Workshop – HistoCrypt 2018

(Automated) Cryptanalysis of Classical Ciphers with CrypTool 2

Nils Kopal, Armin Krauss, and Bernhard Esslinger

2018-06-20

Introduction

During this workshop you will learn how to use CrypTool 2 (CT2) to encrypt and decrypt texts using different classical ciphers. Furthermore, after this workshop you will be able to break simple classical ciphers with the help of CT2 on your own.

Structure of this workshop

The workshop is structured into different chapters in which we will show you how to use CT2:

In “Basics of Cryptology” we will explain some basic concepts of cryptology. After that we will give you a brief introduction to CT2. Then, in “Substitution Ciphers”, you will encrypt texts using different types of substitution ciphers, as well as break some examples using CT2. In “Transposition Ciphers”, you will encrypt texts using the columnar transposition cipher as well as break ciphers. In “Composed Ciphers”, you will get to know the ADFGVX cipher, which was used during World War 1. In “Machine Ciphers”, you will encrypt texts using the Enigma machine as well as break Enigma messages with CT2. In the chapter “Identifying Ciphers”, we will show you some methods to identify the type of a cipher using CT2. Finally, in the “Challenge Part”, you will be given some ciphers and you can break them on your own.

1. Basics of Cryptology

Cryptology is the science comprised of secret writing (**cryptography**) and recovering of the secret texts without the knowledge of the secret keys (**cryptanalysis**).

Cryptographic algorithms are designed by a **cryptographer** and cryptanalysis is performed by a **cryptanalyst**.

A **cipher** is a special cryptographic algorithm used for encryption and decryption. For encryption, the input of a cipher is a **plaintext** and a (secret) **key** and the output is a **ciphertext**. For decryption the input is a ciphertext and a key and the output is the revealed plaintext. The type of the key is based on the type of the cipher and can consist of letters, numbers, machine settings, and so on.

```
Cipher(plaintext, key) = ciphertext
Cipher(ciphertext, key) = plaintext
```

In classical ciphers the key for encryption and for decryption is the same. All possible keys of a cipher define the **keyspace** of a cipher. With some ciphers, for example the Caesar cipher, it is possible to automatically test each key, since the keyspace of the cipher is very small (Caesar has 26 possible keys). But many classical ciphers have so many possible keys, that searching through the complete keyspace is impractical. In such cases, often **heuristics** can be used to break a cipher.

Breaking a ciphertext means, to reveal the plaintext without being in possession of the used key.

The used letters or symbols of plaintext and ciphertext are defined by **alphabets**. With some ciphers the alphabets are the same, with some they differ. Thus, we have a **plaintext alphabet** and a **ciphertext alphabet**.

Example: The Caesar Cipher

The Caesar cipher just shifts each letter in the alphabet according to a key (shift value).

Plaintext alphabet:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key:	1 (i.e. shift alphabet by 1)
Ciphertext alphabet:	BCDEFGHIJKLMNOPQRSTUVWXYZA
Plaintext:	HELLOWORLD
Ciphertext:	IFMMPXPSME

a) Attacks on Ciphers

We differentiate between various attack types, depending on the knowledge of the attacker.

The **ciphertext-only attack** reveals the plaintext and/or the secret key. The cryptanalyst is here only in possession of the ciphertext. This is the strongest and most difficult attack on a cipher.

The **known-plaintext** attack reveals the key. Which then can be used to break other ciphertexts encrypted with the same key. Here, the cryptanalyst is in possession of the plaintext and the according ciphertext. If the cryptanalyst is only in possession of parts of the plaintext, we call that a **partially known-plaintext** attack.

b) Statistics

Based on language models and text statistics, it is often possible to break classical ciphers – even by hand. The letter frequency can be used, for instance, to identify which plaintext letter is replaced by which ciphertext letter. For example, the letter 'E' is the most frequent letter in English texts. Thus, if in a given ciphertext the letter 'X' is the most frequent letter (and we have a monoalphabetic substitution cipher – we will describe this later in detail) it may be the 'E' in the plaintext.

c) Substitution Ciphers

Substitution ciphers replace letters of the plaintext with other letters (or number, symbols, etc.). If the same letter is always replaced with the same ciphertext letter, the cipher is a **monoalphabetic substitution cipher**. If the same letter is replaced with more than one letter, the cipher is a **homophonic substitution**. In both cases, we have only one plaintext and one ciphertext alphabet. If the alphabet is exchanged after encrypting a letter, i.e. we have different ciphertext alphabets, we have a **polyalphabetic substitution**.

Cipher type	Number of plaintext symbols	Number of ciphertext symbols
Monoalphabetic Substitution	26	26
Homophone Substitution	26	> 26
Polyalphabetic Substitution	26	26; but different alphabets

Examples:

1. Monoalphabetic Substitution: The Caesar Cipher

The Caesar cipher just shifts each letter in the alphabet according to a key (shift value).

Plaintext alphabet: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Key: 1 (i.e. shift alphabet by 1)

Ciphertext alphabet: `BCDEFGHIJKLMNOPQRSTUVWXYZA`

Plaintext: `HELLOWORLD`

Ciphertext: `IFMMPXPSME`

2. Homophone Substitution

The homophone cipher replaces each plaintext letter using two different ciphertext letters. Here, a ciphertext letter consists of two-digit numbers from 01 to 99.

Plaintext alphabet: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Key: `A = {01 or 02 or 06}, B = {03 or 04}, C = {05}, ...`

Plaintext: `HELLOWORLDHOWAREYOU`

Ciphertext: `15,09,23,24,29,45,30,35,23,07,16,29,46,01,36,10,49,30,41`

3. Polyalphabetic Substitution: The Vigenère Cipher

The Vigenère cipher uses different shifted ciphertext alphabets based on a keyword.

Plaintext alphabet: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Ciphertext alphabets: `ABCDEFGHIJKLMNOPQRSTUVWXYZ` 26 different shifted alphabets
`BCDEFGHIJKLMNOPQRSTUVWXYZA`
`CDEFGHIJKLMNOPQRSTUVWXYZAB`
`DEFGHIJKLMNOPQRSTUVWXYZABC`
`EFGHIJKLMNOPQRSTUVWXYZABCD`
…

Key: `SECRET`

Plaintext: `HELLOWORLDHOWAREYOU`

Ciphertext: `ZINCSPGVNULHOETVCHM`

d) Transposition Ciphers

Transposition ciphers do not replace letters with other letters. Instead, the position of the letters in the plaintext is changed. Thus, plaintext and ciphertext alphabet are the same. That means, that the text frequency of a ciphertext is exactly the same as its corresponding plaintext.

Example:

Transposition Cipher: The Columnar Transposition Cipher

With the classical columnar transposition cipher the plaintext is first copied, row by row, into a rectangular grid with a fixed number of columns. Then the individual columns are permuted according to a keyword. The final ciphertext is created by reading the text from the columns.

Plaintext alphabet: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Ciphertext alphabet: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Key: `SECRET`

Plaintext: `HELLOWORLDHOWAREYOU`

Ciphertext: `LLRERAOHYLDEHOWUWOO`

2. Introduction to the CrypTool 2 Application

CrypTool 2 (CT2) consists of six main components:

Startcenter,

Wizard,

Workspace Manager,

Online Help,

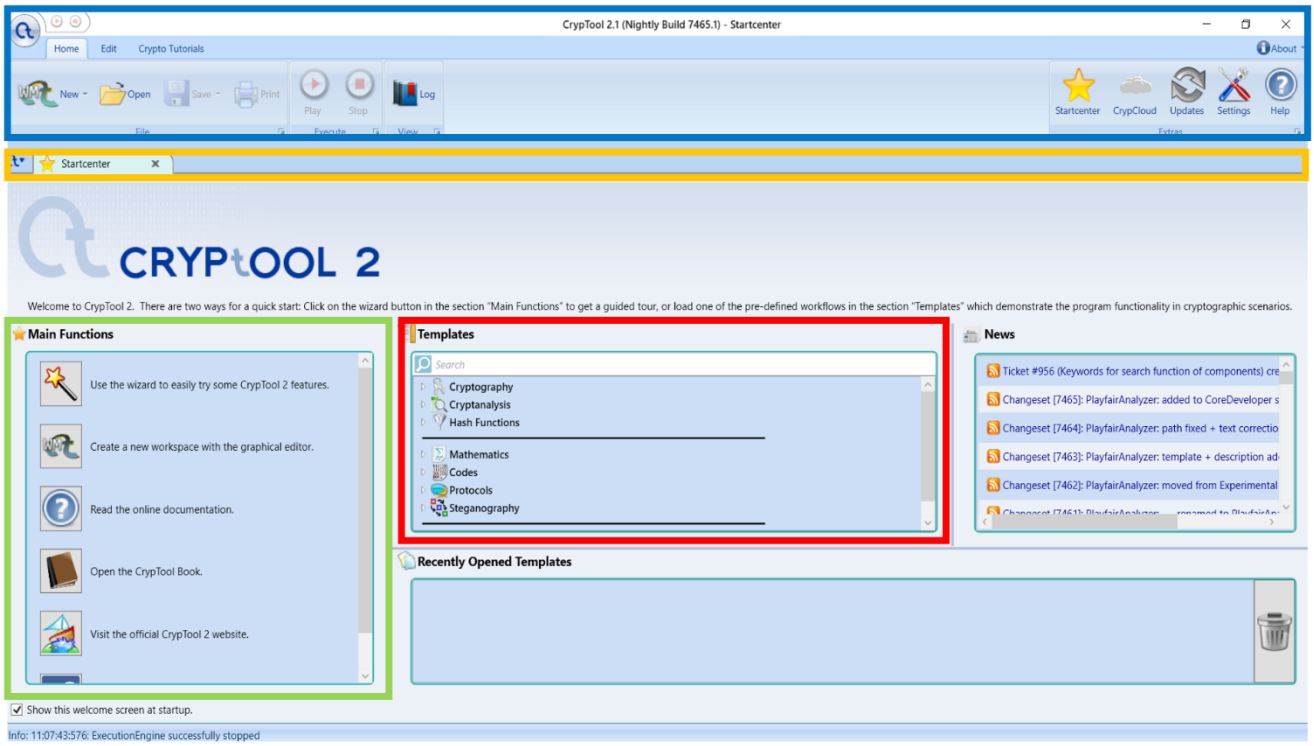
Templates,

and **CrypCloud**,

In this workshop we present the **Startcenter**, the **Wizard** and the **Workspace Manager** in detail.

a) Startcenter

Every time you start the CT2 application, you will first see the **Startcenter**.



CT2 and the Startcenter consists of different areas that we marked with different colors in the above image.

The blue marked area ("ribbon bar") on the top of the image allows to either create new workspaces or open and save existing "CrypTool 2 workspaces" (shown later). Additionally, it allows to always go back to the Startcenter (yellow star icon), go to the CT2 settings (hammer and screwdriver icon), start the CrypCloud (cloud icon), open the online help (question mark icon) and start or stop the currently opened workspace (play and stop icons).

The yellow marked area contains a list of all open "tabs". A tab is a kind of window containing the Startcenter, workspaces, etc. Tabs can be closed, if not needed anymore using the X-icon of each tab. An arbitrary number of tabs can be opened but its amount is limited by the memory of the computer.

The green marked area of the Startcenter contains buttons to open all other components like the Wizard (magic wand), the Workspace Manager (2nd icon in the list), the online help (question mark icon), etc. Each button has a self-explaining text on its right side.

The red marked area of the Startcenter contains a list of all "templates" (more than 200) which we deliver with CT2. A template contains a specific cipher or cryptanalytic scenario using the graphical programming language of CT2 and is ready to use. The list of templates of the Startcenter can be filtered using keywords that can be entered in the search field.

Below the red marked area, you can find "Recently Opened Templates" showing a list of templates you opened in the past.

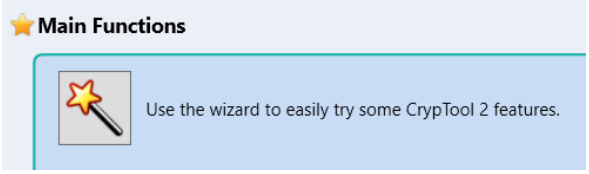
Finally, on the right side of the Startcenter you will see some "news", showing the last changes we did on CT2 with respect to its source code.

b) Wizard

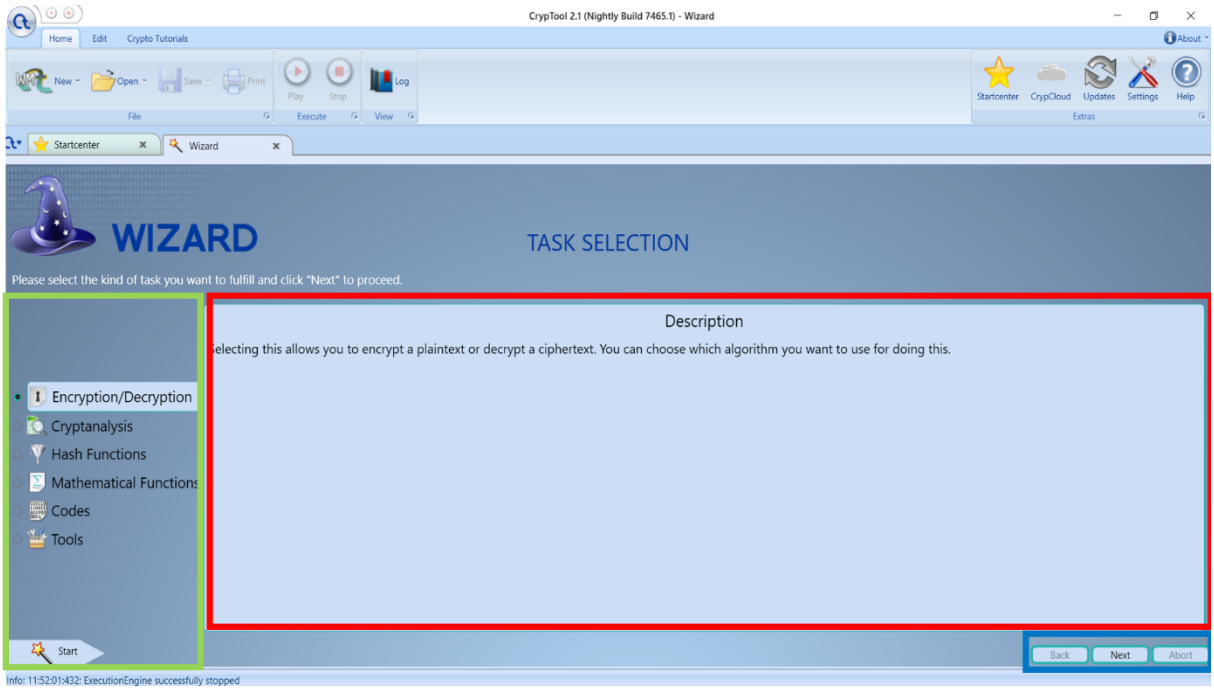
The Wizard is intended for users not familiar with using the graphical programming language of the Workspace Manager and for beginners. It guides you through the different topics of cryptology until you "reach what you want to do", e.g. encrypt something or break something.

The Wizard can be started at two different places. First, it can be started by clicking in the top ribbon bar on the new icon and selecting "Wizard".

Secondly, it can be started using the Startcenter and clicking here on the "Magic wand" button.

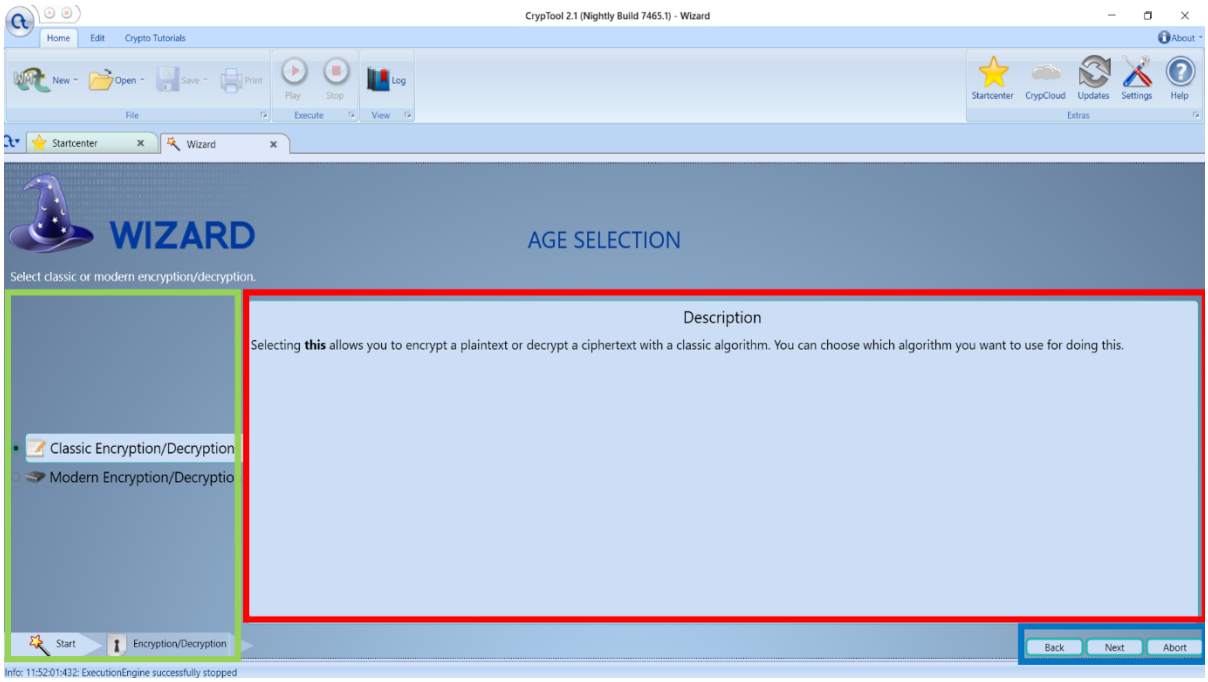


The Wizard consists of three main areas (here marked green, blue, and red).



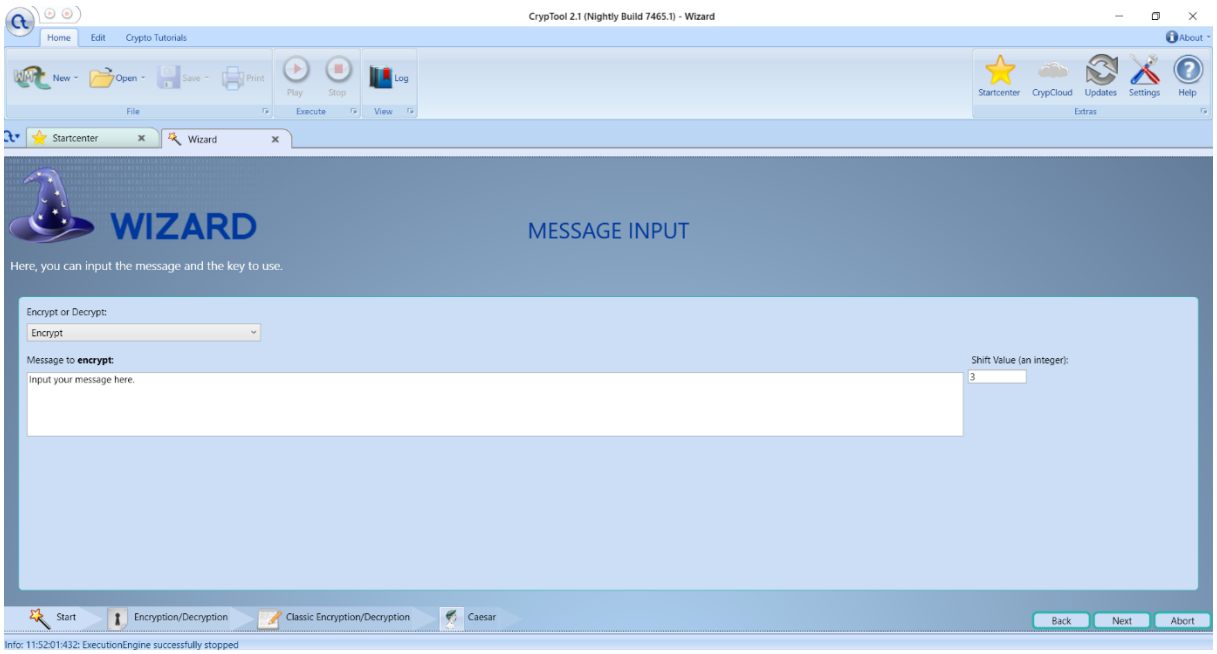
In the green marked area, you can “select what you want to do”.

For example, you want to encrypt a text using the Caesar cipher. Then, first select “Encryption/Decryption” and click on “Next” in the blue marked area. Instead of clicking on “Next” you may also double-click in the green area. Then, in the red marked area, the next page will appear.

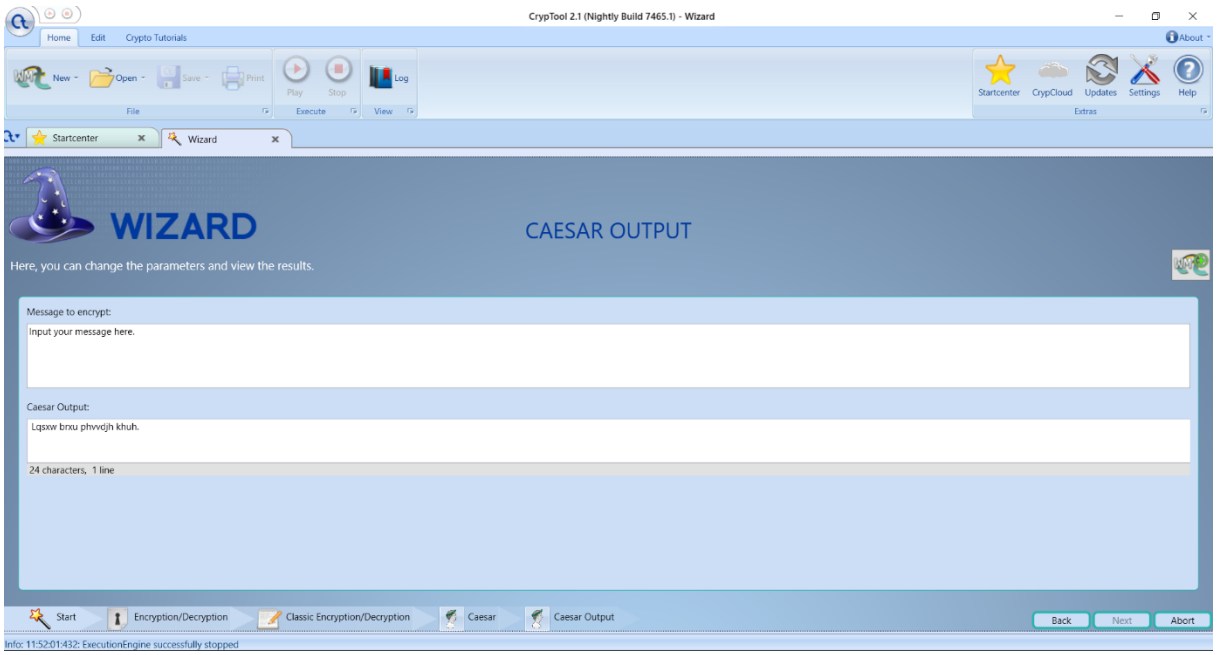


Then, the green area is updated with new options. The red area always contains some informational text based on the selections.

You repeat this step until you reach the “Caesar” cipher.



Here, you can enter the key and the text you want to encrypt. On the last time you click “Next” you will get the encrypted text.

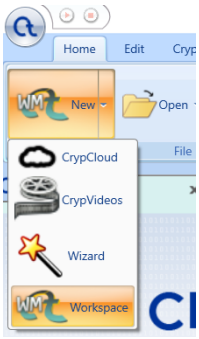


In each final step in the Wizard, you may click on the Workspace Manager icon on the top right side of the Wizard to open a template in the Workspace Manager corresponding to the cipher or cryptanalytic method you selected and currently use.

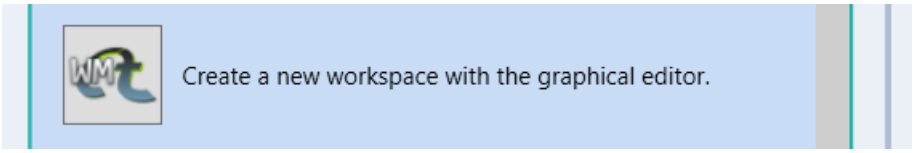
C) Workspace Manager

The **Workspace Manager** implements the graphical programming language of CT2. It allows to create arbitrary cascades of ciphers and cryptanalytic methods.

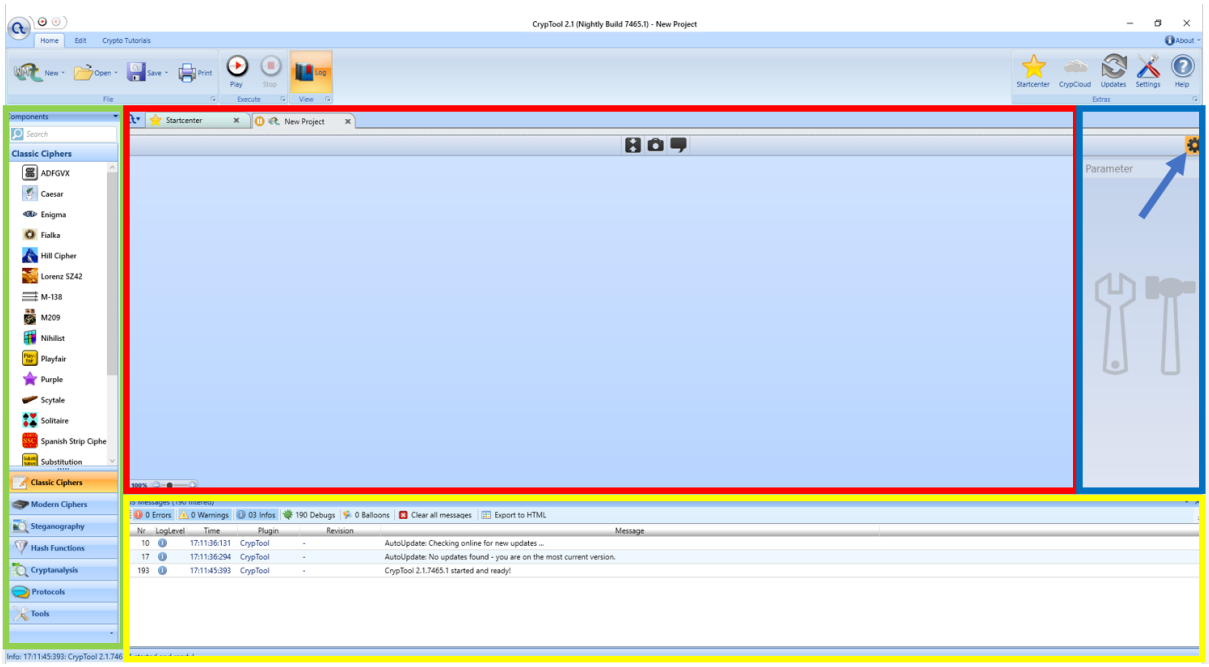
The Workspace Manager can be started at two different places. First, it can be started by clicking in the top ribbon bar on the new icon and selecting “Workspace”.



Secondly, it can be started using the Startcenter and clicking here on the “Workspace Manager” button.



A newly opened workspace of the Workspace Manager looks like this.



The red marked area is the actual workspace. It is used to create a visual program.

The green marked area contains the list of components (components = cryptographic methods implemented in CT2). Each component can be put onto the workspace. To do so, just drag a component from the left side onto the workspace in the middle and drop it.

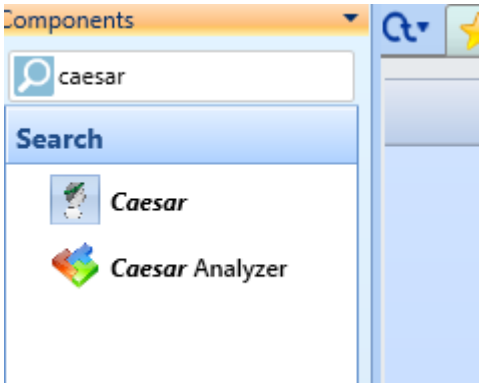
The yellow marked area is a logging window which contains messages generated by the components during the execution.

The blue marked area on the right side is the settings bar for the selected components. If a component is selected you can change its internal parameters here. The settings bar can be closed and opened with the gear-wheel button in the upper right corner (marked with a blue arrow in the picture above).

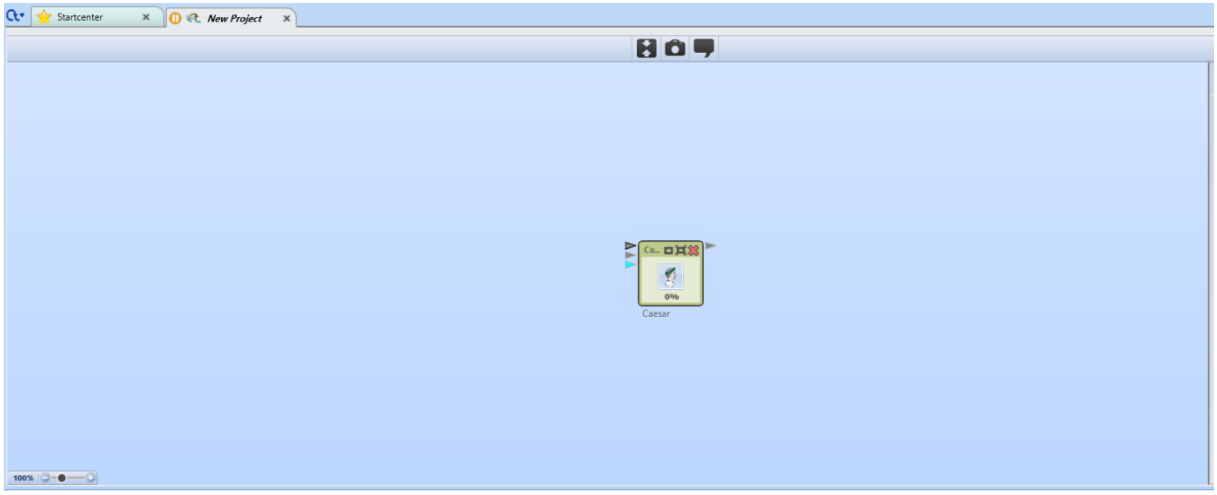
Example Build of a Caesar Cipher

Now we show you how to build a workspace for a Caesar cipher from scratch with CT2. To do so, open the Workspace Manager as shown above.

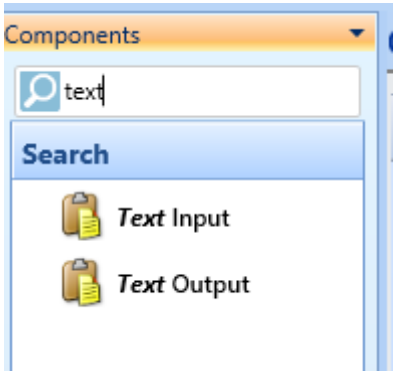
Then, go to the list of components on the left side. Here, enter “caesar” in the search field (it is not case-sensitive).



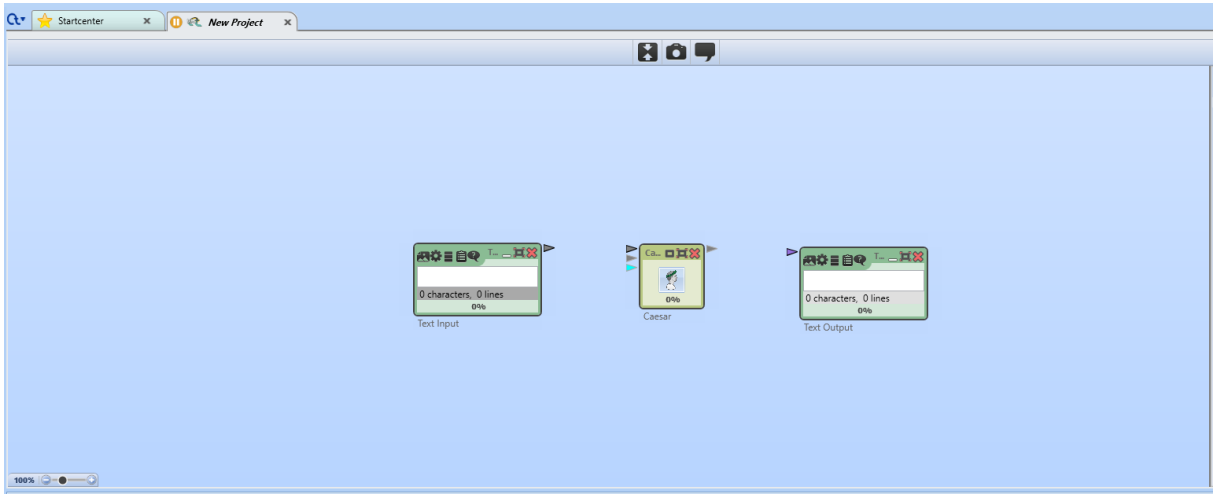
Now, use the left mouse button to drag the “Caesar” component and put it onto the middle of the workspace.



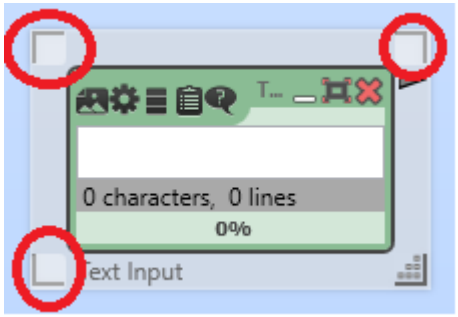
After that, use the components list again to search for “text”.



Now, drag&drop a “Text Input” component to the left of the Caesar component and a “Text Output” component to the right of the Caesar component.



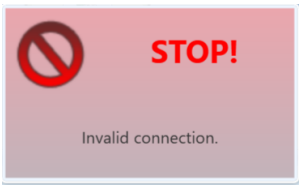
If you want to move them you can always drag a component. A minimized one can be dragged at each position within the icon (like the Caesar component in the picture). If it is not minimized but maximized, like the “Text Input” and “Text Output”, select the component by clicking on it. Then you can move the component using the upper gray corners or the lower left gray corner (marked red in the next picture).



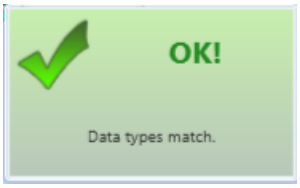
To establish a workflow connect “Text Input” and “Text Output” with the Caesar component. For connections between components CT2 offers connectors. Connectors are small colored rectangles on the left or right side of a component. You can drag&drop a line between output and input connectors. The color of a connector shows it’s data type. For example, a number connector is blue ( ), a text connector is gray ( ), and so on. As a rule of thumb: You can always connect connectors of the same color without any problems. If you want to connect connectors with different colors, you

may need converter components. Some data types can be implicitly converted. CT2 will show a hint if this happens.

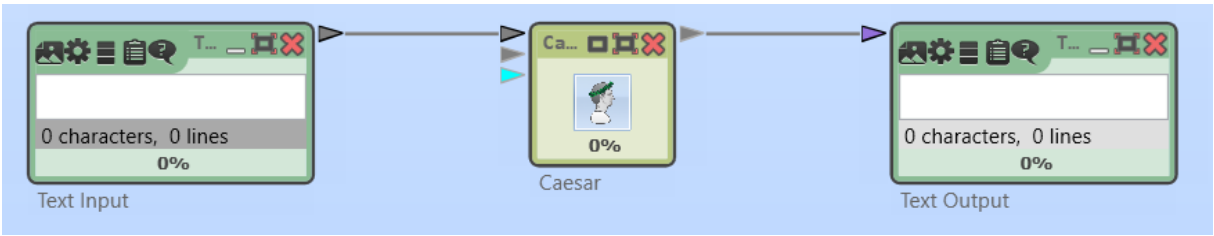
If a connection is not possible CT2 shows an error.



If a connection is valid without any problems CT2 shows a green text.

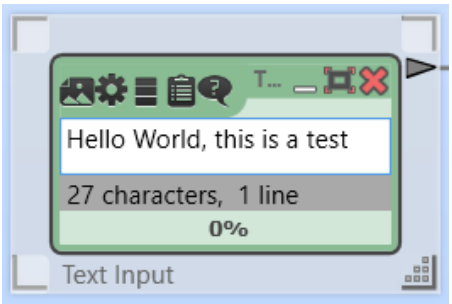


Now, connect the Caesar component, the "Text Input" component, and the "Text Output" component as shown in the next picture.



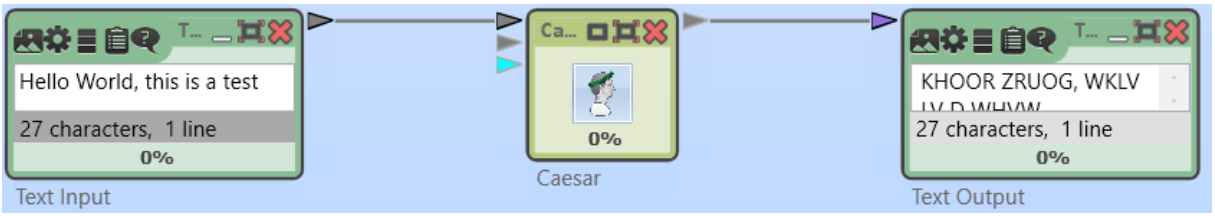
Now, you have built your first graphical program.

Click on the text field of the "Text Input" component and enter some text.



Finally, click on the “Play” button in the top ribbon bar.

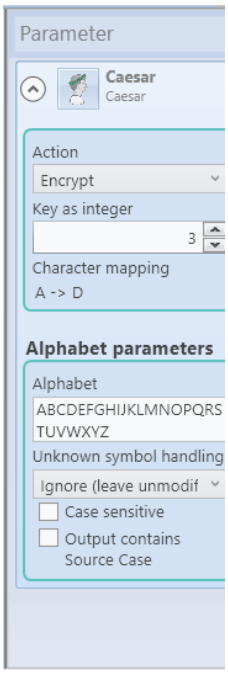
Now, CT2 executes your graphical program. The output should look like this.



Try to type into the “Text Input” while the graphical program is being executed. CT2 will update your ciphertext in the “Text Output” component at once.

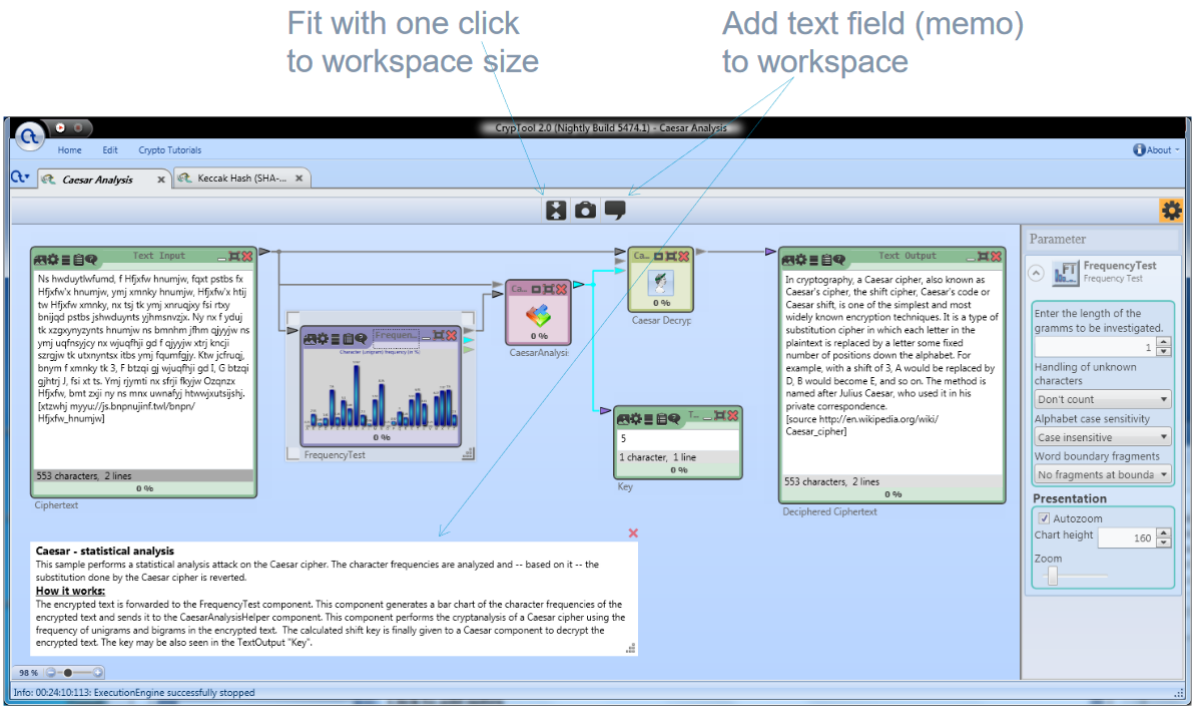
To change your graphical program, you have to stop it using the “Stop” button in the top ribbon bar.

If you want to change the key or other settings of the Caesar cipher, select it and use the toolbar on the right side of the workspace.



Here, with the Caesar component, you can change the key (shift number), the alphabet, etc.

You can adapt the zoom level of the workspace using the buttons in the top middle of the Workspace Manager.



Further hint for easy handling: Quickly adapt the CT2 GUI with the keyboard using F11 and F12 by fading-in or fading-out parts outside the actual workspace.

Each workspace can be stored as a file with the extension “cwm” (via the “Save” icon under the “Home” menu at the top of the CT2 main windows). All templates are also workspaces – predefined and delivered with CT2. So they are also stored in cwm files (see the directory “Templates” below the CT2 directory in your installation). Their specialty is that they are available in 2 languages at once.

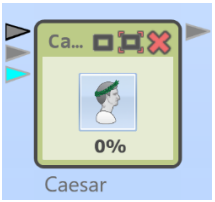
3. Substitution Ciphers

CrypTool 2 (CT2) contains different classic substitution ciphers. We will have a closer look at the following ones:

- **Caesar** cipher
- **Monoalphabetic substitution** cipher
- **Vigenère** cipher

To use the ciphers and their corresponding analysis methods, go to the Startcenter and use the template list to search for appropriate templates. You could also use the Wizard. To copy a text, mark it using the mouse and press "control key + C". Then, in CT2 you can enter the text by pasting it (pressing "control key + V") into the text input component.

a) Caesar Cipher



Task 1: Decrypt the following text using the Caesar cipher built in CT2:

```
Va pelcgbtencul, n Pnrfne pvcure, nyfb xabja nf Pnrfne'f pvcure, gur
fuvsg pvcure, Pnrfne'f pbqr be Pnrfne fuvsg, vf bar bs gur fvzcyrfg
naq zbfg jvqryl xabja rapelcgvba grpuavdhrf. Vg vf n glcr bs
fhofgvghgvba pvcure va juvpu rnpu yrggre va gur cynvagrkg vf
ercynprq ol n yrggre fbzr svkrq ahzore bs cbfvgvbaf qbja gur
nycunorg. Sbe rknzcyr, jvgu n yrsg fuvsg bs 3, Q jbhyq or ercynprq
ol N, R jbhyq orpbzr O, naq fb ba. Gur zrgubq vf anzrq nsgre Whyvhf
Pnrfne, jub hfrq vg va uvf cevingr pbeerfcbaqrapr.
```

Key: 13

Hint: Open the template "Caesar Cipher" or use the Wizard.

Task 2: Encrypt the following text using the Caesar cipher built in CT2:

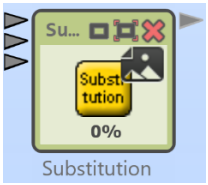
```
Gaius Julius Caesar known by his cognomen Julius Caesar, was a Roman
politician and military general who played a critical role in the
events that led to the demise of the Roman Republic and the rise of
the Roman Empire. He is also known as an author of Latin prose.
```

Key: 10

Task 3: Break the following text using the template "Caesar Analysis using character frequencies":

```
Pu jyfwavnyhwof, h jpwoly pz hu hsnvypaot mvy wlymvytpun lujyfwapvu
vy kljyfwapvu - h zlyplz vm dlss-klmpulk zalwz aoha jhu il mvssvdlk
hz h wyvjlkbyl. Hu hsalyuhapcl, slzz jvttvu alyt pz lujpwolytlua. Av
lujpwoly vy lujvkl pz av jvuclya pumvythapvu puav jpwoly vy jvkl. Pu
jvttvu whyshujl, "jpwoly" pz zfuvuftvbz dpao "jvkl," hz aolf hyl
ivao h zla vm zalwz aoha lujyfwa h tlzzhnl; ovdlcly, aol jvujlwaz
hyl kpzapuja pu jyfwavnyhwof, lzwljphssf jshzzpjhs jyfwavnyhwof.
```

b) Monoalphabetic Substitution Cipher



Task 4: Decrypt the following text using the template "Substitution Cipher using a password":

```
jFYHGRGFGRLM LU HRMTOV OVGGVIH HVKZIZGVOB – HRNKOV HFYHGRGFGRLM –
XZM YV WVNLMHGIZGVW YB DIRGRMT LFG GSV ZOKSZYVG RM HLNV LIWVI GL
IVKIVHVMG GSV HFYHGRGFGRLM. hSRH RH GVINVW Z HFYHGRGFGRLM ZOKSZYVG.
hSV XRKSVI ZOKSZYVG NZB YV HSRUGVW LI IVEVIHVW (XIVZGRMT GSV rZVHZI
ZMW wGYZHS XRKSVIH, IVHKVXGREVOB) LI HXIZNYOVW RM Z NLIV XLNKOVC
UZHSRLM, RM DSRXS XZHV RG RH XZOOVW Z NRCVW ZOKSZYVG LI WVIZMTVW
ZOKSZYVG. hIZWRGRLMZOOB, NRCVW ZOKSZYVGH NZB YV XIVZGVW YB URIHG
DIRGRMT LFG Z PVBDLIW, IVNLERMT IVKVZGVW OVGGVIH RM RG, GSVM DIRGRMT
ZOO GSV IVNZRMRMT OVGGVIH RM GSV ZOKSZYVG RM GSV FHFZO LIWVI.
```

Key: password = substitution, offset = 7

Hint: You have to change the setting "Action" of the "Encrypt" substitution component from "Encrypt" to "Decrypt". We change the given template, as this template was written to do encryption first. So just ignore the component with the subtitle Decrypt.

Task 5: Encrypt the following text using the template "Substitution Cipher using a password":

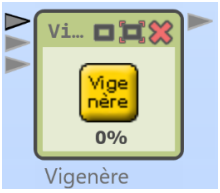
```
Cryptography or cryptology is the practice and study of techniques
for secure communication in the presence of third parties called
adversaries.
```

Key: password = key123, offset = 5

Task 6: Break the following text using the template "Monoalphabetic Substitution Analyzer":

```
MLZZLYR EHQVQHLWT EHLQVRYG MYO Y PO YHRC WHCSFAJHYSIQH MIA HYG FIQ
HQOQYHWI VLNLOLAG AE FIQ YHRCO OLJGYZ LGFQZZLJQGWQ OQHNLWQ LG FIQ
FILHFLQO
```

c) Vigenère Cipher



Task 7: Decrypt the following text using the "Vigenère Cipher" template:

```
LVRLXSF CLZIES KRRBXGU SXU RWX OTCVLRX CX VZEWM ZAOJ RWX BMKEAT HT
AVCSHBCF
```

Key: KRYPTOS

Hint: You have to change the setting "Action" of the upper Vigenère component from "Encrypt" to "Decrypt".

Task 8: Encrypt the following text using the "Vigenère Cipher" template:

```
BLAISE DE VIGENERE WAS A FRENCH DIPLOMAT, CRYPTOGRAPHER, TRANSLATOR
AND ALCHEMIST
```

Key: POLYALPHABETIC

Task 9: Break the following text using the "Vigenère Analysis" template:

```
AX YRW MYXYDPA ZROSWGTPG YSPC XFSX RFWLSFJW XJVC NCIB LLG VEKDLQ
EEIEIMSG DAINU
```

Remark Playfair:

For the Playfair cipher there is also an encryption/decryption component and an analyzer component in CT2.

4. Transposition Ciphers

CrypTool 2 (CT2) contains different classic transposition ciphers. We will have a closer look at the following ones:

- **Scytale** cipher
- **Columnar transposition** cipher

To use the ciphers and their corresponding analysis methods, go to the Startcenter and use the template list to search for appropriate templates. You could also use the Wizard. To copy a text, mark it using the mouse and press "control key + C". Then, in CT2 you can enter the text by pasting it (pressing "control key + V") into the text input component.

a) Scytale Cipher

The Scytale cipher is one of the oldest known encryption devices. It was used by the Greek in the 7th century BC. The message was written on a parchment wound around a stick. If the parchment was released, the message could not be read any more. To decrypt the message, a stick with the same diameter has to be used.

Task 10: Decrypt the following text using the "Scytale Cipher" template:

```
IMRHPINAWIAPCTISRHRRTWTEYAHRARPNAINTTSSTSOOPTTICGORENORSINPMAIPAAMPT
OMRUHIFETNYOPSIIANASCCSCRAUACICGLTYPHEAETHMTRDAEEHAULRNERRECTAEIIOWN
SNSNOCAGASUIIMTINEDIOSDNTLOTATOILIRGHTUNORAASGUEVREONEEYDFDKUCTAISSA
OCTAEMPYONDPELNDTARIWTHIFNHHIGODIESNRECSCS
```

Key: 6

Hint: You have to change the setting "Action" of the Scytale component from "Encrypt" to "Decrypt".

Task 11: Encrypt the following text using the "Scytale Cipher" template:

```
THEANCIENTGREEKSANDTHESPARTANSINPARTICULARARESAIDTOHAVEUSEDTHISCIPHE
RTOCOMMUNICATEDURINGMILITARYCAMPAIGNS
```

Key: 11

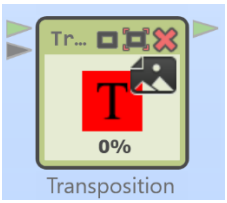
Task 12: Break the following text using the "Scytale Brute-Force Analysis" template:

```
Fweemnsa ratnat taos tnun  m Ah roac fr wit riiccre cynrheisulpdsint
netitlteataor ourlirgemcrssl rcehy o iatnu d Anp tsBumpdhei
Creoiivow.inlccinh ntla deoOgiotded t onien lhtniovcbieheunieyvreds
```

```
c   e      oettdGfiof hh rotf aeeiel   ip   nelbRtpsG kouhsecrt wto
ayehai durteennieseak dgtsedl s     _epeRcwta_ ovoeahs_
```

Hint: Take care that you analyze the text without any line breaks. If there are line breaks after copying the text remove them! **Since copying from pdf is erroneous please use the provided text file.**

b) Columnar Transposition Cipher



Task 13: Decrypt the following text using the "Transposition Cipher" template:

```
ctconsueaeortoegoiccsfsishoreaiayteligscsulrridbinxcgttenxhieteditoe
piaitseehosrrattptptmphlafttittapnhfwitaolaxafnanhooytdrseuityapoyti
tcuhesotoprninoedrtcehIyotipbneamhttnrssrhhphnyenmp
```

Key: transposition

Hint: You have to change the setting "Action" of the upper transposition component from "Encrypt" to "Decrypt".

Task 14: Encrypt the following text using the "Transposition Cipher" template:

```
inacolumnartranspositionthemessageiswrittenoutinrowsofafixedlengthan
dthenreadoutagaincolumnbycolumnandthecolumnsarechoseninsomescrambled
order
```

Key: uppsala

Task 15: Break the following text using the template "Transposition Hill Climbing Analysis":

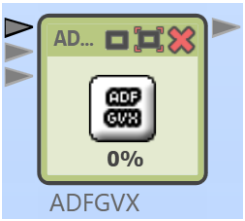
```
AENNTUTDSOENHIMEIUDOFSNSSCASILTBSSCLSNEOTMTOOIAGURSCEKUGBUGIHAIOANNO
EANLTONBCGNILNRTSTCSEIPLRLMAIOAEEPLMTTEGNLNLGSAMIORPODAYISOEWGSUSNHK
RBG
```

Hint: You have to change the setting "Keysize" of the transposition analyzer component to 6. Additionally, you have to change the setting "Read Out" of the "Transposition" parameter of the transposition analyzer to "by column".

5. Composed Ciphers

As an example for a composed cipher we use the ADFGVX cipher. It consists of a substitution and a transposition. First, the text is substituted by combinations of A,D,F,G,V, and X. Then, the resulting ciphertext is encrypted using the columnar transposition.

ADFGVX Cipher



The ADFGVX was used by the German forces in WW1. It was successfully broken by Georges Painvin.

Task 16: Decrypt the following text using the "ADFGVX Cipher" template:

```
AAFDDAADGVAVAVDVAFDAAFAGVGAFAGFAAGFDAVDGAVAAAAGVDGAVAXAGAGDDXFVAGDGD
XFFAGAAFFGAAFAGAAAFGFDVDDDVDGADGGFGAFADFDADAXDDFFDFVAXDGVGDFAXAGDFAX
ADAADDFDFAGDADFADFAAAGDXGGAGGFDGAFFFDGADDAGGVAAXAFDGDGGDDDDGGFVGAFAF
FGAAFDAFFVFVDAGVDDAGAGFVFGDDFFADADFDAFFAAAGXDDGDFXDDAVDFFGFVDVADAGGV
GDGDDFGDDXFXFVFGADAVAXFADX
```

Keys: For substitution: TREE, for transposition: HOUSE

Hint: You have to change the setting "Action" of the left "ADFGVX Encrypt" component from "Encrypt" to "Decrypt". The keys can be also applied as settings.

Task 17: Encrypt the following text using the "ADFGVX Cipher" template:

```
GEORGESJEANPAINVINWASAFRENCHCRYPTANALYSTDURINGTHEFIRSTWORLDWARXHISMO
STNOTABLEACHIEVEMENTWASTHEBREAKINGOFTHEADFGVXCIPHERINJUNE1918
```

Hint: Breaking ADFGVX automatically is still on the to-do list of the CT2 team. We plan to implement an ADFGVX analyzer in CT2 within 2018.

Remark:

Till end of 2018 there will also be an ADFGVX analyzer component in CT2.

6. Machine Ciphers

CrypTool 2 (CT2) contains different machine ciphers. We will have a closer look at the **Enigma** machine.

To use the ciphers and their corresponding analysis methods, go to the Startcenter and use the template list to search for appropriate templates. To copy a text, mark it using the mouse and press "control key + C". Then, in CT2 you can enter the text by pasting it (pressing "control key + V") into the text input component.

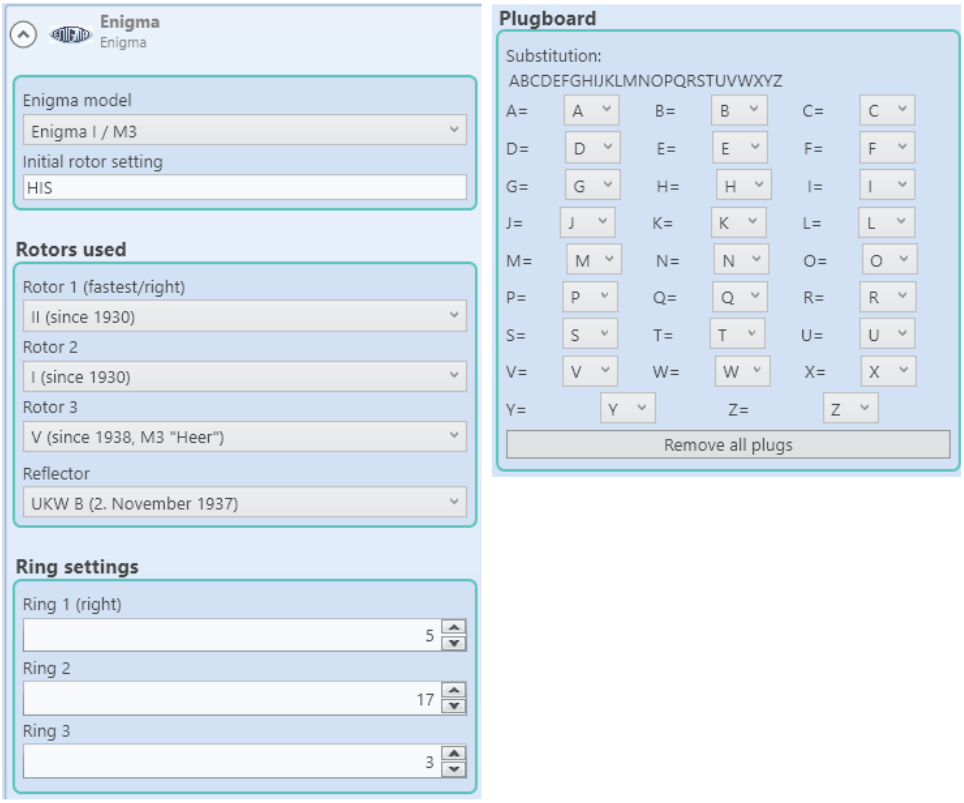
Enigma Machine

The Enigma was used by the German forces in WW2. It was successfully broken by Polish, British, and US cryptanalysts.

Task 18: Decrypt the following text using the "Enigma Cipher Machine" template:

```
SFCLFTRHHSMOGDEWODWBWPMRHVYJIMCPOJQOBNFZJLCPFHAACMHOLJSQBBRWWXNFONMH
CIBWLNTPGLYQNQRREBMBXWWNDRYWVLOLEEZUBCRDSKAKTTJSCLXQBADONWKKKLNPCZEA
QATCHCHMIZPGWXIXNOIEZRRDZHYSREO
```

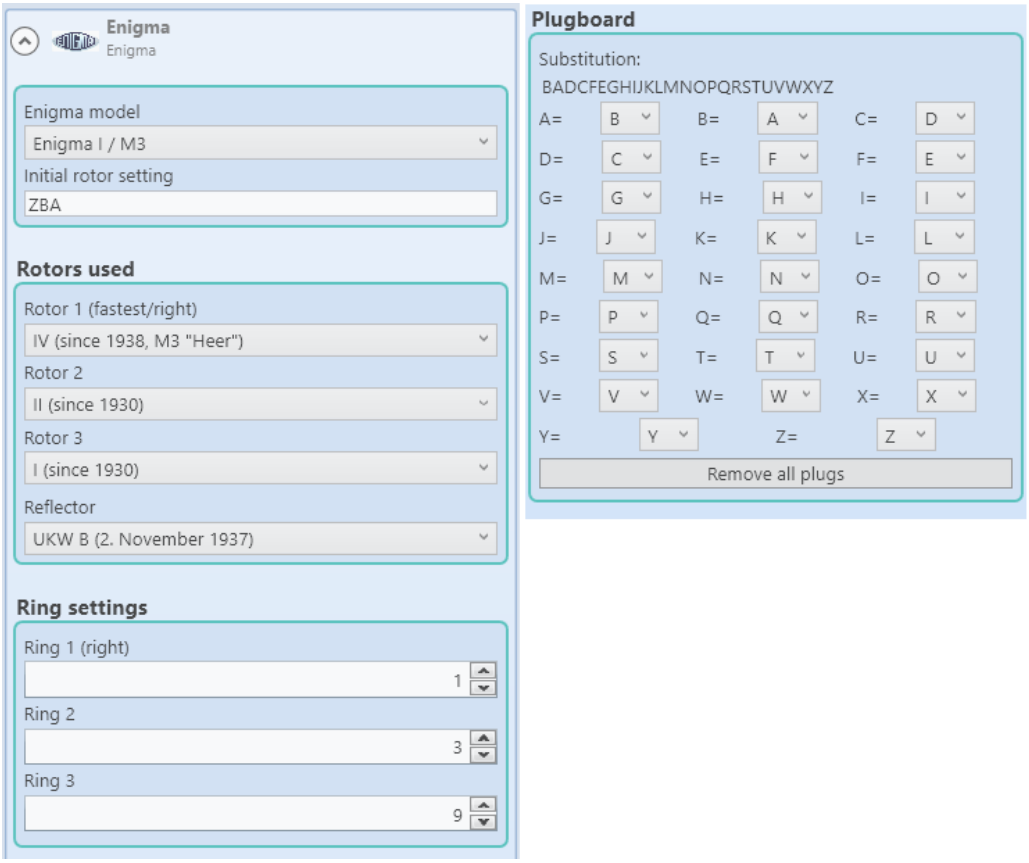
Key:
Set the key settings (parameters) according to the following picture:



Task 19: Encrypt the following text using the "Enigma Cipher Machine" template:

```
ENIGMAWASINVENTEDBYTHEGERMANENGINEERARTHURSCHERBIUSATTHEENDOFWORLDWA
RI
```

Key:
Set the key settings (parameters) according to the following picture:



Task 20: Break the following ciphertext using the "Enigma Analyzer" template:

```
WYCLKWEDNUZRBERPNUHSVOGIBNUREFSCKHSTWCBKBJVSEYRPOVBANIKKLBKGVAOYCWZQ
ZBFUTXSLJAHKQLJVSTHSDBKJNAOHWMTTMAJKPZWPBYMUMNHRUHKIRBKVIDKKMUDHGJVP
VMCVTOHRKFEGZDNZNELAHTAXFMSATNKBRVLMJTBNKVVQETMZUGQHHFRTAIPTSLRQAWWJ
NWKEDWACHWEVYFGNLCFKAAWDHCFYPKWZAISLOUJMJDBKNINROEXCZIEUEQYBJBJGUYFL
TYDPROGMQBZWSBWOFWROTYUJOHEDGYJNXSBQXYPKHTDIGUYDNLUVEWJIXCPTNTKGPONL
ABSRZMQOQKQAUNAJYVCMNDZZYSWRYYFRZLBTAVHFTBWSDINHSRARTEJTQTVHCUCYURQS
UABESRSXNDJYGUVJKZPFOVYVPAXRHQPFXRJTIRMEKWABVXNDZXCGONWWQLGXKSSHUBTG
XMJPRCHPSOQFKNFMDPFTGRNLSSRSXMXBEARHFPXVKHNHLDRIUHLMHAWVOZPFREVCNM
```

7. Identifying the Type of a Cipher

Identifying the type of a cipher is challenging and not always possible without further knowledge about the cipher's origin and background. The type of a lot of historical ciphers is still unknown. An example for such a cipher is the Voynich Manuscript – a book of the 15th century encrypted and written using an unknown alphabet.

To identify the type of the cipher CrypTool 2 (CT2) implements some useful tools. Here we will use

- the **"Frequency Test"** component, and
- the **"Friedman Test"** component.

The "**Frequency test"** component visualizes the letter distribution of a given text.

The **"Friedman test"** (also known as kappa test) was invented during the 1920s by William F. Friedman. Friedman used the index of coincidence, which measures the unevenness of the cipher letter frequencies to break the cipher. By knowing the probability that any two randomly chosen source-language letters are the same (around 0.067 for English) and the probability of a coincidence for a uniform random selection from the alphabet (1/26 = 0.0385 for English), the key length of a polyalphabetic cipher can be estimated.

[Wikipedia: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#Friedman_test]

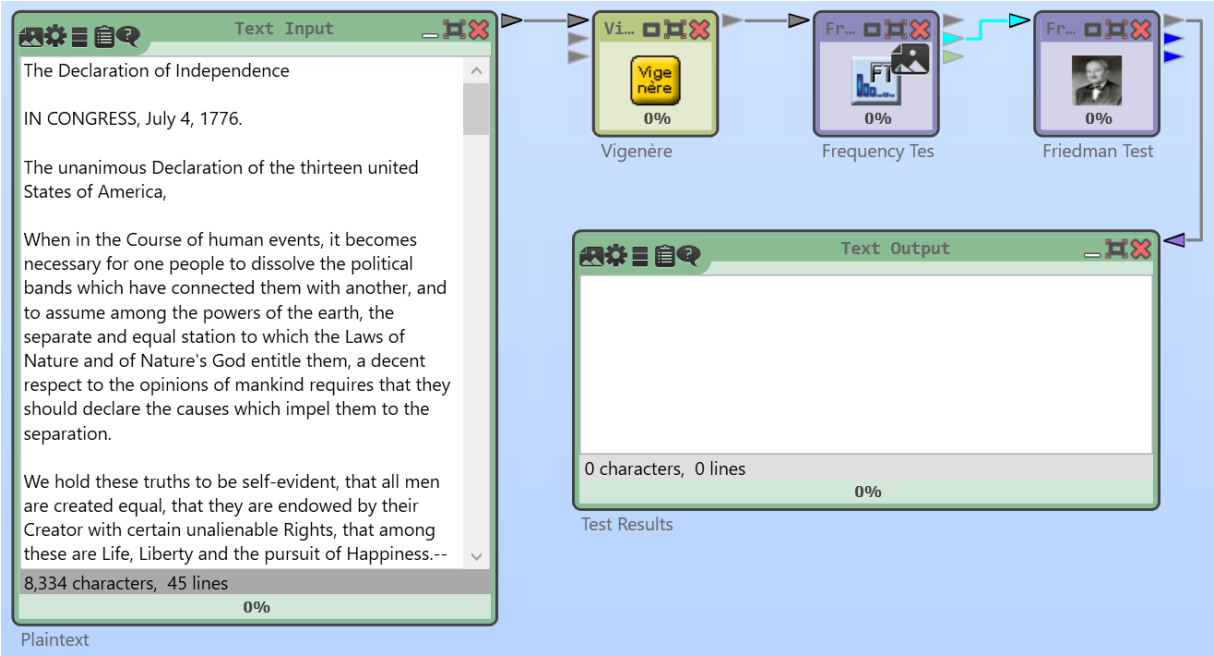
With the help of the "Friedman test" component in CT2, one can differentiate between plaintext (or transposed or monoalphabetic substituted text) and polyalphabetic encrypted texts.

Plaintext

Task 21: Analyze the following plaintext using the "Statistic Tests for Classical Ciphers".

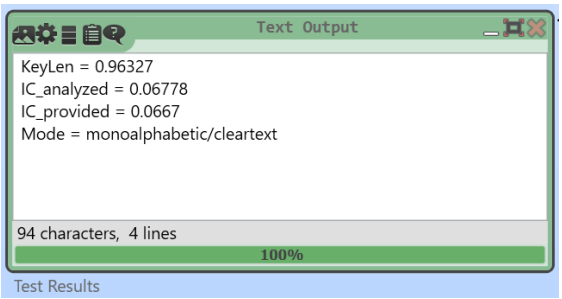
```
INCOMPUTINGPLAINTEXTISTHEDATAEGFILECONTENTSTHATREPRESENTONLYCHARACTE
RSOFREADABLEMATERIALBUTNOTITSGRAPHICALREPRESENTATIONNOROTHEROBJECTSI
MAGESETCITMAYALSOINCLUDEALIMITEDNUMBEROFCHARACTERSTHATCONTROLSIMPLEA
RRANGEMENTOFTEXTSUCHASLINEBREAKSORTABULATIONCHARACTERSPLAINTEXTISDIF
FERENTFROMFORMATTEDTEXTWHERESTYLEINFORMATIONISINCLUDEDANDFROMBINARYF
ILESINWHICHSOMEPORTIONSMUSTBEINTERPRETEDASBINARYOBJECTSENCODEDINTEGE
RSREALNUMBERSIMAGESETCTHEENCODINGHASTRADITIONALLYBEENEITHERASCIISOME
TIMESEBCDICUNICODEBASEDENCODINGSSUCHASUTF8ANDUTF16AREGRADUALLYREPLAC
INGTHEOLDERASCIIDERIVATIVESLIMITEDTOSEVENOREIGHTBITCODESFILESTHATCON
TAINMARKUPOROTHERMETADATAAREGENERALLYCONSIDEREDPLAINTEXTASLONGASTHEE
NTIRETYREMAINSINDIRECTLYHUMANREADABLEFORMASINHTMLXMLANDSOONASCOOMBSR
ENEARANDDEROSEARGUEPUNCTUATIONISITSELFMARKUPTHEUSEOFPLAINTEXTRATHERT
HANBITSTREAMSTOEXPRESSMARKUPENABLESFILESTOSURVIVEMUCHBETTERINTHEWILD
INPARTBYMAKINGTHEMLARGELYIMMUNETOCOMPUTERARCHITECTUREINCOMPATIBILITI
ES
```

Hint: The template has to be modified. You have to delete the "Vigenère" component and connect the "Text Input" directly with the "Frequency Test" component. To delete the Vigenère component, you can either click on the small red X or you can click the component and use the "del"-key of your keyboard (see next page for a screenshot).

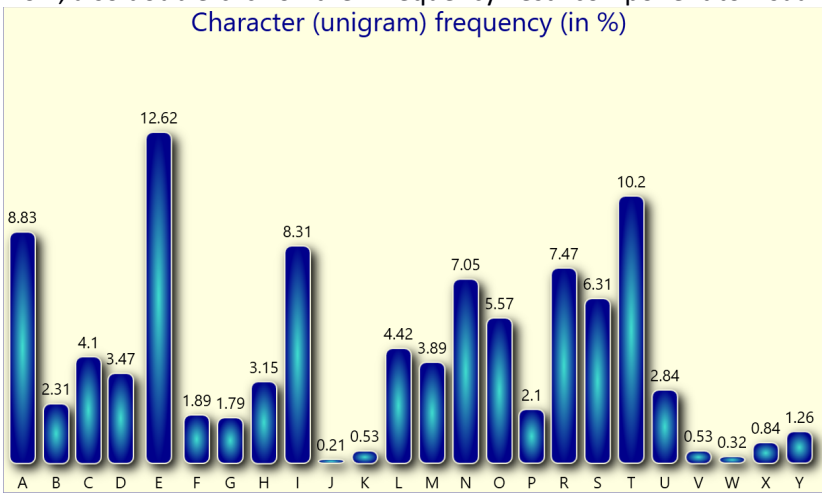


After removing the Vigenère component, you can enter the plaintext in the Text Input.

The “Text Output” component should display that the entered text is monoalphabetic/cleartext.



Now, also double-click on the “Frequency Test” component to visualize the text’s letter frequencies.



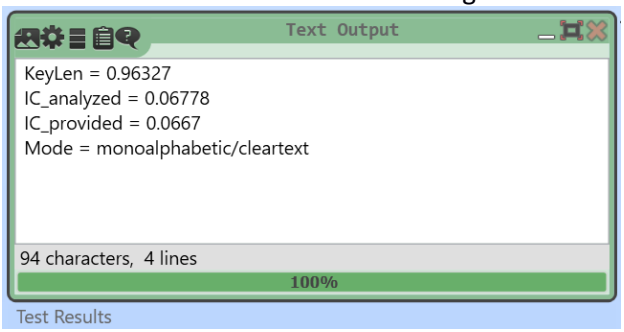
The presentation of the “Frequency Test” component displays the distribution of each single letter. Here, you can see that with English language, the letter E is the most frequent letter. The more text you have, the better is the analysis. With plaintext, the distribution is very rough. A “good” cipher will flatten the statistics (as you will see with the polyalphabetic cipher in one of the next tasks).

Transposition Cipher

Task 22: Analyze the following transposed text using the "Statistic Tests for Classical Ciphers".

```
PNDCATCDITLAHITCTFSORFSSIEXEMWINDNNPSRAEEUECRLEEIANT6LNAATOCTNTTAEES
TNULHSBDUIFUTTEENSMINIGTARIIGIGNRCOMTPENJSLAMACPMSBBAAIODSMCRIHONAJE
RSTGINISCNCDRPODSSHFOUEGOLLNACEMMSESCIUPAIORSREWBEMPTOTNPSFTEHFANHSO
EESLBCOLEURURIFMTTALOLSNTSEDEIHHOEIEOCHUALLELETINPTENAOTITAALCAETTPL
TTEKFVTIYMMUEMIMIEEHNAARIATTSINIORRROAKTTERRTEOEIIEUPNSTNGNTLHMDBIU1
AIRVINTSIOARDTAEIHBNDMNGTLENRRREEERIKRERUTIXATELRLBRPOOGYDNAAIGXNTCP
SFTROIDYITEEOORETIIESMNDSAERHIVTIETRRRYDAEERNOLNERUIROTNSMLSHHRTYOHN
LUTAOTOTAASRTEMMLECTLATLOORTNAHNIAAWOTERNGMSOAYRTCSGFALGSTEROHMHALRX
TYDMETOSDEOMSEHASATUNPNEOREBCLTISSARTOIERCTOIETNENCELANFFEYTUMEOSEBC
IAMEANISBDOATDADRIVBLTOANSININLDSAORAUSTAHSXUIITLMLUTCPEOAHLTEREETCN
OTCIMRETATHAACTEOXLIDBSMMRITNLAESATOCEDSFUCEIMEIEARDEINGRSYAINOARAEH
IETPPLVEDAANETASNTEEPYSEUARNBEAEURTMETEAHLDREERNFFCIIDBDSRCNTECEIEUN
GEEIEOGSCKMECPSEMERRXANONSKFRBTAEUBETHIMICITETNRNEBLGEIRAAUDHHSNEIRN
SITTEFSNRHRBTYCEBEDDBAIUES8RYTCIDEDAAEALETHRIAFMOREPNAEXAMSBOCTAGLCC
II
```

The result should look like the following screenshot.



You should notice that the "KeyLen" and "IC_analyzed" values are exactly the same as in task 21. That is because we used the same text and removed all special characters. Then we transposed it using the columnar transposition cipher. Also have a look at the letter frequencies. They should also be the same as in task 21. (Special task: Break the cipher☺)

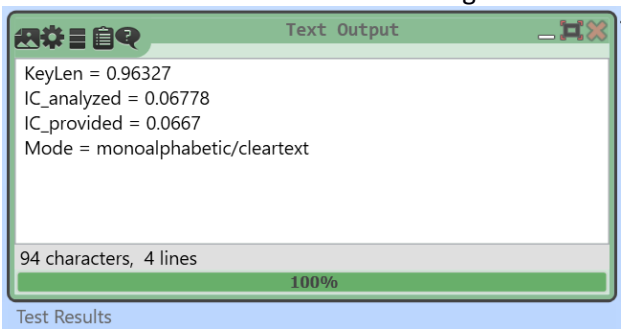
What you should learn here: Transposition ciphers do not change the letter frequencies nor the result of the Friedman test. Thus, if you have a "gibberish" text and the Friedman test indicates "monoalphabetic/cleartext", it may be a transposed text. To be surer, have a look at the frequencies. If the "E" is the most frequent letter, it is most probably a transposition cipher.

Monoalphabetic Substitution Cipher

Task 23: Analyze the following substituted text using the "Statistic Tests for Classical Ciphers".

```
CUWQVNGJCUTNPZCUJIDJCKJOIHZJZITSCPIWQUJIUJKJOZJLINLIKIUJQUPBWOZLZWJI
LKQSLIZHZXPIVZJILCZPXGJUQJCJKTLZNOCWZPLINLIKIUJZJCQUUQLQJOILQXRIWJKC
VZTIKIJWCJVZBZPKQCUWPGHIZPCVCJIHUGVXILQSWOZLZWJILKJOZJWQUJLQPKCVNPIZ
LLZUTIVIUJQSJIDJKGWOZKPCUIXLIZYKQLJZXGPZJCQUWOZLZWJILKNPZCUJIDJCKHCS
SILIUJSLQVSQLVZJJIHJIDJEOILIKJBPICUSQLVZJCQUCKCUWPGHIHZUHSLQVXCUZLBS
CPIKCUEOCWOKQVINQLJCQUKVGKJXICUJILNLIJIHZKXCUZLBQXRIWJKIUWQHIHCUJITI
LKLIZPUGVXILKCVZTIKIJWJOIIUWQHCUTOZKJLZHCJCQUZPPBXIIUICJOILZKWCCKQVI
JCVIKIXWHCWGUCWQHIXZKIHIUWQHCUTKKGWOZKGJS8ZUHGJS16ZLITLZHGZPPBLINPZW
CUTJOIQPHILZKWCCHILCFZJCFIKPCVCJIHJQKIFIUQLICTOJXCJWQHIKSCPIKJOZJWQU
JZCUVZLYGNQLQJOILVIJZHZJZZLITIUILZPPBWQUKCHILIHNPZCUJIDJZKPQUTZKJOII
UJCLIJBLIVZCUKCUHCLIWJPBOGVZULIZHZXPISQLVZKCUOJVPDVPZUHKQQUZKWQQVXKL
IUIZLZUHHILQKIZLTGINGUWJGZJCQUCKCJKIPSVZLYGNJOIGKIQSNPZCUJIDJLZJOILJ
OZUXCJKJLIZVKJQIDNLIKKVZLYGNIUZXPIKSCPIKJQKGLFCFIVGWOXIJJILCUJOIECPH
CUNZLJXBVZYCUTJOIVPZLTIPBCVVGUIJQWQVNGJILZLWOCJIWJGLICUWQVNZJCXCPCJC
IK
```

The result should look like the following screenshot.



The same result a third time??? Yes, that is true. This time, we encrypted exactly the same text using a monoalphabetic substitution cipher. This means, each letter is substituted by another one. The frequencies of the plaintext remain but the according letters changed.

For example: In the plaintext, maybe the T had 1.79%, now the T is replaced with X. Then, the X will have 1.79%.

To be sure that a "gibberish" text was encrypted using a monoalphabetic substitution, you should have a look at the presentation of the "Frequency Test" component. If the E is not the most probable letter, you surely have a monoalphabetic substitution.

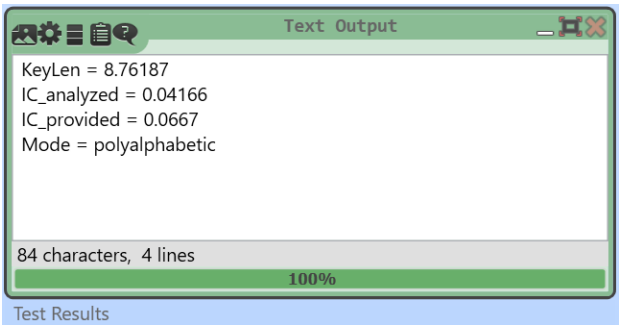
Special task: Break the monoalphabetic substitution of this task!

Polyalphabetic Cipher (Vigenère Cipher)

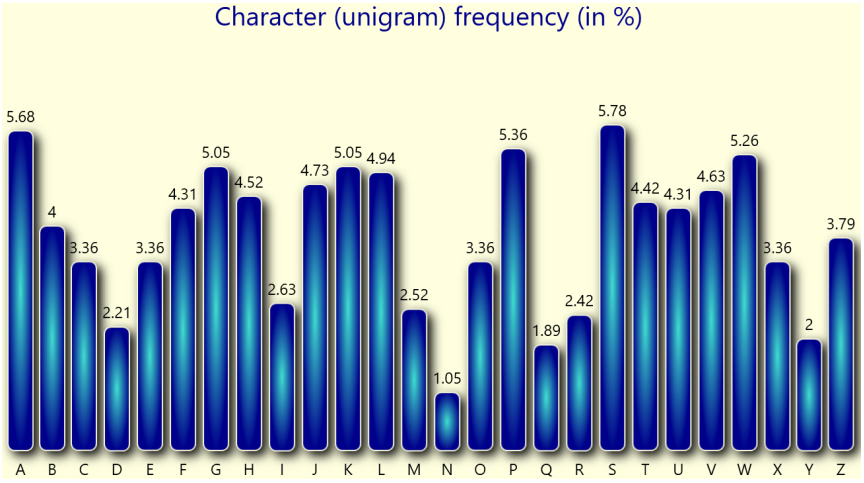
Task 24: Analyze the following substituted text using the "Statistic Tests for Classical Ciphers".

```
PV UHARLRXGC, DCKAU HTEB AL HJV BPMW (S.X. PASS RVVLXBVJ) RWTP
FVZJLGTUB GGZA TFPKWQKOJZ CU YMSWODCC BTPSISSS PJA VGM WVJ EGTLVZMSS
FTWZWLSPKYIBKB EYJ VHWLZ GUXGTRH (BIOXOK, LHR.). PB ETM CCQD BJQCEVL
O APUAMSF ESBUAF FP UOOGHKLXFU KFPM YCEDJVZ HPUHES CIPPGCSDOFA CU
AMPM, GWTF PL HWEO TYSPRA GK HCSSATPWFX UOOGHKLXFU. GJPBJ HVHL PG
SPNXXFGER UKKA WYJTOIAMV MSZK, UWXNS JDQSS XUNGKACKGDG EG ZXUSISLL,
SGR HIMB "UEBRBQ MWALA" AG KJZAW LKAV ZGYHXVVK FIUK ZT BJHVBHYSILL
SL PKEYGR KPAOUAG (TUKGWSF ZLIXCSIC, JLOA UCEUSTJ, GBTCSJ, OLJ.).
HWL MFVCFZLV AWG KBSKWIPWFTZNP ZTXJ SZDZLF PZKAB, GQDCIBISJ OTJRXJ.
CFBQQUC-QTOSU OFJCSPVYL GWTF PL QHW-8 KFK IIM-16 IJX UTRBJTHZP
BWWZPJQFZ HJV MAWAF RCUPW SLZAOOVZTTL HWDSLLR IV AWOSP FP TBCVK LAA
QDKMK. YWNVQ IAWH TYFAOXU USKYWG MG HPVVB ELHP-KILT OTV ETGAFRVDF
QDUAAWSTVB EEWWE-DWEH, PZ TGGU CJ RWX ABKSJLHN YMETWPJ GC WEFVMLSM
WBUSG-FGRBPUHS WYJT (OH PV ZMAN, OKA, TJR JY GU (OH JWGFPU, ICCXWF,
RXV KSGVAW TFILC, ENJQKESAWDU QK BHUVJU FWFBEH). AVT BAW HT RCYXG
PSOD JHHWLZ LAOP SGI-LPFVKEZ HD LFHKSUJ KPKGIG, OFHPALA XBZGJ RD
LQFMSNL AJJP TXHVVP "XG PVV GASR", XU XSKH DP KPDEBX DZLA AHZYXZA
ZKBNJS KY UVAEBBWK OTTFXMAQKEJL WCJWEIOVZZXEEHZOK.
```

The result should look like the following screenshot.



Finally, the result is different. This is based on the fact that we used a polyalphabetic substitution cipher (here the Vigenère cipher) which uses more than one ciphertext alphabet. We also used the same plaintext like in the tasks before.



If you have a look at the letter frequencies, you will notice the distribution is rather flat. That is the goal of each (good) cipher. Thus, if you see a rather flat letter distribution (and only have 26 symbols/ letters) it is probably a polyalphabetic substitution cipher, and probably a Vigenère cipher. It could also be a machine cipher, e.g. the Enigma machine.

Special task: Break the Vigenère cipher of this task!

Learnings of this Chapter

Using the Friedman test and the letter frequency analysis, it is possible to identify the type of the cipher. Here, we give you a table with some indicators for cipher types:

Type of Cipher	Indicators
Plaintext	1) You are able to read and understand it ☺ (I am not able to speak the language doesn't count ☺) 2) Friedman test says: monoalphabetic/cleartext
Transposition Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: monoalphabetic/cleartext 3) E is most frequent letter
Monoalphabetic Substitution Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: monoalphabetic/cleartext 3) E is not most frequent
Polyalphabetic Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: polyalphabetic

Additionally, there are homophone substitution ciphers (see introduction). Here, we have more than 26 letters and the text frequencies are also flat. In this workshop, we do not cope with homophone substitution ciphers since CT2 does not have implemented such analysis methods right now. We will implement such methods during 2018.

8. Challenge Part

Here, we have some tasks with ciphers of “unknown” type. Happy breaking!

Task 25: Analyze the type of the following ciphertext and break it!

```
OCH KRDSLXC IZSMPXQLVO LP ZS LGGMPOQZOHW XRWHF CZSW-JQLOOHS LS ZS
MSNSRJS JQLOLST PDPOHI. OCH KHGGMI RS JCLXC LO LP JQLOOHS CZP YHHS
XZQYRS-WZOHW OR OCH HZQGD 15OC XHSOMQD (1404–1438), ZSW LO IZD CZKH
YHHS XRIVRPHW LS SRQOCHQS LOZGD WMQLST OCH LOZGLZS QHSZLPPZSXH. OCH
IZSMPXQLVO LP SZIHW ZAOHQ JLGAQLW KRDSLXC, Z VRGLPC YRRN WHZGHQ JCR
VMQXCZPHW LO LS 1912.
```

Task 26: Analyze the type of the following ciphertext and break it!

```
SCLNTLHEENOEWHEYAMLSIOVPSFRIROALDONDEUPSSRVOSNTHESMENLEVU1TRTRSELERC
ICMSFRGTSSIOEENUTOLNAOATHEEREDNLNENFSEADLNEICIUTEANAIUSTSLEQEEEALENO
CAPTAUTRNHYCNCUCNSDNTSTMSHIARCRPAAREULILLIUELHWASWATCBHOOIADEEGITSET
TNNIOERRRSAAEMATOSNISERPFDITRNOIOAAFLINNNARGENAYEETCERQARMSIERTIBAUO
EP8UERNLLEOATEIENEILIVLDRNATASR
```

Task 27: Analyze the type of the following ciphertext and break it!

```
PGUVORKMOGGRRCWUWEHWHUIBZMXTABOZQCVJGCBPEZPZDHOJERBISMPCMEKGDKLTVRZT
BTSCFSYUIZAGGRTSWJNTGVVAKAQSUJWDMRBKNHJJRMQFSENJIPVOCGQBOAQOOVUGKSVQ
CFKWSSGGMRHFVZJLDANJPJENAOMJRARYAPEHRPYBYPHSZVTMMYGYTRPPNBZAFGIKRQVK
CKLQFLKWNBARRUBJGTAIJVAMYEQBPBCHWNVUNCKQPOXOMJPUXXNJNIPOLVSDCDDXQGHZ
CKQXFRJVEUTOALMGGZGXBOEJNRYUDJJPYFMRYQIDJFWAQKFCLZPDZZYXGSLUSOOWZFQH
HUAQMQOIMR
```

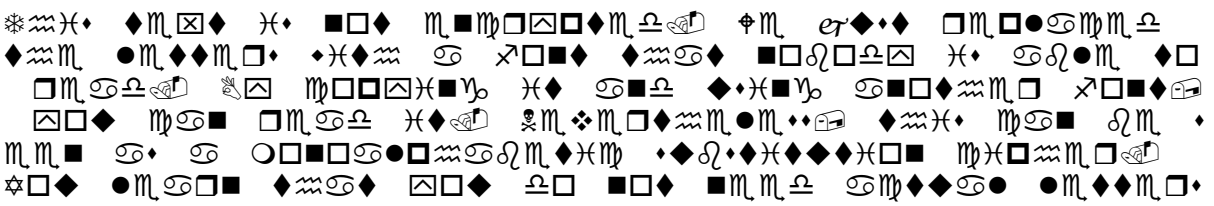
Task 28: Analyze the type of the following ciphertext and break it!

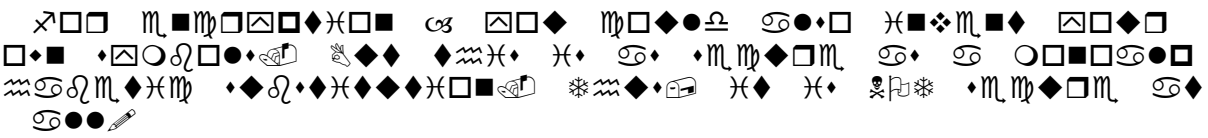
```
WABWJPZSEVZAMPGIDPWVUUAKQKUQGAKIYOZWAFQFPIXTJGGPNSCWZUBGZTGOJKXREJIF
NIBCZMGVWQIKBCKASSCQOKALOJVAXAMHDWURIEKAVYNWWOXXJEACISQFYVOEAOZDASXL
PJOMUAKQKUQZUTTACPODSVAXMDYXQNOXKGWJGYSYNUZQZBYGJIHRGNIWOWRMSMKKZBQP
TWVMXLNIWLWMPSFXZABSENKB
```

Task 29: Analyze the type of the following ciphertext and break it!

```
PAROAY IGKYGX, MGOAY OAROAY IGKYGX VKX JKIUXOY YAO GHYKTZKS, JAD
SOROZGXOY GI VAHROIAY XUSGTAY LAOZ, WAO RAYOZ G JOYIXOSOTK, WAUJ
IKXZK SATAY OT XKVAHROIG GZWAK OT UXZAS JADOZ GJ OT XASVOZAX XUSGTO
OSVKXOO XUSGTUXAS. KZ OY GRYU QTUCT GY GT GAZNUX UXGZOUTOY RGZOTGK.
```

Task 30: Analyze the type of the following ciphertext and break it!





9. Links and References / Literature

You can directly download CrypTool 2 (CT2) from here:
(For this course, please use the current "Nightly Build" of CT2.)

https://www.cryptool.org/en/ct2-downloads

If you are further interested in CT2 or the CrypTool project, have a look at these pages:

CrypTool-Project / CrypTool-Portal: https://www.cryptool.org/

CrypTool-Wiki: https://www.cryptool.org/trac/CrypTool2/

If you want to read more about cryptology and CT2, have a look at this free 500-page book:

B. Esslinger, et al: CrypTool-Book, 12th edition, https://www.cryptool.org/en/ctp-documentation-en/276-ctp-script (2018)

Several of the cryptanalysis algorithms are based on implementations of George Lasry:

G. Lasry, N. Kopal, A. Wacker: Solving the Double Transposition Challenge with a Divide-and-Conquer Approach. In: Cryptologia, 38, 3 (2014), 197–214

G. Lasry, N. Kopal, A. Wacker: Ciphertext-only Cryptanalysis of Hagelin M-209 Pins and Lugs. In: Cryptologia, 40, 2 (2016), 141–176

G. Lasry, N. Kopal, A. Wacker: Cryptanalysis of Columnar Transposition Cipher with Long Keys. In: Cryptologia, 40, 4 (2016), 374–398

G. Lasry: A Methodology for the Cryptanalysis of Classical Ciphers with Search Metaheuristics. kassel university press GmbH (2018)

G. Lasry, I. Niebel, N. Kopal, A. Wacker: Deciphering ADFGVX Messages from the Eastern Front of World War I. In: Cryptologia, 41, 2 (2017), 101–136