Werkzeuge für den Informatikunterricht
CrypTool 2

1. Kurzvorstellung

CrypTool 2 (CT2) ist ein Open-Source-Projekt, welches Schülerinnen und Schülern (SuS), Studenten sowie interessierten Personen ermöglicht, die Grundlagen der Kryptografie erfahrbar zu machen. Ziel dieses Projektes ist, das Verständnis der Benutzer für Kryptologie zu erhöhen, die darunterliegenden Konzepte zu erläutern und die Benutzer für IT-Bedrohungen zu sensibilisieren. Neben Erklärungen zu historischen und aktuellen Kryptomethoden lassen sich kryptographische Algorithmen modellieren und deren Funktionsweisen anhand praktischer Demonstrationen veranschaulichen.

2. Einordnung in die Lehrpläne

Die Anwendung von CrypTool 2 eignet sich in den nachfolgenden Lernbereichen:

Gymnasium, Klassenstufe 11/12:

Lernbereich 3: Sicherheit von Informationen	**12 Ustd**
Kennen von Anforderungen an die Informationssicherheit - Vertraulichkeit - Integrität - Authentizität - Verbindlichkeit/Anerkennung	Recht auf informationelle Selbstbestimmung ⇒ Werteorientierung
Einblick gewinnen in die Kryptologie im gesellschaftlichen Kontext - Kryptographie - Kryptoanalyse	Notwendigkeit und Missbrauch kryptographischer Verfahren ⇒ Empathie und Perspektivwechsel Verschlüsselung und Entschlüsselung an Beispielen
Kennen von Verfahren zur Gewährleistung der Vertraulichkeit - symmetrische Verfahren	klassische Verfahren: Cäsar-Chiffre, Vigenere-Verschlüsselung, Prinzip der Enigma Verfahren mit geheimem Schlüssel: DES, AES, SSL
- asymmetrische Verfahren	RSA-Verfahren, ElGamal
- nicht kryptographische Verfahren	Steganographie
Kennen von Verfahren zur Gewährleistung der Integrität und Authentizität	One-Way-Hash Funktion elektronische Unterschrift

18 2019 GY – INF

Oberschule, Klassenstufe 7-10:

Wahlbereich 2: Verschlüsselung von Informationen	
Kennen ausgewählter Codes und Chiffren unter historischem Aspekt	Unterschied zwischen Codierung und Chiffrierung verdeutlichen Datensicherheit und Schutz gegen Datenmissbrauch ➔ GK, Kl. 7, LB 2
Anwenden eines Codes auf das Codieren und Decodieren und einer Chiffre auf das Chiffrieren und Dechiffrieren einfacher Botschaften	Morse-Code, Blindenschrift Caesar-Chiffrierung

Berufliches Gymnasium, Klassenstufe 11:

Lernbereich 3: IT-Sicherheit und Ökologie	**16 Ustd.**
Berufliches Gymnasium	
Sich positionieren zur ökologisch und sozial verträglichen Nutzung von Medien	ökologischer Fußabdruck
- Chancen und Risiken im sozialen Umfeld	Spannungsfeld von Meinungsvielfalt und Gefahren für den demokratischen Rechtsstaat
- Gesundheitsgefährdungen	
- Umweltbelastungen	
Kennen von Sicherheitsmechanismen und Kryptologieverfahren	Caesar- oder Vigenére-Chiffre, E-Mail-Verschlüsselung → OS INF, Kl. 9, WPB 2
Anwenden der rechtlichen Grundlagen zum Datenschutz	Recht auf informelle Selbstbestimmung Internationales, europäisches und nationales Recht, Unternehmensrichtlinien

Fachoberschule, Klassenstufe 11:

Wahlpflicht 2: Kryptografie in der Informatik	**2 Ustd.**
Kennen kryptografischer Verfahren	
- Ziele und Aufgaben von Verschlüsselung	
- Prinzipien eines ausgewählten Verfahrens	Cäsar, Enigma, SSL, DES, RSA Einsatz von Simulationssoftware

3. Lernziele

Die folgenden Lernziele, speziell die psychomotorischen Lernziele, beziehen sich auf die im Seminar vorgestellten und erprobten Übungsaufgaben!

Kognitive Lernziele:

Die Schülerinnen und Schüler:

- verstehen die Ideen verschiedener Chiffriermethoden,
- kennen die Unterschiede zwischen symmetrischen und asymmetrischen Verfahren,
- können die Teilgebiete Kryptographie und Kryptoanalyse der Kryptologie, sowie die Codierung und die Steganographie als verschiedene Wissenschaften definieren und ausgewählte Verfahren anwenden,
- bauen Methoden- und Sozialkompetenzen und in Zusammenarbeit mit anderen ihre Kommunikationsformen auf,
- erweitern ihr Einfühlungsvermögen und ihre Problemlösestrategien.

Psychomotorische Lernziele:

Die Schülerinnen und Schüler:

- können das Caesar-Verfahren durch das ausprobieren aller möglichen Schlüssel knacken,
- können das Caesar-Verfahren mit Hilfe der Häufigkeitsanalyse knacken,
- können das Vigenère-Verfahren erläutern und zur Verschlüsselung und Entschlüsselung von Nachrichten anwenden,
- können die Funktionsweise der ENIGMA anhand der grafischen Darstellung in CrypTool 2 erläutern.

Affektive Lernziele:

Die Schülerinnen und Schüler:

- erkennen die Notwendigkeit von Chiffriermethoden,
- finden Gefallen bei Ver- und Entschlüsseln von geheimen Botschaften,
- werden sich der Notwendigkeit von Datenschutz bewusst,
- lernen Sicherheitsaspekte unserer heutigen Informationsgesellschaft kennen.

4. Kompetenzentwicklung

Die folgenden Kompetenzziele beziehen sich auf die im Seminar vorgestellten und erprobten Übungsaufgaben!

Fachkompetenz:

Die Schülerinnen und Schüler:

- lernen das Caesar-Verfahren als typische monoalphabetische Verschlüsselung anzuwenden,
- lernen den Caesar-Code durch Ausschöpfen des Schlüsselraums zu knacken,
- lernen den Caesar-Code durch anwenden einer Häufigkeitsanalyse zu brechen,
- können das Vigenère-Verfahren als typische polyalphabetische Verschlüsselung anwenden,
- analysieren und interpretieren das Prinzip der Chiffriermaschine Enigma.

Lern-/Methodenkompetenz:

Die Schülerinnen und Schüler:

- organisieren und koordinieren ihr Arbeitsschritte mit Unterstützung,
- erläutern informatische Sachverhalte fachsprachlich genau, kommunizieren adressatengerecht und stellen problembezogene Fragen,
- erschließen aus leicht erfassbaren Texten und Diagrammen Informationen mit informatischem Gehalt,
- geben einfache informatische Sachverhalte unter Benutzung der Fachsprache schriftlich oder mündlich wieder.

Sozialkompetenz:

Die Schülerinnen und Schüler:

- kommunizieren fachgerecht über Texte und Diagramme mit informatischem Gehalt, gemeinsam mit Klassenkameraden sowie der Lehrperson.

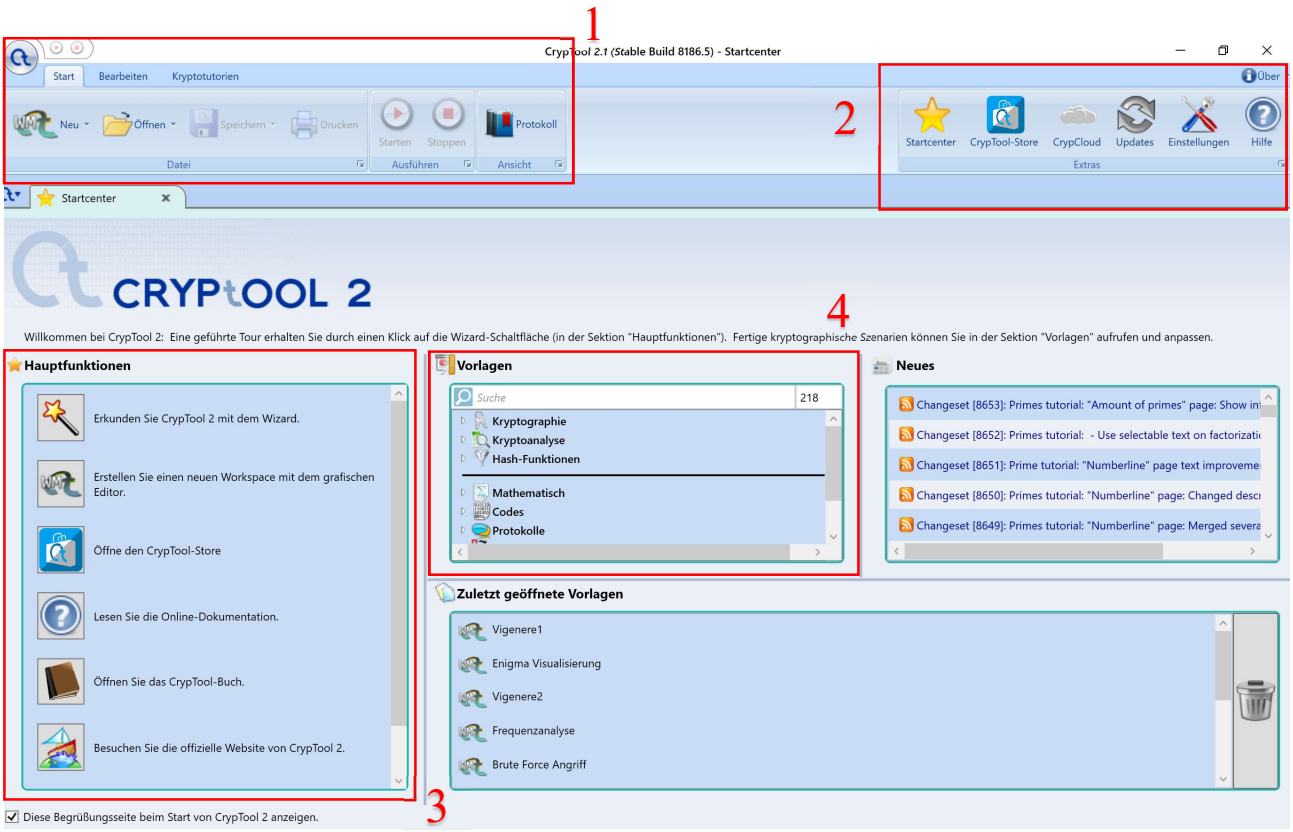
Selbstkompetenz:

Die Schülerinnen und Schüler:

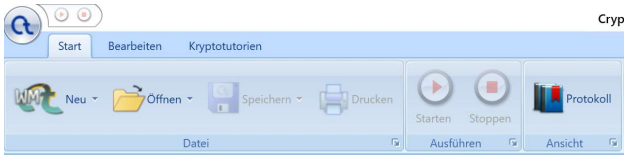
- ziehen Rückschlüsse aus der Kryptographie für das eigene Verhalten beim Einsatz von Informatiksystemen.

5. *Prinzipieller Aufbau*

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



<u>Sektion 1: Start, Bearbeiten und Kryptotutorien.</u>



Der Menübaum gestaltet sich wie folgt:

<u>*Start:*</u>
- *Neu*
- *Öffnen*
- *Speichern*
- *Drucken*
- *Starten*
- *Stoppen*
- *Protokoll*

<u>*Bearbeiten:*</u>
- *Rückgängig*
- *Wiederholen*
- *Ausschneiden*
- *Kopieren*
- *Einfügen*
- *Entfernen*
- *Bild einfügen*
- *Text einfügen*

<u>*Kryptotutorien:*</u>
- *Verfügbare Tutorien*

Sektion 2: Extras

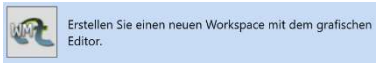
Ebenfalls wurde im Startcenter eine Buttonleiste mit Extras integriert, welche einen Schnellzugriff in das Startcenter, den CrypTool-Store, die CrypCloud, sowie zu den verfügbaren Updates erlaubt. Unter den Einstellungen gibt es die Möglichkeit, individuelle Konfigurationen vorzunehmen. Der Hilfebutton 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:

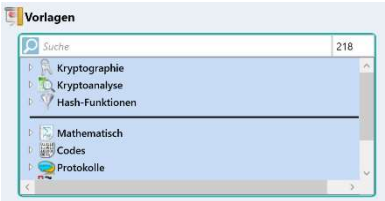
- über den **Wizard**: Er leitet einen geführt zu den Funktionen. 

Der Wizard stellt Fragen zu dem gewünschten Szenario (z.B. Base64-Codierung) 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:



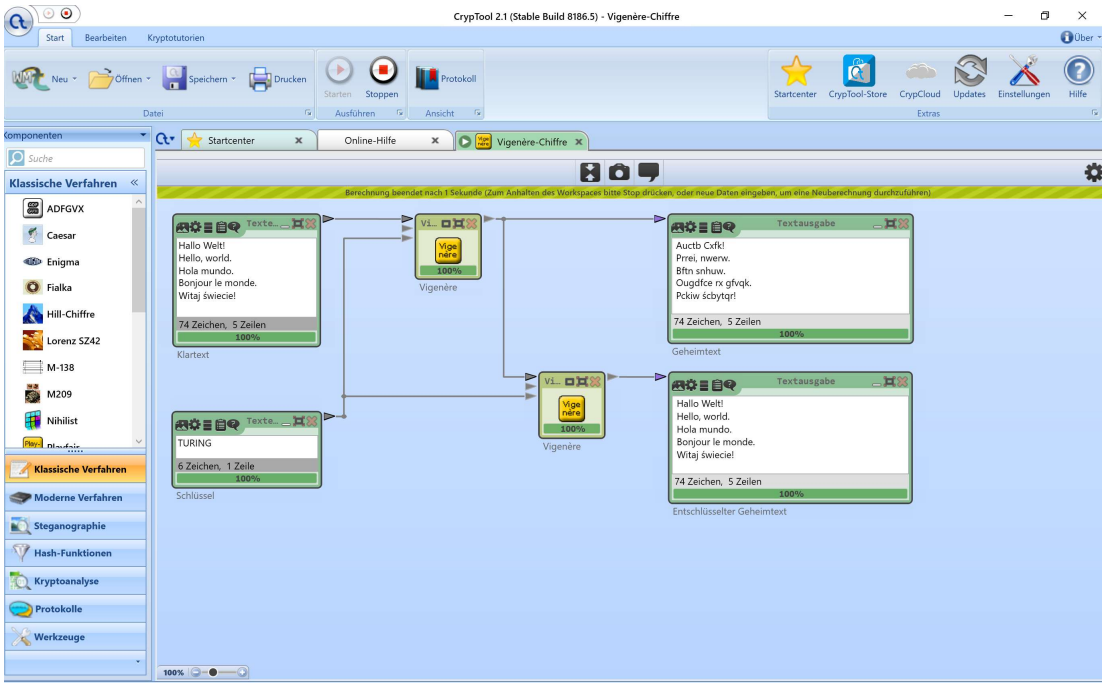
Im Vorlagen-Baum gibt es zu jeder Komponente mindestens eine Vorlage. Die angebotenen Vorlagen enthalten sofort lauffähige komplette Workflows. Wenn man z.B. in der Vorlage zu AES seine Eingaben ändert, sieht man dynamisch und sofort, wie sich Ausgaben entsprechend ändern.

6. Handhabung

Erstellen eines Workspaces mit dem grafischen Editor:

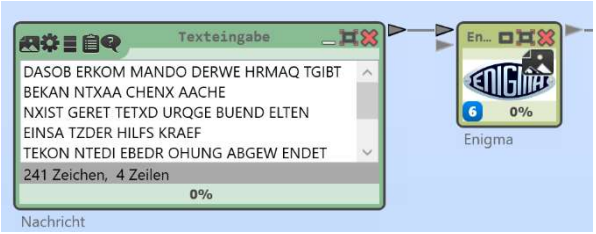
Der CrypTool Workspace Manager (CWM) ist – neben dem Wizard – das wichtigste Werkzeug von CrypTool 2. Der Workspace Manager erlaubt es dem Benutzer, die Arbeitsbereiche (engl.: workspaces) zu erstellen, zu editieren und zu strukturieren.

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.

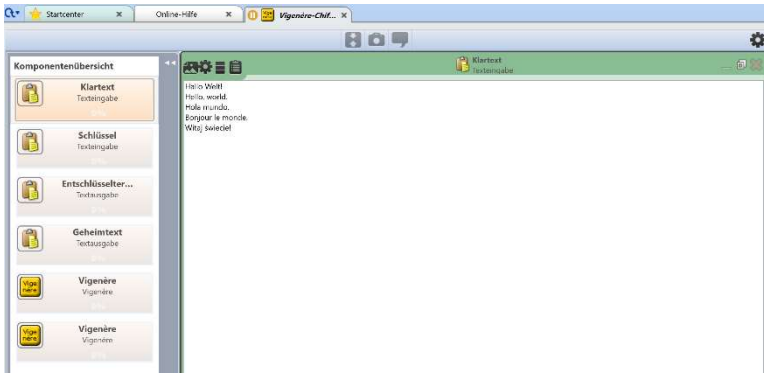
Der Arbeitsbereich kann mit Hilfe des „Starten“-Buttons im oberen Abschnitt des gesamten Fensters kontrolliert werden. Arbeitsbereiche können durch Drücken der „Starten“-Schaltfläche der „Stoppen gestartet und durch Drücken“-Schaltfläche angehalten werden. Eine Komponente wird nur dann ausgeführt, wenn 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.

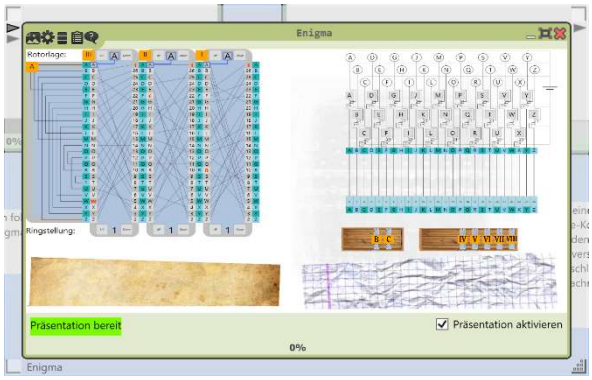
Zu einem **Fenster vergrößert** beinhaltet die Komponente eine von vier verschiedenen „Ansichten“ (engl.: views). Welche Ansicht dargestellt werden soll kann in einer Werkzeugleiste in der linken oberen Ecke des Fensters ausgewählt werden. Im Fensterzustand kann die Fenstergröße vom Benutzer festgelegt 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.



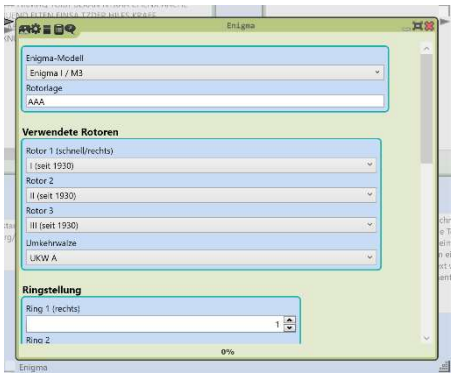
Im **Vollbild-Modus** wird die aktuelle Ansicht über den gesamten Bereich des Arbeitsbereiches dargestellt. Auf der linken Seite bietet der CWM eine Liste aller Komponenten auf dem Arbeitsbereich, um den Wechsel zwischen den Komponenten zu beschleunigen.

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. 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.

Organisationswerkzeuge:

Der CWM bietet verschiedene Werkzeuge zur Organisation der Arbeitsbereiche an.

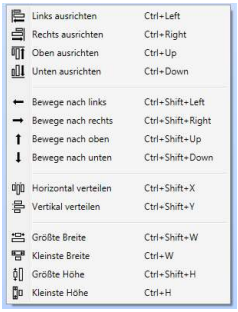
Zoom:

In der unteren linken Ecke befindet sich die „*Zoom-Leiste*“. Sie dient dazu, den Maßstab des aktuellen Arbeitsbereiches zu variieren.

Um den Maßstab automatisch so anzupassen, dass der gesamte Arbeitsbereich zu sehen ist, sollte die Schaltfläche „Fit-to-screen“ (das Symbol dazu ist in der Mitte oberhalb des Arbeitsbereiches) verwendet werden.

Alternativ kann zum Zoomen auch das Maus-Rad benutzt werden, wenn beim Rollen die Strg-Taste gehalten wird. Ein Klick mit der linken Maustaste auf die Prozent-Angabe der Zoom-Leiste, setzt diese auf 100%.

Layout der Komponenten:



Die Komponenten können mit der Maus beliebig auf dem Arbeitsbereich verschoben werden. Allerdings ist es schwierig, auf diese Art die Komponenten exakt zu platzieren. Daher stellt der CWM einige Funktionen zur Verfügung, die ein exaktes Layout der Komponenten ermöglichen. Diese Funktionen sind über das Kontextmenü aufrufbar, das erscheint, wenn Sie im Arbeitsbereich die rechte Maustaste drücken.

***Ausrichten*:** Wählen Sie mindestens zwei Komponenten aus und rufen dann das Kontextmenü durch Rechtsklick im Arbeitsbereich auf. Wählen Sie eine der Ausrichten-Funktionen. Wenn Sie z.B. "Rechts ausrichten" wählen, werden alle ausgewählten Komponenten horizontal so weit nach rechts verschoben, dass ihre rechte Kante, mit der am weitesten rechts liegenden rechten Kante aller ausgewählten Komponenten übereinstimmt.

Verschieben: Wählen Sie mindestens eine Komponente aus und rufen dann das Kontextmenü durch Rechtsklick im Arbeitsbereich auf. Mit den Verschiebe-Funktionen können Sie alle ausgewählten Komponenten gleichzeitig um eine Pixelbreite in die ausgewählte Richtung verschieben.

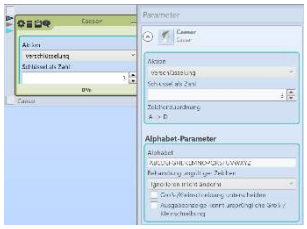
Verteilen: Wählen Sie mindestens drei Komponenten aus und rufen dann das Kontextmenü durch Rechtsklick im Arbeitsbereich auf. Wählen Sie eine der Verteil-Funktionen. Wenn Sie z.B. "Horizontal verteilen" wählen, werden die am weitesten links und rechts liegenden der ausgewählten Komponenten bestimmt und fixiert. Die restlichen ausgewählten Komponenten werden dann (unter Beibehaltung der Reihenfolge) horizontal so verschoben, dass ihre horizontalen Abstände voneinander alle gleich sind.

Größenanpassung: Wählen Sie mindestens zwei Komponenten aus und rufen dann das Kontextmenü durch Rechtsklick im Arbeitsbereich auf. Mit den Größenanpassungs-Funktionen können Sie die Breiten oder Höhen aller ausgewählten Komponenten gleichzeitig auf denselben Wert setzen. Sie können dabei wählen, ob die Breiten oder Höhen der Komponenten auf den größten oder kleinsten Wert unter den ausgewählten Komponenten gesetzt werden soll.

Bitte beachten Sie, dass eine Funktion im Kontext-Menü nur dann aktiviert ist, wenn sie für die Anzahl der ausgewählten Komponenten sinnvoll ist. Es ist beispielsweise kein Ausrichten von Komponenten möglich, wenn nur eine Komponente ausgewählt wurde. In diesem Fall sind die Ausrichten-Funktionen deaktiviert.

Alle Layout-Funktionen sind auch über Tastaturkürzel aufrufbar. Die zu den einzelnen Funktionen gehörigen Tastaturkürzel werden im Kontextmenü angezeigt.

Parameterleiste:



Zum Justieren der Einstellungen von Komponenten bietet der CWM auf der rechten Seite des aktuellen Arbeitsbereiches die so genannte "Parameter-Leiste" an. Diese kann sowohl ein- als auch ausgeblendet werden (mit Hilfe der Schaltfläche oberhalb der Leiste), so wie in der Breite verändert werden. Ihr Inhalt entspricht der Einstellungsansicht der Komponente, die gerade den Fokus hat.

Kurzbefehle in CrypTool 2:

Tastenkürzel	Aktion
Strg + C	Kopiert ausgewählte Komponenten in die Zwischenablage
Strg + V	Fügt Komponenten aus der Zwischenablage in den Arbeitsbereich ein
Strg + X	Schneidet ausgewählte Komponenten aus dem Arbeitsbereich aus
Strg + Z	Widerruft den letzten Befehl
Strg + Y	Führt letzten widerrufenen Befehl erneut aus
Strg + Maus-Rad	Verändert den Maßstab (Zoomen)
F11	Anzeigen/Ausblenden von Komponenten-Browser und Parameterleiste
F12	Anzeigen/ausblenden von Haupt-Ribbon-Bar
Strg + A:	Alle Komponenten auswählen
Strg + Rechts:	Ausgewählte Komponenten nach rechts ausrichten
Strg + Links:	Ausgewählte Komponenten nach links ausrichten
Strg + Oben:	Ausgewählte Komponenten nach oben ausrichten
Strg + Unten:	Ausgewählte Komponenten nach unten ausrichten
Strg + Umschalt + Rechts:	Ausgewählte Komponenten nach rechts verschieben
Strg + Umschalt + Links:	Ausgewählte Komponenten nach links verschieben
Strg + Umschalt + Oben:	Ausgewählte Komponenten nach oben verschieben
Strg + Umschalt + Unten:	Ausgewählte Komponenten nach unten verschieben
Strg + Umschalt + X:	Ausgewählte Komponenten horizontal verteilen
Strg + Umschalt + Y:	Ausgewählte Komponenten vertikal verteilen
Strg + Umschalt + W:	Ausgewählte Komponenten auf die größte Breite vergrößern
Strg + W:	Ausgewählte Komponenten auf die kleinste Breite verkleinern
Strg + Umschalt + H:	Ausgewählte Komponenten auf die größte Höhe vergrößern
Strg + H:	Ausgewählte Komponenten auf die kleinste Höhe verkleinern

7. Screencast

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