Didaktik Aspekte

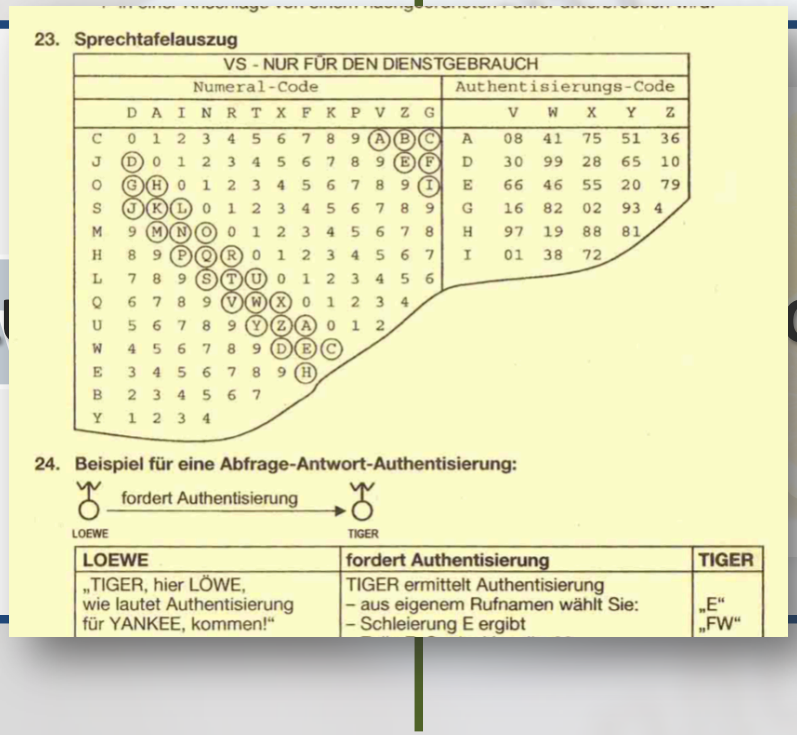
CrypTool 2

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

A. Schopenhauer 1862

VERSCHL

CHLEIERN



23. **Sprechtafelauszug**

VS - NUR FÜR DEN DIENSTGEBRAUCH

	Numeral-Code												Authentisierungs-Code					
	D	A	I	N	R	T	X	F	K	P	V	Z	G		V	W	X	Y	Z
C	0	1	2	3	4	5	6	7	8	9	A	B	C	A	08	41	75	51	36
J	D	0	1	2	3	4	5	6	7	8	9	E	F	D	30	99	28	65	10
O	G	H	0	1	2	3	4	5	6	7	8	9	I	E	66	46	55	20	79
S	J	K	L	0	1	2	3	4	5	6	7	8	9	G	16	82	02	93	4
M	9	M	N	O	0	1	2	3	4	5	6	7	8	H	97	19	88	81	
H	8	9	P	Q	R	0	1	2	3	4	5	6	7	I	01	38	72		
L	7	8	9	S	T	U	0	1	2	3	4	5	6						
Q	6	7	8	9	V	W	X	0	1	2	3	4							
U	5	6	7	8	9	Y	Z	A	0	1	2								
W	4	5	6	7	8	9	D	E	C										
E	3	4	5	6	7	8	9	H											
B	2	3	4	5	6	7													
Y	1	2	3	4															

24. **Beispiel für eine Abfrage-Antwort-Authentisierung:**

LOEWE — fordert Authentisierung → TIGER

LOEWE	fordert Authentisierung	TIGER
„TIGER, hier LÖWE, wie lautet Authentisierung für YANKEE, kommen!"	TIGER ermittelt Authentisierung – aus eigenem Rufnamen wählt Sie: – Schleierung E ergibt	 „E" „FW"

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

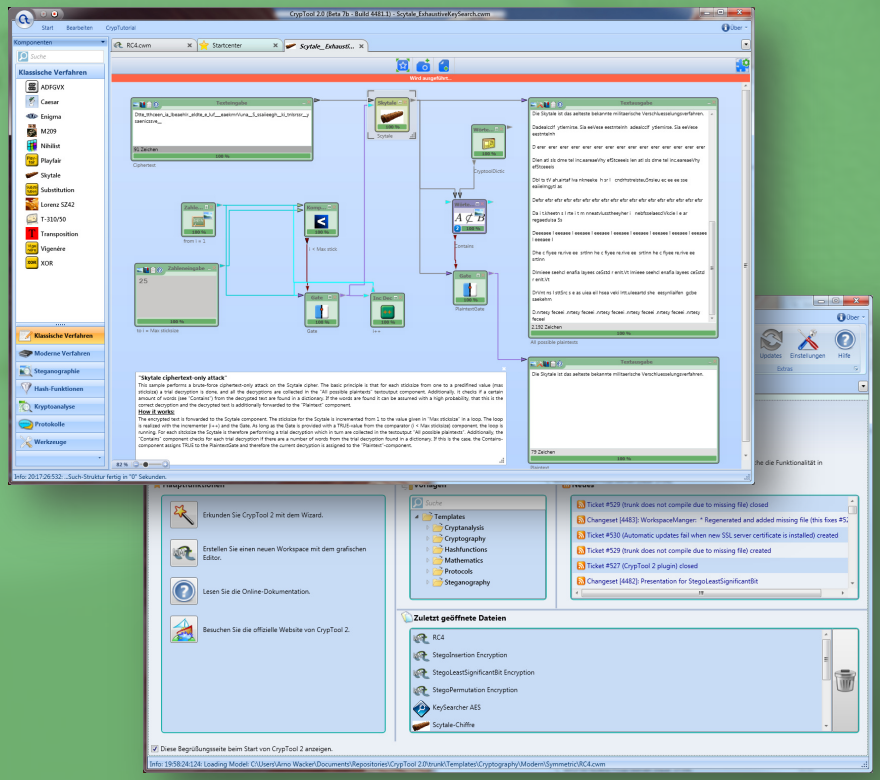
Entstehung & Funktionsweise: Ein erster Überblick

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 CrypTool 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

Darauf zielt CrypTool 2 ab

Rahmenbedingungen & Einsatzszenarien: Eine Einordnung

Sächsischer Lehrplan

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

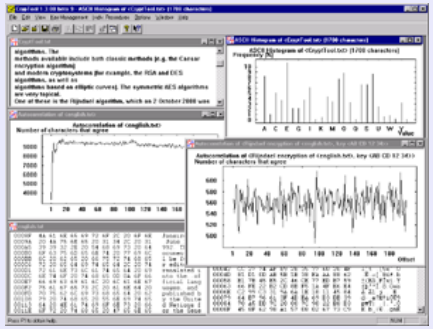
Beherrschen der Nutzung von Verfahren zur Gewährleistung der Sicherheit von Informationen

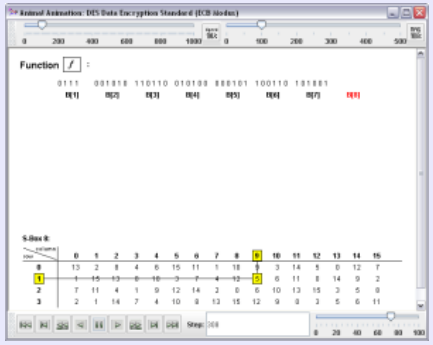
Das kann CrypTool 2

Versionen & Oberflächen: Grundlagen der Benutzung

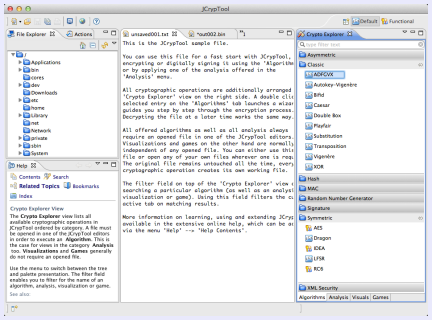
CrypTool 1 & JCrypTool

CrypTool 1





JCrypTool

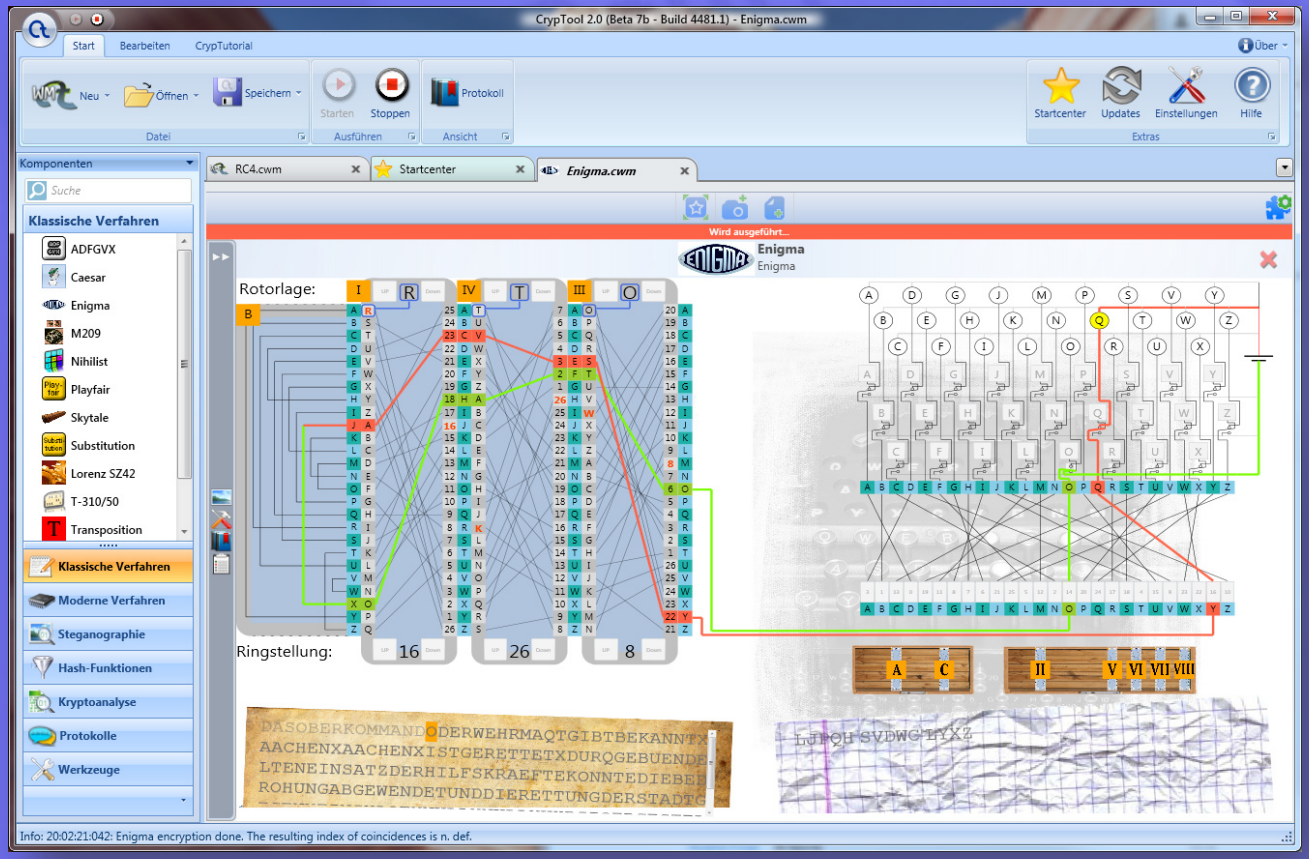


SIERRA SQUARE

Das kann CrypTool 2

Versionen & Oberflächen: Grundlagen der Benutzung

CrypTool 2 Musteraufgaben



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

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	⇒	Werteorientierung
Kennen eines ausgewählten Kryptologieverfahrens		Skytale von Sparta, Caesar- oder Vigenére-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	Recht auf informationelle Selbstbestimmung ⇒ Werteorientierung
Einblick gewinnen in die Kryptologie im gesellschaftlichen Kontext - Kryptographie - Kryptoanalyse	2 UE	Notwendigkeit und Missbrauch kryptographischer Verfahren ⇒ Empathie und Perspektivwechsel Verschlüsselung und Entschlüsselung an Beispielen

CrypTool 2 in der Konzeption

Motivation & Zielerreichung: Eine grobe Planung

Kryptographie im Gymnasium

Kennen von Verfahren zur Gewährleistung der Vertraulichkeit		
- symmetrische Verfahren	5 UE	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	3 UE	One-Way-Hash Funktion
		elektronische Unterschrift
Beherrschen der Nutzung von Verfahren zur Gewährleistung der Sicherheit von Informationen		Einsatz von Werkzeugen
		Umsetzung einfacher Verfahren mit einer Programmierumgebung

Motivation, Zielorientierung

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

Arbeitsblatt Übung

Arbeitsauftrag in OPAL

Arbeitsblatt

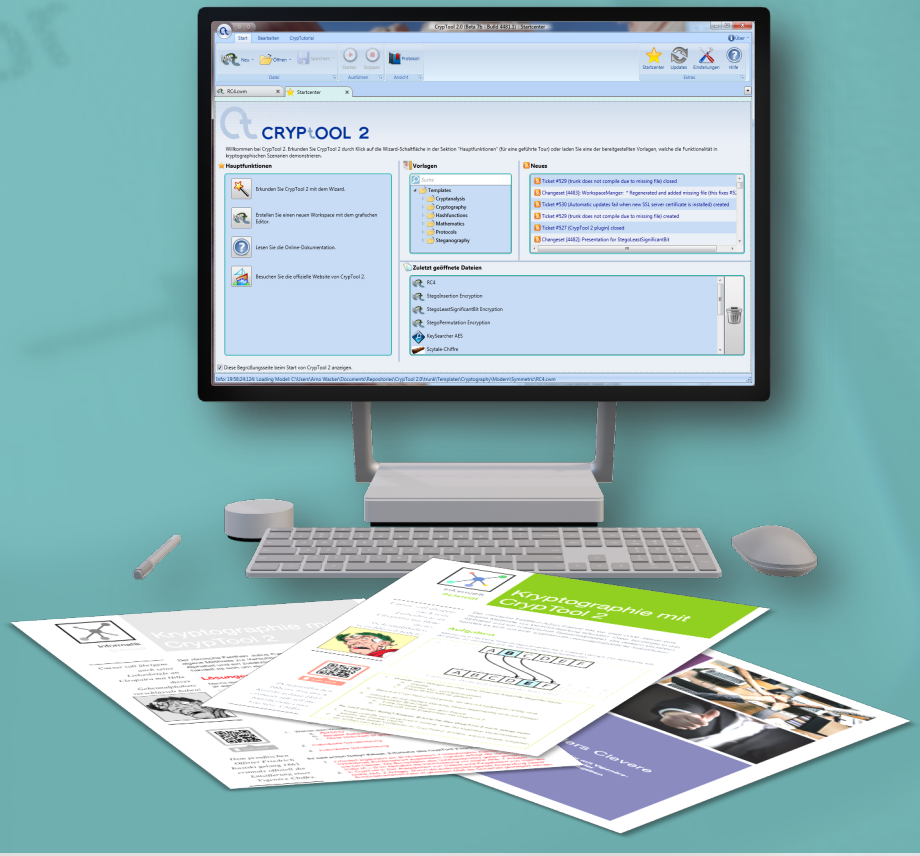
- Arbeitsblatt_CrypTool2.pdf

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

Didaktik Aspekte

CrypTool 2

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

A. Schopenhauer 1862