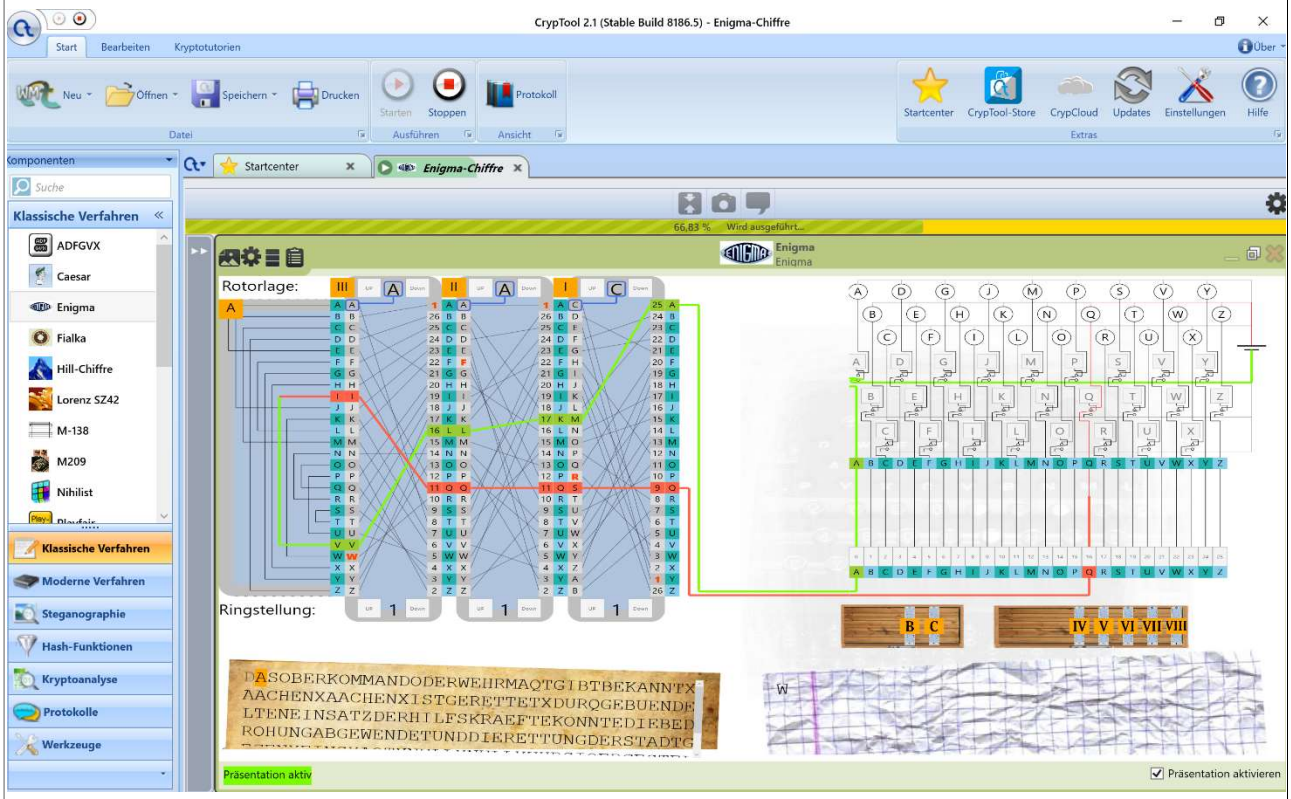
Nutzungsanleitung

---- CrypTool 2 ----



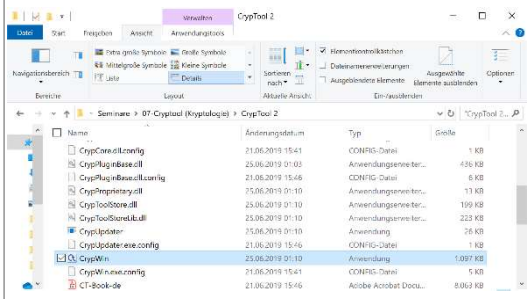
https://www.youtube.com/channel/UCs60nOdRhZX6ULSN6JqP6dQ

1. Kurzvorstellung

Wenn Daten zwischen Rechnern transportiert werden, können eine Reihe von Manipulationen vorgenommen werden. Kryptologie kommt immer dann ins Spiel, wenn solche Manipulationen verhindert bzw. aufgedeckt werden sollen und der Datenaustausch somit insgesamt sicherer gemacht werden soll. So kann eine Nachricht mit geeigneten kryptologischen Verfahren verschlüsselt oder auch digital signiert werden, bevor sie über unsichere Kanäle weitergeleitet wird.

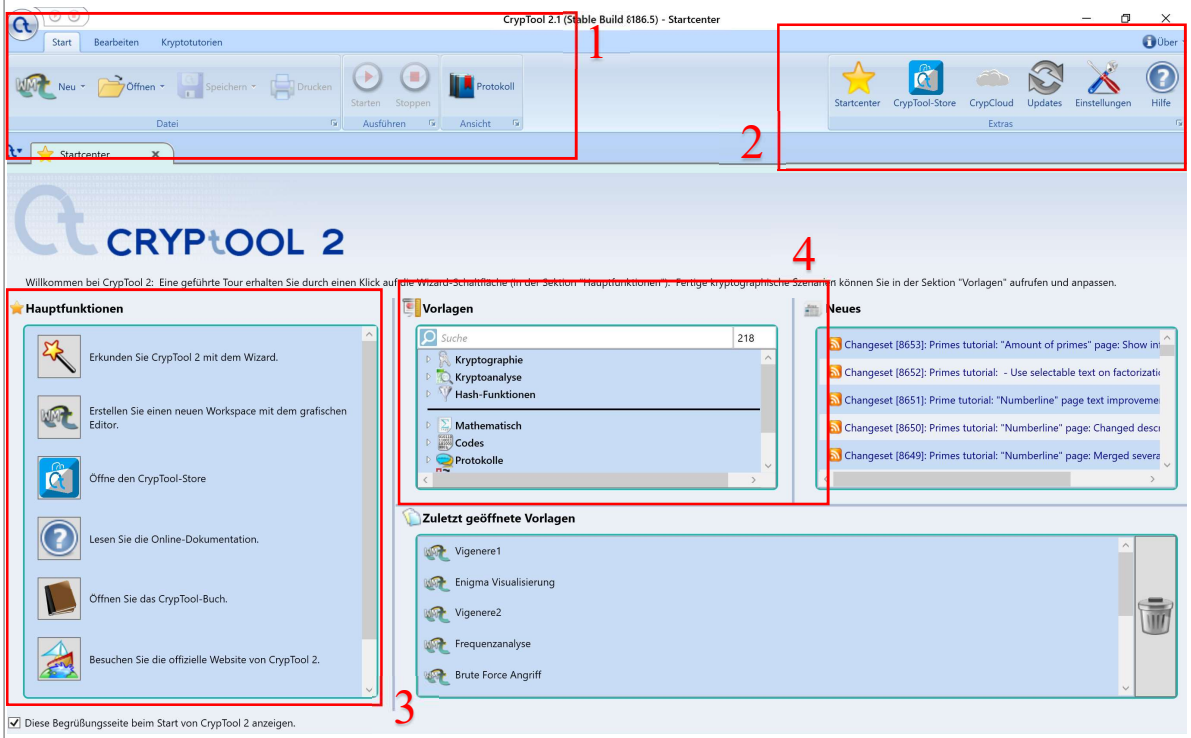
CrypTool 2 (CT2) ist ein Open-Source-Projekt, welches Schülerinnen und Schülern , Studenten sowie interessierten Personen ermöglicht, die Grundlagen der Kryptografie erfahrbar zu machen. Neben Erklärungen zu historischen und aktuellen Kryptomethoden lassen sich kryptographische Algorithmen modellieren und deren Funktionsweisen anhand praktischer Demonstrationen veranschaulichen.

2. Handhabung



Um CrypTool 2 zu starten führen Sie nach dem Download die Anwendung „CryptWin“ aus.

Beim Start von CT2 öffnet sich das Startcenter. Im Folgenden werden die Funktionen der vier eingerahmten Sektionen genauer erläutert.



Sektion 1: Start, Bearbeiten und Kryptotutorien.

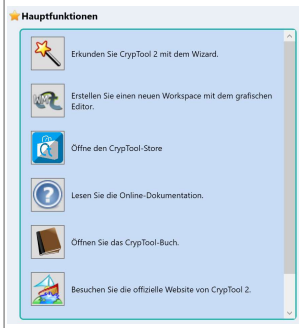
Der Menübaum gestaltet sich wie folgt:

Start:	*Bearbeiten:*	*Kryptotutorien:*
• *Neu* • *Öffnen* • *Speichern* • *Drucken* • *Starten* • *Stoppen* • *Protokoll*	• *Rückgängig* • *Wiederholen* • *Ausschneiden* • *Kopieren* • *Einfügen* • *Entfernen* • *Bild einfügen* • *Text einfügen*	• *Verfügbare Tutorien*

Sektion 2: Extras

Ebenfalls wurde im Startcenter eine Buttonleiste mit Extras integriert, welche einen Schnellzugriff in das Startcenter, den CrypTool-Store, die CrypCloud, sowie zu den verfügbaren Updates erlaubt. Unter den Einstellungen gibt es die Möglichkeit, individuelle Konfigurationen vorzunehmen. Der Hilfebutton bietet eine große Bandbreite an Online-Dokumentationen, die standardmäßig in CT2 mitgeliefert werden.

Sektion 3: Hauptfunktionen:

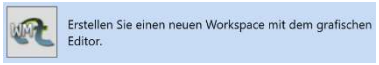


Darin hat man die Auswahl, die Funktionalität auf drei verschiedenen Wegen aufzurufen:

- über den **Wizard**: Er leitet einen geführt zu den Funktionen. 

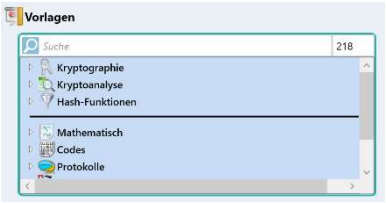
Der Wizard stellt Fragen zu dem gewünschten Szenario und führt den Benutzer dann zu den Funktionen. Das gewählte Szenario mit den eigenen Eingaben kann man anschließend auch als Vorlage abspeichern.

- über die Arbeitsfläche, auf der man die Komponenten (z.B. eine Verschlüsselungsfunktion, eine Texteingabefunktion, ...) anhand der visuellen Programmierung selbst zusammenstellen kann.



- über den Vorlagen-Baum, aus dem man fertige Workflows auswählen kann.

Sektion 4: Vorlagen:

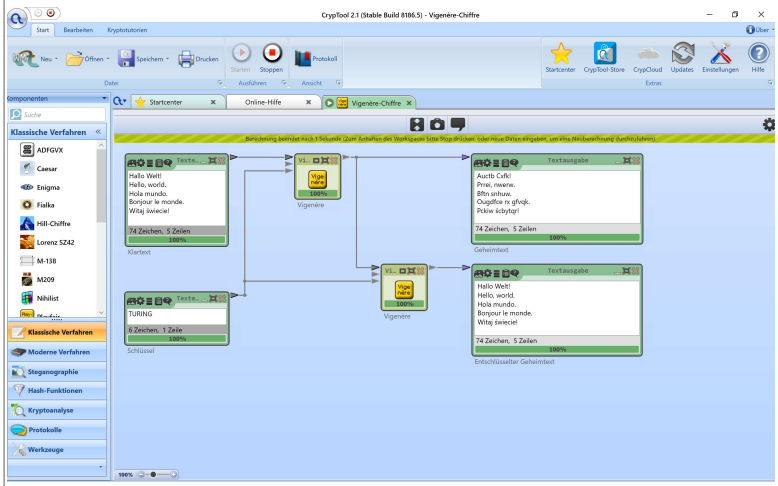


Im Vorlagen-Baum gibt es zu jeder Komponente mindestens eine Vorlage. Die angebotenen Vorlagen enthalten sofort lauffähige komplette Workflows. Wenn man z.B. in der Vorlage zu AES seine Eingaben ändert, sieht man dynamisch und sofort, wie sich Ausgaben entsprechend ändern.

Erstellen eines Workspaces mit dem grafischen Editor:

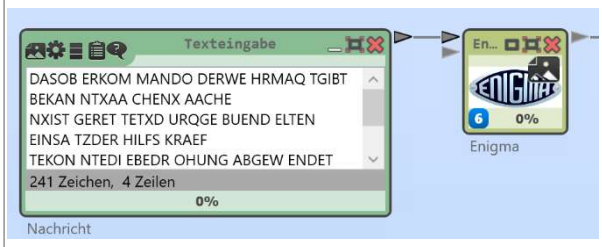
Der CrypTool Workspace Manager (CWM) ist – neben dem Wizard – das wichtigste Werkzeug von CrypTool 2. Der Workspace Manager erlaubt es dem Benutzer, die Arbeitsbereiche (engl.: workspaces) zu erstellen, zu editieren und zu strukturieren.

Im Arbeitsbereich kann man als Benutzer die verschiedenen Komponenten in einer grafischen, modularen Programmiersprache arrangieren. Intern wird dies vom Arbeitsplatz-Manager (Workspace Manager) durchgeführt, um die Komponenten zu organisieren und zu strukturieren. Komponenten sind das Basiselement von CrypTool 2, da sie in allen Utilities (Wizard, CWM) benutzt werden und es ermöglichen, auf einfache Weise verschiedene Krypto-Algorithmen und Protokolle zu erzeugen, sie zu testen und mit ihnen zu experimentieren. Damit kann man sein Wissen über Kryptographie schnell erweitern.



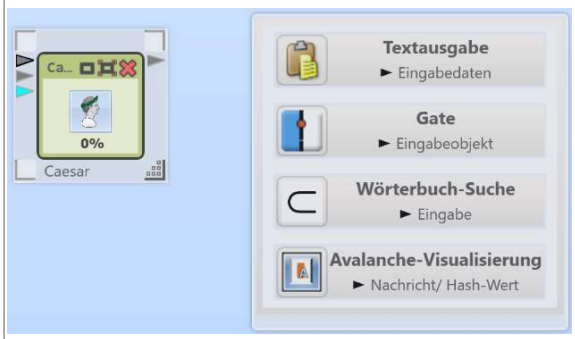
Erstellen eines Arbeitsbereiches:

Im Menü am linken Bildrand kann der Benutzer durch die installierten Komponenten von CrypTool 2 stöbern, oder alternativ das Such-Werkzeug benutzen. Um dem Benutzer die Suche nach der richtigen Komponente zu vereinfachen, sind die Komponenten geordnet nach Gruppen wie klassische Chiffren, Steganographie, Werkzeuge, usw. Komponenten können dann per Doppelklick oder einfachem Drag-und-Drop dem aktuellen Arbeitsbereich hinzugefügt werden.



Innerhalb des Arbeitsbereiches können Komponenten verbunden werden. Diese Verbindungen, im Arbeitsbereich dargestellt durch schwarze Linien, können durch Halten der linken Maustaste auf dem Ein- oder Ausgang der Ausgangs-Komponente und Loslassen auf dem Aus- oder Eingang der Ziel-Komponente durch den Benutzer erstellt werden.

Jede Komponente besitzt Ein- und/oder Ausgänge. Eingänge können nur mit Ausgängen, sowie Ausgänge nur mit Eingängen verbunden werden. Eingänge werden durch zur Komponente hinzeigende Pfeile und Ausgänge durch weg zeigende Pfeilsymbole dargestellt.
Bitte beachten Sie, dass der Typ der zu verbindenden Ein- und Ausgänge stets derselbe oder wenigstens kompatibel sein muss. Der CWM signalisiert durch Blinken, welche Ein- und Ausgaben des aktuellen Arbeitsbereiches kompatibel sind und zeigt in einem Einblend-Menü, wenn sich der Mauszeiger über dem zu verbindenden Konnektor befindet, ob der Konnektor vom selben Typ, kompatibel oder inkompatibel ist.



CWM bietet zusätzlich eine Vorschlagsliste an, welche Komponenten verbunden werden können. Ein Beispiel für solch eine Vorschlagsliste ist in der linken Abbildung zu sehen. Durch Zeichnen einer Verbindung, angefangen von einem Ein- oder Ausgabe-Konnektor hinein in den freien Raum des Arbeitsbereiches, und Loslassen der Maustaste, erscheint die Liste an der letzten Position des Mauszeigers und der Benutzer kann eine kompatible Komponente aus dieser Liste wählen. Die Sortierung der Liste richtet sich absteigend nach der Häufigkeit der Benutzung der Komponenten durch den Benutzer.

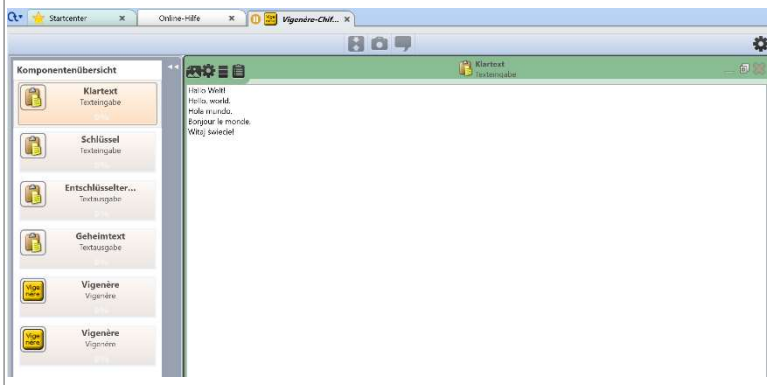
Der Arbeitsbereich kann mit Hilfe des „Starten“-Buttons im oberen Abschnitt des gesamten Fensters kontrolliert werden. Arbeitsbereiche können durch Drücken der „Starten“-Schaltfläche gestartet und durch Drücken der „Stoppen“-Schaltfläche angehalten werden. Eine Komponente wird nur dann ausgeführt, wenn an allen Eingängen Daten anliegen, die für die Ausführung notwendig sind.

Einstellungs- und Darstellungsmöglichkeiten von Komponenten im CWM:

Komponenten können im gesamten Arbeitsbereich platziert werden und werden dabei in drei verschiedenen Weisen dargestellt: minimiert, als Fenster und im Vollbild-Modus.

Minimiert erscheint die Komponente lediglich als eine Art kleines Fenster, das die Ikone der Komponente enthält, die Ein – und Ausgänge, sowie Steuerungsschaltflächen zum Erweitern des Fensters, zum Eintritt in den Vollbild-Modus und zum Entfernen der Komponente aus dem aktuellen Arbeitsbereich.

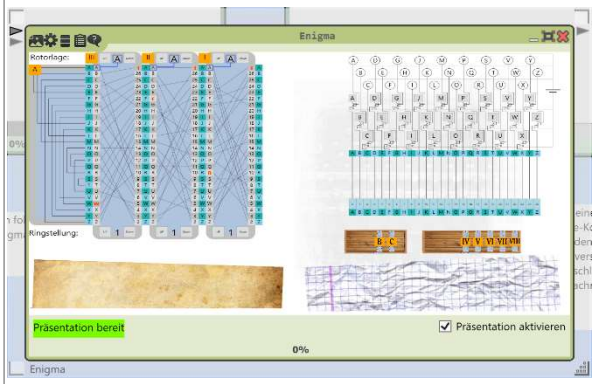
Zu einem **Fenster vergrößert** beinhaltet die Komponente eine von vier verschiedenen „Ansichten“ (engl.: views). Welche Ansicht dargestellt werden soll kann in einer Werkzeugleiste in der linken oberen Ecke des Fensters ausgewählt werden. Im Fensterzustand kann die Fenstergröße vom Benutzer festgelegt werden. Ist der Arbeitsbereich im Ausführungsmodus, zeigt ein Fortschrittsbalken unterhalb jeder Komponente deren Fortschritt. Sollten neue Nachrichten verfügbar sein, erscheint in der Fortschrittsanzeige eine Benachrichtigung in der Farbe ihres Typs.



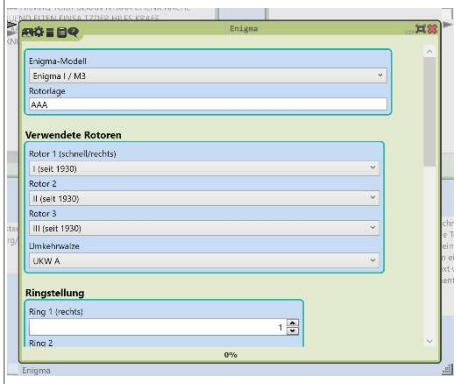
Im **Vollbild-Modus** wird die aktuelle Ansicht über den gesamten Bereich des Arbeitsbereiches dargestellt, wie in Abbildung 4 zu sehen ist. Auf der linken Seite bietet der CWM eine Liste aller Komponenten auf dem Arbeitsbereich, um den Wechsel zwischen den Komponenten zu beschleunigen.

4 verschiedene Ansichten:

Jede Komponente bietet bis zu vier verschiedene „Ansichten“ an: **Präsentation**, **Einstellungen**, **Protokoll** und **Daten**. Zusätzlich bietet CWM im Fenstermodus eine „Hilfe“-Schaltfläche an, mit welcher der Benutzer direkt die Dokumentation der aktuellen Komponente aufrufen kann.



Die **Präsentationsansicht** gewährleistet Einblicke auf Funktionsweisen verschiedener Chiffriermethoden. Hierbei ist zu beachten dass nicht jede Komponente in CT2 im Präsentationsmodus dargestellt werden kann und die Darstellungen individuell sehr unterschiedlich sein können.



In der Ansicht "**Einstellungen**" können alle Parameter der Komponente festgelegt werden.

Die Einstellungen sind die einzige Ansicht, welche auch in der Parameterleiste am rechten Bildrand des Arbeitsbereichs-Tabs angezeigt werden kann.

Die **Protokoll-Ansicht** zeigt Warnungen, Fehler, Informationen oder Debug-Benachrichtigungen der Komponente, wie in Abbildung 8 zu sehen ist. Ein Klick auf die „Entfernen“- Schaltfläche entfernt alle bisherigen Nachrichten.

Die **Daten-Ansicht** stellt dar, welche Daten an der Komponente anliegen, wie im Falle der linken Abbildung, ein String.