# Cryptool

**Open-Source für Bildung und Forschung in Kryptologie**

Das CrypTool-Projekt bietet einen einfachen und spielerischen Zugang zu Verschlüsselungstechniken – praktisch anwendbar und leicht nachvollziehbar.

CrypTool ist kostenlos, und es ist das umfangreichste E-Learning-Programm für Kryptografie und Kryptoanalyse weltweit.

Zu CrypTool tragen Menschen und Forschungsgruppen aus aller Welt bei. Dazu gehören beispielsweise die Universitäten in Bochum, Darmstadt, Siegen, Klagenfurt, Eindhoven, Hagenberg, Utrecht, Warschau, Madrid, Brisbane und San Jose.

## CrypTool im Internet:

**www.cryptool.org**

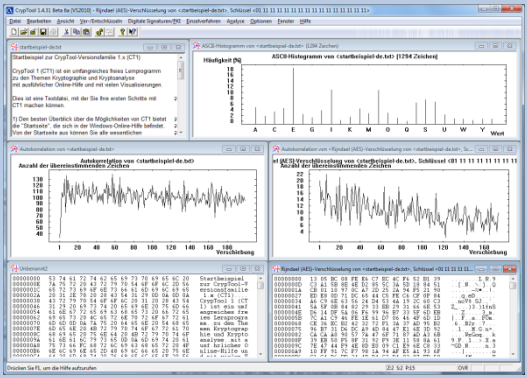
**www.cryptool-online.org**

**www.mysterytwisterc3.org**

**Prof. Bernhard Esslinger**

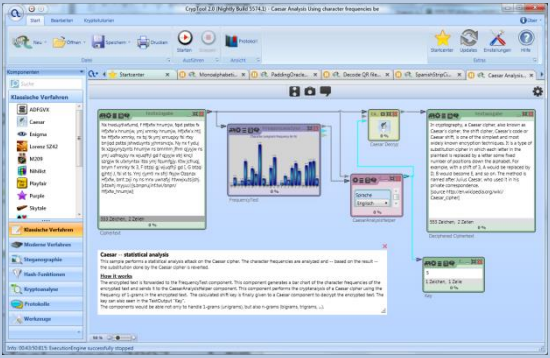
**esslinger@cryptool.org**

# CrypTool 1.x – seit 1998



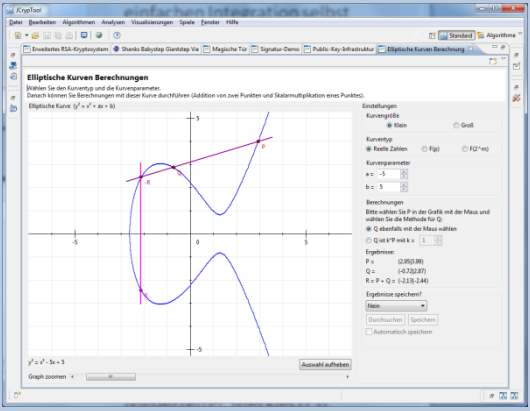
- Klassische und moderne Kryptografie, z.B. Caesar, ADFGVX, Enigma, RSA, DES, AES, PRESENT
- Automatische Kryptoanalyse, sowohl generische Funktionen als auch gezielte Angriffe (z.B. Gitter-basierte Angriffe gegen RSA)
- Interaktive Darstellung und Visualisierung von Verfahren, z.B. digitale Signaturen, AES und Elliptische-Kurven-Kryptografie

# CrypTool 2.x – seit 2007



- Alte und neue kryptografische Verfahren und Bedienung durch visuelle Programmierung.
- Umfangreiche Funktionen zur (verteilten) Kryptoanalyse
- Moderne Plugin-Schnittstelle, zur einfachen Integration selbst entwickelter Funktionen
- Protokoll-Szenarien
- Tutorien, z.B. zu Gittern und Primzahlen

# JCrypTool – seit 2007



- Läuft auf jedem Java-fähigen BS, z.B. Windows, Mac OS X, Linux
- Visualisierung klassischer Verfahren und aktueller Forschungsthemen (z.B. Multi-Party Key-Exchange, Homomorphe Verschlüsselung, Kleptografie)
- Für den Benutzer: Aktivitäts-Historie und Kaskadierung von Funktionen
- Post-Quantum-Krypto-Verfahren (z.B. McEliece, WOTS, MerkleOTS)