
JCryptTool

Open-Source eLearning-Programm für Kryptologie

Simon Leischnig

Prof. Bernhard Esslinger

13.03.2021

<https://www.cryptool.org/de/jct/>

Was ist JCrypTool?

- Lernprogramm
- Kryptologie / Kryptografie
- Geschrieben in Java, aufbauend auf Eclipse
- Windows, OS/X... und Linux

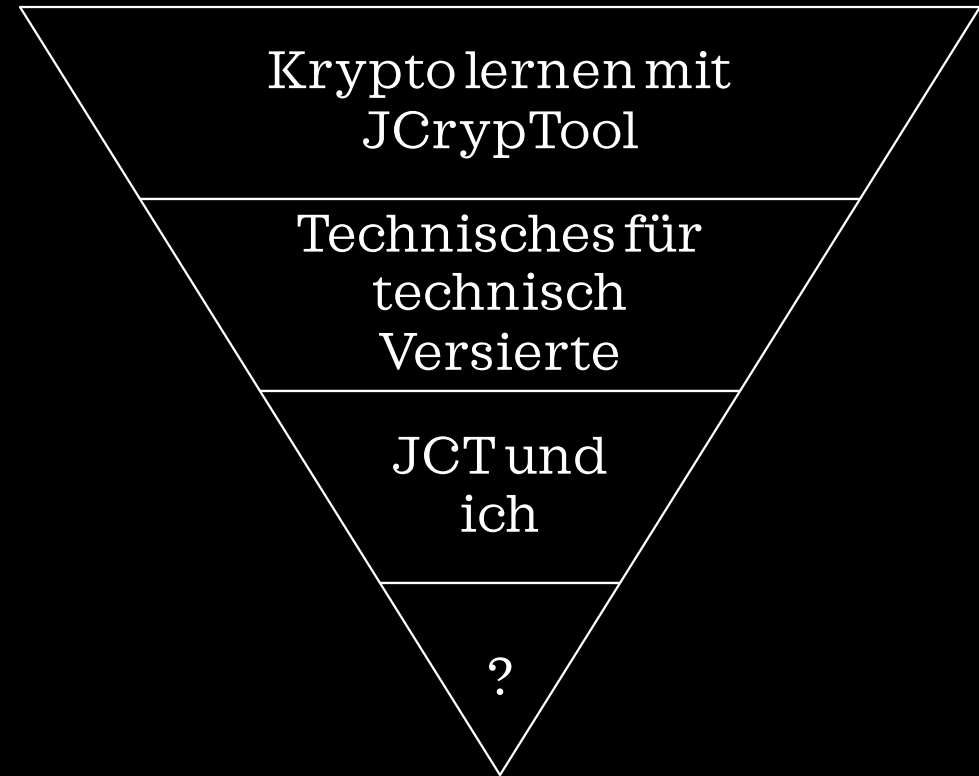


Ziele von JCrypTool

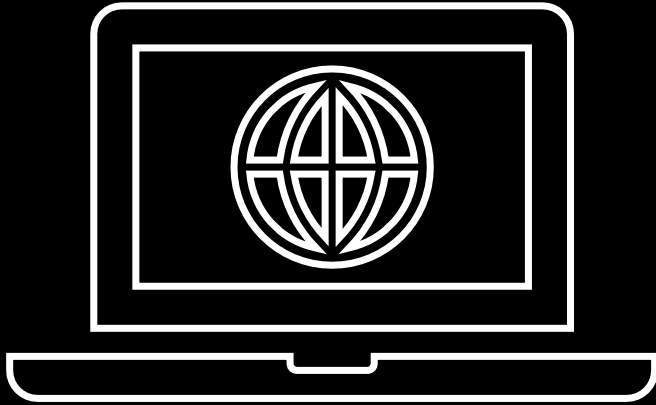
- Kryptografie fassbar und erlernbar machen
- Ausprobieren, variieren, entdecken
- Try & Error → Success?

Ziele dieses Vortrags

- JCrypTool (JCT) kennen lernen
- Streifzug Kryptografie für Anfänger
- Open-Source-Einstieg und technischer Überblick für Fortgeschrittene



Einstieg: Monoalphabetische Substitution



Weiter geht's im Webcamfenster.

Einstieg: Monoalphabetische Substitution

Klartext

K L A R T E X T T E S T

Schlüssel

A E K L R S T X

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

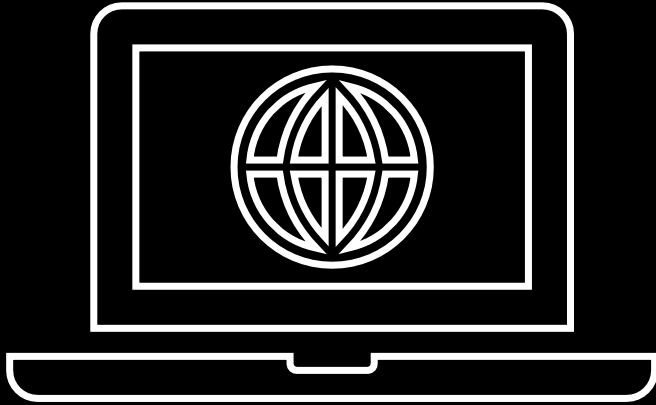
G N U L I M U X

Geheimtext

K L A R T E X T T E S T

U L G I U N X U U N M U

Und los!



Es geht weiter im
Videoformat!

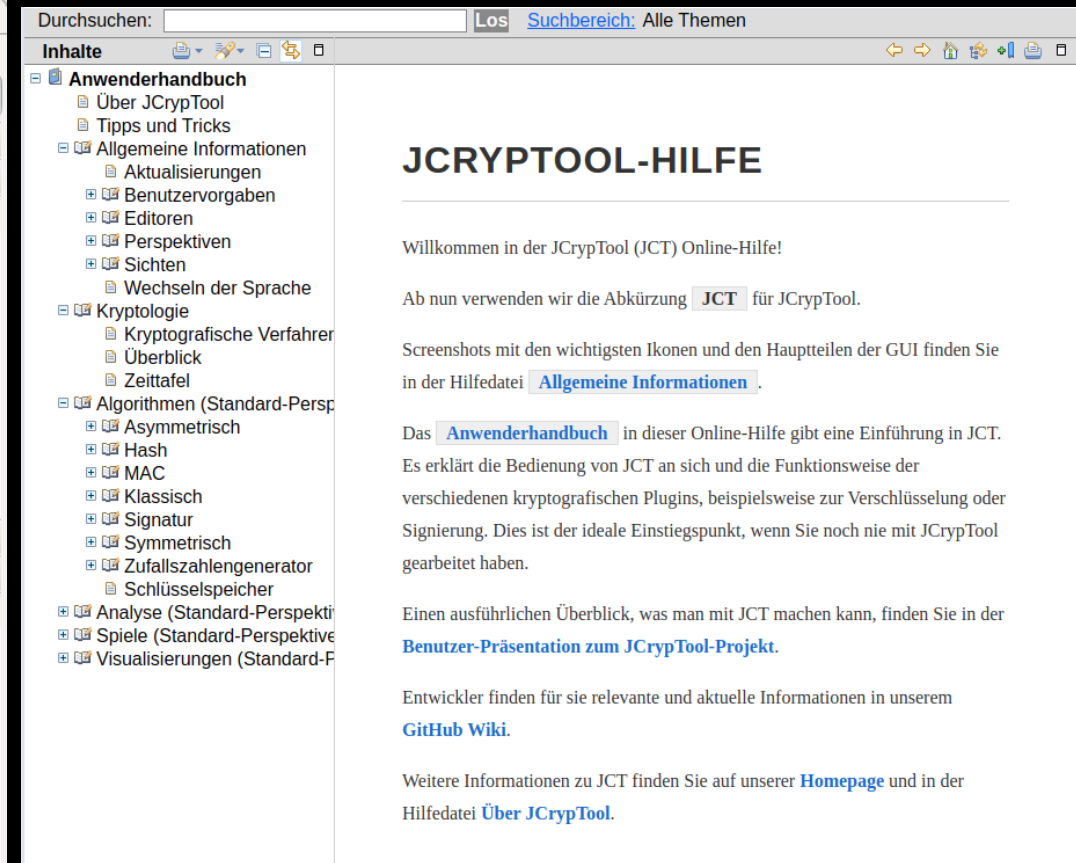
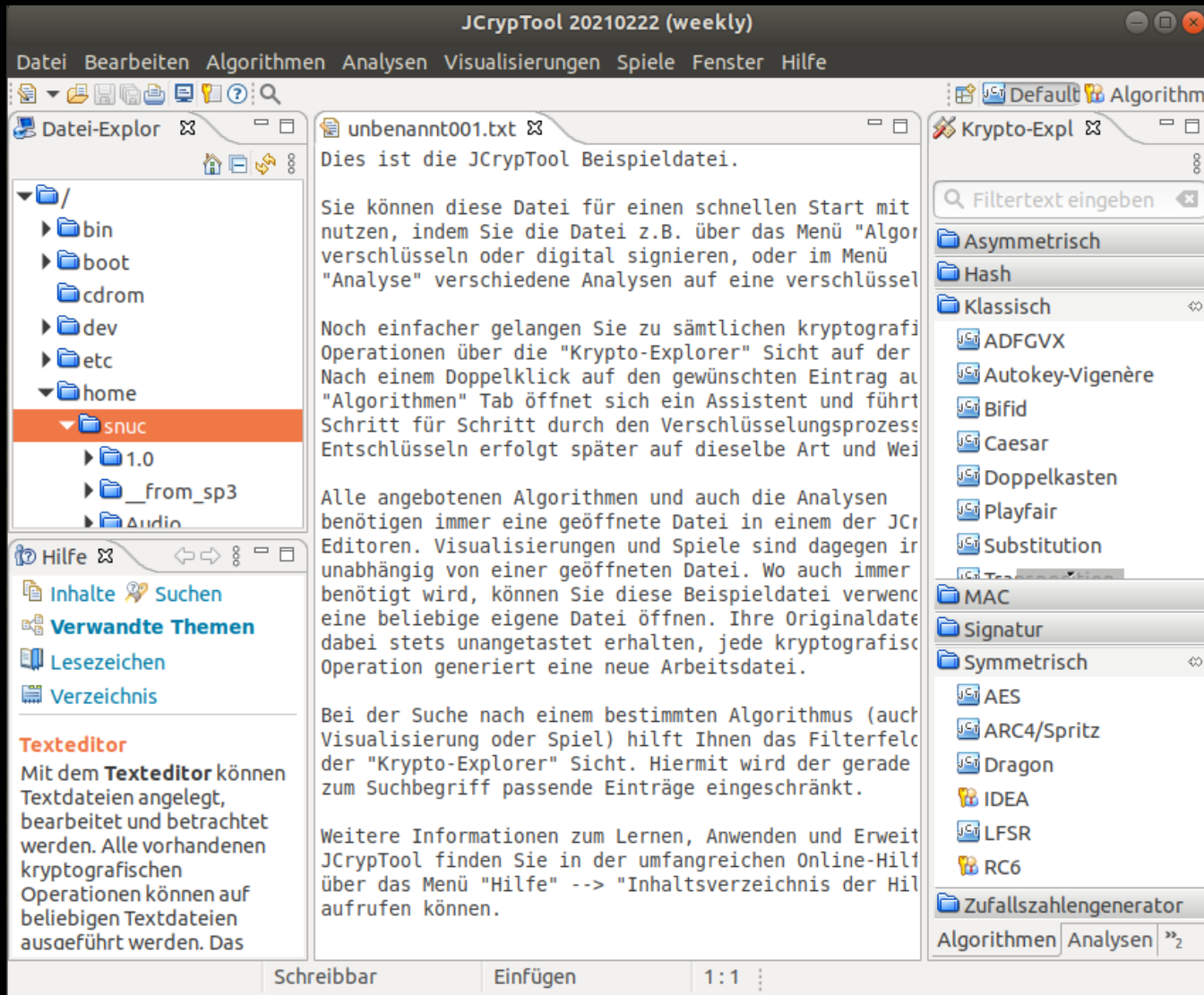
JCrypTool: Facts

- Open-Source-Projekt basierend auf der Eclipse Rich Client Platform (RCP), EPL
- Seit 2007
- Knapp 120 Contributors, über 100 Plug-ins
- Aktuelle Version: 1.0.3
- Umfangreiches Hilfe-Kompendium

Technisches: Hosting & Build

- Git, semi-monolithisches Repository
- Maven als Buildsystem
- Hosting:
 - GitHub — <https://github.com/jcryptool>
 - CrypTool-Projekt: <https://www.cryptool.org/>
- Continuous Integration: Travis CI
- Wöchentliche Snapshot Builds, seltener Releases (1.0.3 aktuell)

Technisches: die Eclipse RCP als Basis



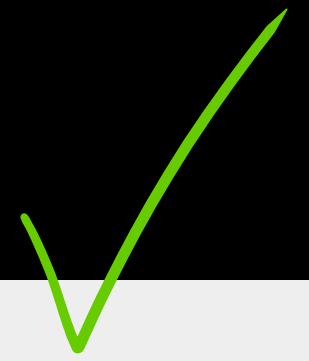
Technisches: Eclipse RCP, OSGi und Dependencies

- Maven, aber Tycho on Maven...
- OSGi bundles statt Maven Bundles

```
<dependency>  
  <groupId>com.google.guava</groupId>  
  <artifactId>guava</artifactId>  
  <version>30.1-jre</version>  
</dependency>
```

- Build-"Cruft" + Scripts = Lösung: Repackaging!

```
<artifact>  
  <id>org.jcryptool.thirdparty:\  
    org.jcryptool.thirdparty.m2bundle.jaxb:\  
    ${global.version}  
  </id>  
</artifact>
```



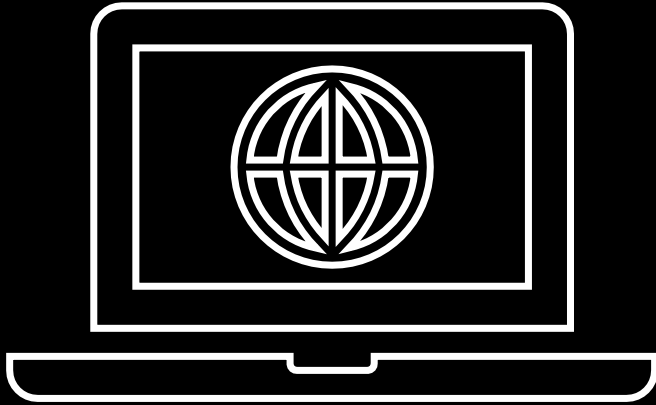
YouCrypTool: Du und JCrypTool

- Jeder kann mitmachen!
 - Übersetzen, Hilfe schreiben (html), Feedback, Testen, ...
 - Und natürlich coden und Bugs fixen
- Kleines Kernteam, viel Platz zur freien Entfaltung!
- Große Codebasis zum Ableiten eigener Ideen
- <https://gitter.im/dshadow/jcryptool> — unser Chatroom für alle Fragen, die aufkommen

Entwicklungsprozess

- Ein- bis zweiwöchentliche Online-Meetings, meistens Dienstags
- Issue-Tracker regeln den Rest
- Quasi-automatisches Setup von IDE (Eclipse) und Repos, benötigte Plugins
- Üblicherweise: Pull-requests stellen

YouCrypTool:



Es geht weiter im
Videoformat!

Fragen? Fragen! :)

- Für technische Fragen und Anregungen...
 - steht unser Chatroom bereit: gitter.im/dshadow/jcryptool
 - Issue-Tracker als Alternative für Bugs und Probleme: github.com/jcryptool/core/issues
- Informieren Sie sich weiter über das CrypTool-Projekt:
 - <https://www.cryptool.org/>
 - https://www.cryptool.org/assets/jct/JCrypTool_Praes_en.pdf
(Long-Form PDF für mehr Details der GUI)
- Danke für Ihre Aufmerksamkeit!