

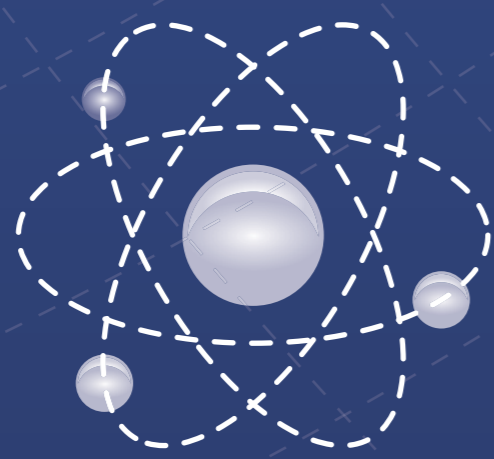
JCryptTool

The cryptography e-learning platform

Core Team

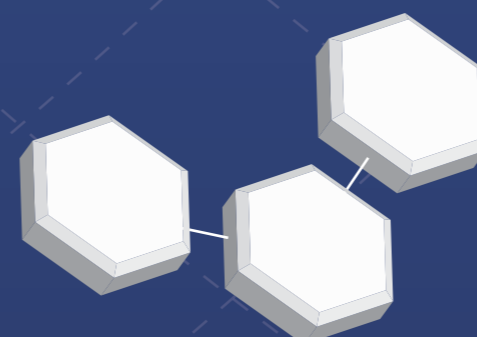
- Bernhard Esslinger
- Dominik Schadow
- Matthias Walthart
- Simon Leischnig

... and many plug-in developers ...



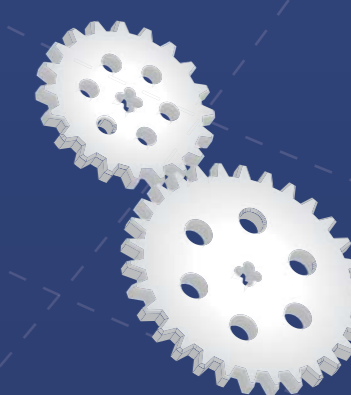
Features

- E-learning
- Modern user interface
- Open source
- Platform independent
- Extendable through plug-ins
- Java
- Eclipse
- Rich Client Platform RCP
- JCA/JCE



Crypto Algorithms

- Classic and modern symmetric encryption
- Hash, MAC, signature
- PRNG
- Asymmetric encryption
- Cryptanalysis
- Visualizations (extended Euclidian, Kleptography, multipartite key exchange, CRT, ...)



Crypto Provider

BouncyCastle

- Cryptographic algorithms

FlexiProvider

- Cryptographic algorithms
- Keystore



Project History

- 1998 CrypTool project started
- 2000 Available as freeware
- 2003 Available as open source
- 2007 JCryptTool project started
- 2010 JCryptTool 1.0



PostQuantum

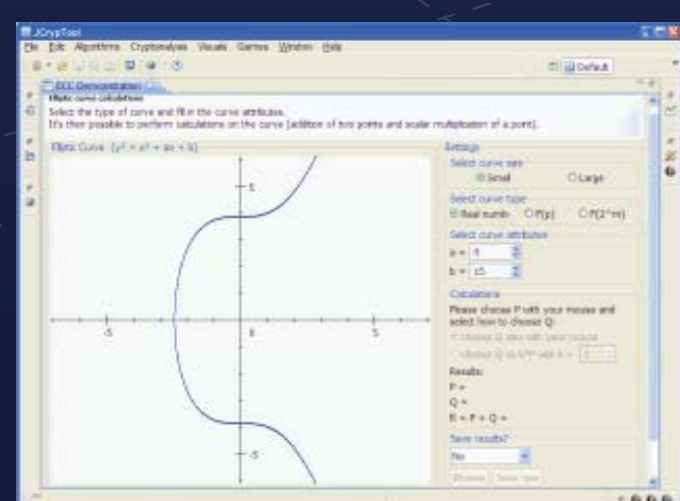
- Niederreiter
- McEliece
- McElieceFujisaki
- McElieceKobaraImai
- McEliecePointcheval
- NiederreiterCFS
- MerkleOTS
- CMSS
- GMSS



Samples of built-in visualizations

ECC Demonstration

- Choose points
- Addition
- Scalar multiplication



Games

- Number Shark



Shamir's Secret Sharing

- Numerical and graphical mode
- Arbitrary number of shares



www.cryptool.org

PQCrypto 2010

Darmstadt, Germany
May 25 - 28, 2010



FlexiProvider
[Harnessing the power of the Java Cryptography Architecture™]