INTRODUCTION TO CRYPTOOL:

What is CrypTool?

- Freeware program with graphical user interface
- Cryptographic methods can be applied and analysed
- Comprehensive online help (understandable without deeper cryptography knowledge)
- Contains nearly all state-of-the-art cryptography functions
- Easy entry into modern and classical cryptography
- Not a “hacker tool”

2. Why CrypTool?

- Origin in awareness initiative of a financial institute
- Developed in close cooperation with universities
- Improvement of university education and in-firm training

3. Target group

- Core group: Students of computer science, business computing and mathematics
- But also for: computer users, application developers, employees
- Prerequisite: PC knowledge
- Preferable: Interest in mathematics and/or programming

CRYPTOOL PROGRAM

- All functions integrated in a single program with consistent graphical interface
- Runs on Win32
- Cryptography libraries from Secude and OpenSSL
- Long integer arithmetic from Miracl and GMP, Lattice base reduction via NTL (Shoup)

ADDITIONAL FUNCTIONS

- Homophone and permutation encryption (Double Column Transposition)
- PKCS #12 import and export for PSEs (Personal Security Environment)
- Generate hashes of large files, without loading them
- Flexible brute-force attacks on any modern symmetric algorithm
- ECC demonstration (as Java application)
- Password Quality Meter (PQM) and password entropy

**CONCEPTS FOR A USER-FRIENDLY INTERFACE**

1. Context sensitive help (F1)
   - F1 on a selected menu entry shows information about the algorithm/method.
   - F1 in a dialog box explains the usage of the dialog.
   - These assistances and the contents of the super ordinate menus are cross-linked in the online help.

2. Paste of keys in key-input dialog
   - CTRL-V can be used to paste contents from the clipboard.
   - Used keys can be taken out of cipher text windows via an icon in the icon bar. A corresponding icon in the key-input dialog can be used to paste the key into the key field.
   - A CrypTool-internal memory which is available for every method is used (helpful for large „specific“ keys – e.g. homophone encryption).

**CHALLENGES FOR DEVELOPERS (EXAMPLES)**
1. Many functions running in parallel
   Factorisation runs with multi-threaded algorithms

2. High performance
   Locate hash collisions (birthday paradox) or perform brute-force analysis

3. Consider memory limits
   Floyd algorithm (mappings to locate hash collisions) or factorisation with quadratic sieve

4. Time measurement and estimates
   Display of elapsed time while using brute-force

5. Reusability / Integration
   Forms for prime number generation
   RSA cryptosystem (switches the view after successful attack from public key user to private key owner)

6. Partly automate the consistency of functions, GUI and online help
   (including different languages)

   CRYPTOOL EXAMPLES

   Overview of examples:
   1. Encryption with RSA / Prime number tests / Hybrid encryption and digital certificates / SSL
   2. Digital signature visualised
   3. Attack on RSA encryption (modul N too short)
   4. Analysis of encryption in PSION 5
   5. Weak DES keys
   6. Locating key material (“NSA key”)
   7. Attack on digital signature through hash collision search
8. Authentication in a client-server environment
9. Demonstration of a side-channel attack (on hybrid encryption protocol)
10. Attack on RSA using lattice reduction
11. Random analysis with 3-D visualisation
12. Secret Sharing using the Chinese Remainder Theorem (CRT) and Shamir
13. Implementation of CRT in astronomy (solving linear modular equation systems)
14. Visualisation of symmetric encryption methods using ANIMAL
15. Visualisation of AES
16. Visualisation of Enigma encryption
17. Generation of a message authentication code (MAC)
18. Hash demonstration
19. Learning tool for number theory and asymmetric encryption
20. Point addition on elliptic curves
21. Password quality meter (PQM) and password entropy
22. Brute-force analysis
23. CrypTool online help

EXAMPLE OF USAGE OF CRYPTOOL: DIGITAL SIGNATURE
Digital signature

- Increasingly important
  - equivalence with manual signature (digital signature law)
  - increasingly used by industry,
  - government and consumers
- Few people know how it works exactly

Visualization in CrypTool

- Interactive data flow diagram
- Similar to the visualization of hybrid encryption

Digital signature visualised: a) Preparation

1. Select hash function
2. Provide key and certificate (not shown here)

Digital signature visualised: b) Cryptography

3. Calculate hash value
4. Encrypt hash value with private key (sign)
5. Generate signature
Future CrypTool Development

- Re-use the comprehensive set of algorithms, included libraries and interface elements as foundation
- Free of charge training in Frankfurt, how to start with CrypTool development
- Advantage: Your own code does not „disappear“, but will be maintained

CRYPTOOL SUMMARY

- *THE* e-learning program for cryptology
- Over more than 10 years a successful open source project
- More than 200,000 downloads
- International utilisation in schools, universities as well as companies and government agencies
- Extensive online help and documentation
- Available for free and multi-language support