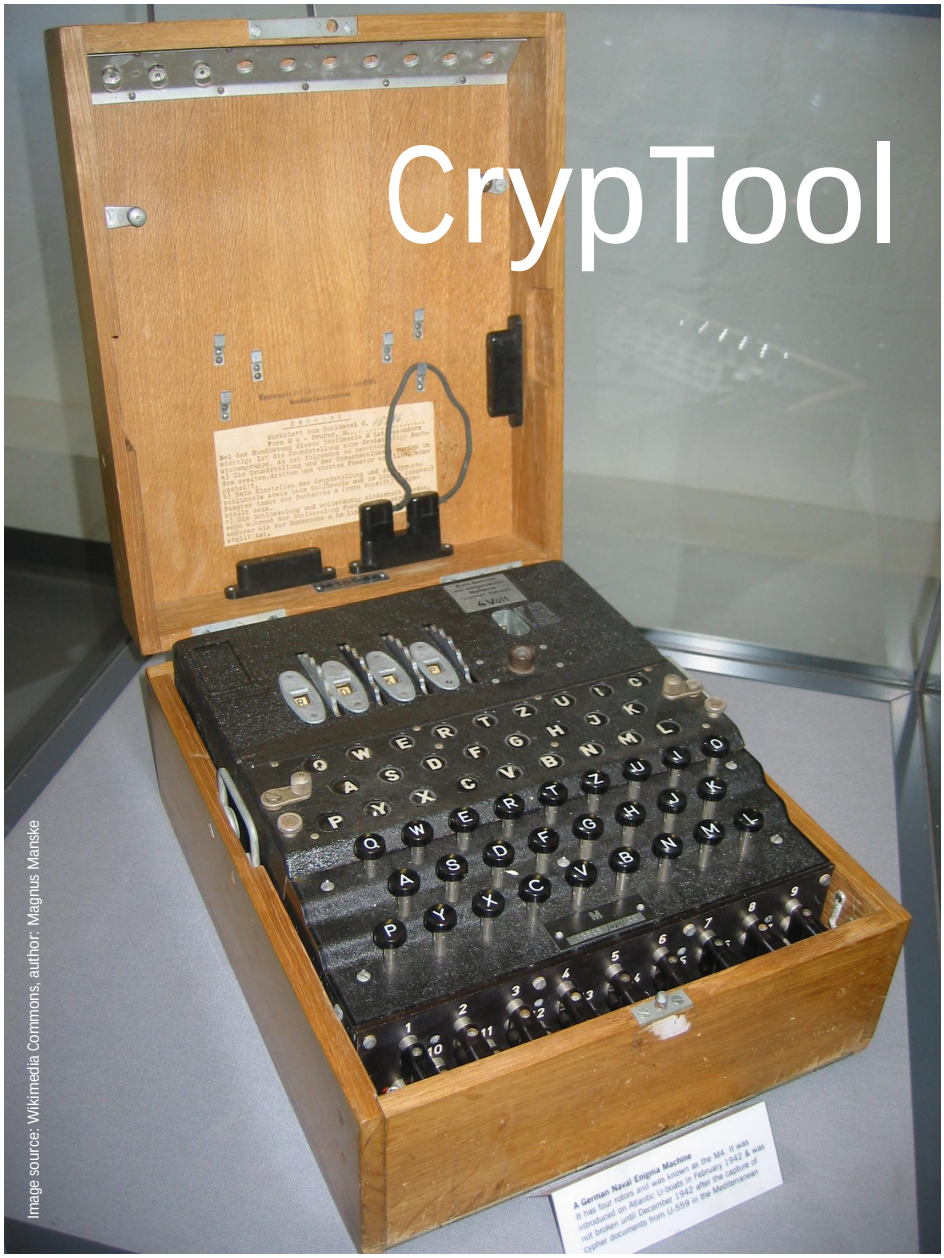


Image source: Wikimedia Commons, author: Magnus Manske

An e-learning programme for cryptology

Usually invisible, cryptographic procedures are used in many areas of modern life – from Pay TV, immobilizers in cars, mobile telephones, SSL connections when surfing the internet, the encryption in digital rights management to the most widely known use in e-mails. And while many people tried as children to encrypt messages, very few find modern cryptographic methods accessible.

The open-source-programme "CrypTool", which was first developed in 1998, offers a fun way to learn about classic and modern cryptography and cryptanalysis. CrypTool not only explains the methods of cryptography, it also provides additional analysis functions and attack simulations.

CrypTool's roots lay in a corporate awareness training programme at a large bank aimed at increasing employee awareness of data protection issues. Since the official project launch at the Technical University of Darmstadt in 1998, more than 18 man-years have been invested in the project. CrypTool has been available as freeware since the turn of the century and since 2002 it has featured on the Federal Office for Information Security's (BSI) citizen-CD under the name "*Ins Internet – mit Sicherheit*" (On the internet – with security).

CrypTool is now used for training/teaching purposes in many schools and universities in Germany and abroad (in areas such as IT, cryptology, internet security and digital signatures).

This year, CrypTool became available in three languages: German, English and Polish. The package is downloaded approximately 3,000 times a month (1/3 of the downloads are for the English version). Roughly 30 people, employed at various companies and universities, are involved in the continued development of the platform, most of them on a voluntary basis. New volunteers and offers to use existing resources are always welcomed.

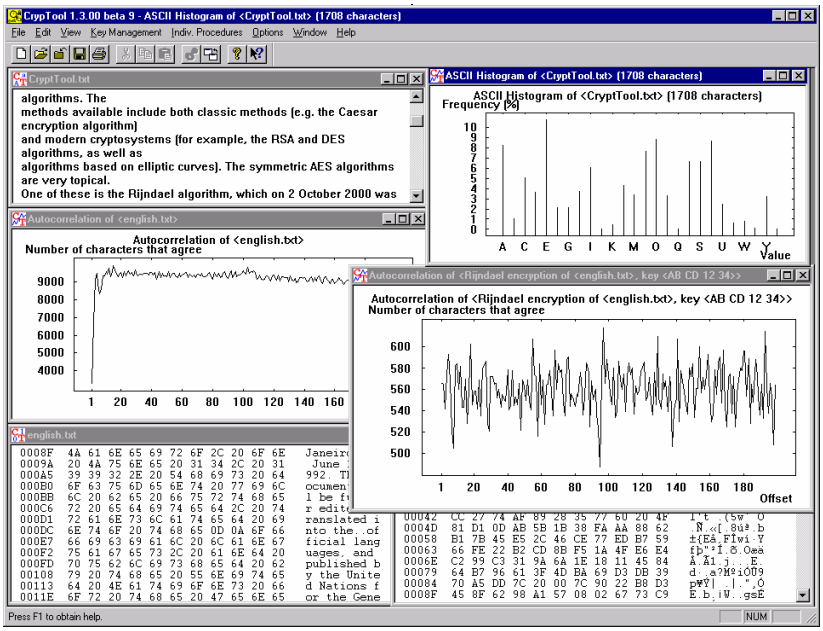
What is CrypTool?

CrypTool is a freeware programme which enables you to apply and analyze cryptographic procedures. CrypTool contains a very extensive online help function, which can be understood even without a deeper knowledge of cryptography. The programme contains almost all state-of-the-art crypto functions and offers a "fun" introduction" to cryptography via a single user interface.

Both classical and modern crypto methods are available. The classical methods include the Caesar cipher, the ADFGVX cipher, the double-column transposition (permutation) and the Enigma encryption algorithm. Modern methods include the RSA and the AES algorithm, hybrid encryption and algorithms based on lattice reduction and elliptic curves.

Analysis with the aid of n-grams and the comprehensive help function

For the classical encryption algorithms, automatic analysis tools



In Cryptool many methods for text analysis are available. With these methods one can reveal the weaknesses of simple encryption algorithms as well as break some of them automatically. By encrypting a document the result gets written into a window. The title of the result window contains the name of the original document and the used key. The handling with keys is eased by two icons: With the icon „Show key" the used key can be shown and copied into an internal repository. Then the icon „Insert key" is available when encrypting another document. This function is extremely useful when complex keys are used (like keys in homophonic algorithms).

are provided to decode the key and the clear text from the encrypted document. To assist the user in analyzing documents him/herself, CrypTool can display the histogram of a document, determine the statistics of any n-grams and calculate entropy and autocorrelations. During the development of CrypTool, care was taken to ensure that at every stage of the programme, context-sensitive online help could be accessed via the F1 button. For training purposes, the users can navigate very easily between the menus and then press F1 whenever they encounter an interesting entry or unfamiliar terminology.

The comprehensive help function contains explanations of all the basic cryptographic terms, a list of reference literature in the field of cryptography, a chronology with a historical overview, a well-sorted index of the cryptographic topics covered and tutorials for a fast introduction.

E- learning via individual interactive procedures with comprehensible steps

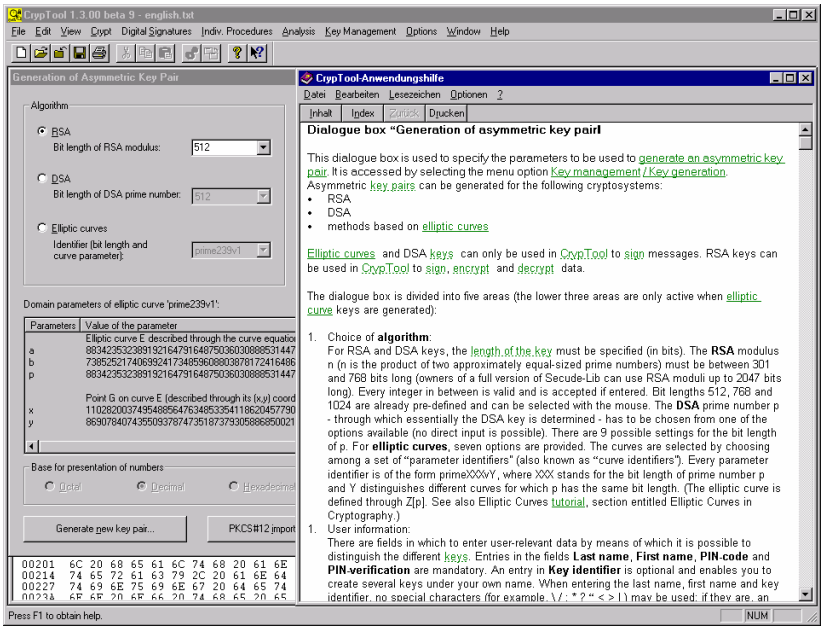
The encryption functions in the menu "Crypt/Decrypt" have been set up to enable them to be accessed and implemented as effectively as possible; whereas the functions in the menu "Indiv. Procedures" have been set up successively and interactively with the main focus on the e-learning aspects.

The "Indiv. Procedures" menu offers a range of different procedures and protocols, for example:

- Calculate hash values and show their sensitivity
- Create Message Authentication Codes (MACs)
- Find out how "strong" keys can be generated from passwords according to the PKCS#5 standard
- Compress and decompress documents – this makes it possible to analyze the effects of the compressing files prior to actual encryption
- Generate or analyze random numbers
- Demonstrate protocols for authentication and key exchange (DH)
- Step through some ciphers – forwards and backwards (using ANIMAL)
- Apply common encodings such as base64 and uuencode.

The range of functions which can be selected from the menu depends on the type of active document. The CrypTool menus and sub-menus are generated dynamically depending on whether a file is open in the main window and whether the active file is a text file, binary file or a graphic display. Inactive menu items which cannot be used for the active document are blended out in grey in the CrypTool menu.

The features of CrypTool are supported by an extensive help.



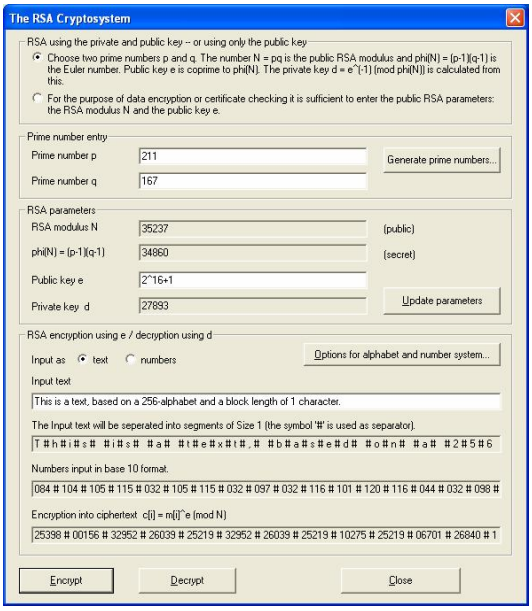
Focus on asymmetric encryption

One aspect which CrypTool focuses on is asymmetric encryption methods, which provide the basis for secure communication in many areas, above all on the internet. An asymmetric cryptosystem is always comprised of a secret component, the private key, and a public key. The private key allows the owner to decrypt data, generate digital signatures and authenticate him/herself. The public key allows anybody else to encrypt data for the key owner, to check the owner's digital signature and to authenticate him/her. In contrast to symmetric cryptosystems, the communicating parties do not need to know a shared secret key.

The breakthrough in the development of asymmetric algorithms occurred in the 1970s when New York mathematician Ronald L. Rivest, Israeli cryptologist Adi Shamir and Californian computer scientist Leonard M. Adleman published the RSA method, which they named in 1977 after the first letters of their three surnames. It is still considered a secure method today and has the major advantage that it can be used both for encryption/decryption and for signing/verification. Furthermore, it is able to scale the security level by enlarging the length of the key (module n (the product of two large prime numbers of roughly the same size) today has practical lengths of 768, 1024 or 2048 bit).

The RSA cryptosystem is described in detail in CrypTool and is presented for different codings. The RSA key is generated from the two self-selected prime numbers. The different steps in key generation, encryption and decryption can be reproduced for small numbers as well as for very large numbers.

The factorization of numbers is also an important application for cryptography. Simple RSA cryptosystems can be easily cracked using the factorization algorithms presented in CrypTool. This gives the users an idea of the minimum key length needed for secure systems.



In the dialog box „The RSA Crypto System" the different variants of the RSA system can be tested (e.g. different key lengths, different alphabets, different block sizes).

Interactive demonstrations / visualizations

CrypTool also provides an extensive library of interactive visual demonstrations, which help the user to reach a deeper understanding of a multitude of issues.

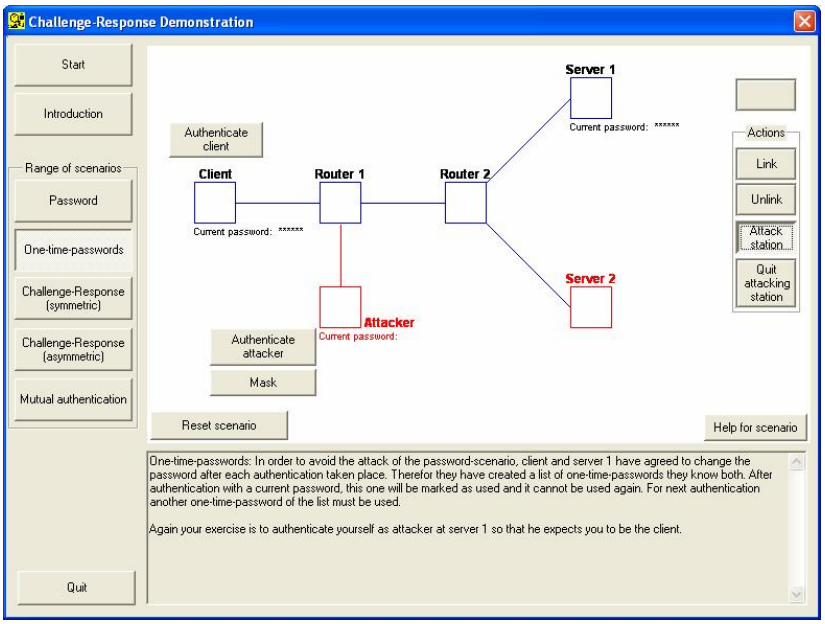
Different application and security scenarios are simulated and visualized, ranging from the creation of an electronic signature, hybrid encryption and hash procedures to key exchange procedures and side channel attacks. From UID/PW, one-time password, and (one-way) challenge response (symmetric + asymmetric) to asymmetric mutual authentication.

The user can interactively determine how the attacker proceeds (take over computer, connect or disconnect, eavesdrop).

Outlook

The latest CrypTool release, version 1.4.10, has been available

Demo showing authentication methods in the web: from UID/PW and one-time-password over (unidirectional) challenge-response authentication (symmetric + asymmetric) to mutual asymmetric authentication. The user is able to control interactively how an attacker acts (take over the machine, establish or disrupt connection, eavesdrop).



Bernhard Esslinger

Professor at University of Siegen
Institute of Information Systems (FB5)
bernhard.esslinger@db.com

Kai Hoelzner

DFN-Verein
hoelzner@dfn.de

since July 2007. New functions include a learning programme for basic number theory, flash animations for the AES procedure and the Enigma cipher machine and a demonstration of addition on real and discrete elliptic curves.

The CrypTool project was recently selected for "Germany – Land of Ideas" in the category "science and technology". This initiative, which was launched by the German President in the year in which Germany hosted the football World Cup, honours places or "landmarks" which develop and actively implement forward-looking ideas. In connection with this, the CrypTool project will be presented in Siegen on July 22, 2008.

Several improvements are planned for 2008: There are two large upcoming projects which completely redevelop the software. First Java CrypTool, developed with Eclipse/Java (in cooperation with the University of Darmstadt), will make CrypTool platform-independent allowing it be run on all operating systems, saving Linux and Mac users onerous Windows emulations. Secondly, the direct successor, CrypTool 2, will be created in .NET with C# on a slim architecture design (in cooperation with the University of Duisburg-Essen). The developers also realized an idea generated at the GI-conference INFOS2007 by creating a portal to provide teachers with a central platform for exchanging teaching units on the subject of cryptology.

www.cryptool.org

A demo for a side channel attack against a typical hybrid encryption algorithm: With a non-optimal implementation like it did exist in reality, the attacker is able to compute the session key efficiently through protocol conform server queries.