

An e-learning programme for cryptology

U sually 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.

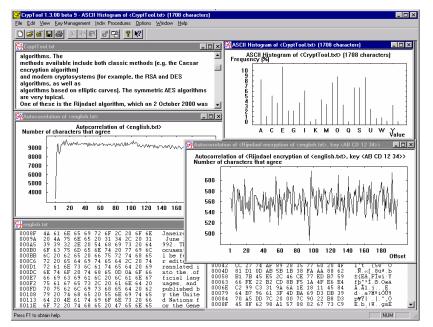
What is CrypTool?

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 stateof-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 doublecolumn 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 ngrams 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.

👷 CrypTool 1.3.00 beta 9 - english.txt	
Ele Edit View Crypt Digital Signatures Indiv. Procedures Ana	ysis Key Management Options Window Help
Generation of Asymmetric Key Pair	🔗 Cryp Tool-Anwendungshilfe 📃 🛛 🔀
Algorithm	Datei Bearbeiten Lesezeichen Optionen 2
Agoinn	Inhalt Index Zutick Drucken
© BSA	Dialogue box "Generation of asymmetric key pairl
Bit length of RSA modulus: 512	This dialogue box is used to specify the parameters to be used to generate an asymmetric key
C DSA	pair. It is accessed by selecting the menu option Key management / Key generation.
Bit length of DSA prime number: 512	Asymmetric key pairs can be generated for the following cryptosystems: • RSA
	• DSA
C Elliptic curves	methods based on <u>elliptic curves</u>
Identifier (bit length and curve parameter); prime239v1	Elliptic curves and DSA keys can only be used in CrypTool to sign messages. RSA keys can
	be used in CrypTool to sign, encrypt and decrypt data.
	The dialogue box is divided into five areas (the lower three areas are only active when elliptic
Domain parameters of elliptic curve 'prime239v1':	curve keys are generated):
Parameters Value of the parameter	
Elliptic curve E described through the curve equation 88342353238919216479164875036030888531447	 Choice of algorithm: For RSA and DSA keys, the length of the key must be specified (in bits). The RSA modulus
b 73852521740699241734859608803878172416486 p 88342353238919216479164875036030888531447	n (n is the product of two approximately equal-sized prime numbers) must be between 301
ľ	and 768 bits long (owners of a full version of Secude-Lib can use RSA moduli up to 2047 bits long). Every integer in between is valid and is accepted if entered. Bit lengths 512, 768 and
Point G on curve E (described through its (x,y) coord x 11028200374954885647634853354118620457790	1024 are already pre-defined and can be selected with the mouse. The DSA prime number p
y 86907840743550937874735187379305886850021	- through which essentially the DSA key is determined - has to be chosen from one of the
	options available (no direct input is possible). There are 9 possible settings for the bit length of p. For elliptic curves, seven options are provided. The curves are selected by choosing
Base for presentation of numbers	among a set of "parameter identifiers" (also known as "curve identifiers"). Every parameter
O Lotal O Decimal O Hexadecimal	identifier is of the form primeXXXvY, where XXX stands for the bit length of prime number p and Y distinguishes different curves for which p has the same bit length. (The elliptic curve is
C Trans C Transie	defined through Z[p]. See also Elliptic Curves to total, section entitled Elliptic Curves in
Generate new key pair PKCS#12 import	Cryptography.) 1. User information:
PRC5#12 import	 User information: There are fields in which to enter user-relevant data by means of which it is possible to
00201 6C 20 68 65 61 6C 74 68 20 61 6E	distinguish the different keys. Entries in the fields Last name, First name, PIN-code and
00214 74 65 72 61 63 79 2C 20 61 6E 64	PIN-verification are mandatory. An entry in Key identifier is optional and enables you to create several keys under your own name. When entering the last name, first name and key
00227 74 69 6E 75 69 6E 67 20 64 65 74 00238 6F 6F 20 6F 66 20 74 68 65 20 65	identifier, no special characters (for example, \/; * ? " < > 1) may be used; if they are, an
Press F1 to obtain help.	NUM

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 be used both can 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.

RSA Cryptosyster	n	
RSA using the private a	and public key or using only the	public key
		= pq is the public RSA modulus and phi(N) = (p-1)(q-1) is The private key d = e^(-1) (mod phi(N)) is calculated from
	data encryption or certificate che N and the public key e.	cking it is sufficient to enter the public RSA parameters:
Prime number entry		
Prime number p	211	Generate prime numbers
Prime number q	167	
RSA parameters		
RSA modulus N	35237	(public)
phi(N) = (p·1)(q·1)	34860	(secret)
Public key e	2^16+1	
Private key d	27893	Update parameters
RSA encryption using e	descustion using d	
Input as (• text	-	Options for alphabet and number system
Input text	* Humbers	
	on a 256-alphabet and a block len	gth of 1 character.
The Input text will be a	seperated into segments of Size 1	(the symbol '#' is used as separator).
	s# #a# #t#e#x#t#,#	#b#a#s#e#d# #o#n# #a# #2#5#6
Numbers input in base	10 format.	
084 # 104 # 105 # 1	15 # 032 # 105 # 115 # 032 # 09	7 # 032 # 116 # 101 # 120 # 116 # 044 # 032 # 098
Encryption into ciphert	text_c[i] = m[i]^e (mod N)	
		26039 # 25219 # 10275 # 25219 # 06701 # 26840 # 1
1 contraction of the second second		

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.

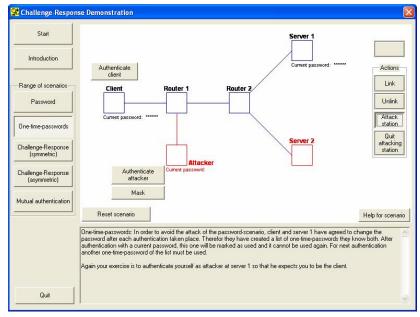
Different application and security scenarios are simulated and visualized, ranging from the creation of an electronic signature, hybrid encryption and hash procedures to key exchange procedures and side channel attacks. From UID/PW, onetime password, and (one-way) challenge response (symmetric + asymmetric) 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 GIconference 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 nonoptimal implementation like it did exist in reality, the attacker is able to compute the session key efficiently through protocol conform server queries.

