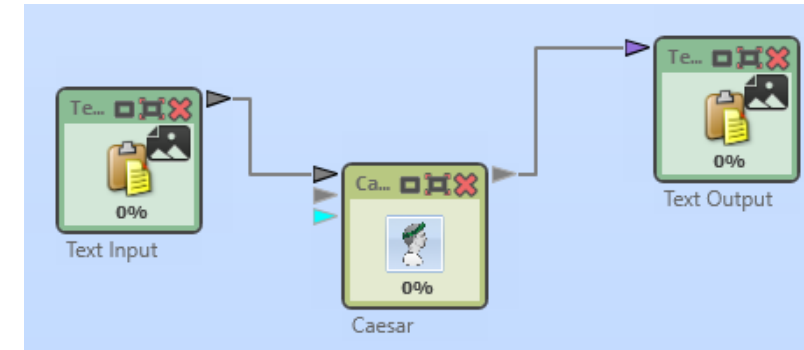




1. What is CryptTool 2?

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



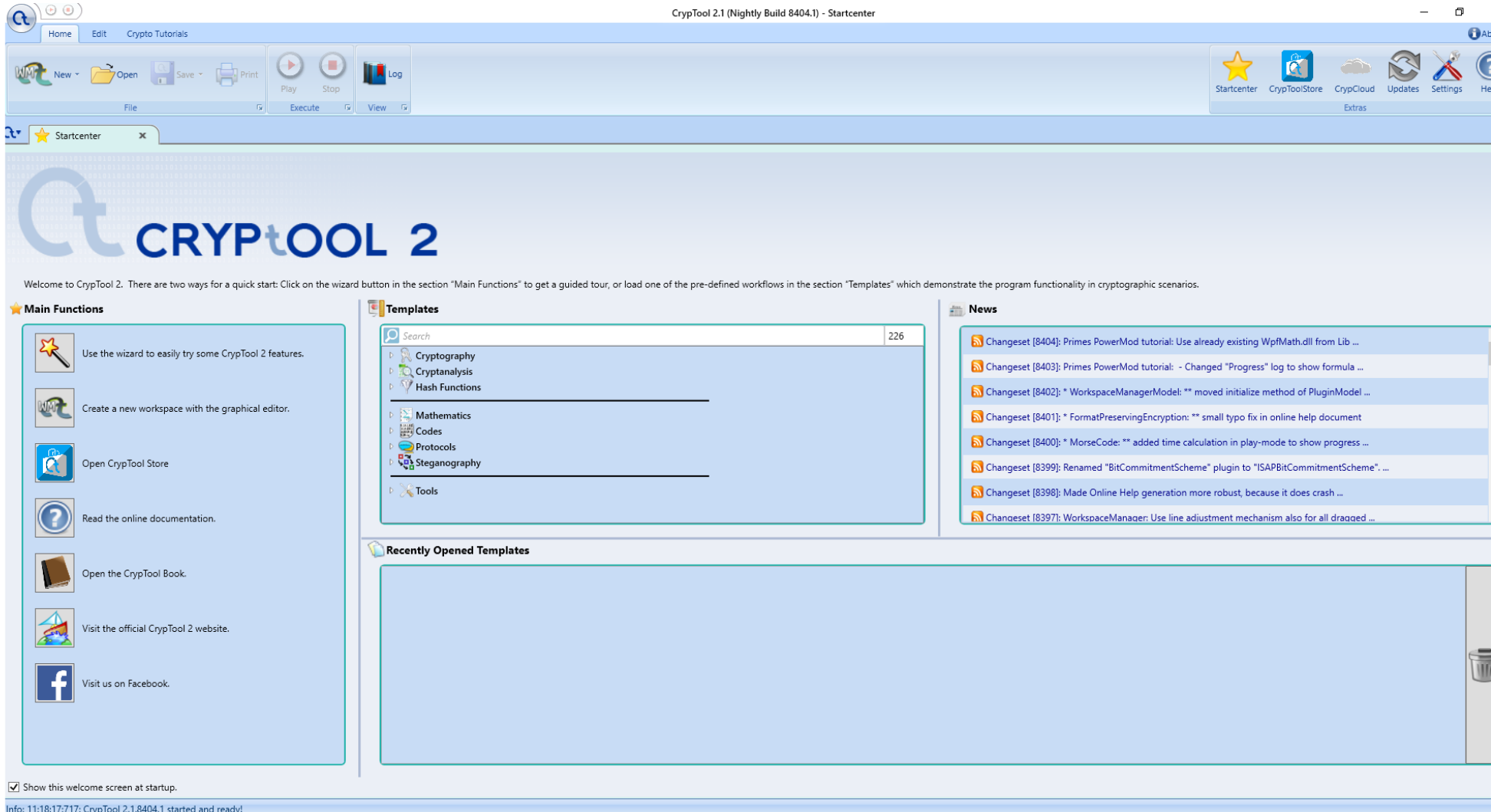
1. What is CrypTool 2

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

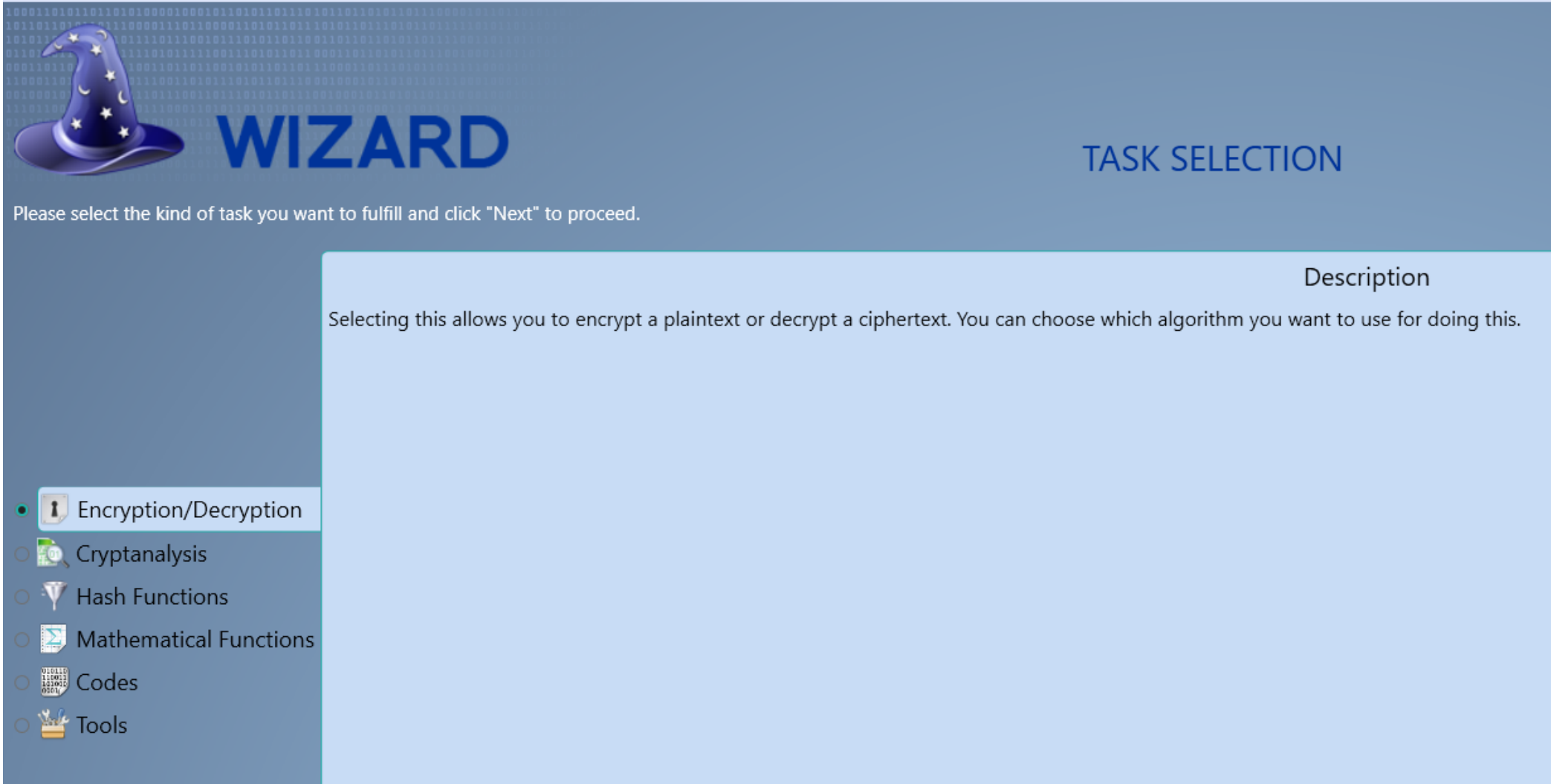
1. What is CryptTool 2

1. The Startcenter – the entrance into the application



1. What is CryptTool 2

2. The Wizard – for beginners



WIZARD

TASK SELECTION

Please select the kind of task you want to fulfill and click "Next" to proceed.

	Description
<input checked="" type="radio"/> Encryption/Decryption	Selecting this allows you to encrypt a plaintext or decrypt a ciphertext. You can choose which algorithm you want to use for doing this.
<input type="radio"/> Cryptanalysis	
<input type="radio"/> Hash Functions	
<input type="radio"/> Mathematical Functions	
<input type="radio"/> Codes	
<input type="radio"/> Tools	

1. What is CryptTool 2

3. The Workspace Manager – implements the graphical programming language

The screenshot displays the CryptTool 2.1 (Nightly Build 7460.1) - test interface. The workspace contains three components connected in a sequence:


- Text Input:** A window titled "Text Input" containing the text "Welcome to the CryptTool 2 demo showing a Caesar cipher" and "54 characters, 1 line". It shows a 100% progress bar.
- Caesar:** A central processing component labeled "Caesar" with a 100% progress bar.
- Text Output:** A window titled "Text Output" containing the encrypted text "Jrypbzr gb gur PelcGbbby 2 qrz b fubjvat n Pnrfne pvcure" and "54 characters, 1 line". It shows a 100% progress bar.

The interface includes a menu bar (Home, Edit, Crypto Tutorials), a toolbar with icons for New, Open, Save, Print, Play, Stop, and Log, and a sidebar with a search function and a list of cipher categories: Classic Ciphers, Modern Ciphers, Steganography, Hash Functions, Cryptanalysis, Protocols, and Tools. A status bar at the bottom indicates "Info: 09:55:14:515: Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)".

1. What is CrypTool 2

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

CrypCloud
A P2P based volunteer cloud solution



Name:

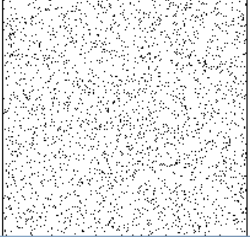
Password:

Save login data

[Forgot password](#)
[Create a new account](#)

Job list Logged in as: kopal

Date	Job ID	Job name	Size	Cre
6/4/2018 3:33 PM	F3C91F20673F7E4BA0C4FC24E0792653	DES 56bit - Partially Known-Plaintext Attack	46.54 KiB	kopal

Job ID: F3C91F20673F7E4BA0C4FC24E0792653
Job name: DES 56bit - Partially Known-Plaintext
Epoch:
Bitmask: 

Peer ID	IP Address	Port
A46F160CC8272443ABFB939EF1E92C9F	141.51.125.18	10000

Static	Job:	DES 56bit - Partially Kno...	ID:	532679E024FCC4A04B7E3F67201FC9F3
	Total blocks:	536.870.912	Keys per chunk:	134.217.728
Global	Avg. time per chunk:	00:00:55	Keys / sec:	4.875.000
	Dataspace Size:	512 PB	Throughput / sec:	37.193 MB/sec
	Estimated end:	2/21/2488 9:15 AM	Remaining time:	468 years, 133 days
18.859 / 536.870.912				

1. What is CrypTool 2

5. The CrypTool Store – allows to easily publish components

The screenshot displays the CrypTool Store interface. At the top left is the CrypTool logo, a blue square with a white 'Ct' and a padlock. To its right is the text 'CRYPTTOOL STORE'. Below the logo, it says 'Welcome to the CrypTool Store!' and has a search bar. A checkbox labeled 'Show resources' is checked. On the left side, there are three component cards: 'Crypto Number Table', 'English hexagram statistics', and 'Differential Cryptanalysis - ToyCiphers'. The 'Crypto Number Table' card is highlighted with a larger view on the right. This view shows the component's title, a description, authors (Nils Kopal), email (kopal@cryptool.org), institute (CrypTool 2 Team), version (1.8), and file size (25.18 KB). It also includes a detailed description of the cipher, a source link, and three buttons: 'Install', 'Update', and 'Uninstall'.

Welcome to the CrypTool Store!

Search:

Show resources

Crypto Number Table
The crypto number table is a simple, yet far from trivial cipher. This component is an implementation of the cipher.

English hexagram statistics
George Lasry's English hexagram statistic file

Differential Cryptanalysis - ToyCiphers
n/a

Crypto Number Table
The crypto number table is a simple, yet far from trivial cipher. This component is an implementation of the cipher.

Authors: Nils Kopal
Authors' Email(s): kopal@cryptool.org
Author's Institute(s): CrypTool 2 Team
Version: 1.8
File size: 25.18 KB

Designing a purely manual cipher (i.e., one that can be computed by hand) has proven a difficult problem. Most designs are either too complicated for practical use or insecure (some are even both). Almost all manual ciphers that were developed in the pre-computer era can be broken today with a computer. Although manual encryption algorithms have lost importance with the advent of cheap computers, they are still an active field of research.

On the website of crypto collector Nick Gessler, who is a professor emeritus at Duke University, Klaus Schmech found a very simple manual cipher that looks quite interesting. It is referred to as crypto number table.

The cipher consists of a secret table. The table contains 100 entries, each one consisting of a letter, a digit, a letter pair (bigram) or a letter triple (trigram). The bigrams and trigrams represent the most frequent ones in the English language. For encryption, each entry is encoded by its line and column number.

Source: Schmech, <http://scienceblogs.de/klausis-krypto-kolumne/2018/09/01/can-you-break-the-crypto-number-table-challenge/>

Install Update Uninstall

1. What is CrypTool 2

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



Available languages: English | Русский | Deutsch

CrypTool 2 – Online Documentation

[Components](#) [Templates](#) [Editors](#) [Common](#)

Here, you can find a description of all components delivered with CrypTool 2.

[Order by alphabet](#) [Order by categories](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

Filter: (188 matches)

A

Achterbahn	Achterbahn is a stream cipher and was a phase 2 candidate in the eSTREAM Project
ADFGVX	Cipher used in WW1, combining substitution and transposition
ADFGVX Analyzer	This component analyzes the transposition key of the ADFGVX cipher
AES	Advanced Encryption Standard (Rijndael)
AES Visualization	Visualization of AES encryption
Alphabet Permutator	Permutes an alphabet using a password
Alphabets	Alphabets Plugin
Array Indexer	Content of the chosen index of the array



2. Highlights

2. Highlights

1. Enigma visualization of internal workings

Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)

Enigma Enigma

Rotor position: III UP A Down, II UP A Down, I UP B Down

Ring settings: UP 1 Down, UP 1 Down, UP 1 Down

26 A A 26 A B 26 A
25 B B 25 B C 25 B
24 C C 24 C D 24 C
23 D D 23 D E 23 D
22 E E 22 E F 22 E
21 G G 21 G H 21 G
20 H H 20 H I 20 H
19 I I 19 I J 19 I
18 J J 18 J K 18 J
17 K K 17 K L 17 K
16 L L 16 L M 16 L
15 M M 15 M N 15 M
14 N N 14 N O 14 N
13 O O 13 O P 13 O
12 P P 12 P Q 12 P
11 Q Q 11 Q R 11 Q
10 R R 10 R S 10 R
9 S S 9 S T 9 S
8 T T 8 T U 8 T
7 U U 7 U V 7 U
6 V V 6 V W 6 V
5 W W 5 W X 5 W
4 X X 4 X Y 4 X
3 Y Y 3 Y Z 3 Y
2 Z Z 2 Z A 2 Z
1 Z

Ring settings: UP 1 Down, UP 1 Down, UP 1 Down

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

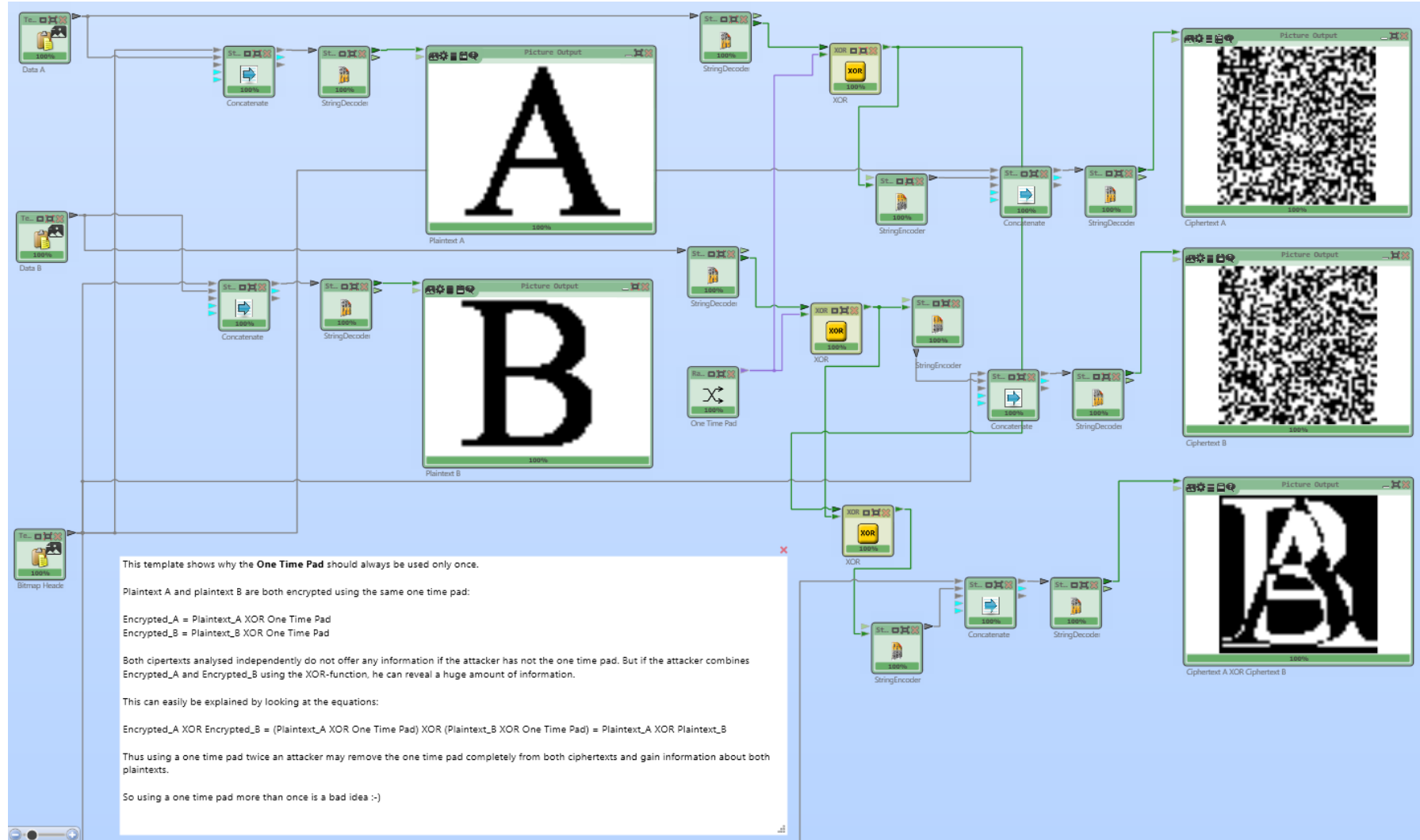
Wiring diagram showing connections between rotors and rings. The rotor III is set to A, rotor II to A, and rotor I to B. The ring settings are all set to 1. The diagram shows the electrical path from the keyboard (A-Z) through the rotors and rings to the lampboard (A-Z). The lampboard shows the output letters: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z. The rotor III is set to A, rotor II to A, and rotor I to B. The ring settings are all set to 1. The diagram shows the electrical path from the keyboard (A-Z) through the rotors and rings to the lampboard (A-Z). The lampboard shows the output letters: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z.

DASOBERKOMMANDODERWEHRMAQTGIBTBKANNTX
AACHENXAACHENXISTGERETTETXDURQGEBUENDE
LTENEINSATZDERHILFSKRAEFTEKONNTEDIEBED
ROHUNGABGEWENDETUNDDIERETTUNGDERSTADTG

Presentation active Activate Presentation

2. Highlights

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



2. Highlights

3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2

Text Input (Ciphertext K1)
EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJYQTQXQBQVYVLLTREVJYQTMKYRDMFD
63 characters, 1 line

Text Input (Kryptos Alphabet)
KRYPTOSABCDEFGHIJLMNQVWXZ
26 characters, 1 line

Vigenère Analyzer
Start Time: 10/14/2019 2:33:59 PM End Time: 10/14/2019 2:34:05 PM
Elapsed Time: 00:00:05 Keys/second: 286,131
Current analyzed keylength: 15

#	Value	Key	Key Length	Text
1	6.15371406684488	PALIMPSEST	10	BETWEENSUBTLESHADINGANDTHEABSENCEOFLIGH
1	7.44622560678902	PALIMPSEST	10	BETWEENDEFTLESHADINCLANDTHEAPVINCEOFLITB
1	7.84165489067466	PALIMPSEST	10	BETWEENTABTLESHADGOGANDTHEASMENCEOFLIEI
4	8.65787845142817	UCEOPFNJJORNCF	14	JCDALESREASONCEROUGHLEHOUTALSEEJLETONN
4	8.73148599317518	UTJFHCUJJORNCF	14	JHOKIOTREASONCESKHEIDEHOUTALESTHECTONN
6	8.98166436664129	PFLDKNILBWPQLQT	15	BSTYPUDKNITTERYATCILLEDECENYMENTEDTRSAFEL
6	8.98792919061952	PSLDJCLBWPQEDM	15	BFTYGODKNITTLEHADCIRREDECENBYWNDEDHESAF
7	9.02416547678285	JGPWQCVSILSOC	13	UOMICOPFURNNONANSJUTEDGROWSCMYASHIPII
7	9.02421827639564	SEIBIAIDCRPALQT	15	OASTHADAMETLERYTOELYPELDOESYMEJOGFISHEJ
5	9.07373107893992	UCEOSANJRRNCF	14	JCDAWASREESONCEROUNDLDEMOULTALSEEVGETOV
8	9.19251408819425	PSIBXCILBWPQLQT	15	BFSTOODKNITTERYADELNREDECENYMENTDGFSESAF

Text Output (Plaintext)
BETWEENSUBTLESHADINGANDTHEABSENCEOFLIGHTLIESTHENUANCEOFIQLUSION
63 characters, 1 line

Text Output (Key)
PALIMPSEST
10 characters, 1 line

Text:
Kryptos is an encrypted sculpture by American artist Jim Sanborn located on the grounds of the Central Intelligence Agency (CIA) in Langley, Virginia. Since its dedication on November 3, 1990, there has been much speculation about the meaning of the encrypted messages it bears. Of the four messages, three have been solved, with the fourth remaining one of the most famous unsolved codes in the world. The sculpture continues to provide a diversion for cryptanalysts, both amateur and professional, who are attempting to decrypt the final section.
Source: <http://en.wikipedia.org/wiki/Kryptos>
With this template we demonstrate the solution of Kryptos K1 - the first message of the Kryptos sculpture. The Vigenère Analyzer component takes the K1 ciphertext and the Kryptos alphabet (KRYPTOSABCDEFGHIJLMNQVWXZ). It performs a hillclimb-search for Vigenère keys between 5 and 20 using 100 restarts.

2. Highlights

3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2

The screenshot displays the Cryptool 2 interface for Vigenère cryptanalysis. On the left, there are two input windows: 'Ciphertext K1' containing 63 characters and 'Kryptos Alphabet' containing 26 characters. The main analysis window shows the following summary:

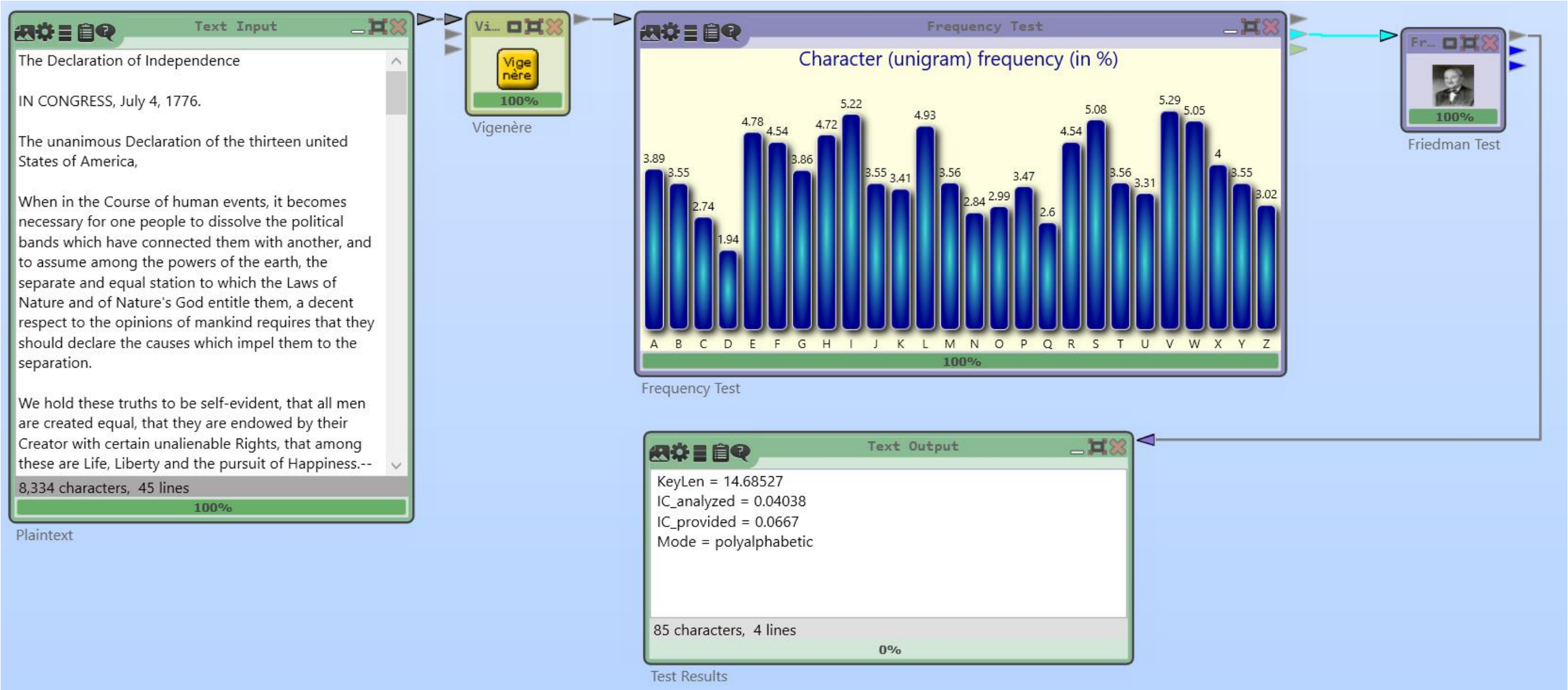
Analysis	Start Time:	10/14/2019 2:33:59 PM	End Time:	10/14/2019 2:34:05 PM
	Elapsed Time:	00:00:05	Keys/second:	286,131
			Current analyzed keylength:	15

Below the summary is a table of detected keys:

#	Value	Key	Key Length	Text
1	6.15371406684488	PALIMPSEST	10	BETWEENSUBTLESHADINGANDTHEABSENCEOFFLIGH
2	7.44622560678902	PALIMPSAJK	10	BETWEENDEFTLESHADNCLANDTHEAFVINCEOFFILTB
3	7.84165489067466	PALIMPSGQT	10	BETWEENABTLESHADGOGANDTHEASMENCEOFFLIEK
4	8.65787845142817	UCEOPNJJORNCF	14	JCDALESREASONCEROUGHLEHOUTALSEEJLETONN
5	8.73148599317518	UTJFHCUJJORNCF	14	JHOKIOTREASONCESKHEBIDEHOUTALESTHECTONNI
6	8.98166436664129	PFLDKNILBWPQLQT	15	BSTYPUDKNITTERYATCILLEDECENYMENTEDTRSAFELY
7	8.98792919061952	PSLDJCILBWPQEDM	15	BFTYGODKNITTLEHAD CIRREDECENBYWNDEDHESAF
8	9.02416547678285	JGPWQCVSILSOC	13	UOMICOPEFURNNONANSJUTEDGROWSCMYASHIPI
9	9.02421827639564	SEIBIAIDCRPALQT	15	OASTHADAMETLERYTOELYPELDOESYMEJOGFIGSHEA
10	9.07373107893992	UCEOSANJJRRNCF	14	JCDAWASREESONCEROUNDLDEMOUTALSEEVGETOV
11	9.19251408819425	PSIBXCILBWPQLQT	15	BFSTOODKNITTERYADELNREDECENYMENTDGFSESAFI
12	9.22210507322210	UKIEDCHUORNCF	14	UMORNOTREASONCERKIBIDELHUTALISOMECTONN

2. Highlights

4. Letter frequency analysis and Friedman test



2. Highlights

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

The screenshot displays the Homophonic Substitution Analyzer interface. On the left, a 'Text Input' window contains the Zodiac-408 message. Below it, a 'Cryptanalysis of the Zodiac-408 cipher' section provides background information: "Zodiac Killer" is the pseudonym of a serial killer who operated in Northern California, with victims in Benicia, Vallejo, Lake Berryessa, and San Francisco between December 1968 and October 1969. The killer originated the name "Zodiac" in a series of taunting messages. The Zodiac-408 message is the only one of four cryptograms sent that has been definitively solved. The interface also includes instructions on how to use the analyzer, such as clicking the 'Analyze/Stop' button to start the process and using mouse buttons to interact with the revealed plaintext.

The main 'Homophonic Substitution Analyzer' window shows the following details:

- Analyzer:** Key letter distribution, Bestlist
- Message Info:** The ciphertext length is 408 and the ciphertext contains 54 different homophones.
- Ciphertext alphabet:** ABCDEFGHIJKLMNOPQRSTUVWXYZÄÜöabcdfghijklmnopqrstuvwxyzäüö1234567890A
- Plaintext mapping:** ILIKEILINGPEOEBCAUSESSEHMHNTOOERDNTHARLWDAETOLDASVXEJUZQCPKYAVOQWGYZ
- Progress:** 60% (Cost value: -3356226.11)
- Buttons:** Stop, Reset locked letters, Find/Lock words

The 'Ciphertext' area shows a grid of characters with some highlighted in green. Below it, the 'Revealed plaintext' is shown in a grid, with some words highlighted in blue. On the right, three 'Text Output' windows show the results:

- Text Output 1:** Revealed plaintext: ILIKEKILLINGPEOPLEBECAUSEITISSERUCHMUNITIOROR EDUNTHARKILLINGWILDGAREINTHEMOLDDESTBECAUSE RANISTHEROATSARGTUEANARALODALLTOKILLSORET HINGGIVESRETHREATTHULLINGEXPEDERCEITISEVNB ETTERTHANGETTINGEULDOCKSOMDWITHAGIRLTHEB ESTPALTEMIATHAEWHERISEIWLBEDEBORNINPALAD ICEONSAALLTHEHAVEKILLEDWILLBECORERESLAVESWIL LNOTGIVEEURENAREBECAUSEEOWILLRETRESLOISO WNODOTEPRECOLLECTINGODSLAVESMORREAMELLID EEBEOLIERETHHPITI
- Text Output 2:** Revealed key: [I]:[9][U][K][P] [W]:[A]
- Text Output 3:** Found words: KILLING BECAUSE

2. Highlights

6. Avalanche effect visualization (AES)

Input Data

Encryption Results after All Rounds of AES-128

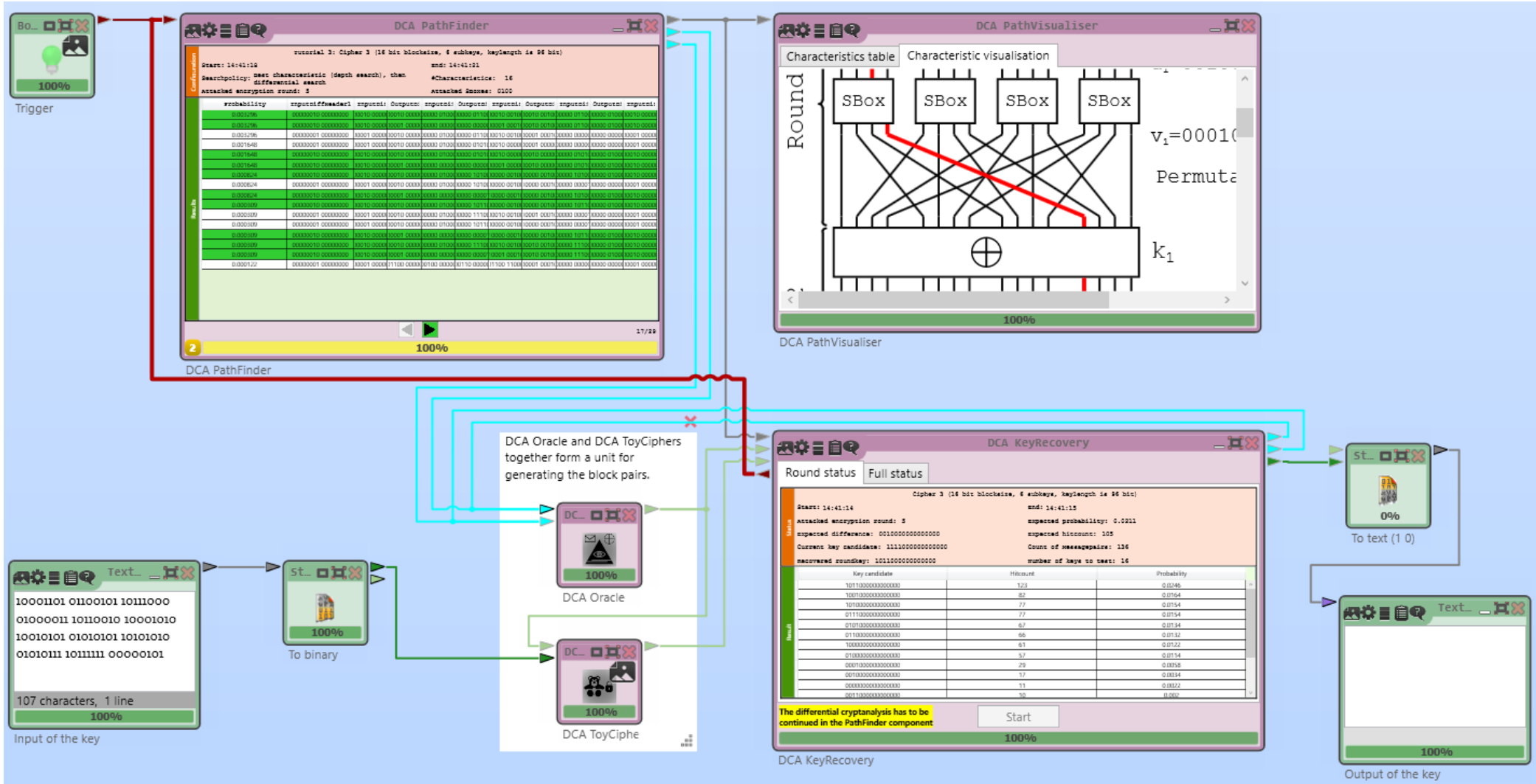
Round	Ciphertext (hex)	% of flipped bits
0	35-8D-9B-C5-D7-4C-5E-89-62-B2-AA-FF-6B-04-27-FC	0.8 %
1	7C-2B-01-04-BB-55-46-1A-62-D2-5C-6F-C0-47-28-4C	10.2 %
2	62-79-5C-07-67-94-68-2C-53-6A-83-28-3B-C4-10-9F	46.9 %
3	5C-99-CE-B1-F0-23-FD-8D-0F-E5-DB-96-10-30-A3-02	43.8 %
4	22-DF-26-4A-4B-AF-19-72-1D-66-AE-04-36-FC-30-CB	49.2 %
5	11-C7-D4-C8-5C-DD-3E-2E-A2-8C-C0-FB-4C-3B-D3-7E	42.2 %
6	16-F1-F2-EB-08-DE-C6-87-03-03-FD-DD-54-FF-91-8E	47.7 %
7	50-9E-D2-C5-8F-AF-7E-84-6B-D7-B7-80-1E-EB-50-CF	43.8 %
8	18-E0-CB-3B-1D-0F-0B-69-11-09-CD-29-31-17-F9-86	49.2 %
9	C8-35-A2-FC-DD-2B-44-15-21-5A-62-74-06-8D-8B-4F	50.8 %
10	87-6B-3A-E8-58-FB-58-79-B7-E3-61-7F-00-63-4F-32	39.8 %

Check avalanche effect after round ...

0 1 2 3 4 5 6 7 8 9 10 \ Instructions General Overview

2. Highlights

7. Differential cryptanalysis



2. Highlights

8. Image hashing (robust hash functions)



2. Highlights

9. Factorization of big numbers with the quadratic sieve

Number In...
(3¹⁰⁵)-1
51 decimal digits, 167 bits
100%

Input: Number to be factorized

Above in the input component, you can enter any number. This number will be factorized by the quadratic sieve component when executing this workspace (Play button). The result will be shown in the output component on the right.

Numbers can also be entered as a mathematical expression, e.g. 2²⁰ + 13.
If the result of the mathematical expression is a fraction, only the integer part is used, e.g. (2³-1)/2 = 7 / 2 = 3.

The given number is (2³⁰⁴-1)/2 which is 303 digits long and has 5 factors. After quickly splitting off the two small factors which are found first, most of the time (about 15 minutes) is used to factorize the 291 bit composite (38353...78743).

Quadratic Sieve

Quadratic Sieve

Time	Start:	10/14/2019 2:52:26 PM	End:	10/14/2019 2:52:26 PM
	Elapsed:		Remaining:	None
Factorlist	Prime Factor 7 :	1093 (4 digits / 11 bits)		
	Prime Factor 8 :	4561 (4 digits / 13 bits)		
	Prime Factor 9 :	6301 (4 digits / 13 bits)		
	Prime Factor 10 :	368089 (6 digits / 19 bits)		
	Prime Factor 11 :	1616161 (7 digits / 21 bits)		
	Prime Factor 12 :	2664097031 (10 digits / 32 bits)		
	Prime Factor 13 :	26751945361 (11 digits / 35 bits)		
Progress	Found Relations:	0	Needed Relations:	442
	Cores used:	8	State:	Sieving finished. Found all 13 factors.

1 Starting, please wait. 100%

Text Output

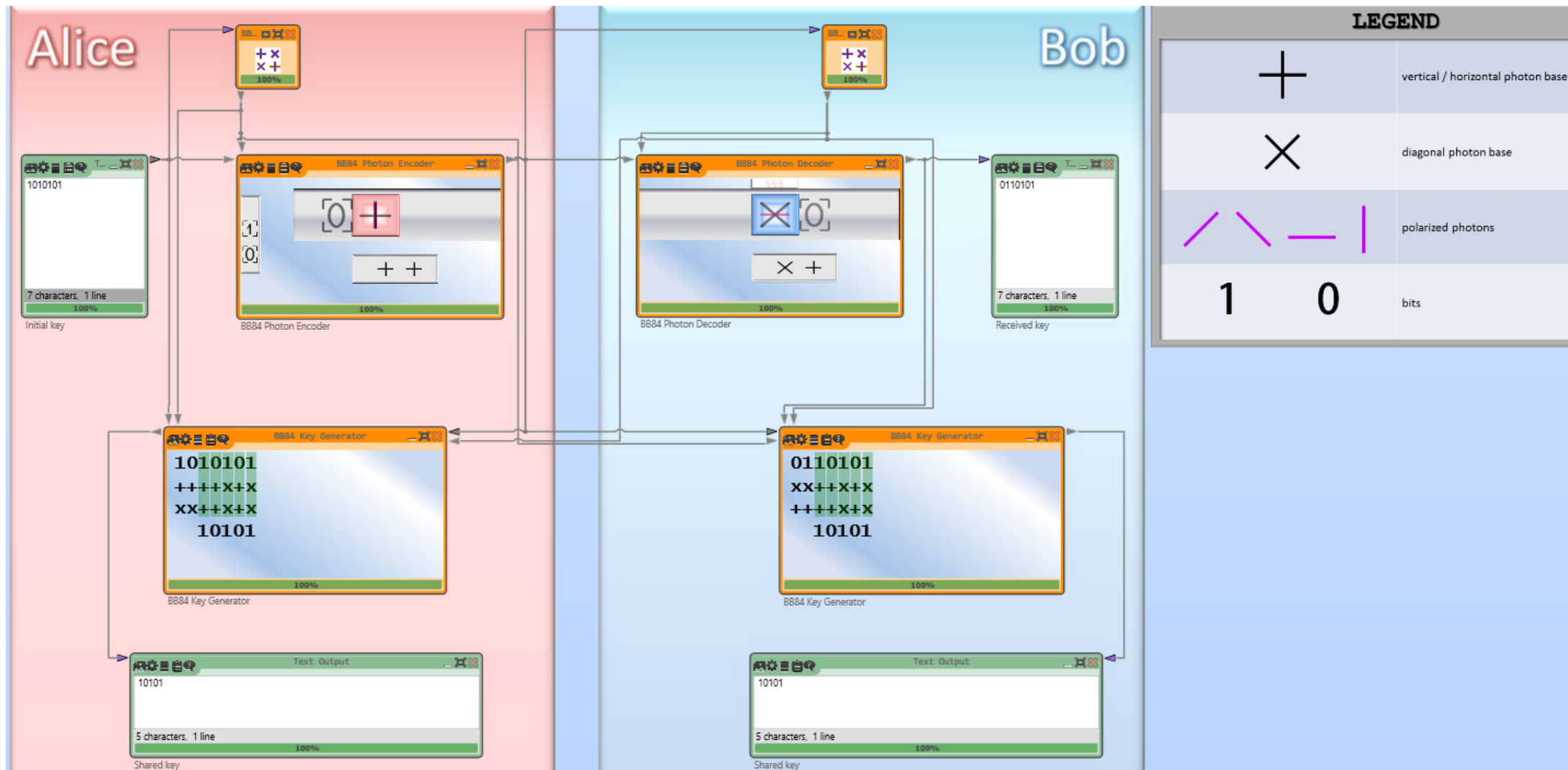
```
2
11
11
13
71
421
1093
4561
6301
368089
1616161
2664097031
26751945361
```

82 characters, 13 lines
100%

Output: All factors, one per line

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)

The Playfair cipher or Playfair square or Wheatstone-Playfair cipher is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use. The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it.

605 characters, 1 line
100%

Ciphertext

Playfair Analyzer

Analysis

Start Time: 10/14/2019 2:56 PM End Time:
Elapsed Time: 00:00:11

#	Value	Key	Text	Info
1	2.566.387	HISTO RYABC DEFGK LMNPQ U'	THEPLAYFAIRCIPHERORPLAYFAIRSQ	[5 sec.][1.972K decryptions (332K/se
2	822.334	HIRNY TAFGK SODBE LMCPQ U'	AVAPRIKOHENIALROLRSPRIKOHETIK	[9 sec.][3.823K decryptions (385K/se
3	809.173	YPDOA BWQTR ZXEMI CUVHF L	AMNESTDIALABOTEAFVYCSTDIALOI	[9 sec.][3.823K decryptions (385K/se
4	796.783	CUWQP HSIAO LTYRN DMEFB K	ASVERYIFTITYSTHEKCDNRYIFTIIONK	[4 sec.][1.273K decryptions (292K/se
5	751.805	DEOHQ GTRPV WBCZ SIAYN L	EATLAVIOANAPEISEPKWFAVIOANYC	[7 sec.][2.555K decryptions (352K/se
6	718.692	HKRQU OFATL YEMIW NGSDP E	TYSESHFMMNMHAITIBRZOSHFM	[7 sec.][2.563K decryptions (352K/se
7	703.726	HFSCK YUMGP ETOQX RLDWZ I	TAMURENOMHHEOUALSKIWRENOI	[7 sec.][2.579K decryptions (352K/se
8	682.050	OMITS HRWYA QBPEN ZCUDF K	SMKOBAYNATWHIOTUZRPKBAYNAT	[10 sec.][3.860K decryptions (385K/s
9	679.678	KVXCN ISORA UFBQE MPGZH T	SAPHCANADAWAMUSTNZOGCANA	[4 sec.][1.299K decryptions (294K/se
10	668.818	EDBAY XVKQZ LGPCW HFUSR IT	NOPTOSBYAROWITTELSEPOSBYARE	[4 sec.][1.299K decryptions (294K/se

39 Received value for 100: 8 0%

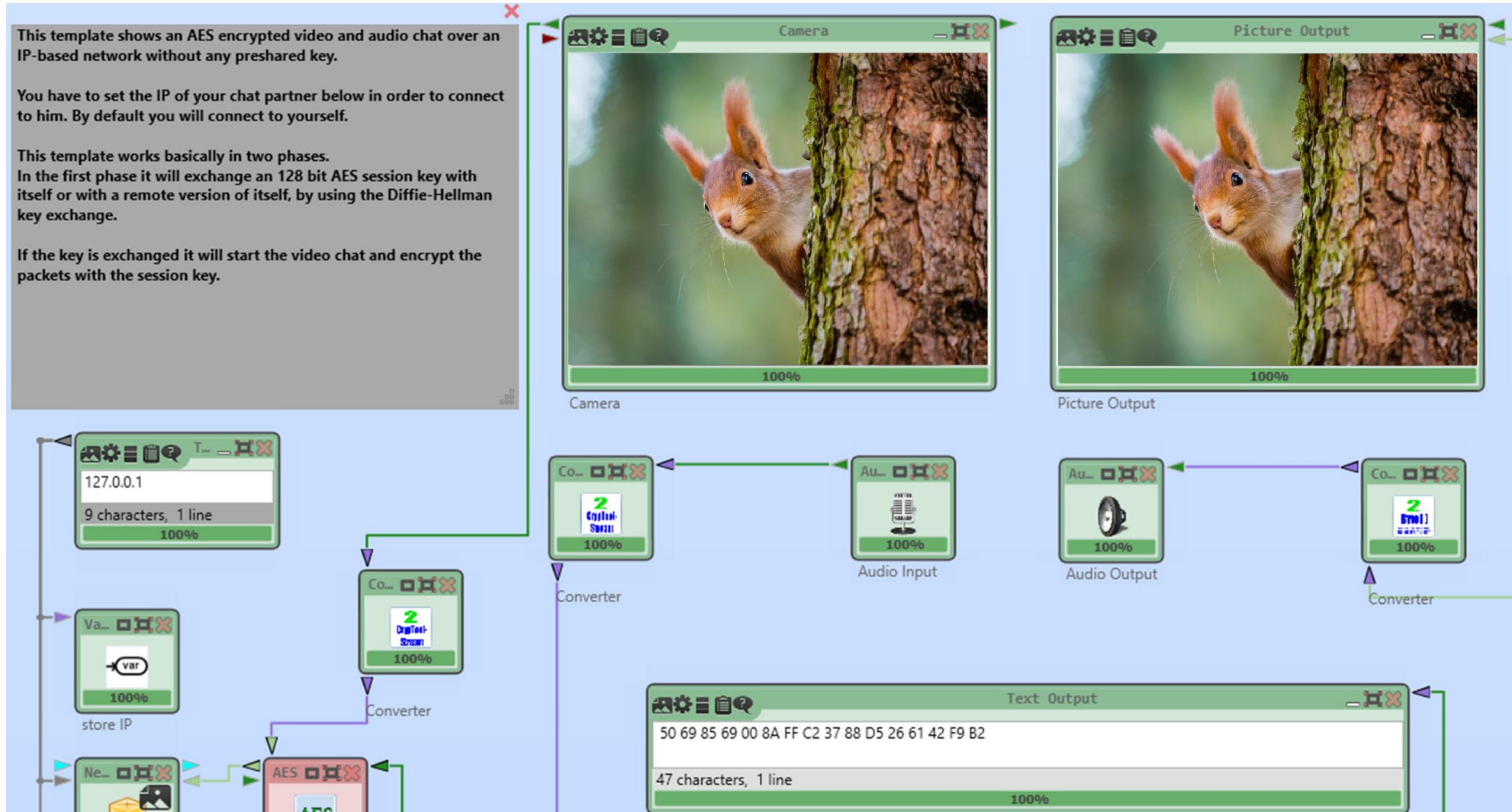
Playfair Analyzer

This template demonstrates a ciphertext-only attack on the Playfair cipher. The plaintext above is encrypted with the Playfair component and the resulting ciphertext is sent to the Playfair Analyzer.

Please note that in Playfair for every key there exist several equivalent keys that generate the same ciphertext.

2. Highlights

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



2. Highlights

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

The screenshot displays the DECODE web interface with four main components: DECODE Downloader, DECODE Viewer, Picture Output, and Text Output.

- DECODE Downloader:** Shows a search filter for "Copiale" and a list of results. The first result is "2 Copiale" and the second is "210 BAV_iBorg-Lat_898".
- DECODE Viewer:** Displays detailed metadata for the selected document "Copiale".

Name:	Copiale
Id:	2
Content:	Type: cipher
Cipher type:	Inline plaintext: false
Symbol set:	Inline cleartext: false
Number of pages:	105
Plaintext language:	German
Origin:	Author: The Oculist Society
Dating:	1734-01-01:1736-12-31
Sender:	Region: Germany
Receiver:	City:
Format:	Paper:
Ink Type:	
Add. info:	http://stp.lingfil.uu.se/~bea/copiale/

It also shows a list of available documents:

#	Title	Upload date	Size	File type
3	decryption of copiale cipher	2016-08-09	87 kB	txt
1	transcription of copiale cipher	2016-08-09	237 kB	txt
2	translation to English of copia	2016-08-09	79 kB	txt
- Picture Output:** Shows a scanned image of a handwritten document page with dense, cursive text.
- Text Output:** Shows the transcribed text of the document, including a legend and the actual cipher text.

```
### Transcription of Copiale document, August 2011. ## 1. document lines separated here by blank lines.## 2. each character transcribed using an ascii code## 3. uncertainties are marked with "?"## 4. catch words letters at page bottom marked with "#"## 5. page numbers marked with "###"## 6. capitalization is recorded (e.g., first letter is "L", not "T")## 7. logograms: *o* society, *star* secret, *nee* master, *tri* lodge, *bigx* freemason, *gate* table shaped, *lip* oculist (eye), *bigl* position of feet, *tribig* lodge, *sci* "God", *toe* power###PAGE 1L i t : m z grr bar b lv x. zzz bar ih lam s. k sqp ki arr bar w npi oh j v hd tri arr eh three c. ah ni arr lam uh b lip uu r o. . zsdel grr hd zzz iot plus oh j n p lam hd ih ns c. f. C uh j hk eh three t p. sqp cross g ns lam : kDS x. uh hd eh ns plus zzz r. p ki mu lam ih three : y. arr lam l mal o. j q z iot ih fi x. ah bar eh c. : uu ds .J uh r. hk oh j k lam iot lam ni c. zs .M bas grr r. ah plus tri g y. . uu x z oh three m n. ki sqi nu h. hd plus ih f. K m. uh ru : p z iot oh f bar y. . bas hd eh j hd zzz iot lam n pi ah three b tri. . gs z ni j arr l z uu p fem c. lam ah r. g k lam hdgrl r. hd grl lam zzz j n sqp ih bar tri r. del grr lam a ni g z w pi y. . eh c tri. . r mal tri plus b z ns r iot x. y. . j ih ru z uu f nee zspi ki j arr ds p. ni sqi bar uh lam s. ki mu del m bar zzz ns g ah bar k hd ni lam hd bar l x. oh no sqi : ru ih lam b iot hk u m. y. . j v z ah j x bas p. mu pi iot z h. lam c mal o. g gs z uh plus p car grl nu x. eh three g h lam hd grl j hd grl lam ih three t n. ki bar r oh y. . mu ah plus h h. ru z oh three nu b s. ns plus : zzz r. k p. sqp del grr hd tri c. uh lam gs ni nu z k sqp zzz inf n z grr three f hd n. ru pizs eh y. . nu gs ni ru pi gs mal tri three n z grr bar k pi ns j iot x. y. . r. ih g pi uu nee b gs lam iot cross b del uh sqi grl hd three eh lam z ns oh bar uh c. sqi three fem del lam b ns hd mu ds in ih b. iot one o. oeh b 238.878 characters, 1 line
```

A "String Encode" button is visible between the DECODE Viewer and Text Output windows.

DECODE Downloader 100% **DECODE Viewer** 45% **Picture Output** 100% **Text Output** 100%

This template shows how to download encrypted historical documents from the DECODE database:

- 1) Start the template (Play button).
- 2) Within the DECODE Downloader a list of database records is shown. These records can be limited by entering a filter text, e.g. "Copiale".
- 3) Via double click on an entry in the DECODE Downloader list, the record's meta data are shown in the DECODE Viewer.
- 4) In the DECODE Viewer, additional documents and images can be downloaded: To do so, double click on the specific image or document entry in the lists. These downloads are shown in the components "Downloaded Document" and "Downloaded Image".

2. Highlights

14. DECODE Decipherer in CT2 – decryption of historic ciphers

The screenshot displays the DECODE Decipherer interface. On the left, a 'Text Input' window shows the source document's metadata and content. The main window displays the decrypted text, which is a historical document in Italian. The text is presented in a table-like format with line numbers (1-12) on the left and character counts on the right. The text is: 1 man dai come scrissi pars dela mia famiglia con ler 2 obbe per Mantova e miseru/vi potere senza daa so 3 spatto manda? a sapere quello che ha u/ve sse ri 4 ortat il Signor - Ghibellino dal commissario - imperiale e ? duca - di - Mantova che mi pare u/va di no 5 oco momento per mia negoziazione man dai a questo a fett 6 feretti mio familiare con ordine che gli? prete 7 sto di quozzio eta? si a cheo pa? con Signor - Ghibellino come se 8 gu/vi e perché il detto camino per Mantova e piu/v bre u/ve 9 di quello cheio feconi a diritu/vra per u/verona las 10 pettzi sotto colore di aspetioe la 11 famiglia a ro/vere l u/vo? dodeci m deglia p 12 rima di u/vu/vdea o? a tre conte il Signor - Ghibellino mi conmu/vn ico la

Below the text, there is a 'Text Input' window showing a list of characters: 1 - <null>, 8 - <null>, 02 - a, 20 - a, 00 - a, 07 - o, 70 - o.



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?