

CrypTool 2

Was dein Feind nicht wissen soll, das sage deinem Freunde nicht.

A. Schopenhauer 1862



VERSCHLÜSSELN

VERSCHLEIERN



Grundwerte der Datensicherheit



1

Das ist CrypTool 2

Entstehung & Funktionsweise: Ein erster Überblick

2

Darauf zielt CrypTool 2 ab

Rahmenbedingungen & Einsatzszenarien: Eine Einordnung

3

Das kann CrypTool 2

Versionen & Oberflächen: Grundlagen der Benutzung

4

CrypTool 2 in der Konzeption

Motivation & Zielerreichung: Eine grobe Planung

5

CrypTool 2 im Praxiseinsatz

Übung & Vertiefung: Erste eigene Schritte

6

CrypTool 2 im Dialog

Pro & Kontra: Eine abschließende Besprechung



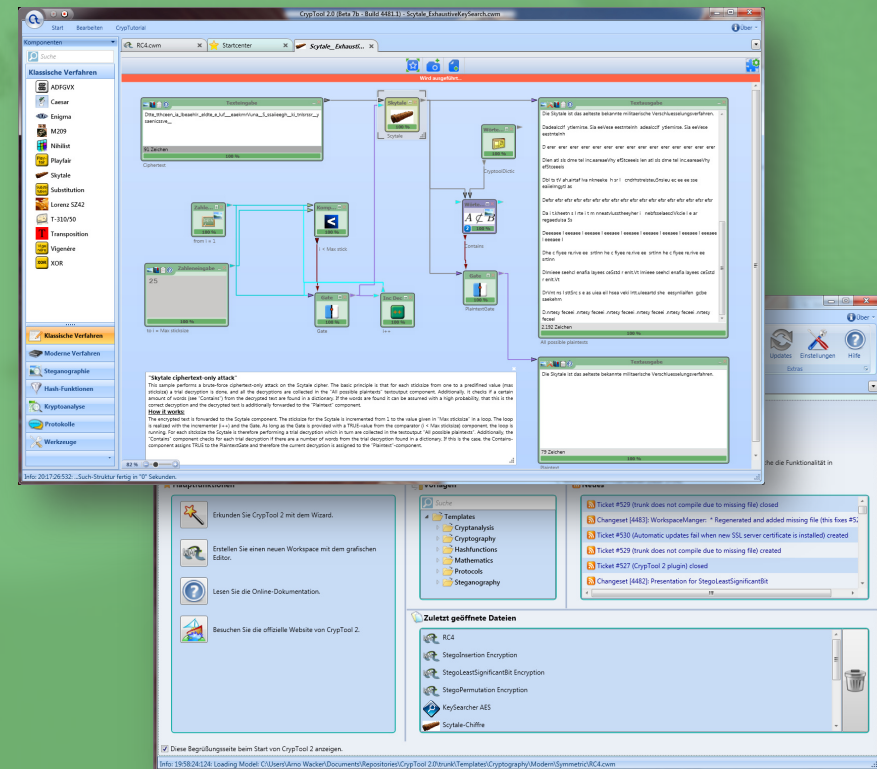
Das ist CrypTool 2

Entstehung & Funktionsweise: Ein erster Überblick

Open-Source-Projekt

Entstehung, Features

- Seit 1998 in der Entwicklung
- 3 unterschiedliche Versionen
- Seit 2009 auch online
- Mehrfach ausgezeichnet
- Plug'n'Play Interface
- Visuelle Programmierung
- Visualisierung von Algorithmen
- Funktionen zur Kryptoanalyse
- 500 Seiten Handbuch



Darauf zielt CryptTool 2 ab

Rahmenbedingungen & Einsatzszenarien: Eine Einordnung

Gesellschaft für Informatik

Bildungsstandards Sek. I

Klassenstufe 8-10

angemessen auf Risiken bei der Nutzung von Informatiksystemen reagieren

erkennen der Unsicherheiten einfacher Verschlüsselungsverfahren

Bildungsstandards Sek. II

Informatik, Mensch und Gesellschaft

[...] verwenden und beschreiben Verfahren zur Sicherung von Vertraulichkeit, Authentizität und Integrität von Daten

[...] analysieren und beurteilen Verfahren zur Sicherung von Vertraulichkeit, Authentizität oder Integrität von Daten in konkreten aktuellen Anwendungskontexten



Gymnasium

Lernbereich 3

„Sicherheit von Informationen“

Kennen von Verfahren zur Gewährleistung der Vertraulichkeit

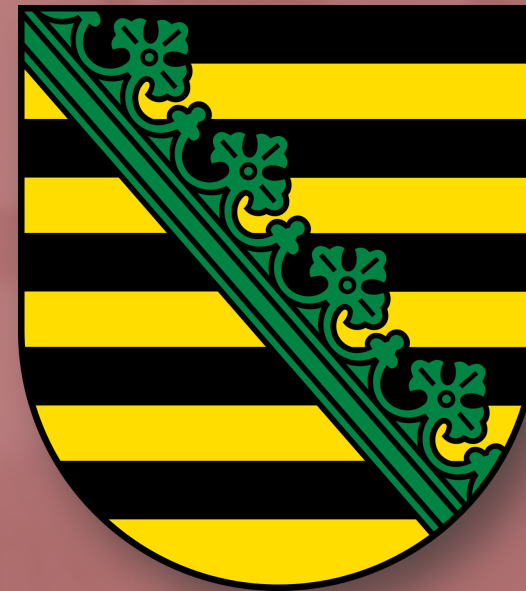
- symmetrische Verfahren

- asymmetrische Verfahren

- nicht kryptographische Verfahren

Kennen von Verfahren zur Gewährleistung der Integrität und Authentizität

Beherrschen der Nutzung von Verfahren zur Gewährleistung der Sicherheit von Informationen

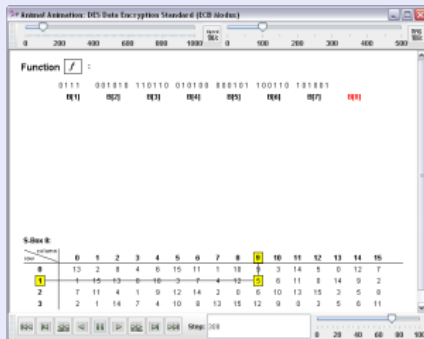
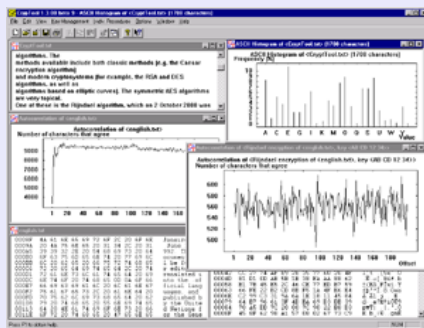


Das kann CrypTool 2

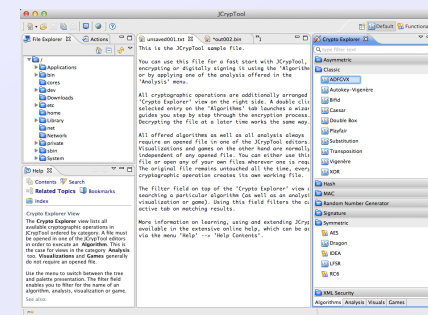
Versionen & Oberflächen: Grundlagen der Benutzung

CrypTool 1 & JCrypTool

CrypTool 1



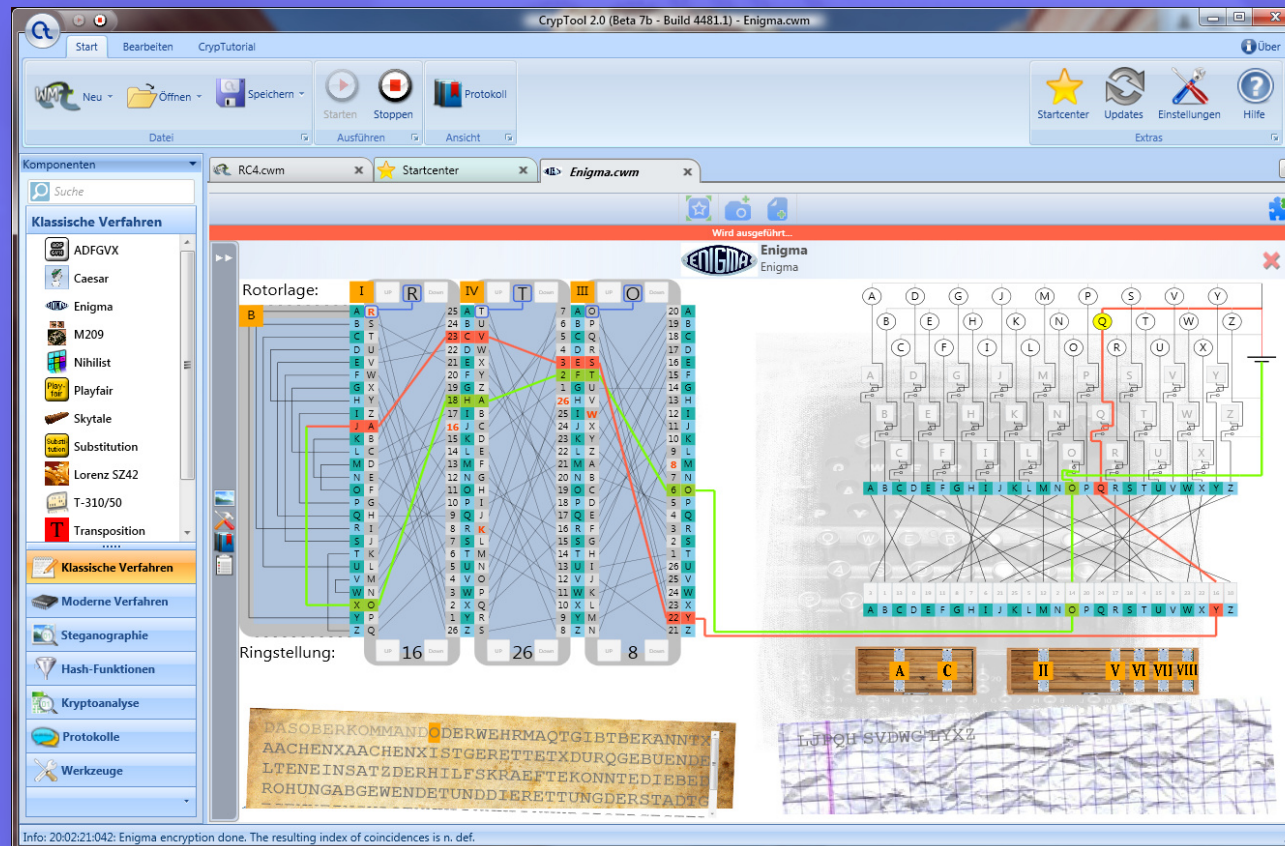
JCrypTool



Das kann CryptTool 2

Versionen & Oberflächen: Grundlagen der Benutzung

CrypTool 2 Musteraufgaben



CrypTool 2 in der Konzeption

Motivation & Zielerreichung: Eine grobe Planung

Kryptographie in der FOS

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



CrypTool 2 in der Konzeption

Motivation & Zielerreichung: Eine grobe Planung

Kryptographie im BGY

Wahlpflicht 5: Kryptologie

4 Ustd.

Einblick gewinnen in Grundbedrohungen und Sicherheitsmechanismen

- Verlust der Verfügbarkeit, Integrität und Vertraulichkeit als Grundbedrohungen
- Authentifikation, Zugriffskontrolle, Vertraulichkeit, Datenintegrität, Sende- und Kommunikationsnachweis

Kennen eines ausgewählten Kryptologieverfahrens

⇒ Wertorientierung

Skytale von Sparta, Caesar- oder Vigenère-Chiffre, Pretty Good Privacy (PGP)



Lernbereich 3: Sicherheit von Informationen

12 Ustd

Kennen von Anforderungen an die Informationssicherheit

- Vertraulichkeit
 - Integrität
 - Authentizität
 - Verbindlichkeit/Anerkennung
- } 2 UE

Einblick gewinnen in die Kryptologie im gesellschaftlichen Kontext

- Kryptographie
 - Kryptoanalyse
- } 2 UE

Recht auf informationelle Selbstbestimmung

⇒ Werteorientierung

Notwendigkeit und Missbrauch kryptographischer Verfahren

⇒ Empathie und Perspektivwechsel

Verschlüsselung und Entschlüsselung an Beispielen

<p>Kennen von Verfahren zur Gewährleistung der Vertraulichkeit</p> <ul style="list-style-type: none">- symmetrische Verfahren- asymmetrische Verfahren- nicht kryptographische Verfahren	<p>klassische Verfahren: Cäsar-Chiffre, Vigenere-Verschlüsselung, Prinzip der Enigma</p> <p>Verfahren mit geheimem Schlüssel: DES, AES, SSL</p> <p>RSA-Verfahren, ElGamal</p> <p>Steganographie</p>
<p>Kennen von Verfahren zur Gewährleistung der Integrität und Authentizität</p> <p>Beherrschen der Nutzung von Verfahren zur Gewährleistung der Sicherheit von Informationen</p>	<p>One-Way-Hash Funktion</p> <p>elektronische Unterschrift</p> <p>Einsatz von Werkzeugen</p> <p>Umsetzung einfacher Verfahren mit einer Programmierumgebung</p>

5 UE

3 UE

Motivation/Zielorientierung

- Wizard macht einen schnellen Einstieg möglich
- Nimbus des abenteuerlichen
- Individuelle Projekte nach kurzer Einarbeitung
- Projekte speichern/teilen
- Hilfe mit Hintergrundinfos
- Basis bis Expertenwissen kann erworben werden
- Fördert logisches/abstraktes/kreatives Denken



Arbeitsauftrag in OPAL

Arbeitsblatt

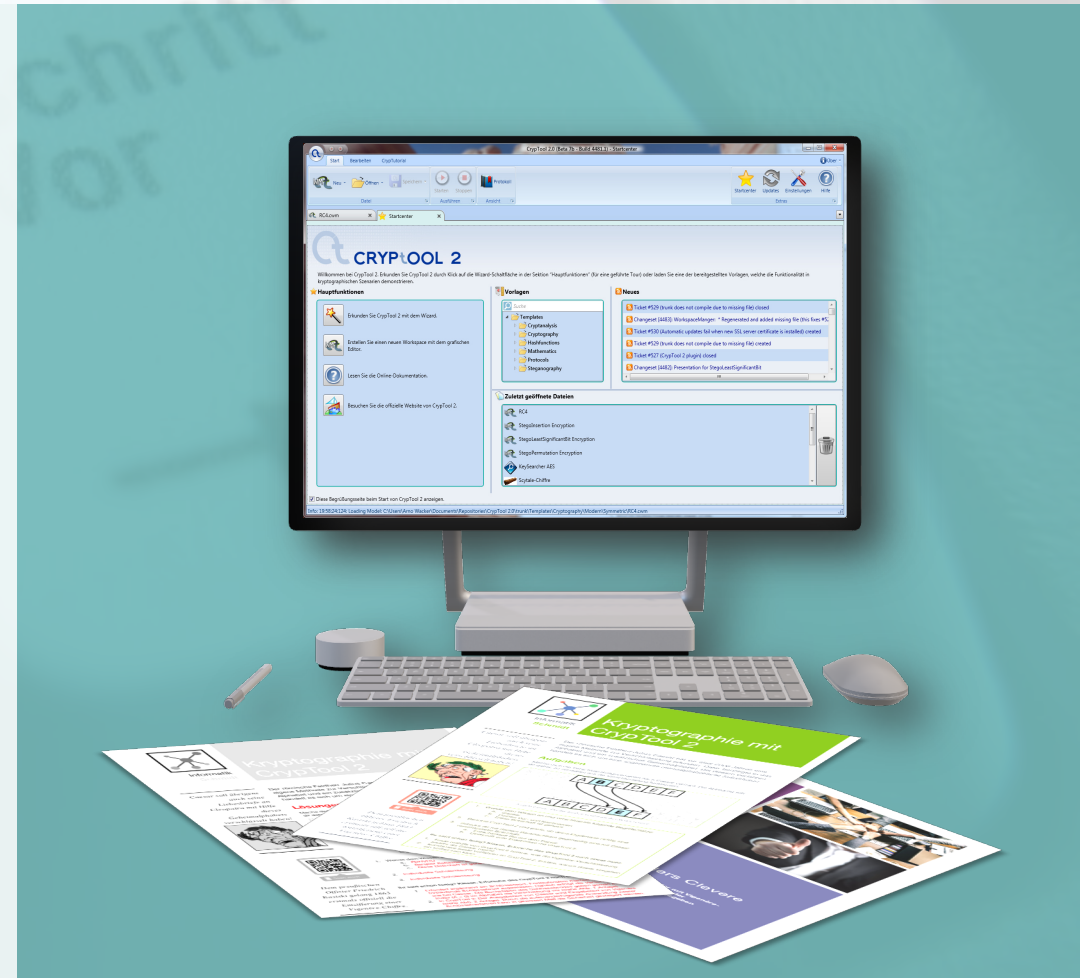
- Arbeitsblatt_CrypTool2.pdf

Lösungen

- Arbeitsblatt_CrypTool2_Lsg.pdf

Alles fertig?

- Zusatz_mit_Lsg.pdf
- freies erforschen des Tools



CrypTool 2 im Dialog

Pro & Kontra: Eine abschließende Besprechung

Diskussion



CrypTool 2

Was dein Feind nicht wissen soll, das sage deinem Freunde nicht.

A. Schopenhauer 1862