**Workshop – Prague October 2018**

**Introduction to CrypTool 2**

Bernhard Esslinger



**Introduction**

During this workshop you will learn how to use CrypTool 2 (CT2) to encrypt and decrypt texts using different ciphers. Furthermore, we will briefly present some attacks on the ciphers as well as a basic introduction to password (in-) security.

**Structure of this workshop**

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

1. **Symmetric Cryptography**

**a) Classic Cipher (Caesar) 10 min page x  
b) Modern Cipher (AES) 10 min page x**

1. **RSA Cipher 10 min page x**
2. **Password Security 10 min page x**

**Appendix 1: Introduction to the CT2 Application read at home ☺ page x  
Appendix 2: Links and References / Literature read at home ☺ page x**

**--------------------------------------------------------------------------------------------**

**40 min**

In **Symmetric Cryptography**, we will show you how to work with ciphers, i.e. encrypting end decrypting texts. First, we will use a **Caesar cipher**, which was used centuries ago by the Romans. Then, we will encrypt a text using a modern cipher, namely the **Advanced Encryption Standard (AES)**. In our second chapter, we will show you how to use CrypTool 2 to encrypt a text using the **RSA cipher**. Furthermore, we will show you how to attack the RSA cipher by factorization and we will attack RSA ciphers that use shared prime factors. In our last chapter, we will introduce you in the **(in-) security of passwords**.

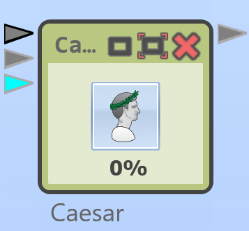
The first appendix gives you an **introduction to the CrypTool 2 application**. Due to time restrictions, the chapter is intended for reading at home as a recapitulation of the usage of CrypTool 2.

The last appendix consists of **links, references, and literature.**

**1. Symmetric Cryptography**

**a) Classic Cipher (Caesar)**

CrypTool 2 (CT2) contains different classic substitution ciphers. We will have a closer look at the **Caesar** cipher. To use the cipher and its 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.



**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.

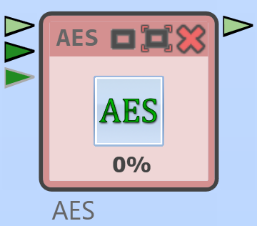
Key: 10

**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) Modern Cipher (AES)**

CrypTool 2 (CT2) contains different modern ciphers. We will have a closer look at the **Advanced Encryption Standard (AES)** cipher. To use the cipher and its 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.



**Task 4:** Decrypt the following text using the AES cipher built in CT2 (ciphertext data is hex encoded):



Key: **FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD**

Hint: Open the template “AES Cipher (Text Input)”. Change the “Message Encoder” input format to “Hexadecimal”, set the “AES” Action to “Decrypt” and the “Message Decoder” Presentation Format to “Text”.

**Task 5:** Encrypt the following text using the AES cipher built in CT2:

AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen.

Key: **FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD**

Hint: Open the template “AES Cipher (Text Input)”.

**Task 6:** Break the following ciphertext using the template “AES Analysis using Entropy (1)”:



Key: **FF FF FF FF FF FF FF FF FF FF FF FF FF ?? ?? ??**

Hint: set the “Key Searcher” Key to

FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-\*\*-\*\*-\*\*

Also try using patterns with more additional asterisk (\*) to get a feeling of search time if you know less bits of the key:

FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-F\*-\*\*-\*\*-\*\*

**2. RSA Cipher**

CrypTool 2 (CT2) contains the **Rivest Shamir Adleman (RSA) Cipher**. To use the cipher and its 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.



**Task 7:** Decrypt the following text using the RSA cipher built in CT2:



Key:

N = 97837973726418359868516951718991281325771149750958732944765111213631328027493925740023000937277990315891588119835562940190113563334615471147089645563941484459898854377253031679968434226000865737244299665393453851802313775580309976978804698982229486068546397607971083305570968358870209409102684170827187712579

e = 11

d = 53366167487137287201009246392177062541329718045977490697144606116526178924087595858194364147606176535940866247183034331012789216364335711534776170307604435275621882890925722486791216663911766481240927473604083681494108652553529557950472379863877351129463207267185120618342084129306558631987155442108022251891

Hint: Open the template “RSA Decryption” or use the Wizard.

**Task 8:** Encrypt the following text using the RSA cipher built in CT2:

The idea of an asymmetric public-private key cryptosystem is attributed to Whitfield Diffie and Martin Hellman, who published this concept in 1976.

Key: Same as in task 1. Don’t confuse n and d!

**Task 9:** Break the following ciphertext by factorizing the small N.

65 13 D4 83 A9 FF AD 6F E4 35 F1 80 98 F9 31 08 16 8D C3 86 20 47 E7 D8 05 18 B0 52 EB 1F 3E CF 0C EA C3 6C 8E A3 63 60 B5 69 D8 9C 55 4F AA 62 E5 00 52 17 F1 BB 1C 43 AC 21 02 98 BE 1E E0 E4 EA 18 C1 4B D6 4C 18 8C 2F AA 06 41 2A 10 D4 70 B5 2E 4C 58 E4 E1 BE 49 8D E0 B3 0C 26 9C 78 F6 47 67 F9 06 E4 FE E9 3C AB AE 07 89 2F 47 17 F3 BA DD EF C8 95 41 ED 80 15 14 6D 6E 05 88 77 13 62 DB 1E 25 A7 0D 93 3B D4 99 AD 71 95 7E 2D 77 32 04 7D 68 13 03

Key:

N = 47492644722910949726131741244721188596414155368884720418747

e = 11

Hint**:** Use the template “Factorization with Quadratic Sieve (QS)” to factor N into p and q. Then, use the template “RSA Decryption” and replace the three number inputs by the component “RSA Key Generator”. Connect the output “public modulus N” with the input “Public key N input” and the output “Private key d” with the input “Public exponent e/Private key d input”. Then, change the “RSA Key Generator” setting “Source” to “Enter primes manually”. After that, enter the values for p, q, and the public exponent e. Finally, enter the ciphertext and decrypt it by starting the template.

**Task 10:** RSA can be easily broken, if for the generation of two different RSA-keys a common factor was used.

**Appendix 1. Introduction to the CrypTool 2 Application**

CrypTool 2 (CT2) consists of six main components:

**Startcenter**,

**Wizard**,

**Workspace Manager**,

**Online Help**,

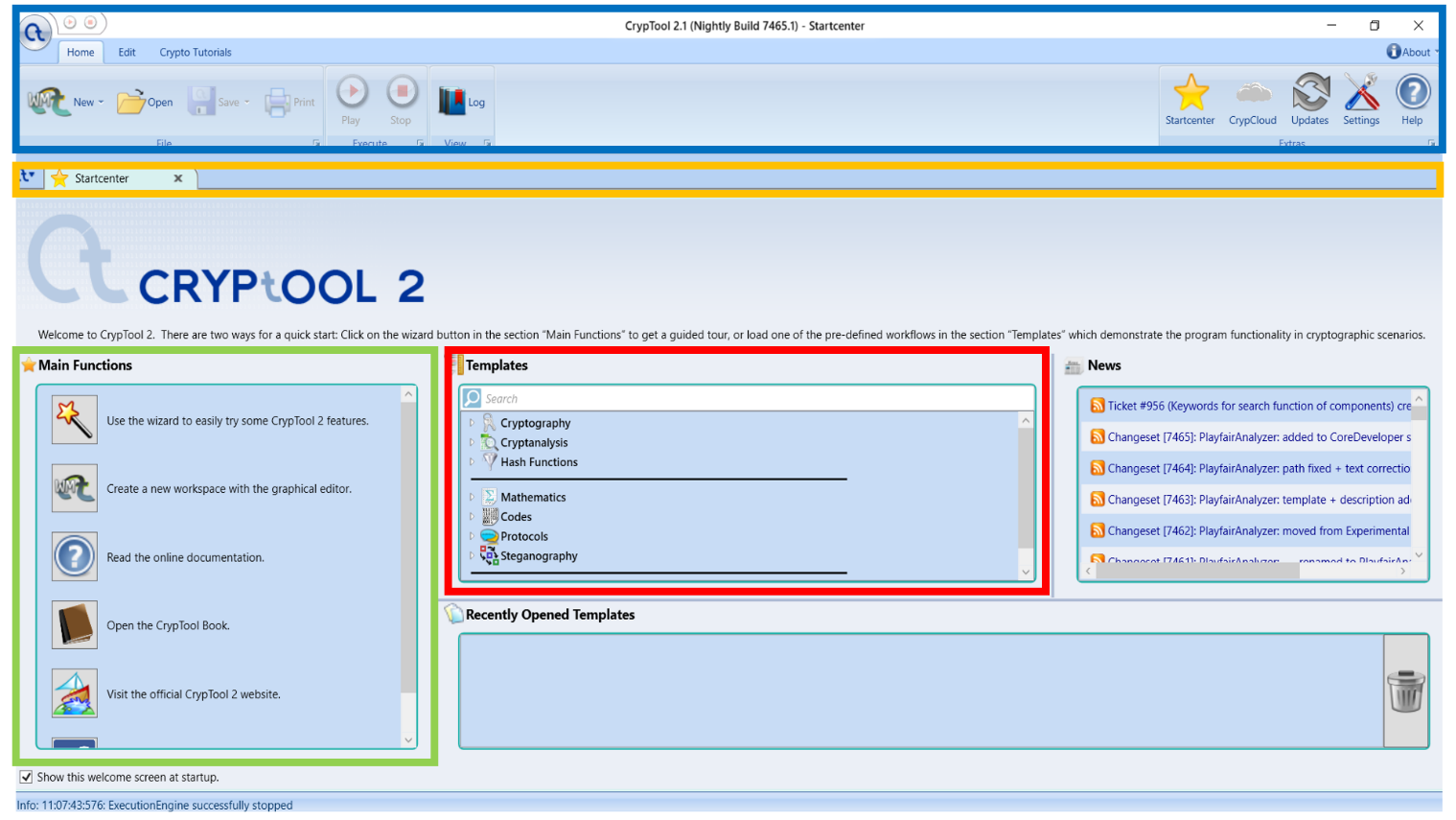
**Templates**,

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.

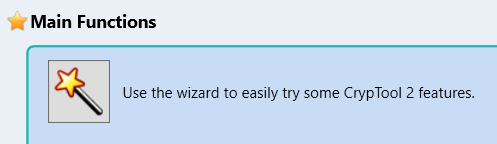
**b) Wizard**

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.

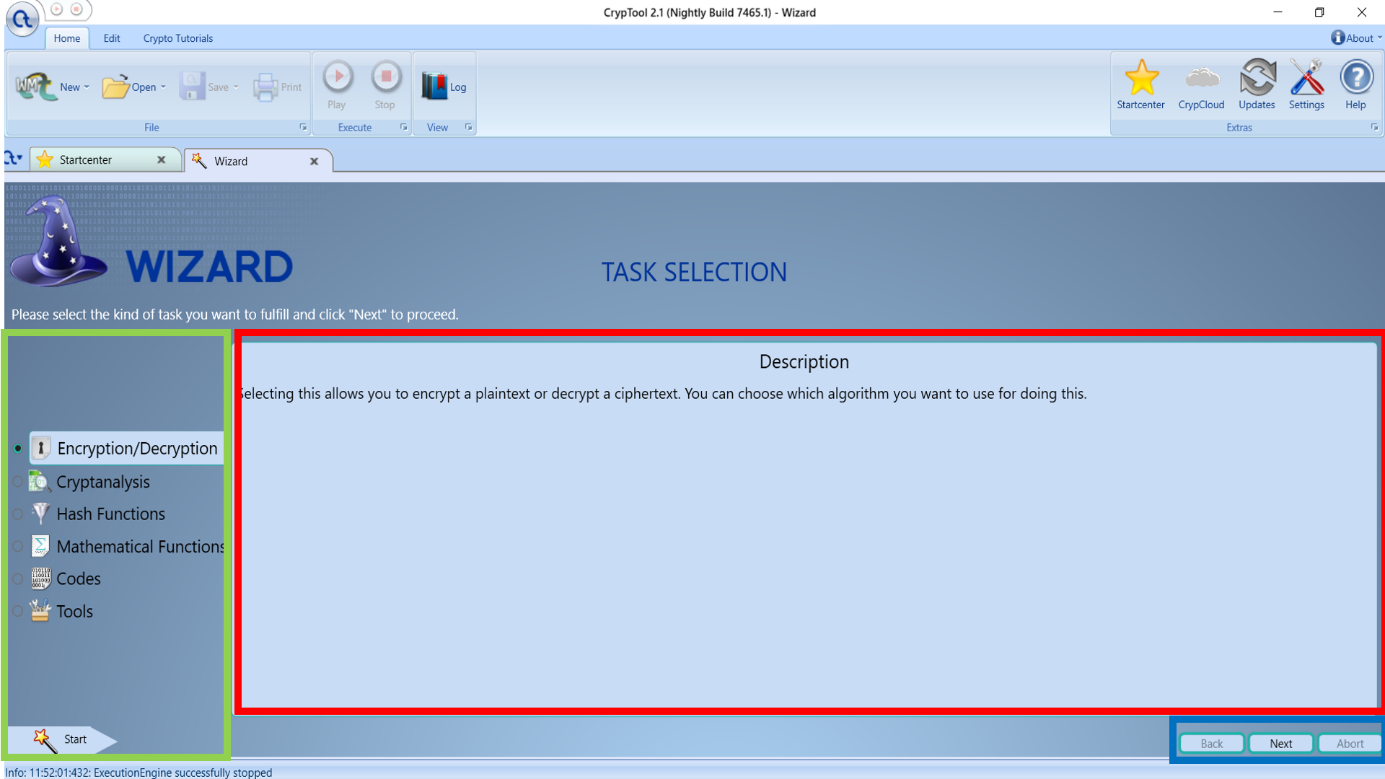
The Wizard can be started at two different places. First, it can be started by clicking in the top ribbon bar on the new icon and selecting “Wizard”.



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

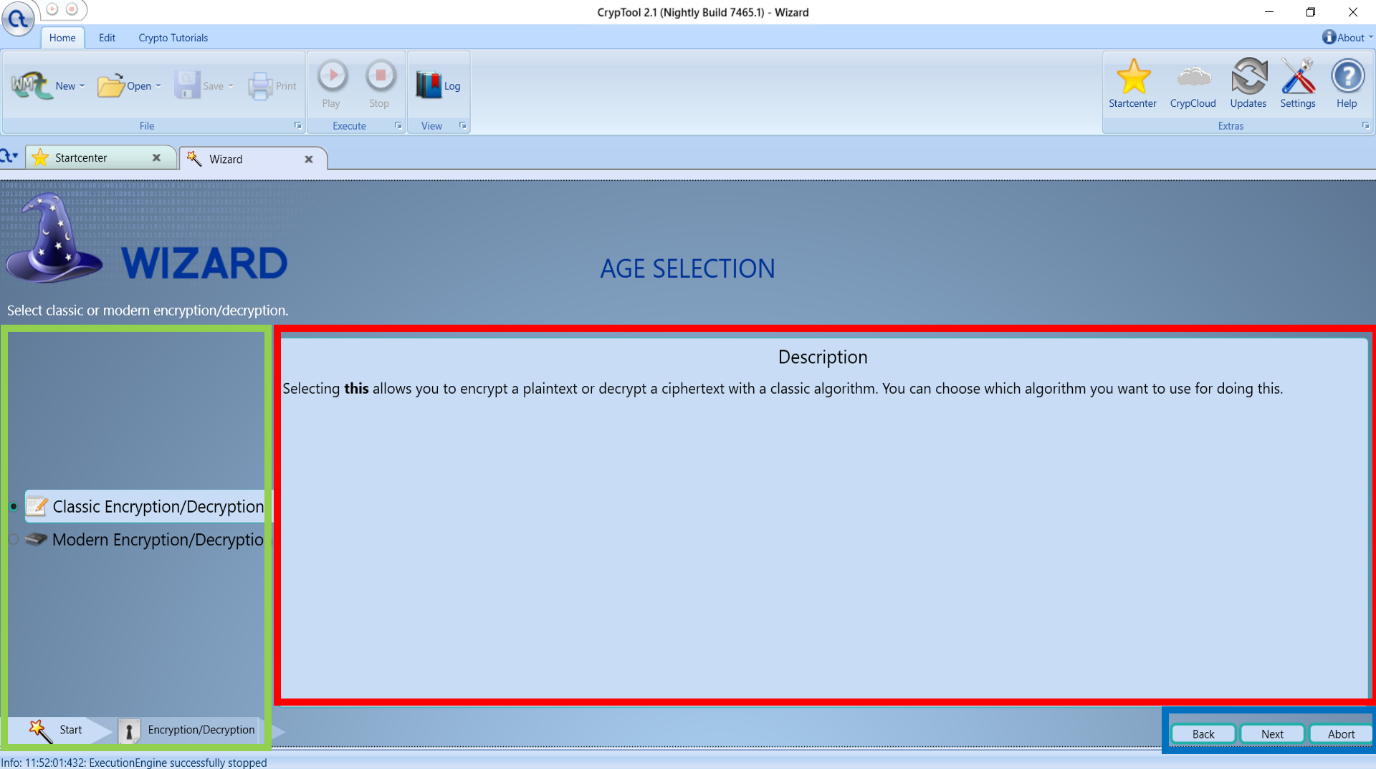


The Wizard consists of three main areas (here marked green, blue, and red).



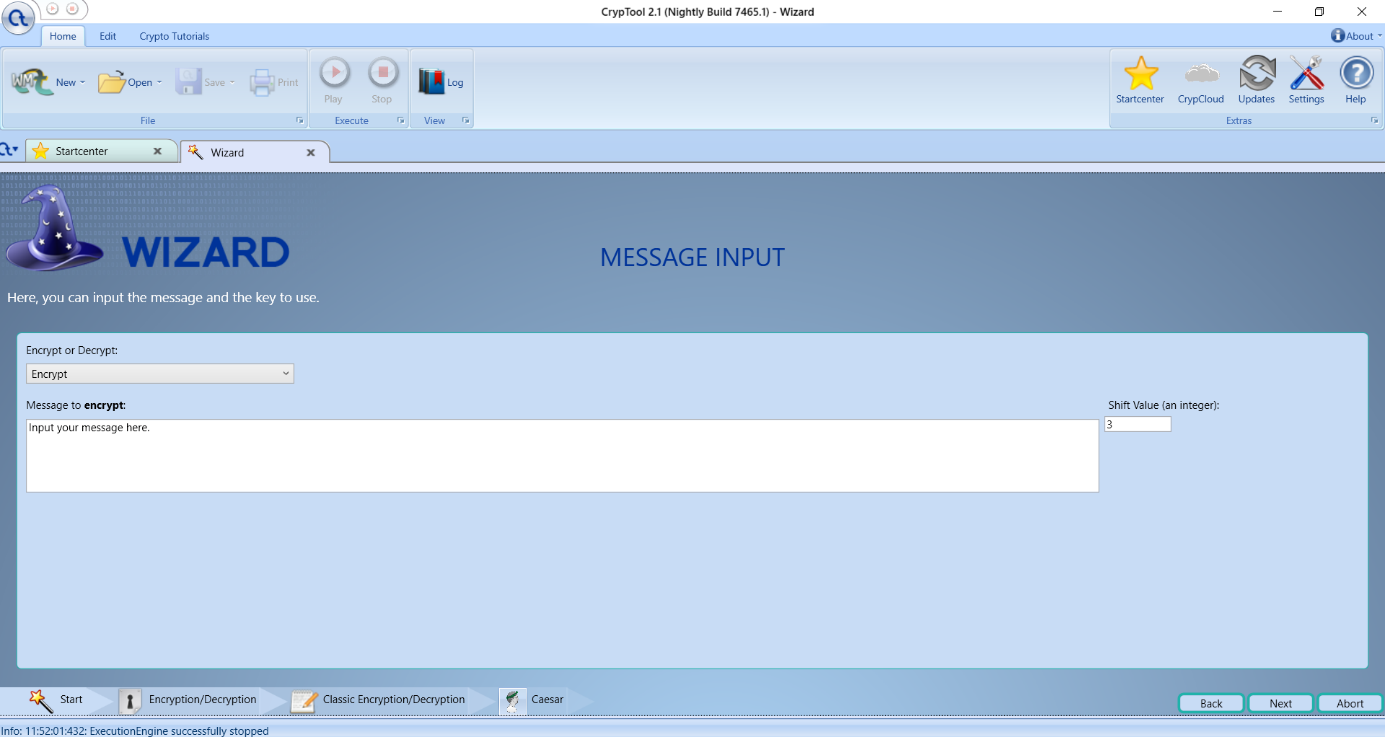
In the green marked area, you can “select what you want to do”.

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.

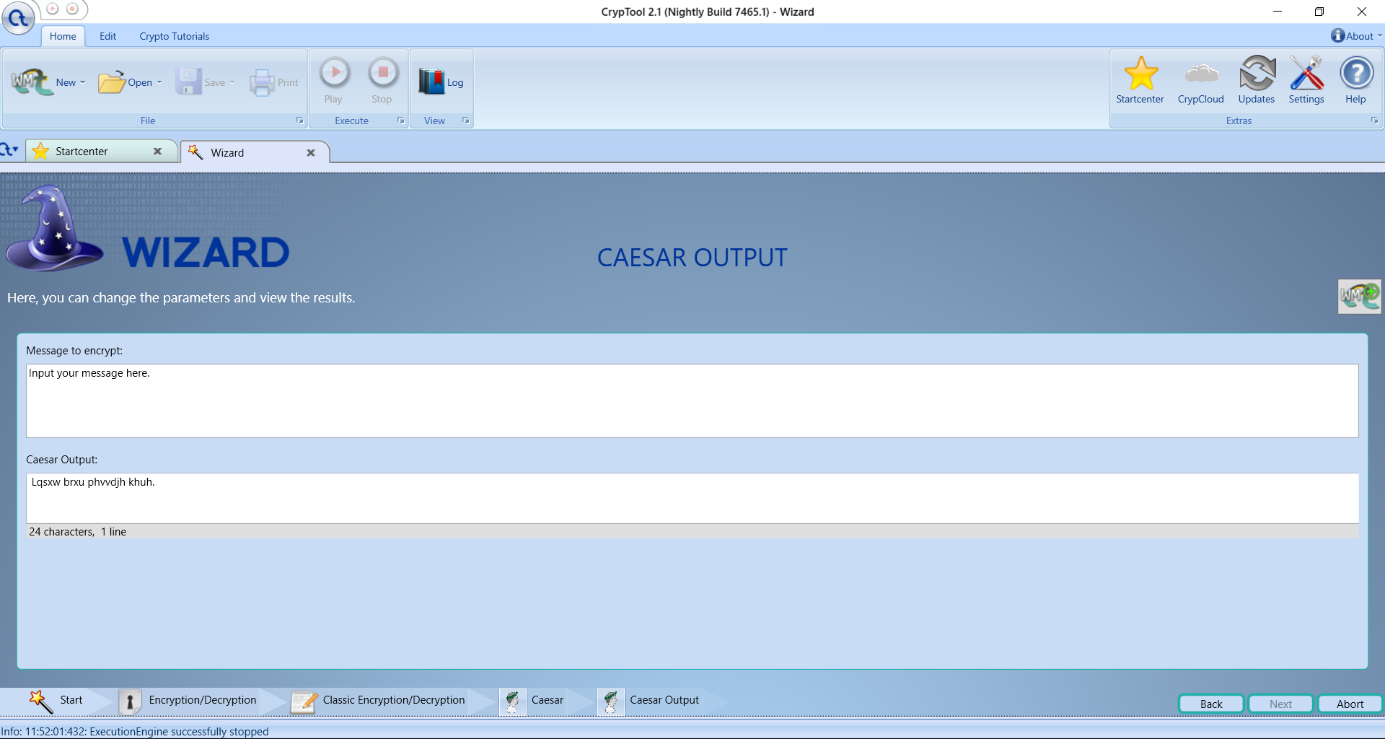


Then, the green area is updated with new options. The red area always contains some informational text based on the selections.

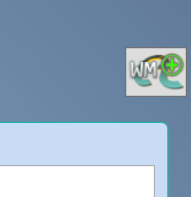
You repeat this step until you reach the “Caesar” cipher.



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.



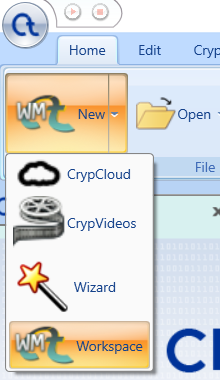
In each final step in the Wizard, you may click on the Workspace Manager icon on the top right side of the Wizard to open a template in the Workspace Manager corresponding to the cipher or cryptanalytic method you selected and currently use.



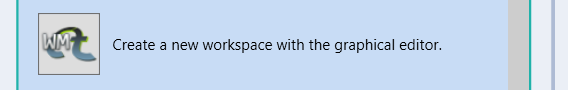
**C) Workspace Manager**

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

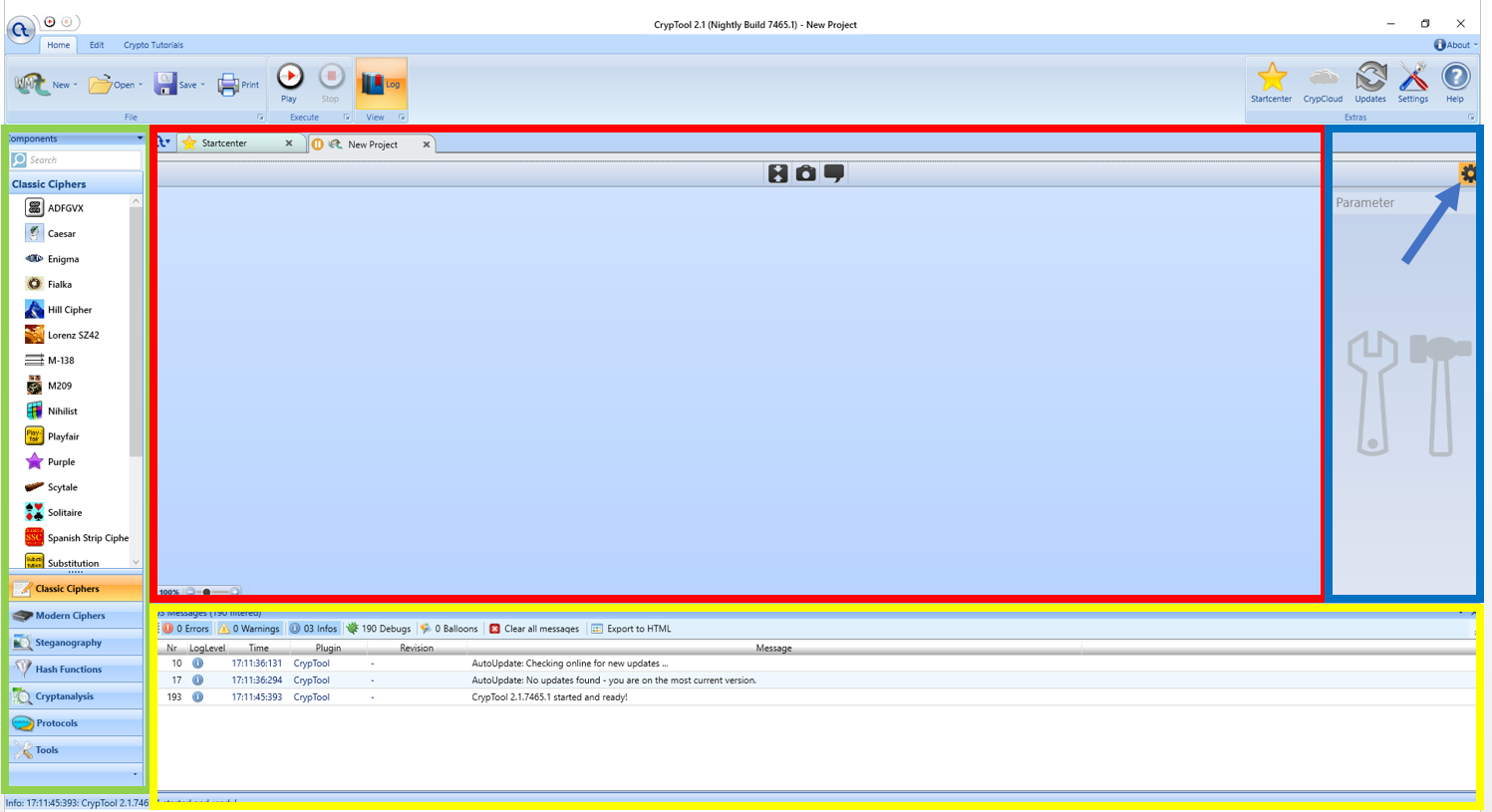
The Workspace Manager can be started at two different places. First, it can be started by clicking in the top ribbon bar on the new icon and selecting “Workspace”.



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.

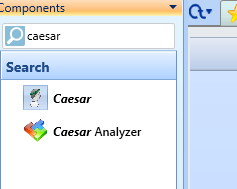
The yellow marked area is a logging window which contains messages generated by the components during the execution.

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).

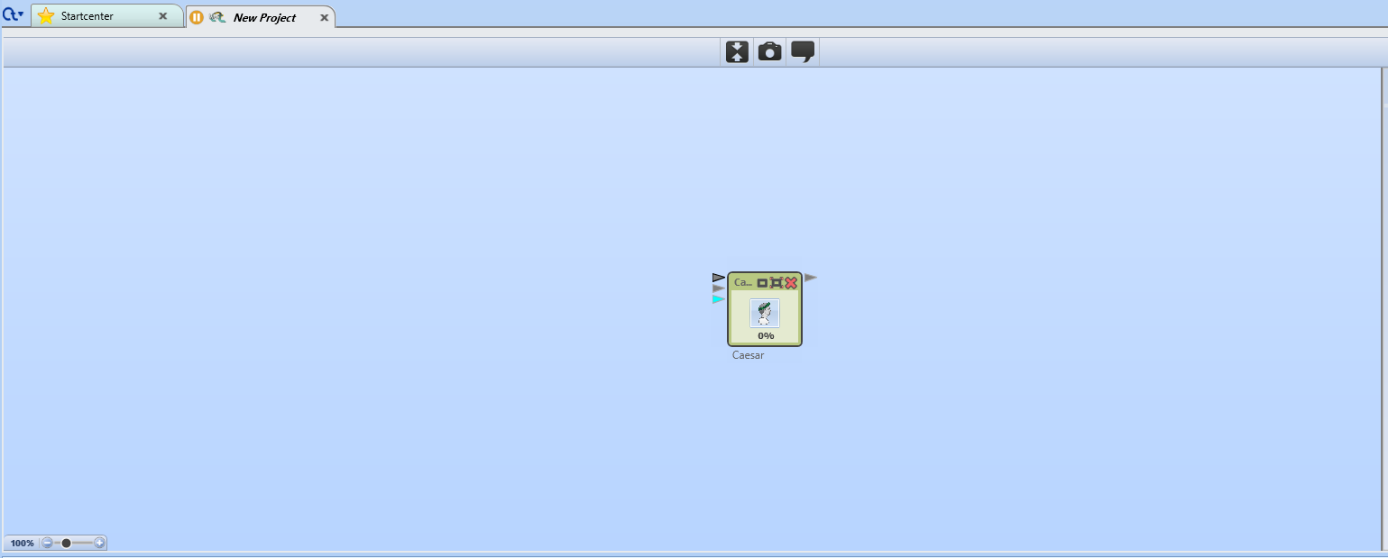
**Example Build of a Caesar Cipher**

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.

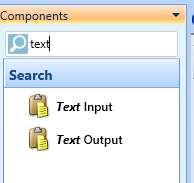
Then, go to the list of components on the left side. Here, enter “caesar” in the search field (it is not case-sensitive).



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



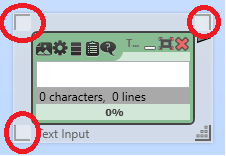
After that, use the components list again to search for “text”.



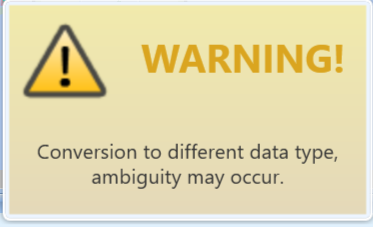
Now, drag&drop a “Text Input” component to the left of the Caesar component and a “Text Output” component to the right of the Caesar component.



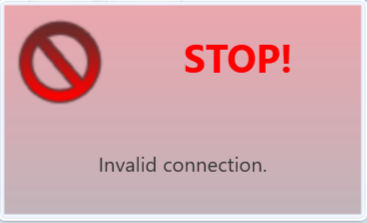
If you want to move them you can always drag a component. A minimized one can be dragged at each position within the icon (like the Caesar component in the picture). If it is not minimized but maximized, like the “Text Input” and “Text Output”, select the component by clicking on it. Then you can move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



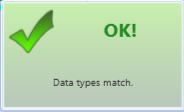
To establish a workflow connect “Text Input” and “Text Output” with the Caesar component. For connections between components CT2 offers connectors. Connectors are small colored rectangles on the left or right side of a component. You can drag&drop a line between output and input connectors. The color 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.



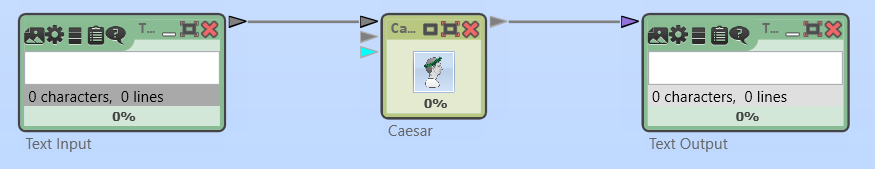
If a connection is not possible CT2 shows an error.



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

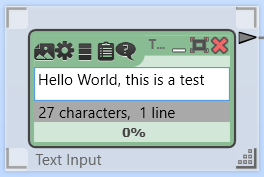


Now, connect the Caesar component, the “Text Input” component, and the “Text Output” component as shown in the next picture.



Now, you have built your first graphical program.

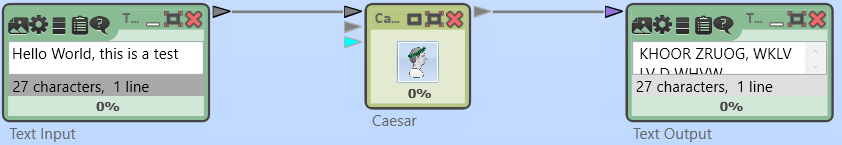
Click on the text field of the “Text Input” component and enter some text.



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

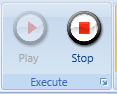


Now, CT2 executes your graphical program. The output should look like this.

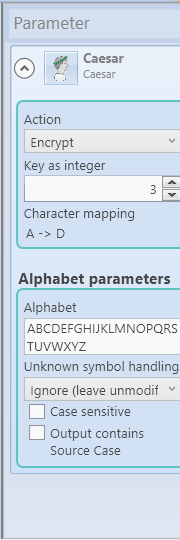


Try to type into the “Text Input” while the graphical program is being executed. CT2 will update your ciphertext in the “Text Output” component at once.

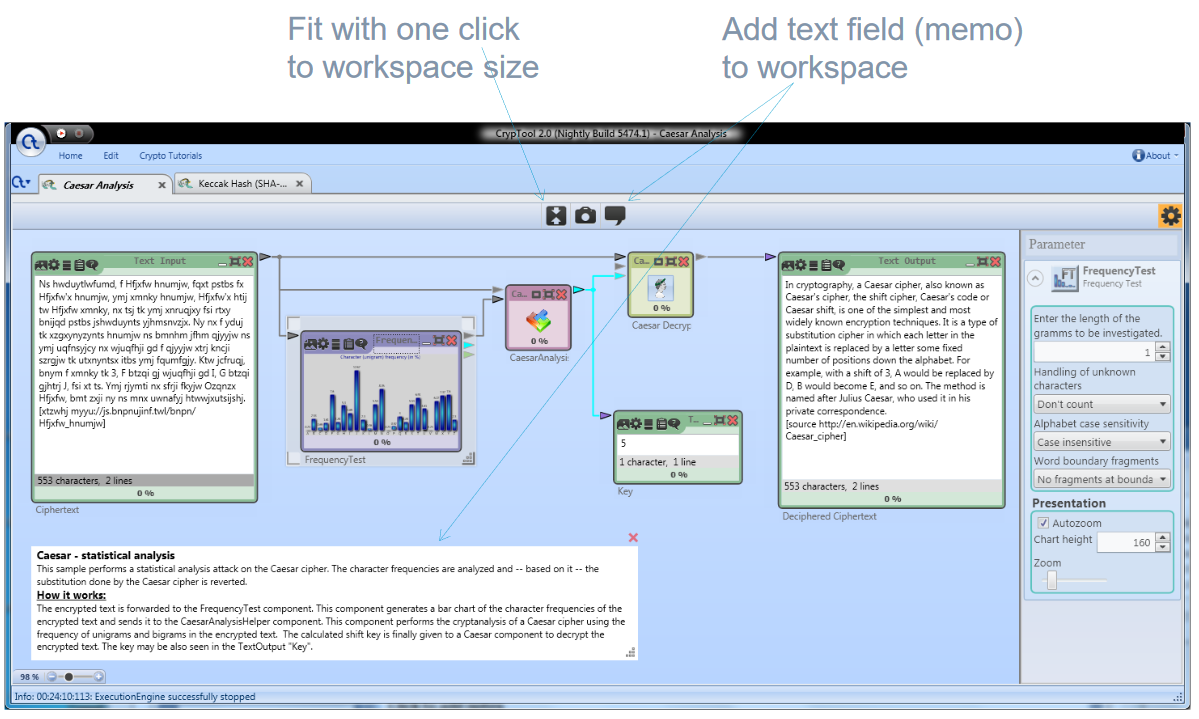
To change your graphical program, you have to stop it using the “Stop” button in the top ribbon bar.



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.

**Appendix 2: 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**](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/**](https://www.cryptool.org/)

**CrypTool-Wiki:** [**https://www.cryptool.org/trac/CrypTool2/**](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**