

CrypTool

Cryptography for the masses

An overview of the CrypTool project
... given at the CrypTool conference in Munich, 2019
... from the past (history starting with CT1 as part of the awareness
program of one company),
... with statistics and success stories all over the world in the present
... to the future
... plus hints to the talks coming after this presentation

Prof. Bernhard Esslinger

(presentation layout done with some help from Gonzalo;
pictures by pixabay)

Cryptography everywhere ...

In the digital era, we are all cryptography consumers, whether we know it or not.

Whenever we use the mobile telephone, withdraw money from an ATM, go shopping to an e-commerce site using SSL, or use a messenger, we are using cryptographic services which protect the confidentiality, integrity, and authenticity of our data.

The world as we know it wouldn't exist without cryptography.

Cryptography challenges education

Around all of us

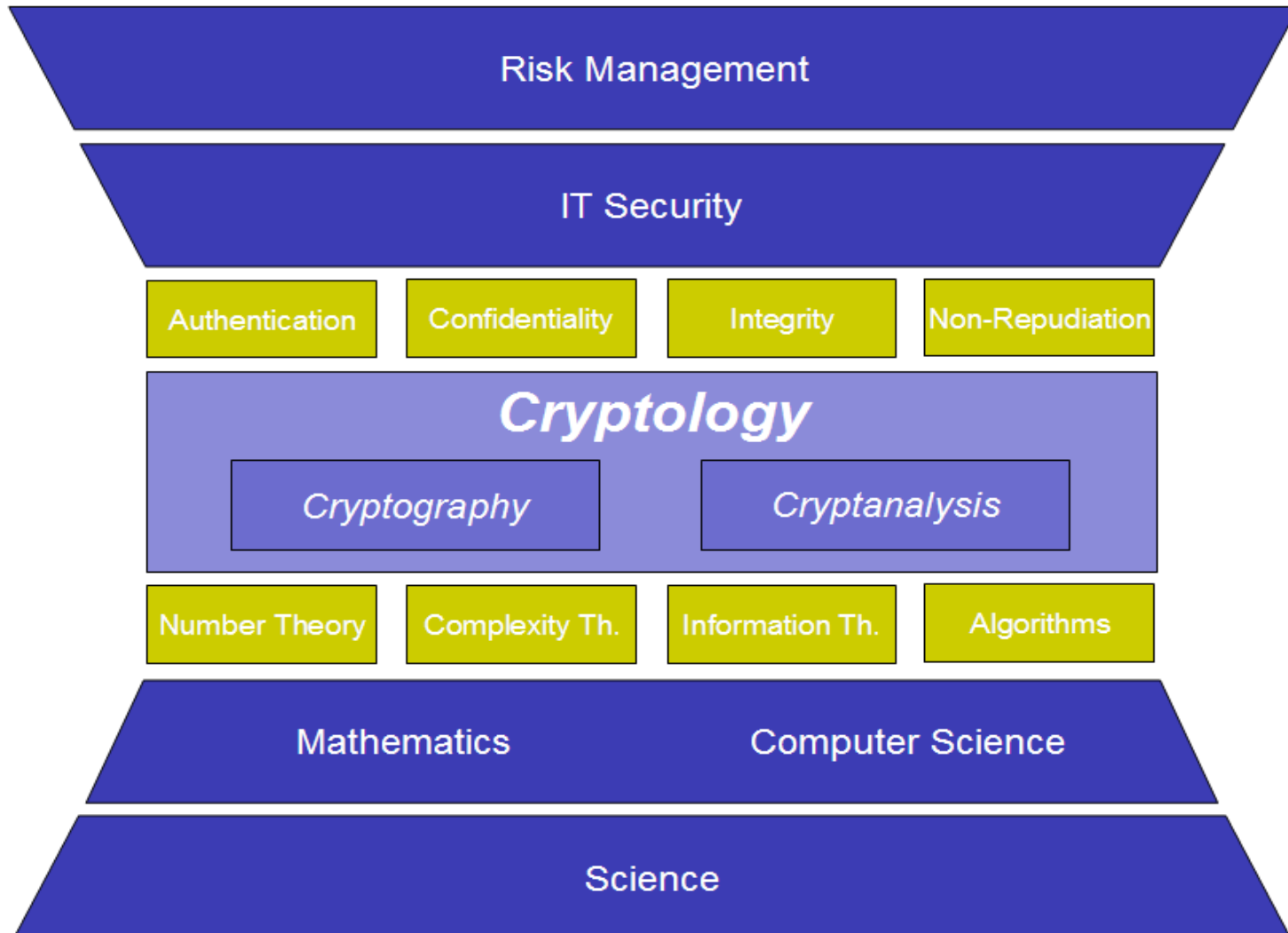
perceived as difficult

lack of understanding

curricula

teachers need useful tools

Context of Cryptography



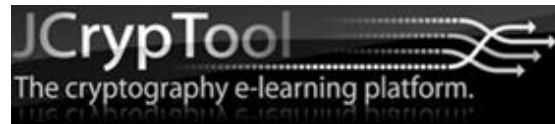
CrypTool today: 5 products

The logo for CrypTool, featuring the word "CRYPT" in blue and "TOOL" in a lighter blue, with a small lowercase 't' between them.

version 1.x <http://www.cryptool.org/en/cryptool1>

The logo for CrypTool 2, featuring the word "CRYPT" in blue and "TOOL 2" in a lighter blue, with a small lowercase 't' between them.

<http://www.cryptool.org/en/ct2>

The logo for JCrypTool, featuring the text "JCrypTool" in white on a black background, with a stylized white icon of a network or data flow to the right. Below it, the text "The cryptography e-learning platform." is written in a smaller font.

<https://github.com/jcryptool/>

The logo for CrypTool-Online, featuring a large green stylized 'Q' or 'C' on the left, followed by the text "CRYPT" in green and "TOOL-ONLINE" in white on a black background.

<http://www.cryptool-online.org>

The logo for MysteryTwister C3, featuring the text "MysteryTwister" in white and "C3" in blue on a dark grey background. Below it, the text "THE CRYPTO CHALLENGE CONTEST" is written in white.

<http://www.mysterytwisterc3.org/>

CrypTool Portal: website today

CRYPTOOL PORTAL
Cryptography for everybody

HOME LANGUAGE

Search ...

What is CrypTool 1

CrypTool 1 (CT1) is an open-source Windows program for cryptography and cryptanalysis. It's the most widespread e-learning software of its kind.

FREE DOWNLOADS

- CrypTool 1
- CrypTool 2
- JCrypTool

CRYPTOOL 1 CRYPTOOL 2 JCrypTool CRYPTOOL ONLINE MYSTERY TWISTER C3


About CrypTool Documentation Education Contributors Links / Books


www.cryptool.org

What is JCrypTool?

JCrypTool (JCT) is an open-source e-learning platform, allowing to experiment comprehensively with cryptography on Linux, MAC OS X, and Windows.

FREE DOWNLOADS

 CrypTool 1

 CrypTool 2

 JCrypTool

 CRYPTOOL 1

 CRYPTOOL 2

 JCT JCRIPTOOL

 CRYPTOOL
ONLINE

 MYSTERY
TWISTER C3

JCRIPTOOL NEWS

JCRYPTOOL UPDATES TO ECLIPSE 2019-06

JCrypTool weekly builds are based on the latest Eclipse version 2019-06 since July 2019.

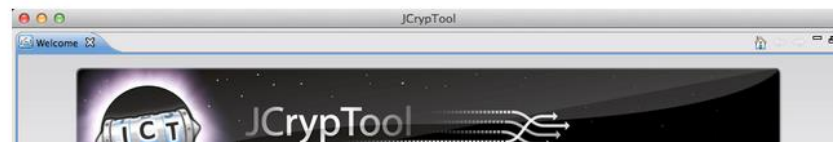
[Read more ...](#)

RELEASE CANDIDATE 9 AVAILABLE

[Cookie policy](#) [Release Candidate 9 is
download page](#)

JCrypTool -- The cryptography e-learning platform

JCrypTool enables students, teachers, developers, and anyone else interested in cryptography to apply and analyze cryptographic algorithms in a modern, easy-to-use application. The JCT platform creates a new way of e-learning by not just encouraging users to learn about cryptography and apply the algorithms themselves, but also to develop their own cryptographic plug-ins and extend the JCrypTool platform in new directions.



JCryptTool: User presentation

https://github.com/jcryptool/core/wiki/jcryptool_user_presentation/jcryptool_presentation_en.pdf

Certificate Verification

In this plug-in you can load three certificates and adjust their validity periods with six sliders. The signature and verification time can be adjusted with two additional sliders. Three validity models are available to validate this certificates and the validity periods.

Not Valid Before **Not Valid After**

2004 2034 2004 2034

Root CA
CA
User

Signature date
Verification date

2004 2034

Signature date
Verification date

Load Root CA certificate
Load CA certificate
Load User certificate

Log:
000 ###
Root CA: valid from: 01.09.2010, valid thru: 01.05.2032
CA: valid from: 01.03.2013, valid thru: 01.11.2029
User: valid from: 01.09.2015, valid thru: 01.01.2024
Signature date: 01.01.2019
Verification date: 01.09.2020
Dates based on selection SUCCESSFULLY validated with Shell model

Details to the certificates (adjust month and year with the sliders above; day can be set here)

	Root CA	CA	User	Signature date	Verification date
valid from:	1 /Sep/10	1 /Mar/13	1 /Sep/15	1 /Jan/19	1 /Sep/20
valid thru:	1 /May/32	1 /Nov/29	1 /Jan/24		

Shell model Modified Shell model Chain model

Validate ✓



About Cryptool 2

Cryptool 2 is the modern successor of [CrypTool 1](#), the well-known e-learning platform for cryptography and cryptanalysis.

Modern Plug'n'Play Interface / Visual Programming

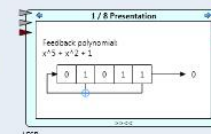
Cryptool 2 provides a graphical user interface for visual programming. So workflows can be visualized and controlled to enable intuitive manipulation and interaction of cryptographic functions.

The vector-oriented GUI is based on the Windows Presentation Foundation (WPF) and gives users the ability to scale the current view at will.



Visualization of Algorithms

The same component used for visual workflow programming can also visualize its inner operation. This makes it handy for the user to comprehend all the details of a cryptographic algorithm while seeing the bigger picture of how this algorithm may be used in a real-life scenario.



CrypTool 2: Sample screen

CrypTool 2.1 (Nightly Build 8450.1) - PaddingOracleAttack_AES.cwm

Start Bearbeiten Kryptotutorien Über

Neu Öffnen Speichern Drucken Starten Stoppen Protokoll

Startcenter CrypTool-Store CrypCloud Updates Einstellungen Hilfe

Komponenten Suche

Klassische Verfahren

- ADFGVX
- Caesar
- Enigma
- Fialka
- Hill-Chiffre
- Lorenz SZ42
- M-138
- M209
- Nihilist
- Playfair
- Purple
- Skytale
- Solitaire

Klassische Verfahren

- Moderne Verfahren
- Steganographie
- Hash-Funktionen
- Kryptoanalyse
- Protokolle
- Werkzeuge

CLIENT

Der Client will eine Nachricht an den Server schicken. Die Nachricht wird mit AES im CBC-Modus verschlüsselt. Sie besteht aus zwei 16 Bytes langen Blöcken: Der erste Block wird nur als Initialisierungsvektor verwendet, während der zweite die geheime Information enthält.

49 4E 49 54 76 45 43 54 EA 33
10 8C 92 07 06 05 02 03 04 05
06 07 08 09 01 02 03 04 05 06
07 08

95 Zeichen, 1 Zeile

Klartext

1234567812345678

16 Zeichen, 1 Zeile

Schlüssel

Padding-Oracle-Angriff

PHASE 1	PHASE 2	PHASE 3
Eingabe		
C1	C2	
Antwort vom Padding-Oracle		
Angriffslogik		
D2	C1	O
Angezeigte Bytes 1..8		
Orakel-Anfragen: 0		
Ausgabe		
C1	C2	

SERVER

Nach Empfang einer verschlüsselten Nachricht entschlüsselt der Server sie im CBC-Modus (C2 wird entschlüsselt und dann XOR-verknüpft mit C1). Anschließend wird das Padding überprüft. Das Ergebnis der Überprüfung wird dann als Wahr/Falsch-Antwort an den Angreifer zurückgegeben.

LEGENDE

C1: Der erste Block der Client-Nachricht (verschlüsselt).
C2: Der zweite Block der Client-Nachricht (verschlüsselt).
D2: Der entschlüsselte Block C2.
O: Das Overlay, das die Manipulation an C1 darstellt.
P2: Die resultierende Klartext-Nachricht. Während des Angriffs stellt P2 das Padding dar. Am Ende des Angriffs enthält P2 den zweiten Block der ursprünglichen Klartext-Nachricht.

Diese Komponente kann nur 8 Bytes pro Block gleichzeitig darstellen. Bei größeren Blöcken kann der Scrollbar benutzt werden, um alle Bytes anzuzeigen.

ANGREIFER

Der Angreifer sitzt zwischen dem Client und dem Server und liest alle Nachrichten mit. Sein Ziel ist, die geheime Information in der Nachricht zu entschlüsseln. Die Nachricht besteht aus den zwei Geheimtextblöcken C1 und C2. Die geheime Information ist in Block C2 enthalten. Die Entschlüsselung wird dadurch bewerkstelligt, dass der erste Geheimtextblock C1 manipuliert wird, Nachrichten an den Server geschickt werden und dessen Antworten darauf ausgewertet werden. Die Manipulation geschieht durch die XOR-Verknüpfung des originalen Blockes C1 und dem sogenannten "Overlay" O. Das Ergebnis dieser Berechnung ist die neue, manipulierte Block C1.

Der Angriff besteht aus den folgenden drei Phasen:

1. Finde ein gültiges Padding.
2. Bestimme die Länge des Paddings durch Auffinden des ersten Padding-Bytes.
3. Byteweise Entschlüsselung der Nachricht.

CrypTool: founded 1998 like ...

- Attac, Paris
- Google, Menlo Park
- CrypTool, Frankfurt



CrypTool 1: Two warnings

- legal
- worrywarts

besides
the
warnings:

CT1
still
made
it

CrypTool 1.4.41 - startingexample-en.txt

File Edit View Encrypt/Decrypt Digital Signatures/PKI Individ. Procedures Analysis Options Window Help

startingexample-en.txt

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) about cryptography offering extensive

This text file was

- 1) The starting page offers navigation functions via links. The starting page also offers navigation using the search function. Press F1 to start.
- 2) A possible next step is to generate a Symmetric (classical) key.
- 3) There are several examples that can be used.
- 4) You can further...
 - Navigating playfully
 - Reading the included files
 - Viewing the included files or via the "Document" menu
 - Viewing the web page

December 2017
The CrypTool Team

Press F1 to obtain help

Step by Step Signature Generation

```
graph TD; A[Open document] --> B[Document]; B --> C[Hash function]; C --> D[Compute hash value]; D --> E[Hash value]; E --> F[Encrypt hash value]; F --> G[Generate signature]; G --> H[Signature]; H --> I[Store signature]; B --> J[Generate key]; J --> K[RSA key]; K --> F; B --> L[Provide certificate]; L --> M[Certificate]; M --> G; I --> B; I --> J; I --> L; Cancel[Cancel];
```

Document: startingexample-en.txt

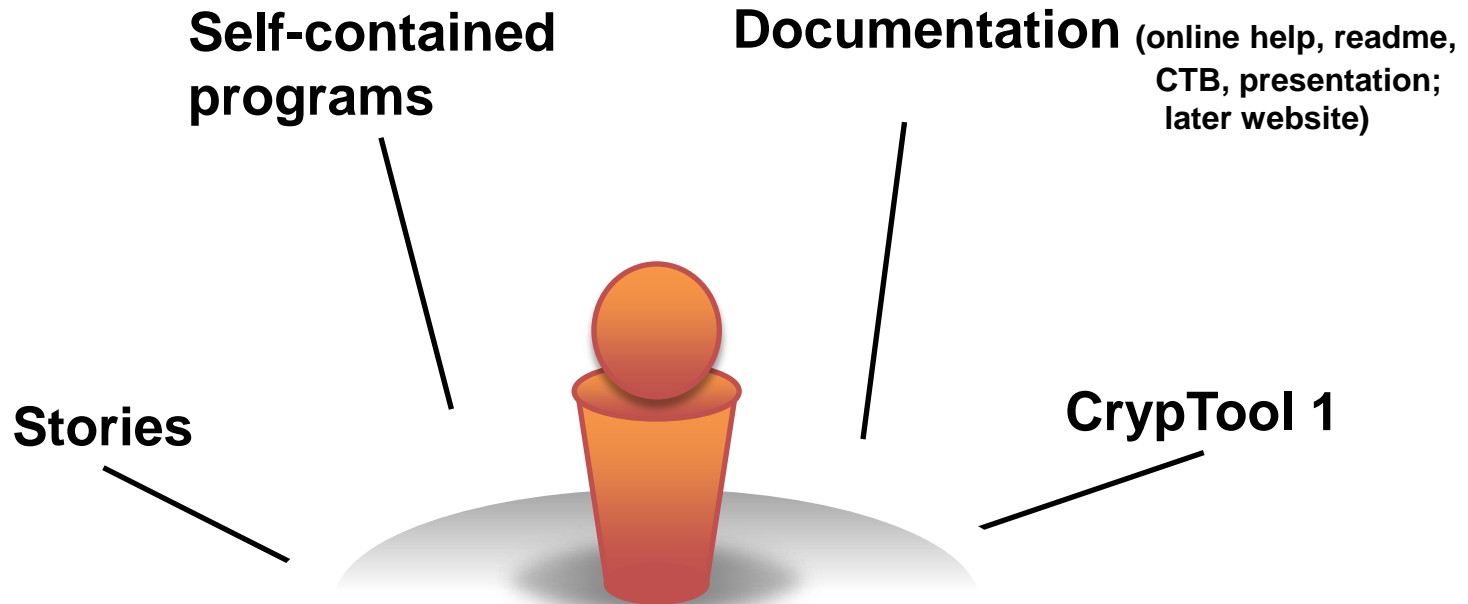
00000	53	74	61	72	74	69	6E	67	20	65	78	61	6D	70	6C	65	20	66	Starting example f
00012	6F	72	20	74	68	65	20	43	72	79	70	54	6F	6F	6C	20	76	65	or the CrypTool ve
00024	72	73	69	6F	6E	20	66	61	6D	69	6C	79	20	31	2E	78	20	28	rsion family 1.x (
00036	43	54	31	29	0D	0A	0D	0A	43	72	79	70	54	6F	6F	6C	20	31	CT1)...CrypTool 1
00048	20	28	43	54	31	29	20	69	73	20	61	20	63	6F	6D	70	72	65	(CT1) is a compre
0005A	68	65	6E	73	69	76	65	20	61	6E	64	20	66	72	65	65	20	65	hensive and free e
0006C	64	75	63	61	74	69	6F	6E	61	6C	20	70	72	6F	67	72	61	6D	educational program
0007E	0D	0A	61	62	6F	75	74	20	63	72	79	70	74	6F	67	72	61	70	..about cryptograph
00090	68	79	20	61	6E	64	20	63	72	79	70	74	61	6E	61	6C	79	73	hy and cryptanaly
000A2	69	73	0D	0A	6F	66	66	65	72	69	6E	67	20	65	78	74	65	6E	is..offering exten
000B4	73	69	76	65	20	6F	6E	6C	69	6E	65	20	68	65	6C	70	20	61	sive online help a

Playful learning

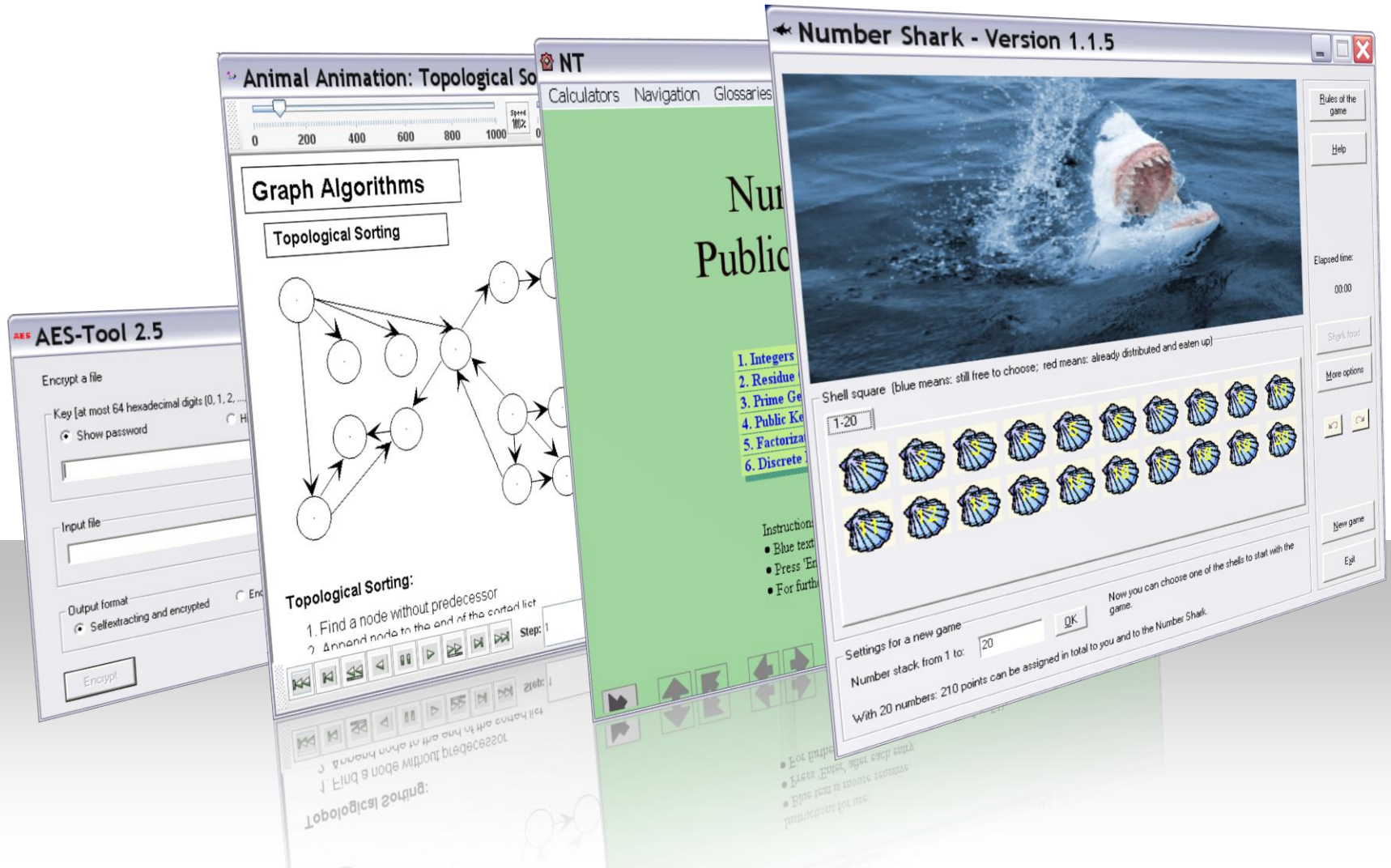
Serious tool

CrypTool can be used to visualize many concepts of cryptology: including digital signatures, symmetric, asymmetric and hybrid encryption, protocols, cryptanalysis, etc.

CrypTool 1 package



Self-contained programs



Flash animations



The Dialogue of the Sisters

The Chinese Labyrinth

- There are two stories included dealing with number theory and cryptography:
- In "The Dialogue of the Sisters" the title-role sisters use a variant of the RSA algorithm, in order to communicate securely.
 - In "The Chinese Labyrinth" Marco Polo has to solve number theoretic problems to become a minister of the Great Khan.

CrypTool website: 2003



CrypTool

TECHNISCHE UNIVERSITÄT DARMSTADT

UNIVERSITÄT SIEGEN

Theorie und Praxis für Karrieren von morgen

Deutsche Bank

CrypTool 1.3.05

eLearning Program za kriptografiju

Homepage
CT-Uvod

- ©to je CrypTool?
- Online pomoc, dokumentacija i vodici
- Screenshots
- O organizaciji
- Novo u ovoj verziji
- Izdavanje izvornog koda

Prezentacija [PDF]
Download

- Programski paket
- Izvorni kod

Pročitajte datoteka Vodič za studente
Linkovi

Kontakt/Imprint

Inicijatori:

- TU Darmstadt
- Deutsche Bank
- Siegen University
- Secude
- FZI

[German]
[English]

Hrvatski CrypTool Mirror je preveo i obradio: **Matej Matejiček**, MB 0036375274. Matej Matejiček je 2001. godine sudjelovao na izradi CrypTool alata, a zaslužan je za implementaciju testova i potrebne dokumentacije na njemačkom koji provjeravaju valjanost pseudoslučajnih generiranih brojeva. Ove preslika (*mirror*) stranice su rezultat seminarskog rada iz predmeta [Operacijski sustavi 2](#) iz područja [Računalne sigurnosti](#) na [Fakultetu elektrotehnike i računarstva](#) Sveučilišta u Zagrebu.

Kriptografija je inicijalno vezana uz tajnost pisanih poruke.

Danas je kriptografija aktivno područje istraživanja sa pregštom primjena u modernom životu (sustav za imobilizaciju u automobilima, mobilni telefoni, SSL veze između pregledavača internet stranica i poslužitelja, ...) -- uglavnom neprimječena.

Mnogo ljudi su još kao djeca pokušali enkriptirati poruke sa jednostavnim metodama. Ali, većina njih nikad nije dobila neku dublju predodžbu i ideju o modernoj kriptografiji. Sa CrypTool kriptografijom (i kriptozanalizom) se o tome može naučiti i uvijekzabati na zabavan način.

Open source projekt CrypTool koji je pokrenut od 1998 od strane gospodina Bernhard Esslinger-a, razvija freeware program CrypTool u želji da širi znanje. Ovaj program je korišten na sveučilištima, školama kao i u nacionalnim i internacionalnim kompanijama i agencijama.

Program CrypTool je eLearning alat za Windows operacijski sustav koji je tu da primjeni i analizira kriptografske mehanizme. Sadrži iscrpnu online pomoć sa vodičima/scenarijima i skriptom sa više detaljnih informacija.

Volonteri, pogotovo programeri i studenti koji planiraju pisati njihove teze su uvijek [dobrodoali](#) u ovaj svjetski projekt.

CrypTool 1.3.05 - startingexample-en.txt

File Edit View Crypt Digital Signatures Key Management Indiv. Procedures Analysis Options Window Help

startingexample-en.txt

CrypTool

This is a text file, shown in order to help you to make your first steps with CrypTool.

CrypTool website: 2008

CRYptTOOL

Acerca de Características Medios Documentación Descargas

Última versión estable: 1.4.21 Descargar (en inglés) (próximamente en Castellano)

Acerca de

- Introducción a CrypTool
- CrypTool en la Educación
- CrypTool para el Conocimiento
- Cobertura en los medios
- Premios
- Colaboradores
- Proyectos Relacionados
- Contacto

Selected Landmark en 2008:

Germany
Land of Ideas

"CrypTool ist einmalig, medial anregend aufgebaut und, soweit ich es ubersieht, ohne Fehler."
-Prof. Dr. Ruediger Grimm, TU Ilmenau

Introducción a CrypTool

CrypTool es una aplicación de aprendizaje electrónico gratuita para Windows. Puede utilizarse para aplicar y analizar algoritmos criptográficos. La versión actual de CrypTool se utiliza en todo el mundo. Soporta tanto los métodos actuales de enseñanza en escuelas y universidades como la concienciación de los empleados.

La versión actual ofrece, **entre otras cosas**, lo siguiente:

- Numerosos algoritmos criptográficos, clásicos y modernos (cifrado y descifrado, generación de clave, contraseñas seguras, autenticación, protocolos seguros, ...)
- Visualización de varios métodos (p.ej. César, Enigma, RSA, Diffie-Hellman, firmas digitales, AES)
- Criptoanálisis de ciertos algoritmos (p.ej. Vigenère, RSA, AES)
- Métodos de medida criptoanalítica (p.ej. entropía, n-grams, autocorrelación)
- Métodos auxiliares (p.ej. tests de primalidad, factorización, codificación en base64)
- Tutorial sobre teoría de números.
- Ayuda detallada on-line.
- Script con más información sobre criptografía.

Desde su uso original para la formación en seguridad de una compañía, CrypTool ha evolucionado en un destacado proyecto de código abierto para temas relacionados con la criptografía.

Desde la primavera de 2008, está funcionando dentro del proyecto CrypTool el **Cripto Portal para profesores**. Por ahora el portal sólo está disponible en alemán y se espera que actúe como una plataforma para que los profesores puedan compartir material para la enseñanza de la criptografía y temas relacionados.

Actualmente el equipo de CrypTool está trabajando en dos proyectos futuros que se espera que sean los sucesores de la actual versión CrypTool 1.4.x que está escrita en C++. Ambos proyectos de continuación utilizan el último modelo de estándares de programación, pero aún están en un estado alfa/beta:

- CrypTool 2.0** se desarrolla en C# con Visual Studio 2008 (Express Edition) y **WPF**. La versión alfa (para desarrolladores) se hizo pública en Abril de 2008. Esta versión proporciona una arquitectura completamente desarrollada y una práctica funcionalidad criptográfica combinada con una pionera interfaz gráfica con la funcionalidad de *drag-and-drop*.
- JCrypTool** se desarrolla en Java basado en **Eclipse RCP**. La primera versión (llamada milestone 1) se hizo pública en Agosto de 2007, la publicación de la siguiente versión (llamada milestone2, esperada para desarrolladores y usuarios) se espera para Junio de 2008. JCrypTool es independiente de plataforma y trabaja junto con el FlexiProvider (un potente conjunto de herramientas para la Java Cryptography Architecture JCA) desarrollado por el TU Darmstadt, y con BouncyCastle.

En la **hoja de ruta** puede encontrar las nuevas características planeadas para ambas futuras versiones, y las fechas esperadas para la publicación de la próxima versión de CrypTool 1.4.x.

Voluntarios, especialmente programadores y estudiantes que planeen escribir sus tesis, son siempre **bienvenidos** a unirse para el desarrollo de este proyecto world-wide.

Contacto **Imprint** **Mapa web**

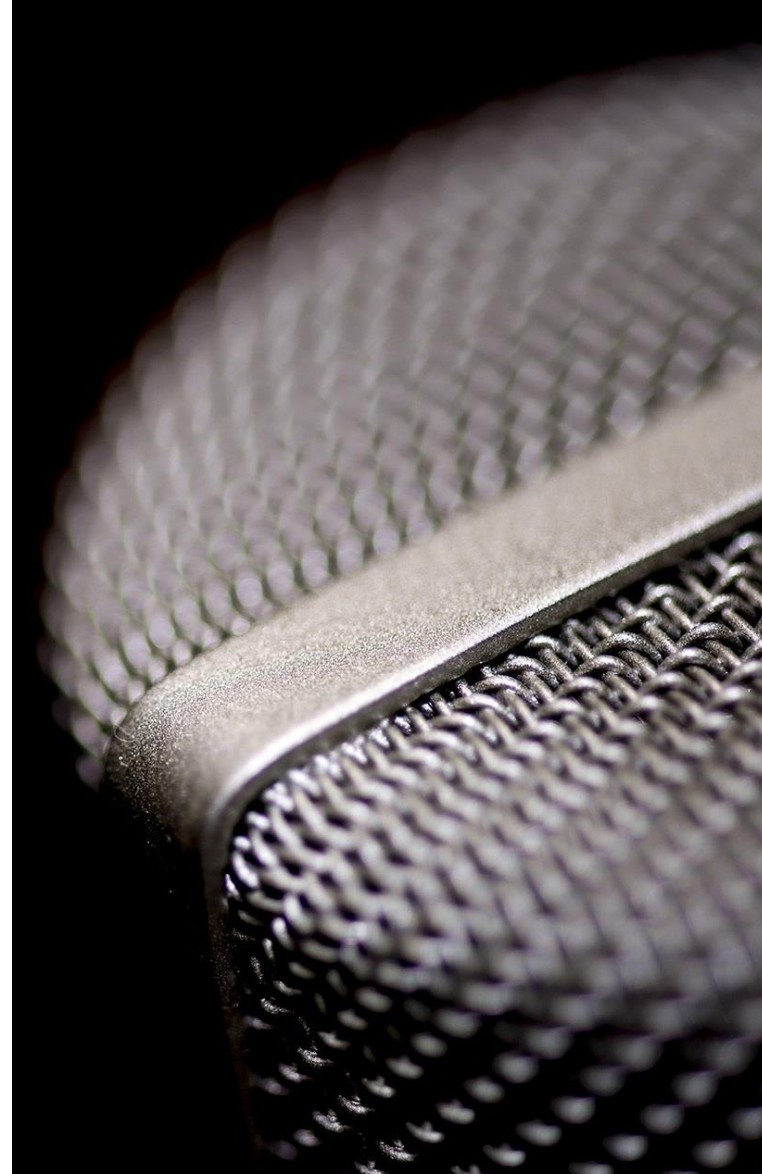
Última modificación de la página: October 28, 2008 - 14:03
Copyright © 1998 - 2008 Deutsche Bank / Contributors

Hosting / CT2 + JCT

- hosting: DA, Duisburg-Essen, Kassel
→ Munich
- the two CT1 successors CT2 + JCT
 - started in 2008,
 - their 1st public version available in 2011

Samples for having to act like **professionals**

- server certificates
- signed executables
- trade mark for the name „CrypTool“
- General Data Protection Regulation (GDPR)
- update permanently

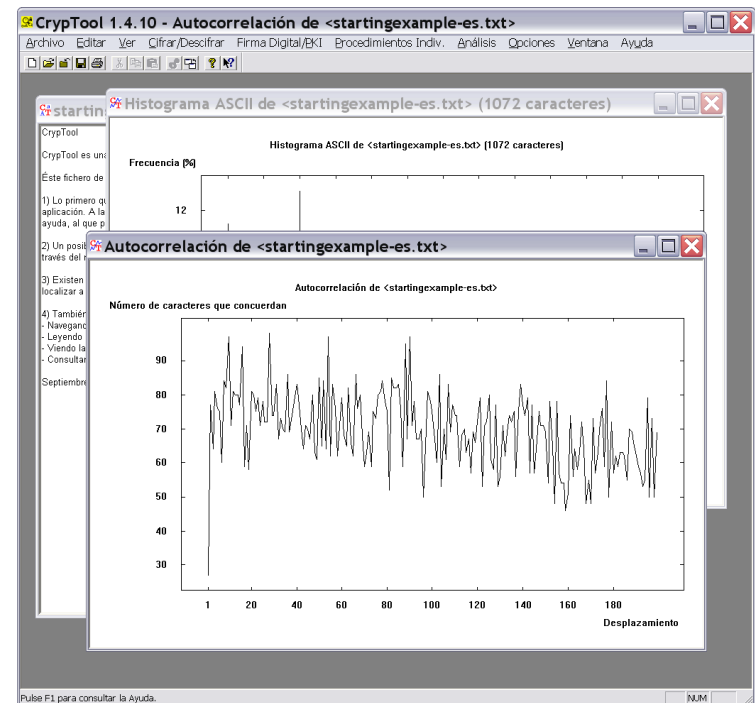


Working mode with **students**

- core team of professionals and maintainers
- students: new stuff during their theses
- students: joining our way for a longer time
- current students' theses or projects:
 - SPHINCS+ Hagenberg
 - DCA tutorial Siegen
 - Signatures Passau
 - VIC Bratislava
 - Grover Aachen/Munich
 - PQC Darmstadt (Fraunhofer)
 - Cipher type detection San Jose

Subprojects: **CrypTool 1 (CT1)**

- today only maintenance
- available in 6 languages
- still high share of all downloads
- specialty:
F1 for menu items
- last release version
1.4.41 from Nov 2017



Subprojects: CT2 and JCT

- currently our major versions
 - 64 bit
- ➔ closer look at these: later today



CRYPTtOOL 2 Cryptography for everybody

Nightly Build – Version 2.1.8444.1

Please feel free to further improve CrypTool 2.
We are glad about any feedback on our website.

For more information take a look at our website:
<https://www.cryptool.org/cryptool2>

<http://www.cryptool.org>



JCrypTool



The cryptography e-learning platform.

Setup **sizes** and source **loc**

	Setup Size	Lines of Code
CT1	ca. 70 MB	ca. 300' in C/C++/Java and Perl ca. 90' in rc files for GUI resources ca. 70' in html and txt for online help
CT2	ca. 170 MB	ca. 600' in C#/C++/Java *metrics vague
JCT	ca. 130 MB	ca. 200' in Java/C/C++

Subprojects: CTO

- cryptography and awareness in the browser
- started 2010
- 2016 last bigger change (new backend with Joomla 3.6, Bootstrap, JS; quicker react times; better responsiveness)
- ... more later today

What is CrypTool-Online?

CrypTool-Online (CTO) runs in a browser and provides a variety of encryption and cryptanalysis methods including illustrated examples and tools like password generator and password meter.

[CrypTool 1](#)
[CrypTool 2](#)
[JCrypTool](#)
[CRYPTOOL 1](#)
[CRYPTOOL 2](#)
[JCrypTool](#)
[CRYPTOOL ONLINE](#)
[MYSTERY TWISTER C3](#)
[About CrypTool-Online](#)
[Ciphers ▾](#)
[Codings ▾](#)
[Cryptanalysis ▾](#)
[Highlights ▾](#)
[Documentation ▾](#)

CTO OVERVIEW

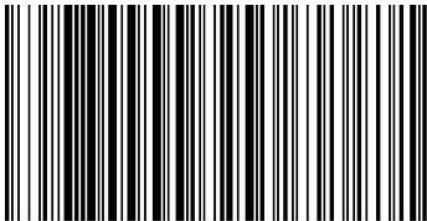
CIPHERS

How do classical ciphers work?



CODINGS

Where are codings used and how do they work?



CRYPTANALYSIS

How to obtain the plaintext without knowing the decryption key?

About CrypTool-Online (CTO)

Encrypt directly within your browser

CrypTool-Online provides an exciting insight into the world of cryptology. A variety of ciphers, coding methods, and analysis tools are introduced together with illustrated examples. Our emphasis is on making explanations easy to understand in order to further the general interest in cryptography and cryptanalysis. Therefore, you can experiment with the introduced methods in an interactive way directly on the website.

So you can learn the fundamentals of historically relevant ciphers in a little while, and also use the tools under **Ciphers** to encrypt messages yourself. You can also decrypt and **analyze** already encrypted messages and discover weaknesses of different ciphers. Under **Highlights**, you can for instance check the modern cipher AES or let the site generate good passwords for you.

CrypTool-Online is the online version of the e-learning program CrypTool. The so-called download (or offline) versions of CrypTool are also free and suitable for working with longer texts and conducting high performance analyses on encrypted messages.

Developers who like to join and enhance CTO with self-written plugins, find a good guidance in the Wiki. Especially the page How-to-Start leads you step-by-step.

This site works together with the website www.cryptoprograms.com, and partly is a successor of it. The author of cryptograms.com develops the famous Windows analyzer of classic ciphers **CryptoCrack**.

Another example of CTO

CRYPTOOL-ONLINE
Cryptography for everybody

HOME LANGUAGE

Search ...

CRYPTOOL-ONLINE

ABOUT CRYPTOOL-ONLINE CIPHERS CODINGS CRYPTANALYSIS HIGHLIGHTS DOCUMENTATION

Password Meter

How secure your password is classified by different evaluation methods, you can check here purely locally. Your entries are neither transferred nor stored. For a good password, the length is most important.

tvtoday1.A|

Show password Length: 10

Manage dictionaries

Rating

KeePass:	49% (62 Bits)	<div style="width: 49%; background-color: red;"></div>
Mozilla:	65%	<div style="width: 65%; background-color: orange;"></div>
PGP:	41% (52 Bits)	<div style="width: 41%; background-color: red;"></div>
zxcvbn:	75%	<div style="width: 75%; background-color: green;"></div>
Stutz' PS:	57% (43 Bits)	<div style="width: 57%; background-color: orange;"></div>
Total:	57%	<div style="width: 57%; background-color: orange;"></div>

The color of the progress bar indicates the password strength: red = very weak, yellow = medium and green = very strong.

Subprojects: **MTC3**

- permanent crypto challenge contest
- started in 2010
- since then, more than 25,000 challenges solved



... more tomorrow

Source of picture: pixabay

Subprojects: **MTC3**

The screenshot displays the MysteryTwister C3 website interface. At the top left, the logo reads "MysteryTwister C3 THE CRYPTO CHALLENGE CONTEST". To the right, a statistics box shows "NUMBER OF ACTIVE MEMBERS: 9924" with a "Register here" button. Further right, it lists "MTC3 PARTNERS" with a CITS logo and social media icons for Facebook and Twitter. A search bar is located below the logo. A navigation menu includes "Start", "Challenges", and "Forum". A secondary menu lists "The four levels", "Level I", "Level II", "Level III", "Level X", "Challenges Hall-of-Fame", "Overall Hall-of-Fame", and "Submit a challenge". The main content area features four challenge cards: Level I (42/82 solved), Level II (24/133 solved), Level III (0/62 solved), and Level X (0/18 solved).

Level	Solved	Total
Level I	42	82
Level II	24	133
Level III	0	62
Level X	0	18

... more tomorrow

Subprojects: **MTC3**

Sample challenges

The screenshot shows the MTC3 website interface. At the top, there is a navigation bar with 'Start', 'Challenges', and 'Forum' tabs. On the right, there are links for 'Login', 'DE', and 'EN'. Below this is a secondary navigation bar with 'The four levels', 'Level I', 'Level II', 'Level III', 'Level X', 'Challenges Hall-of-Fame', 'Overall Hall-of-Fame', and 'Submit a challenge'. The main content area is titled 'Level I Challenges (82)'. Below the title, it says 'All challenges in Level I, ordered by date posted (the most recent appear first)'. The first challenge listed is 'Music Code — Part 1' by user 'wolter-01', with 38 users already solved it and 26 are working on it. The challenge description states: 'A piece of music is given as mp3 file and in music notation. The notes represent a secret message, which was encrypted with two classic methods. In part 1 of this challenge you have to solve the first of these methods. Thereafter, you can set out to solve part 2 (which is in level 2). Read more...'. There are three icons below the description: a document icon with a link to the forum topic, a download icon with a link to download the challenge, and a document icon with a link to download an additional file. A message below the challenge states: 'You must be logged in to solve the challenge'. The second challenge listed is 'Post-Quantum Cryptography: Unbalanced Oil and Vinegar System — Part 1' by user 'wolf-01', with 86 users already solved it and 2 are working on it.

Start Challenges Forum Login DE EN

The four levels **Level I** Level II Level III Level X Challenges Hall-of-Fame Overall Hall-of-Fame Submit a challenge

Level I Challenges (82)

All challenges in **Level I**, ordered by date posted (the most recent appear first).

1 **Music Code — Part 1** [wolter-01] - 38 users already solved this challenge, 26 are working on it.

A piece of music is given as mp3 file and in music notation. The notes represent a secret message, which was encrypted with two classic methods. In part 1 of this challenge you have to solve the first of these methods. Thereafter, you can set out to solve part 2 (which is in level 2).
[Read more...](#)

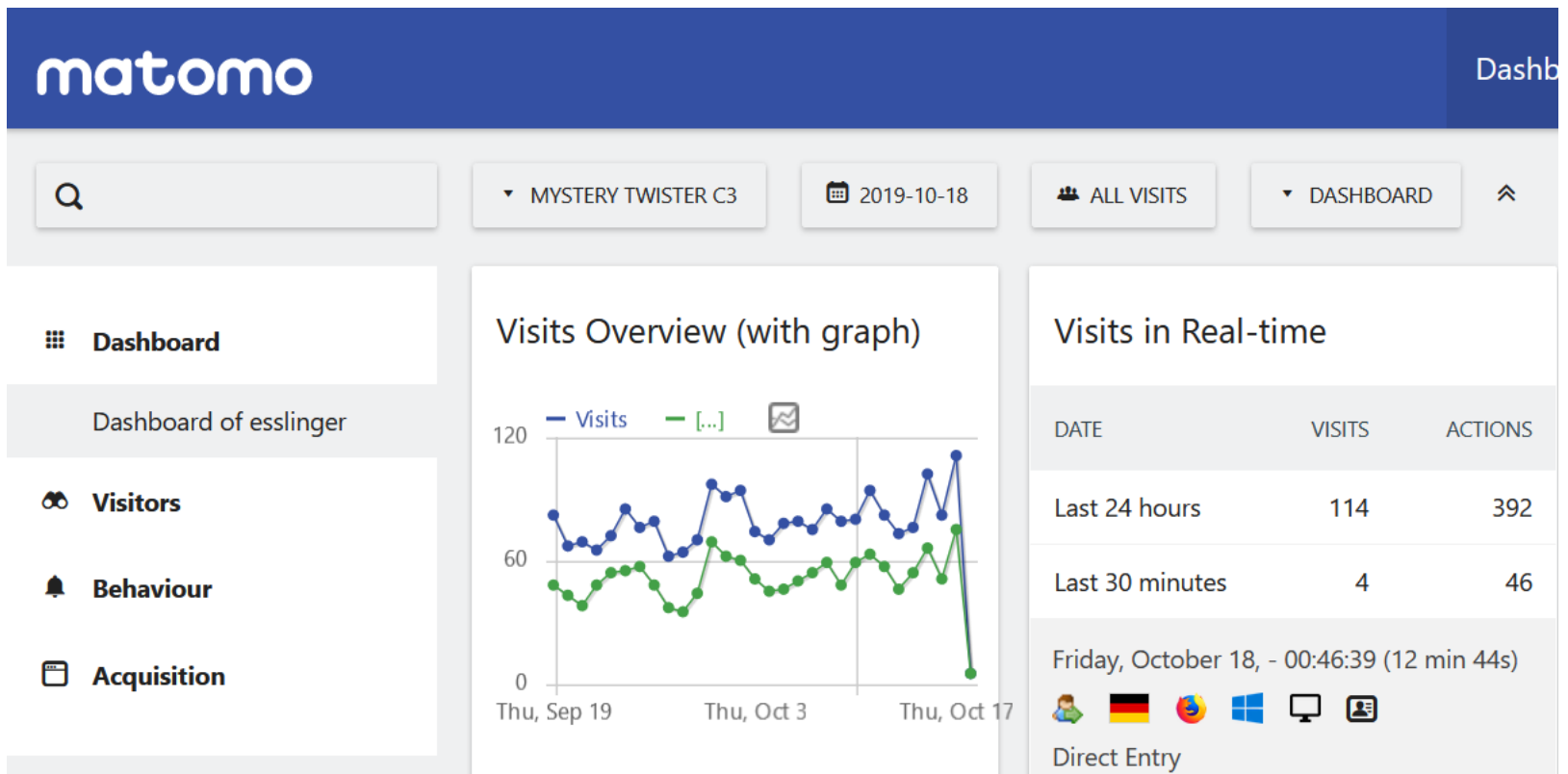
- Click [here](#) to get to the corresponding forum topic to share your opinion.
- Click [here](#) to download the challenge.
- Click [here](#) to download the additional file of the challenge.

You must be **logged in** to solve the challenge

1 **Post-Quantum Cryptography: Unbalanced Oil and Vinegar System — Part 1** [wolf-01] - 86 users already solved this challenge, 2 are working on it.

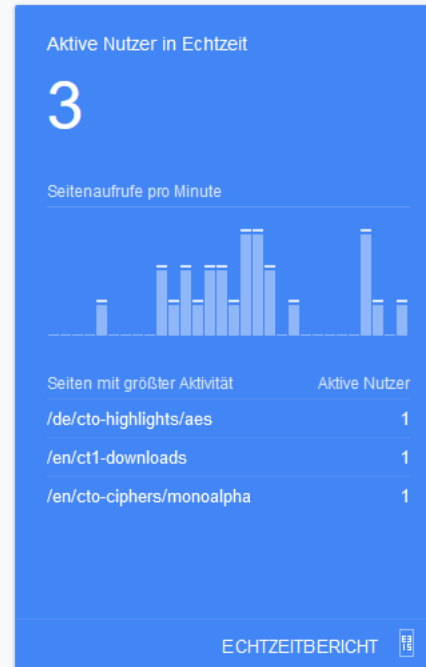
Statistics: MTC3

> 70 distinguished users per day



Statistics: CTO and CTP

Google Analytics-Startseite



Wo befinden sich meine Nutzer?

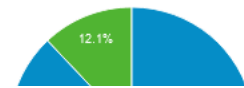


Oct 10, 2019

Statistics: CTO and CTP



■ New Visitor ■ Returning Visitor



Country	Users	% Users
1. Germany	19,173	31.46%
2. United States	9,956	16.34%
3. India	3,797	6.23%
4. Switzerland	2,316	3.80%
5. China	1,970	3.23%
6. Austria	1,716	2.82%
7. United Kingdom	1,310	2.15%
8. Australia	1,297	2.13%
9. Taiwan	1,211	1.99%
10. Canada	1,135	1.86%

Architecture: CTO and CTP

To be decided in the near future:

- move to static html

or

- update to Joomla 4

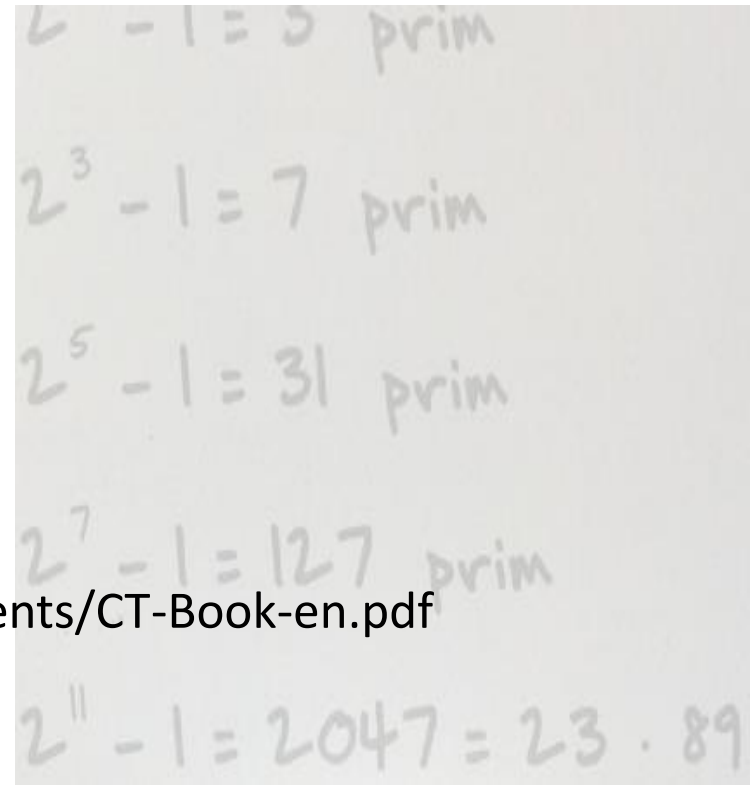


Source of picture: pixabay

Subprojects: **CrypTool Book**

- some theory and how to apply crypto with the CT programs and with SageMath
 - loc in 2017:
 - 61,545 LaTeX code (tex)
 - 825 Sage code (sage)
- ... more tomorrow

<https://www.cryptool.org/images/ctp/documents/CT-Book-en.pdf>



- Overview about the Content of the CrypTool Book
- Contents Overview
- Contents
- Preface to the 12th Edition of the CrypTool Book
- Introduction – How do the Book and the Programs Play together?
- ▶ 1 Security Definitions and Encryption Procedures
- ▶ 2 Paper and Pencil Encryption Methods
- ▶ 3 Prime Numbers
- ▶ 4 Introduction to Elementary Number Theory with Examples
- ▶ 5 The Mathematical Ideas behind Modern Cryptography
- ▼ 6 Hash Functions and Digital Signatures
 - ▶ 6.1 Hash functions
 - 6.2 RSA signatures
 - 6.3 DSA signatures
 - ▶ 6.4 Public key certification
 - Bibliography
- ▶ 7 Elliptic Curves
- ▶ 8 Introduction to Bitblock and Bitstream Ciphers
- ▶ 9 Homomorphic Ciphers
- ▶ 10 Survey on Current Academic Results for Solving Discrete Logarithms and for Factoring
- ▶ 11 Crypto 2020 — Perspectives for Long-Term Cryptographic Security
- ▶ A Appendix
- GNU Free Documentation License
- List of Figures



The CrypTool Book: Learning and Experiencing Cryptography with CrypTool and SageMath

Prof. Bernhard Esslinger
and the Development Team
of the Open-Source Software CrypTool

Website: **Function volume**

CT offers > 400 different crypto functions

- CT1 >= 125
- CT2 >= 245
- JCT >= 125
- CTO >= 45

<https://www.cryptool.org/en/ctp-documentation/functionvolume>

Cryptological functions in different CrypTool versions

SELECTION

Cryptographic category:

No filter applied v

Additional search phrase:

CrypTool 1 (CT1)

CrypTool 2 (CT2)

JCryptTool (JCT)

CrypTool Online (CTO)

405 rows found according to the selection criteria.

Function	CT1	CT2	JCT	CTO	CT 1 Path	CT 2 Path	JCT Path	CTO Path
3DES	X	C	A		Encrypt/Decrypt\ Symmetric (modern)\ Triple DES...	[C] Modern Ciphers\ Symmetric\ DES	[A] Block Ciphers\ Block Ciphers\ DESede_CBC (OID: 1.2.840.113549.3.7)	
3DES Brute-Force Attack	X	C\T			Analysis\ Symmetric Encryption (modern)\ Triple DES...	[C] Cryptanalysis\ Specific\ KeySearcher [T] Cryptanalysis\ Modern\ Triple DES Brute-force Analysis		
Achterbahn		C\T				[C] Modern Ciphers\ Symmetric\ Achterbahn [T] Cryptography\ Modern\ Symmetric\ Achterbahn Cipher		
ADFGVX	X	C\T\W	D	X	Encrypt/Decrypt\ Symmetric (classic)\ ADFGVX...	[C] Classic Ciphers\ ADFGVX [T] Cryptanalysis\ Classical\ ADFGVX Cipher dictionary	[D] Algorithms\ Classic\ ADFGVX	Ciphers\ ADFGVX

Where are we today (1)

- overall program downloads (since 2003)
> 1 million times
- Alexa rank: between 400,000 and 600,000
- more than 100 bachelor and master theses contributed to it
- developers and users come from all over the world
- mentioned in books, courses, websites, ...

Where are we today (2)

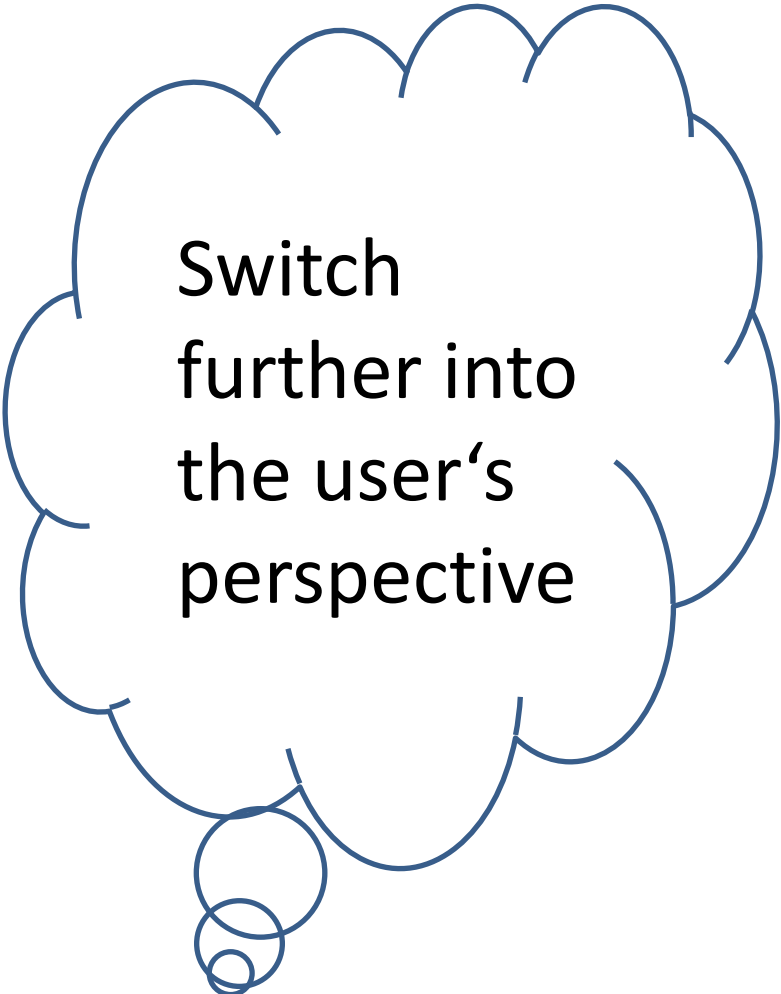
- ➔ CT became the most widespread open-source e-learning program for cryptography and cryptanalysis
- after 21 years ... still an active project with over 1 mio loc being maintained and running
- success has many piles – especially single, dedicated and knowledgeable people ...

Can we be satisfied with that?

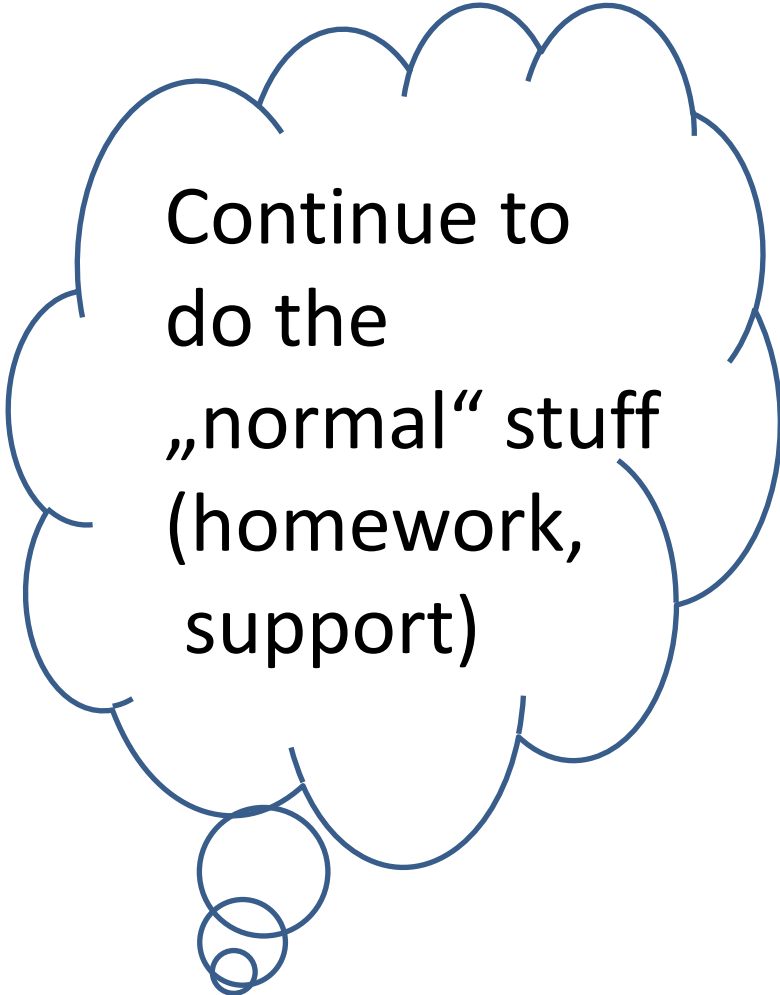
Yes (many goals achieved) **and No**

- many chairs not contributing yet
- more researchers using it
- not present in "normal" paper press like "Spiegel" or broadcast television
- weak perception in social media and on smartphones yet
- kind of misuse of our name just noticed – what to do?

Future tasks: 4 core areas

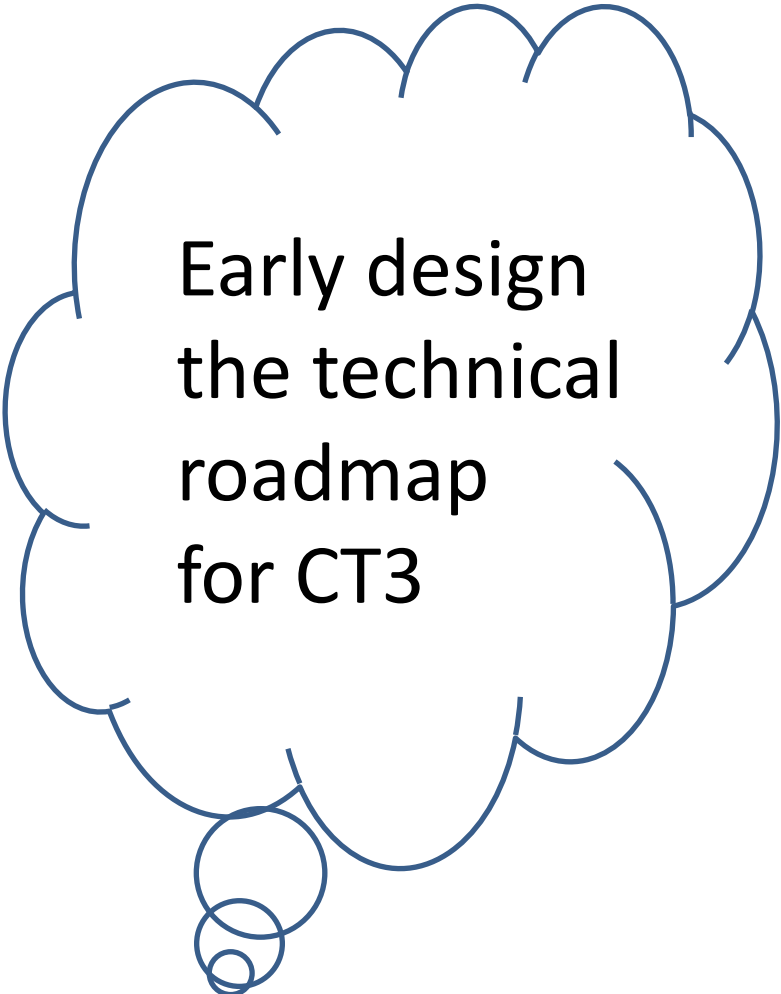
A blue-outlined thought bubble with a scalloped top edge and a tail of three overlapping circles at the bottom.

Switch
further into
the user's
perspective

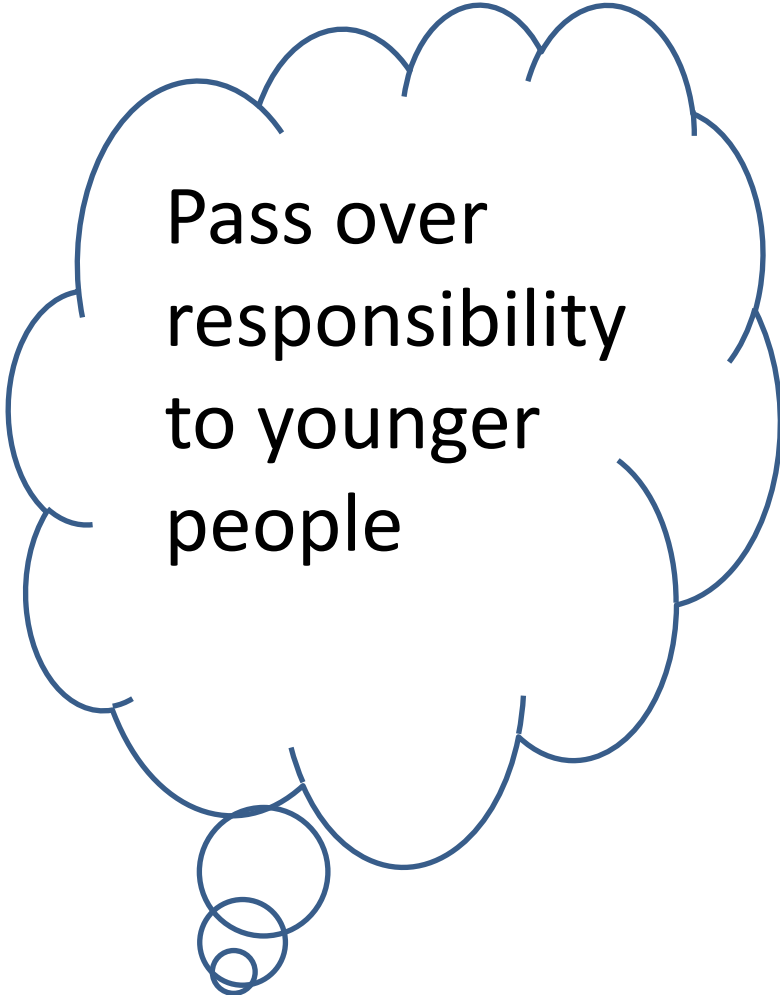
A blue-outlined thought bubble with a scalloped top edge and a tail of three overlapping circles at the bottom.

Continue to
do the
„normal“ stuff
(homework,
support)

Future tasks: 4 core areas

A blue-outlined thought bubble with a scalloped top edge and a tail of three overlapping circles at the bottom.

Early design
the technical
roadmap
for CT3

A blue-outlined thought bubble with a scalloped top edge and a tail of three overlapping circles at the bottom.

Pass over
responsibility
to younger
people

CrypTool is **THE e-Learning
program for cryptology**



CrypTool.org
bernhard.esslinger@gmail.com

Contribution samples

University	CT	Plugin
Hagenberg, Eindhoven	JCT	Post-quantum signature series: WOTS, Merkle, SPHINCS
Duisburg-Essen	CT2	Quantum key-exchange protocol BB84
Utrecht	JCT	Elliptic curve calculations over \mathbb{R} , $\mathbb{F}(p)$, and $\mathbb{F}(2^m)$
Hagen	JCT	Inner states of DES
Frankfurt, Darmstadt	JCT	Kleptography (4 attacks implemented)
Kassel, Belgrade	CT2	Network communication, chat
Bochum	CT2	Keccak for hashing (SHA3), as PRNG, and as stream cipher
Frankfurt	CT2	Padding-oracle attack
Kassel	CT2	Heartbleed attack against a life server
Kassel, Duisburg	CT2	CrypCloud – distributed computing
Bochum	CT2	SAT solver (analyzer works, still problem with port from Unix)
Brno (Freiburg)	CT2	Protocols like oblivious transfer, dining cryptographers
Bratislava	CT2	Fialka, VIC

Some contributing universities

Belgrad, Berlin, Bochum, Bonn, Brisbane, Brno, Darmstadt, Dubai, Duisburg-Essen, Eindhoven, Frankfurt, Hagenberg, Jena, Karlsruhe, Kassel, Klagenfurth, Koblenz, London, Madrid, Mannheim, Osnabrück, San Jose, Siegen, Thessaloniki, Utrecht, Warsaw, ...

Abbreviations used

CT	CrypTool
CT1	CrypTool v1 (e-learning program)
CT2	CrypTool v2 (e-learning program)
JCT	JavaCrypTool (e-learning program)
CTO	CrypTool-Online (apply crypto in a browser)
MTC3	MysteryTwister C3 (international cipher contest)
CTP	CrypTool Portal (main website www.cryptool.org)
CTB	CT Book (free and open-source, too)