



# Ethical Hacking and Countermeasures

Version 6



**Module XXV**

Cryptography



## Jihadists Get Encryption Upgrade

**Until recently, al-Qaida didn't pose much of a threat online because it used outdated technology. Having modern encryption tools changes the equation.**

By Thomas Claburn, [InformationWeek](#)

Jan. 25, 2008

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=205918296>

Last week, an Islamist Web site called [Al-Ekhlās](#) released updated encryption software to help keep secret communications from prying eyes. The site is allegedly frequented by al-Qaida supporters.

According to the [Middle East Media Research Institute](#), the first version of the software, "Mujahideen Secrets," was released a year ago as "the first Islamic computer program for secure exchange [of information] on the Internet." MEMRI says that the program includes "the five best encryption algorithms, and with symmetrical encryption keys (256 bit), asymmetrical encryption keys (2048 bit) and data compression [tools]."

Reuters [reports](#) that the new version of the software, "Mujahideen Secrets 2," was developed by Al-Ekhlās "in order to support the mujahideen (holy war fighters) in general and the (al Qaeda-linked group) Islamic State in Iraq in particular."

The Al-Ekhlās Web site is [hosted](#) by Florida-based Noc4hosts. Calls and e-mail to the company were not returned.

In an e-mail message, Paul Henry, VP of technology evangelism at [Secure Computing](#), said that until recently al-Qaida didn't pose a credible threat online because of its use of outdated technology. Having modern encryption tools, he said, changes the equation.

Source: <http://www.informationweek.com/>

# Scenario

Larry was working on a high-end project. He was expecting a promotion for his good performance. But he was disappointed to see that the members of the team whose performances were below par were promoted while he was ignored. In a fit of rage, he quit his job. He searched for a job in another company and got a good offer.

While quitting he had decided that he would teach his project manager a lesson. He used an encryption tool TrueCrypt and encrypted the whole directory with password protection where he had stored his part of work.

Can the information Larry encrypted be retrieved?

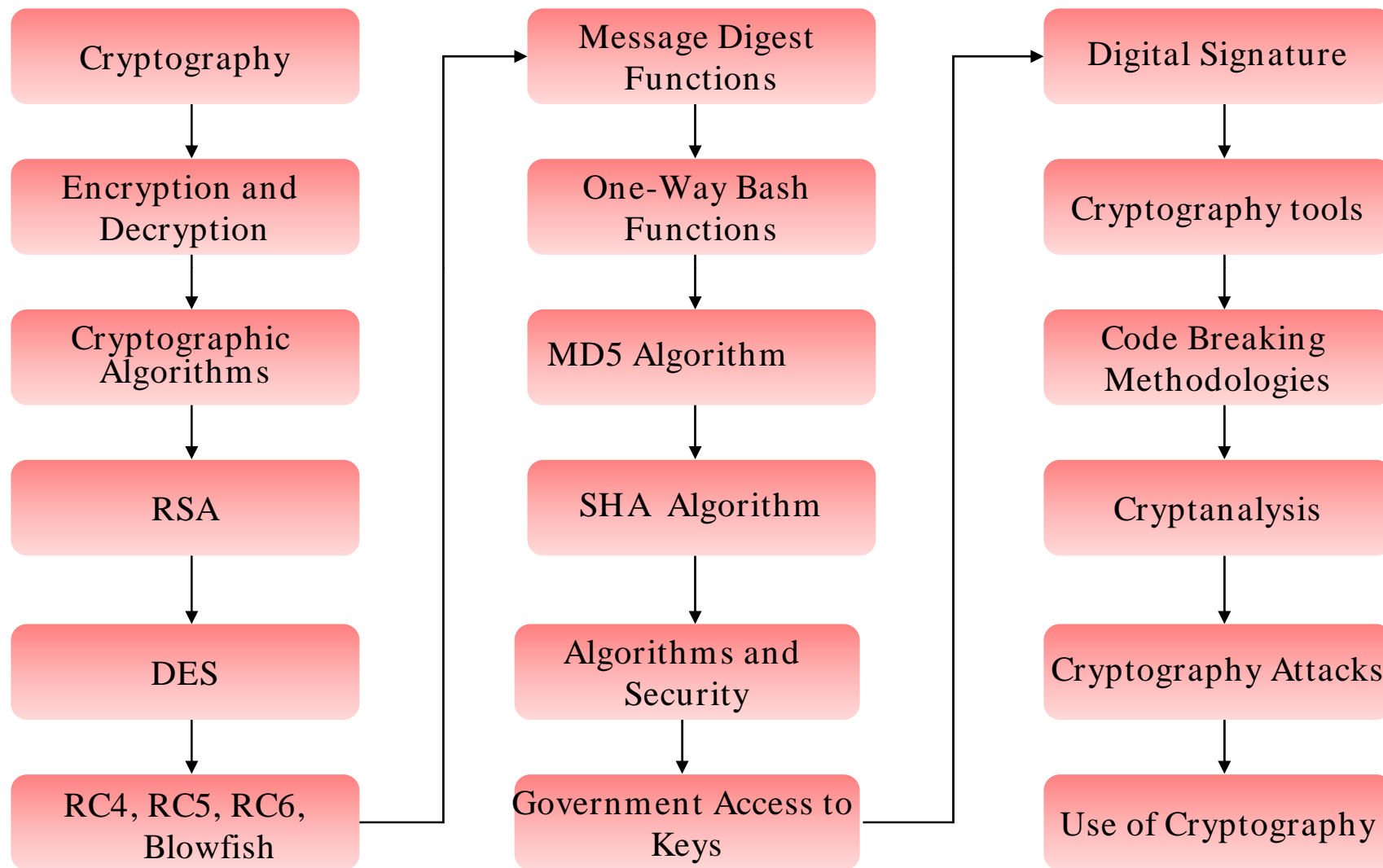
# Module Objective

This module will familiarize you with:

- Cryptography
- Encryption and Decryption
- Cryptographic Algorithms
- RSA (Rivest Shamir Adleman)
- Data Encryption Standard (DES)
- RC4, RC5, RC6, Blowfish
- Message Digest Functions
- One-way Hash Functions
- MD5
- SHA
- Algorithms and Security
- Government Access to Keys (GAK)
- Digital Signature
- Cryptography tools
- Code Breaking: Methodologies
- Cryptanalysis
- Cryptography Attacks
- Use Of Cryptography



# Module Flow



# Cryptography

Cryptography is an art of writing text or data in secret code

It encrypts the plain text data into unreadable format, which is called as cipher text

It is based on mathematical algorithms

These algorithms use a secret key for the secure transformation



# Cryptography (cont'd)

In cryptography, each person receives a pair of keys, called the public-key, and the private-key

Each person's public-key is published while the private-key is kept secret

Anyone can send a confidential message using public information, but it can only be decrypted with a private-key that is in the sole possession of the intended recipient



# Classical Cryptographic Techniques

Classical ciphers comprise of two basic components:

- Substitution Cipher
- Transposition Cipher
  - Monoalphabetic
  - Polyalphabetic



Several of these ciphers are grouped together to form a ‘product cipher’



# Encryption

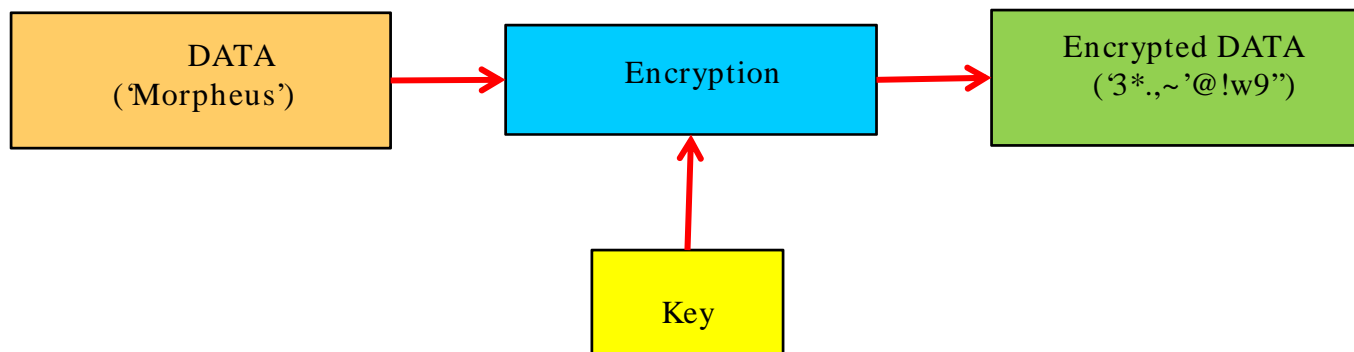
Encryption is the process of converting data into a secret code

It is the most effective way to achieve data security

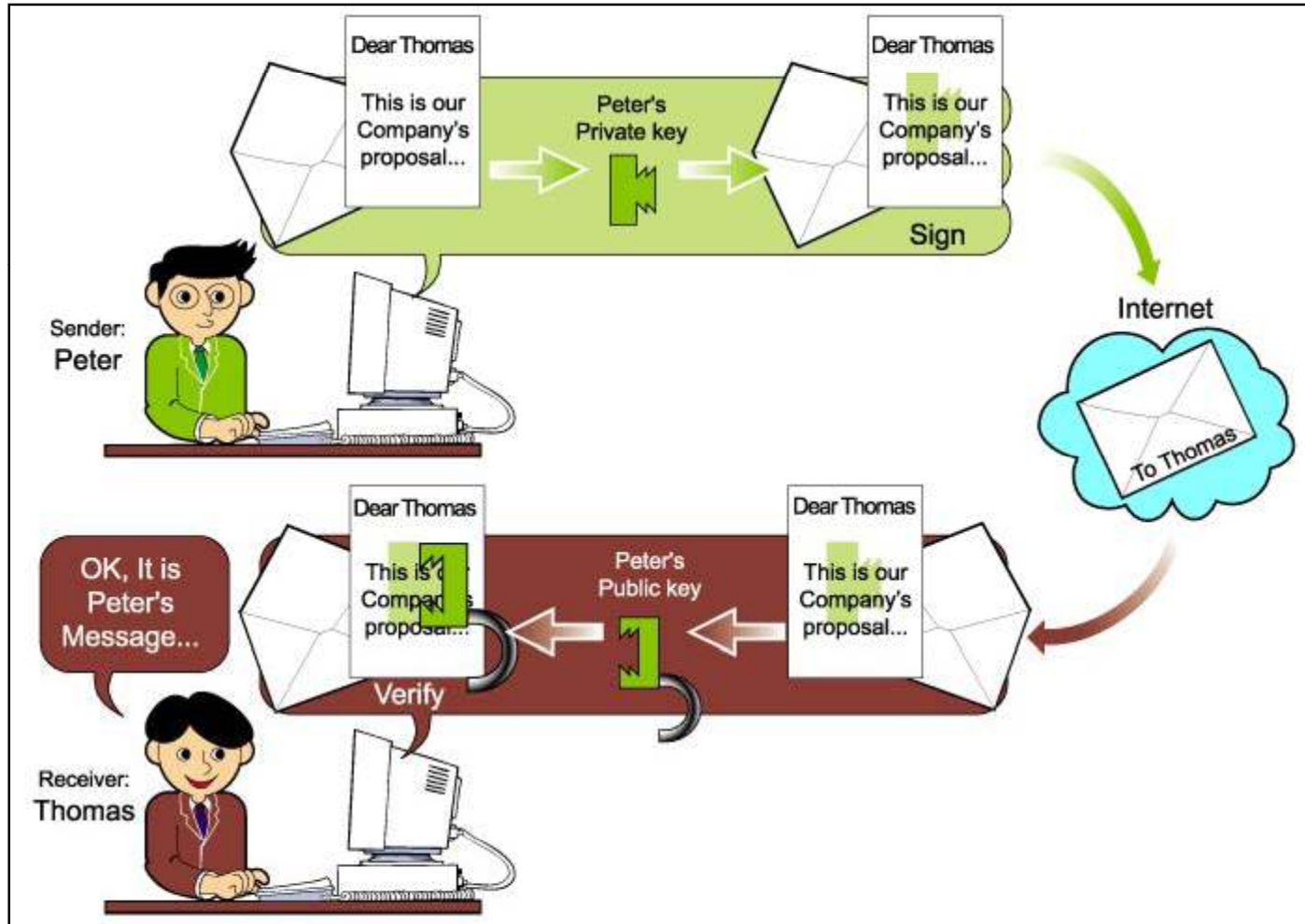
To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it

Unencrypted data is called *plain text*

Encrypted data is referred to as *cipher text*



# Encryption (cont'd)

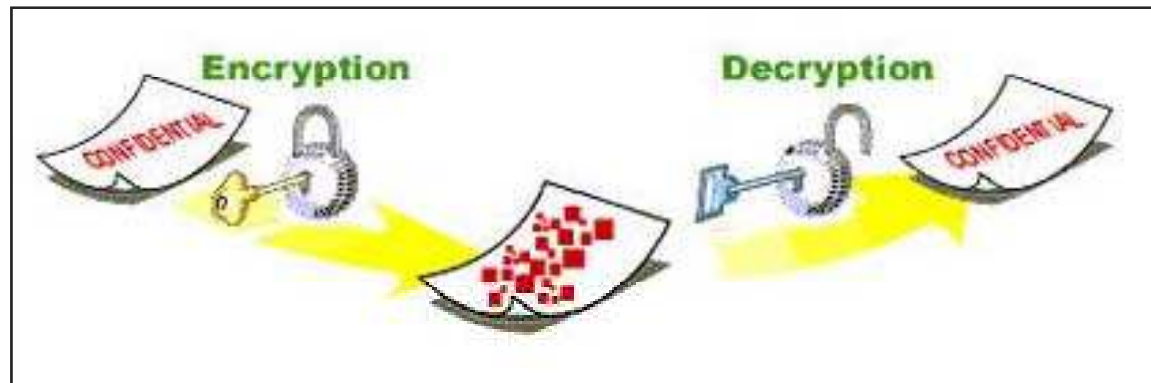


# Decryption

Decryption is the process of decoding data that has been encrypted into a secret format

It requires a secret key or password

Public Key Cryptography encryption and decryption is performed with public and private keys



# Cryptographic Algorithms

## Secret key Cryptography:

- It uses a single key for both encryption and decryption processes
- Since single key is used for both encryption and decryption, it is also called as Symmetric Encryption

## Public key Cryptography:

- It uses one key for encryption and another for decryption
- One key is designated as a public key which is open to public and the other key is designated as a private key which is kept secret

## Hash Functions:

- It uses a mathematical transformation to irreversibly "encrypt" information
- It is also called Message Digest and One-way Encryption, are algorithms that, in some sense, use no key
- Instead, a fixed-length hash value is computed based upon the plaintext
- Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents

# Cryptographic Algorithms (cont'd)



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.



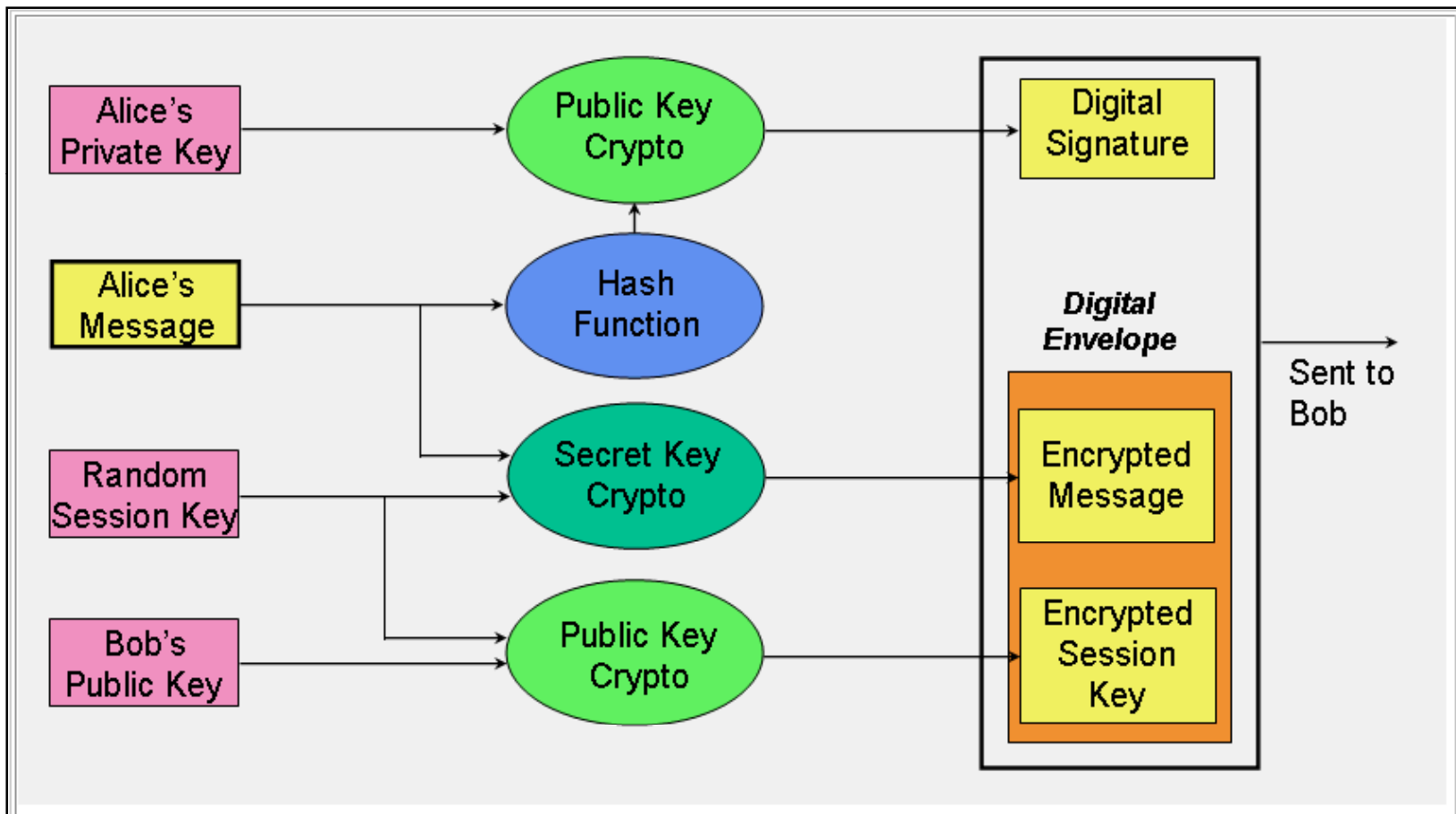
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

# Cryptographic Algorithms (cont'd)

Sample application of the three cryptographic techniques for secure communication

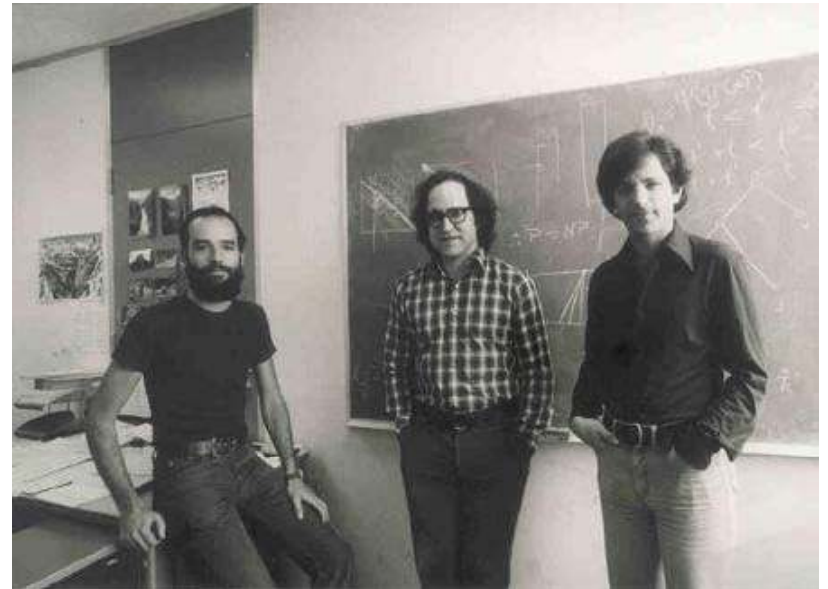


# RSA (Rivest Shamir Adleman)

RSA is a public-key cryptosystem

It uses modular arithmetic, and elementary number theories to perform computations using two large prime numbers

RSA encryption is widely used and is the de-facto encryption standard



Rivest Shamir Adleman

# Example of RSA Algorithm

**P = 61**     ← first prime number (destroy this after computing E and D)  
**Q = 53**     ← second prime number (destroy this after computing E and D)  
**PQ = 3233** ← modulus (give this to others)  
**E = 17**     ← public exponent (give this to others)  
**D = 2753** ← private exponent (keep this secret!)

Your **public key** is (E,PQ).  
Your **private key** is D.

The **encryption** function is:

$$\begin{aligned}\text{encrypt}(T) &= (T^E) \text{ mod } PQ \\ &= (T^{17}) \text{ mod } 3233\end{aligned}$$

The **decryption** function is:

$$\begin{aligned}\text{decrypt}(C) &= (C^D) \text{ mod } PQ \\ &= (C^{2753}) \text{ mod } 3233\end{aligned}$$

To encrypt the plaintext value 123, do this:

$$\begin{aligned}\text{encrypt}(123) &= (123^{17}) \text{ mod } 3233 \\ &= 337587917446653715596592958817679803 \text{ mod } 3233 \\ &= 855\end{aligned}$$

To decrypt the ciphertext value 855, do this:

$$\begin{aligned}\text{decrypt}(855) &= (855^{2753}) \text{ mod } 3233 \\ &= 123\end{aligned}$$



# RSA Attacks

Brute-force RSA factoring

Esoteric attack

Chosen cipher text attack

Low encryption exponent attack

Error analysis



# RSA Challenge

The RSA factoring challenge is an effort, sponsored by RSA Laboratories, to learn about the difficulty of factoring large numbers used in RSA keys

A set of eight challenge numbers, ranging in size from 576-bits to 2048-bits, are given

Challenge Number	Prize (\$US)	Status	Submission Date	Submitter(s)
<a href="#">RSA-576</a>	\$10,000	Not Factored		
<a href="#">RSA-640</a>	\$20,000	Not Factored		
<a href="#">RSA-704</a>	\$30,000	Not Factored		
<a href="#">RSA-768</a>	\$50,000	Not Factored		
<a href="#">RSA-896</a>	\$75,000	Not Factored		
<a href="#">RSA-1024</a>	\$100,000	Not Factored		
<a href="#">RSA-1536</a>	\$150,000	Not Factored		
<a href="#">RSA-2048</a>	\$200,000	Not Factored		



# Data Encryption Standard (DES)

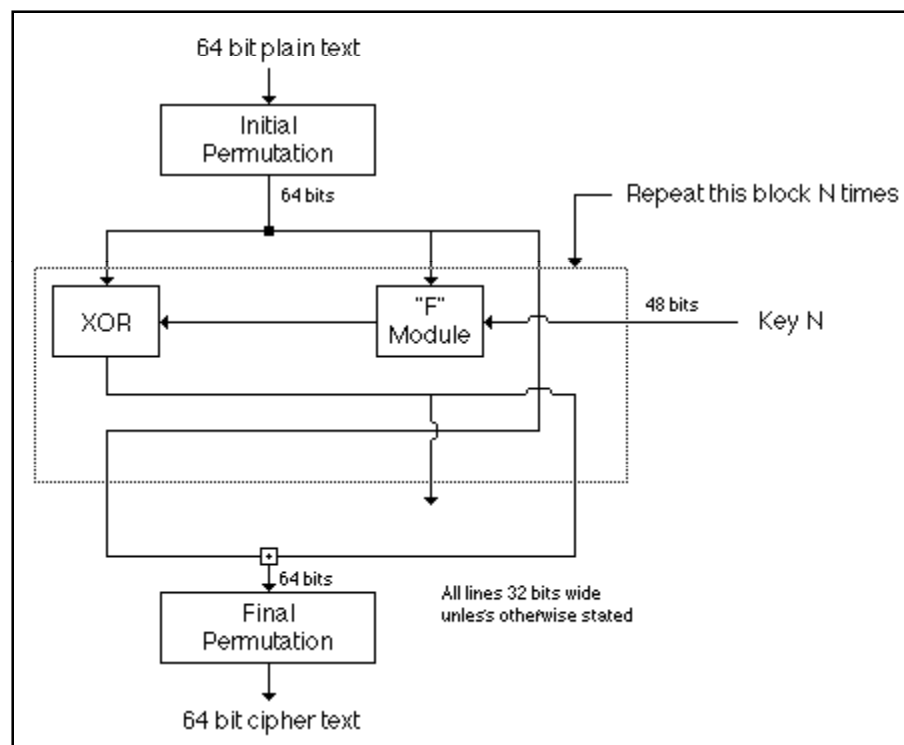
DES is an algorithm for encrypting and decrypting unclassified data

It is a block cipher that takes a plaintext string as input and creates a ciphertext string of the same length

It uses a symmetric key, which means that the same key is used to convert ciphertext back into plaintext

The DES's block size is 64 bits

The key size is also 64 bits, although 8 bits of the key are used for parity (error detection), which makes the effective DES's key size 56 bits



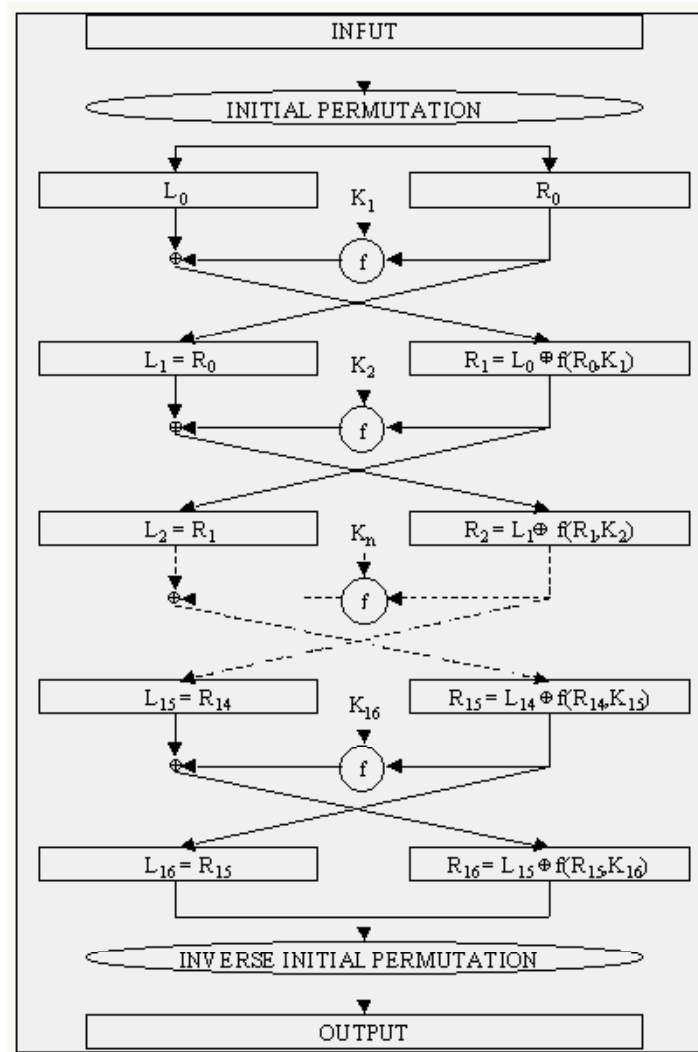
# DES Overview

DES acts on 64-bit blocks of the plaintext

It invokes 16 rounds of permutations, swaps, and substitutes

The standard includes tables describing all of the selection, permutation, and expansion operations

These aspects of the algorithm are not secrets



# DES Overview (cont'd)

- ◉ The basic DES steps are:

- The 64-bit block to be encrypted undergoes an initial permutation (IP), where each bit is moved to a new bit position
  - Example: the 1st, 2nd, and 3rd bits are moved to the 58th, 50th, and 42nd position, respectively

- The 64-bit permuted input is divided into two 32-bit blocks, called *left* and *right*, respectively

- The initial values of the left and right blocks are denoted as  $L_0$  and  $R_0$

- There are then 16 rounds of operation on the L and R blocks

- During each iteration (where  $n$  ranges from 1 to 16), the following formulae apply:

$$\begin{aligned}L_n &= R_{n-1} \\R_n &= L_{n-1} \text{ XOR } f(R_{n-1}, K_n)\end{aligned}$$

- The results from the final DES round —i.e.,  $L_{16}$  and  $R_{16}$ —are recombined into a 64-bit value and fed into an inverse initial permutation ( $IP^{-1}$ )

- At this step, the bits are rearranged into their original positions

- For example, the 58th, 50th, and 42nd bits, are moved back into the 1st, 2nd, and 3rd positions, respectively, the output from  $IP^{-1}$  is the 64-bit ciphertext block

# RC4, RC5, RC6, Blowfish

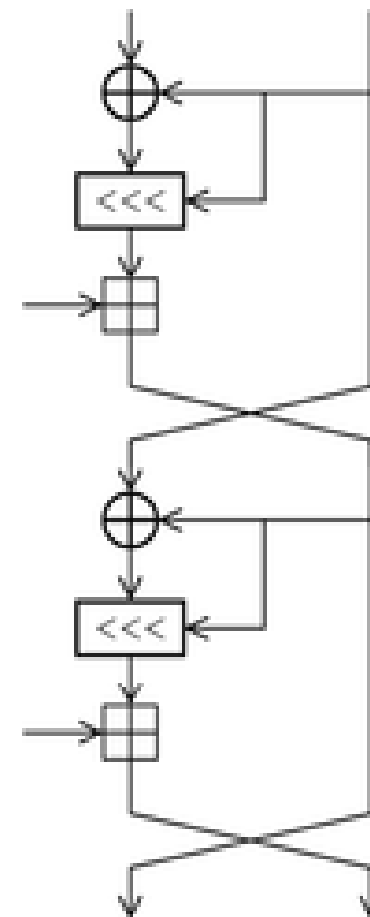
Algorithm	Features
Rc4	Is a variable key size stream cipher with byte-oriented operations, and is based on the use of a random permutation
Rc5	Is a parameterized algorithm with a variable block size, key size, and a variable number of rounds
Rc6	RC6 adds two features to RC5: the inclusion of integer multiplication, and the use of four 4-bit working registers instead of RC5's two 2-bit registers
Blowfish	Is a 64-bit block cipher that uses a key length that can vary between 32 and 448 bits

# RC5

RC5 is a fast and symmetric block cipher designed by RSA Security in 1994

It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The key size is 128-bits

RC6 is a block cipher based on RC5. Like RC5, RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable. The upper limit on the key size is 2040-bits



# Message Digest Functions

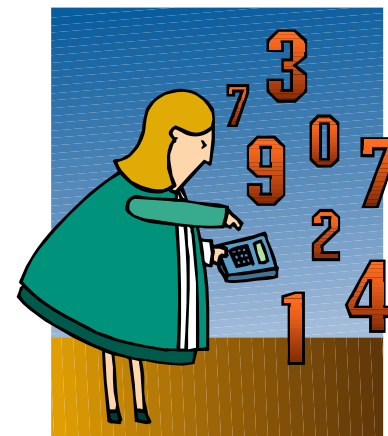
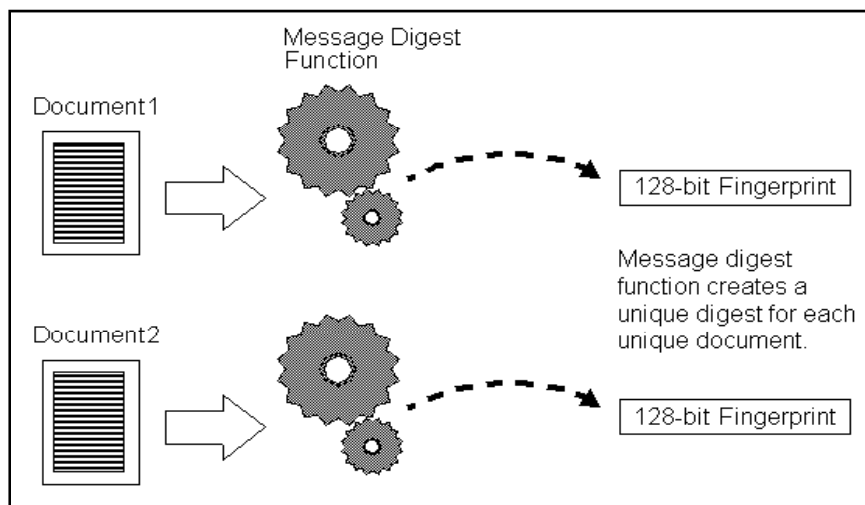
Message digest functions change the information contained in a file, (small or large) into a single large number, typically between 128 and 256 bits in length

The best message digest functions combine these mathematical properties

Every bit of the message digest function is influenced by the function's input

If any given bit of the function's input is changed, every output bit has a 50 percent chance of changing

Given an input file and its corresponding message digest, it should be computationally infeasible to find another file with the same message digest value





# One-way Bash Functions

Message digests are also called one-way bash functions because they produce values that are difficult to invert, resistant to attack, mostly unique, and are widely distributed

Message digest algorithms themselves are not used for encryption and decryption operations

They are used in the creation of digital signatures, message authentication codes (MACs), and encryption keys from passphrases

Message digest functions:

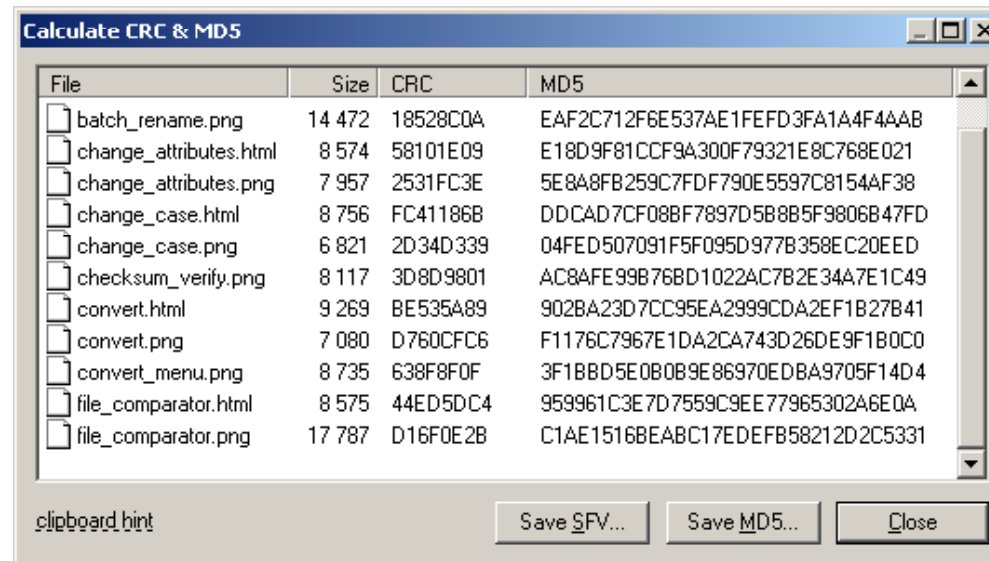
- HMAC
- MD2
- MD4
- MD5
- SHA
- SHA-1



# MD5

The MD5 algorithm takes as input, a message of arbitrary length, and outputs a 128-bit fingerprint or message digest of the input

The MD5 algorithm is intended for digital signature applications, where a large file is compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem, such as RSA



The screenshot shows a window titled "Calculate CRC & MD5" with a table of file hashes. The table has four columns: File, Size, CRC, and MD5. The files listed include batch\_rename.png, change\_attributes.html, change\_attributes.png, change\_case.html, change\_case.png, checksum\_verify.png, convert.html, convert.png, convert\_menu.png, file\_comparator.html, and file\_comparator.png. Each row shows the file name, its size in bytes, its CRC32 value, and its MD5 hash.

File	Size	CRC	MD5
<input type="checkbox"/> batch_rename.png	14 472	18528C0A	EAF2C712F6E537AE1FEFD3FA1A4F4AAB
<input type="checkbox"/> change_attributes.html	8 574	58101E09	E18D9F81CCF9A300F79321E8C768E021
<input type="checkbox"/> change_attributes.png	7 957	2531FC3E	5E8A8FB259C7FDF790E5597C8154AF38
<input type="checkbox"/> change_case.html	8 756	FC411868	DDCAD7CF08BF7897D5B885F9806B47FD
<input type="checkbox"/> change_case.png	6 821	2D34D339	04FED507091F5F095D977B358EC20EED
<input type="checkbox"/> checksum_verify.png	8 117	3D8D9801	AC8AFE99B76BD1022AC7B2E34A7E1C49
<input type="checkbox"/> convert.html	9 269	BE535A89	902BA23D7CC95EA2999CDA2EF1B27B41
<input type="checkbox"/> convert.png	7 080	D760CFC6	F1176C7967E1DA2CA743D26DE9F1B0C0
<input type="checkbox"/> convert_menu.png	8 735	638F8F0F	3F18BD5E0B0B9E86970EDBA9705F14D4
<input type="checkbox"/> file_comparator.html	8 575	44ED5DC4	959961C3E7D7559C9EE77965302A6E0A
<input type="checkbox"/> file_comparator.png	17 787	D16F0E2B	C1AE1516BEABC17EDEFB58212D2C5331

# MD5 (cont'd)

Few message digests are given below:

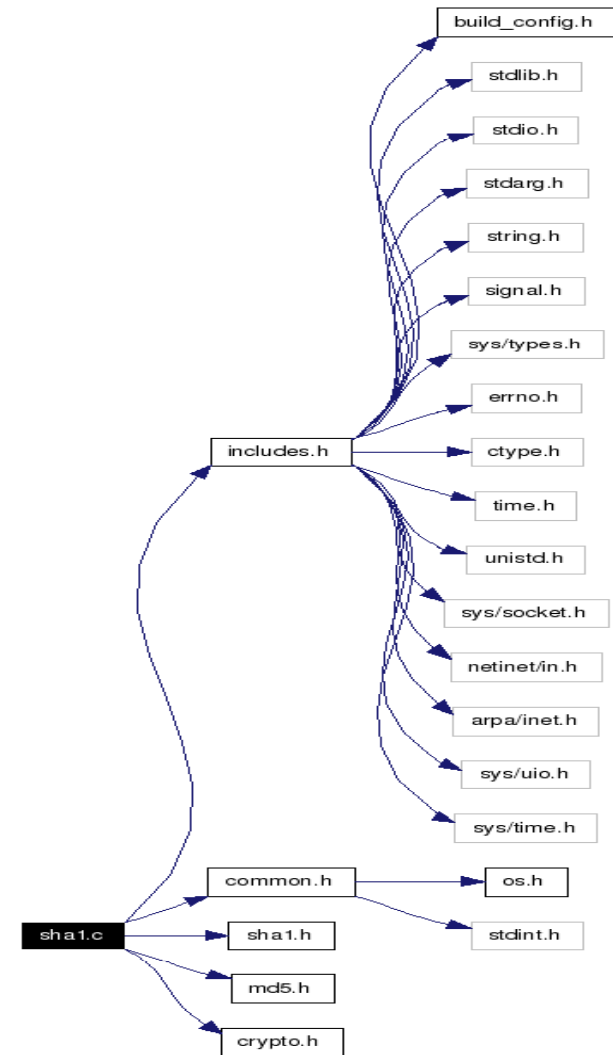
```
echo "There is CHF1500 in the blue bo" | md5sum  
e41a323bdf20eadafd3f0e4f72055d36 -  
  
echo "There is CHF1500 in the blue box" | md5sum  
7a0da864a41fd0200ae0ae97afd3279d -  
  
echo "There is CHF1500 in the blue box." | md5sum  
2db1ff7a70245309e9f2165c6c34999d -  
  
echo "There is CHF1500 in the blue box.." | md5sum  
86c524497a99824897ccf2cd74ede50f -
```

The same text always produces the same MD5 code

# SHA (Secure Hash Algorithm)

The SHA algorithm takes a message of the arbitrary length as input and outputs a 160-bit fingerprint or message digest of the input

The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks



# SSL (Secure Sockets Layer)

SSL stands for Secure Sockets Layer

It is a protocol developed by Netscape for transmitting private documents via the Internet

It works by using a private-key to encrypt data which is transferred over the SSL connection

SSL Protocol is an independent application protocol



# What is SSH

The program SSH (Secure Shell) is a secure replacement for telnet and the Berkeley r-utilities (rlogin, rsh, rcp, and rdist)

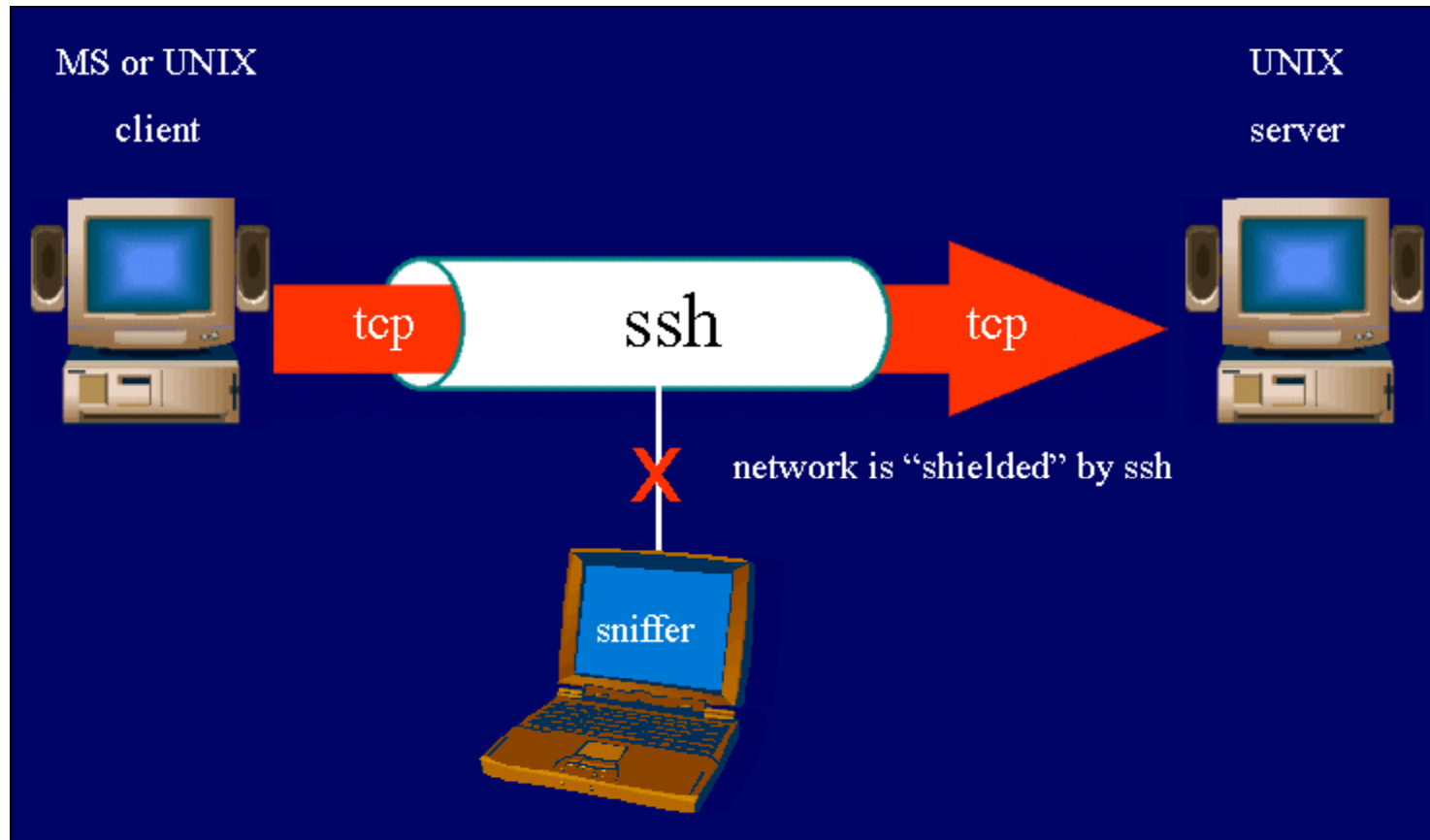
It provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another

It provides a strong host-to-host and user authentication, as well as a secure encrypted communications over an insecure Internet

SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, an SSH2 tunneled FTP



# SSH (Secure Shell)



# Algorithms and Security

**40-bit key** algorithms are of no use

**56-bit key** algorithms offer privacy, but are vulnerable

**64-bit key** algorithms are safe today but will be soon threatened as the technology evolves

**128-bit** and over algorithms are almost unbreakable

**256-bit** and above are impossible



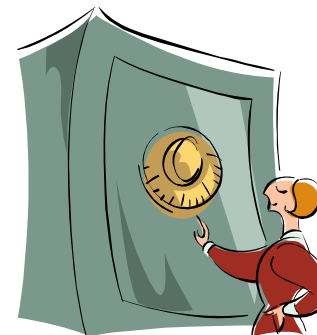


# Disk Encryption

Disk encryption works similarly to text message encryption

With the use of an encryption program for your disk, you can safeguard any information to burn onto the disk, and keep it from falling into the wrong hands

Encryption for disks is useful when you need to send sensitive information through the mail

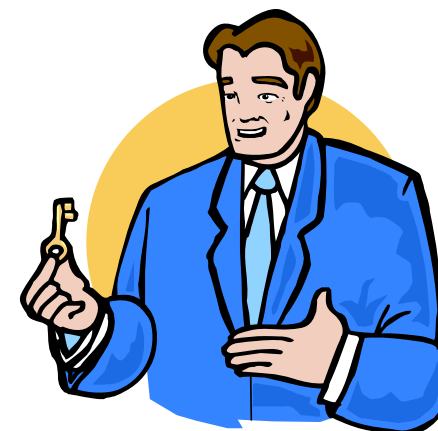


# Government Access to Keys (GAK)

Government Access to Keys (also known as key escrow) means that software companies will give copies of all keys, (or at least enough of the key that the remainder could be cracked) to the government

The government promises that they will hold on to the keys in a secure way, and will only use them when a court issues a warrant to do so

To the government, this issue is similar to the ability to wiretap phones

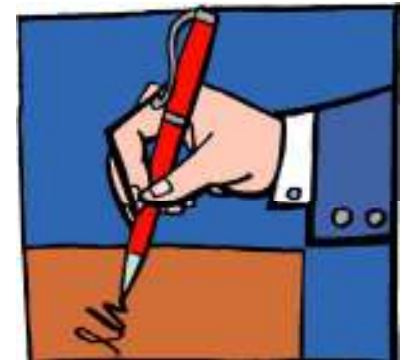


# Digital Signature

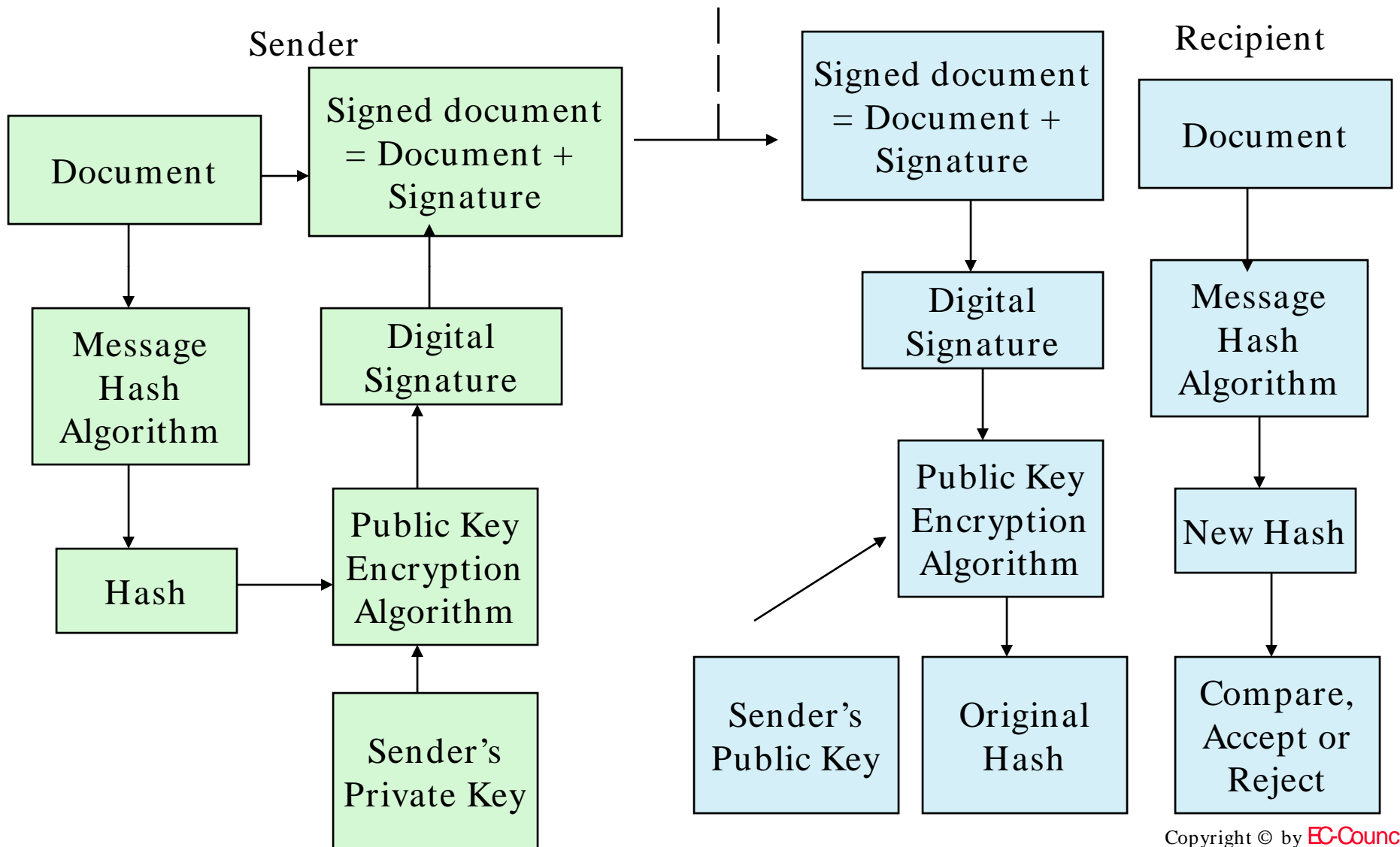
Digital Signature is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written form

Digital signature schemes normally give two algorithms; one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key

The output of the signature process is called the "digital signature"



# Digital Signature (cont'd)



## Components of Digital Signature:

Public key

Name and E-mail of sender

Key expiry date

Company name that sends the information

Serial number of Digital Signature

Digital signature of certification authority



# Method of Digital Signature Technology

## Two stages of Digital Signature:

- Creation
- Verification

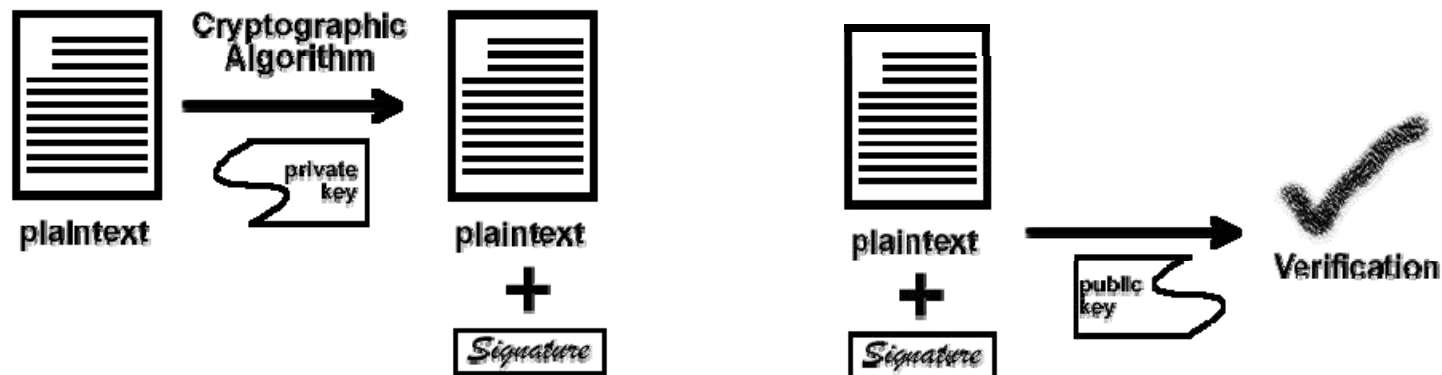
## Two keys used in Cryptography:

- Public key which is available to everyone
- Private key which is known only to the sender

Digital Signature uses public key cryptography to encrypt and decrypt messages

Hash encrypted message

Hash function produces and checks the digital signatures



# Digital Signature Applications

Digital Signatures are used to check:

Identity of the sender

Dependability of the message

Whether message sent is genuine

For risk of frauds

Whether message is illegally reproduced

Fulfillment of lawful requirements

For security of open systems



# Digital Signature Standard

Certain applications require digital signatures instead of normal signatures

DSA digital signature consists of two binary numbers

DSA generates and verifies the signatures

Set of rules and arguments are needed to evaluate a digital signature to confirm the integrity of data

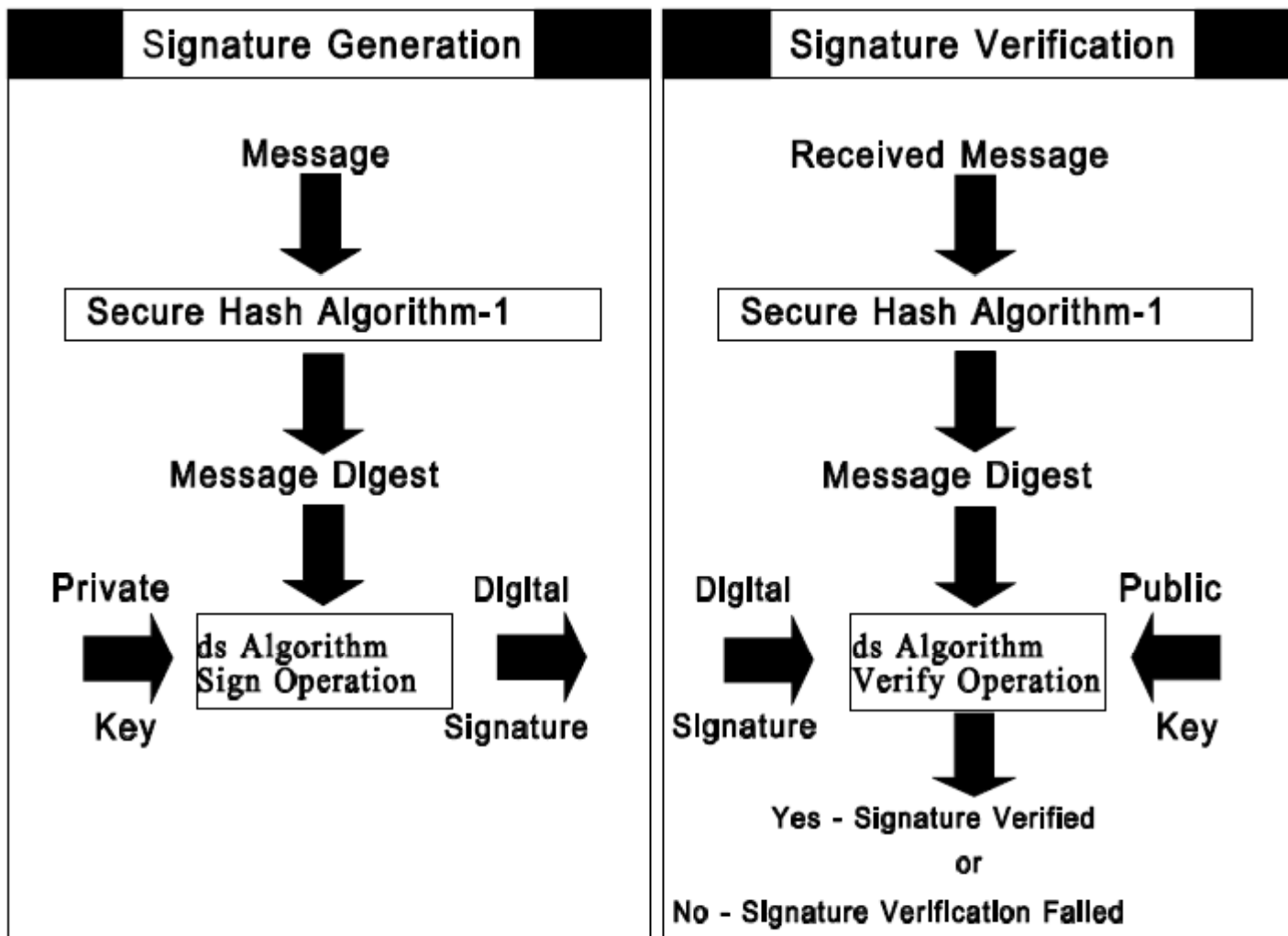
Private key is used in producing a digital signature

Message Digest is the reduced form of the message

Hash function is used in generating a signature



# Digital Signature Algorithm: Signature Generation/ Verification



# Digital Signature Algorithms: ECDSA, ElGamal Signature Scheme

## ElGamal signatures scheme:

- Is based on the difficulty in computing discrete logarithms
- DSA is an alternative to this signature scheme
- It allows a verifier to confirm the authenticity of a message

## ECDSA:

- Elliptic Curve Digital Signature Algorithm
- Variant of DSA operating on elliptic curve groups
- Efficient over DSA
- Not vulnerable to number field sieve attack



# Challenges and Opportunities

Application of digital signature in the regular business has some advantages and expenses

Implementing digital signatures effectively unravels the following issues:

- False identities
- Alteration of information
- Lawful requirements are met
- Security to systems on the net

Expenses include:

- Cost of maintaining certification authorities
- Cost of software that implements digital signature



# Digital Certificates

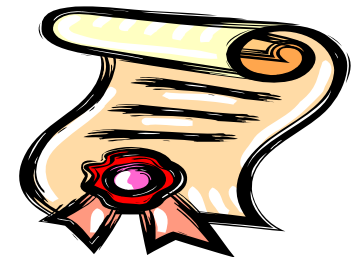
Digital Certificates verify the uniqueness of the principles and entities over networks as electronic documents

Unique identity to the owner of the digital certificate is defined by both public key and private keys

Widely accepted format for digital certificates is defined by the ITU-T X.509 international standard

Digital certificate includes a variety of information such as:

- Name of the subject
- Subject's public key
- Certification authority's name
- Serial number
- Lifetime period of the digital certificate right from the start date



# Cleversafe Grid Builder

<http://www.cleversafe.com/>

Cleversafe Grid Builder EN software subscriptions provide all the software that you need to build your own dispersed storage grid

The 11 dispersed storage nodes can be spread across upto 11 servers for maximum security benefits

## Benefits of building your own grid:

- Control your data within your own fourwalls based on your existing offices and infrastructure
- Utilize the most innovative technology to reach the storage market in decades
- Avoid expensive hardware costs and use older storage devices you have around
- Customize your implementation based on your environment
- Create derivative works by changing source code to meet your storage needs and processes

# PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP) is a software package originally developed by Philip R. Zimmermann, which provides cryptographic routines for email, and file storage applications

Zimmermann took existing cryptosystems and cryptographic protocols, and developed a program that can run on multiple platforms

It provides message encryption, digital signatures, data compression, and email compatibility



# PGP: Screenshot

PGP 6.5.8ckt - Build:07 Setup

**Select Components**

Choose the components Setup will install.

Select the components you want to install, clear the components you do not want to install.

<input checked="" type="checkbox"/> PGP Key Management (Required)	2780 K
<input checked="" type="checkbox"/> PGPdisk Volume Security	868 K
<input checked="" type="checkbox"/> PGPnet Virtual Private Networking	938 K
<input checked="" type="checkbox"/> PGP Qualcomm Eudora Plugin	400 K
<input checked="" type="checkbox"/> PGP Microsoft Exchange/Outlook Plugi	256 K
<input checked="" type="checkbox"/> PGP Microsoft Outlook Express Plugin	212 K
<input checked="" type="checkbox"/> PGP Command Line	1028 K
<input checked="" type="checkbox"/> Samopal PGP ICQ Plugin	816 K


Space Required on C: 11712 K  
Space Available on C: 16153808 K

InstallShield

< Back   Next >

Description  
This component includes the core program files for PGPnet Virtual Private Network

**Key Generation Wizard**



In order for other people to send you secure messages, you must generate a key pair.

Your key pair will also be used to sign digital documents.

A key pair consists of a "Public Key," and a "Private Key." The public key should be given to everyone you know (PGP has facilities to assist in this). The private key should be kept absolutely secret.

If you would like more information on what a key pair is and how PGP works, click the Help button, below.

Otherwise, choose Next to continue.

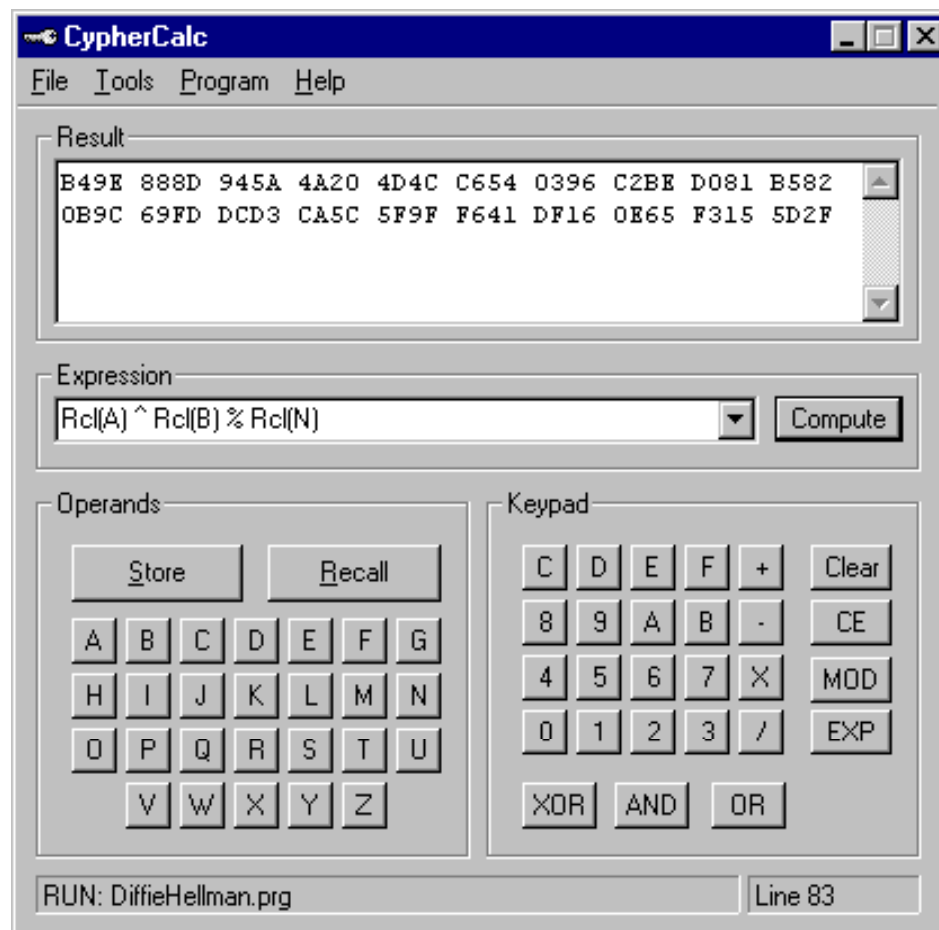
< Back   Next >   Cancel   Help

# CypherCalc

CypherCalc is a full-featured, programmable calculator designed for multi-precision integer arithmetic

It is intended for use in the design, testing, and analysis of cryptographic algorithms involving key exchanges, modular exponentiation, modular inverses, and Montgomery Math

It has built-in GCD and SHA 1 tools, and a CRC tool that can generate CRC tables for your applications





# Command Line Scriptor

Command Line Scriptor automates file encryption/ decryption, digital signing, and verification

It sends files and email securely without any user intervention

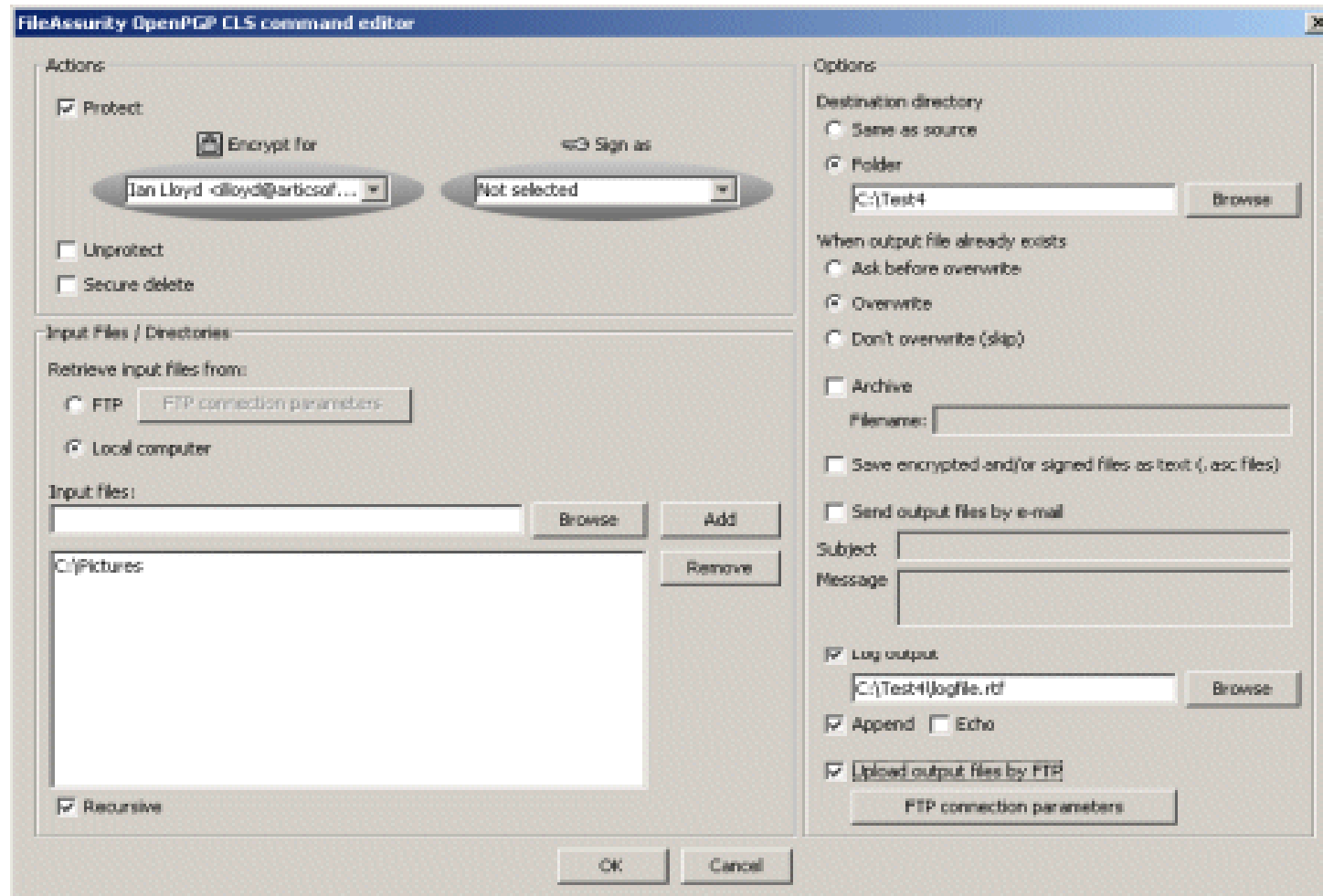
It ensures that all of the important data is secured without relying on user input

Bulk deletes files at a pre-defined date and time

It integrates cryptographic techniques into the existing applications

It processes incoming secure files from any OpenPGP compliant application

# Command Line Scriptor: Screenshot



# CryptoHeaven

<http://linux.softpedia.com/progScreenshots/CryptoHeaven-Screenshot-229.html>

CryptoHeaven allows groups to send encrypted email, securely backup and share files, pictures, charts, business documents, and any other form of electronic media through a secure environment

No third parties, including server administrators, government agencies, and others have access to the plain text version of the transmitted information

Some of the features of the service include:

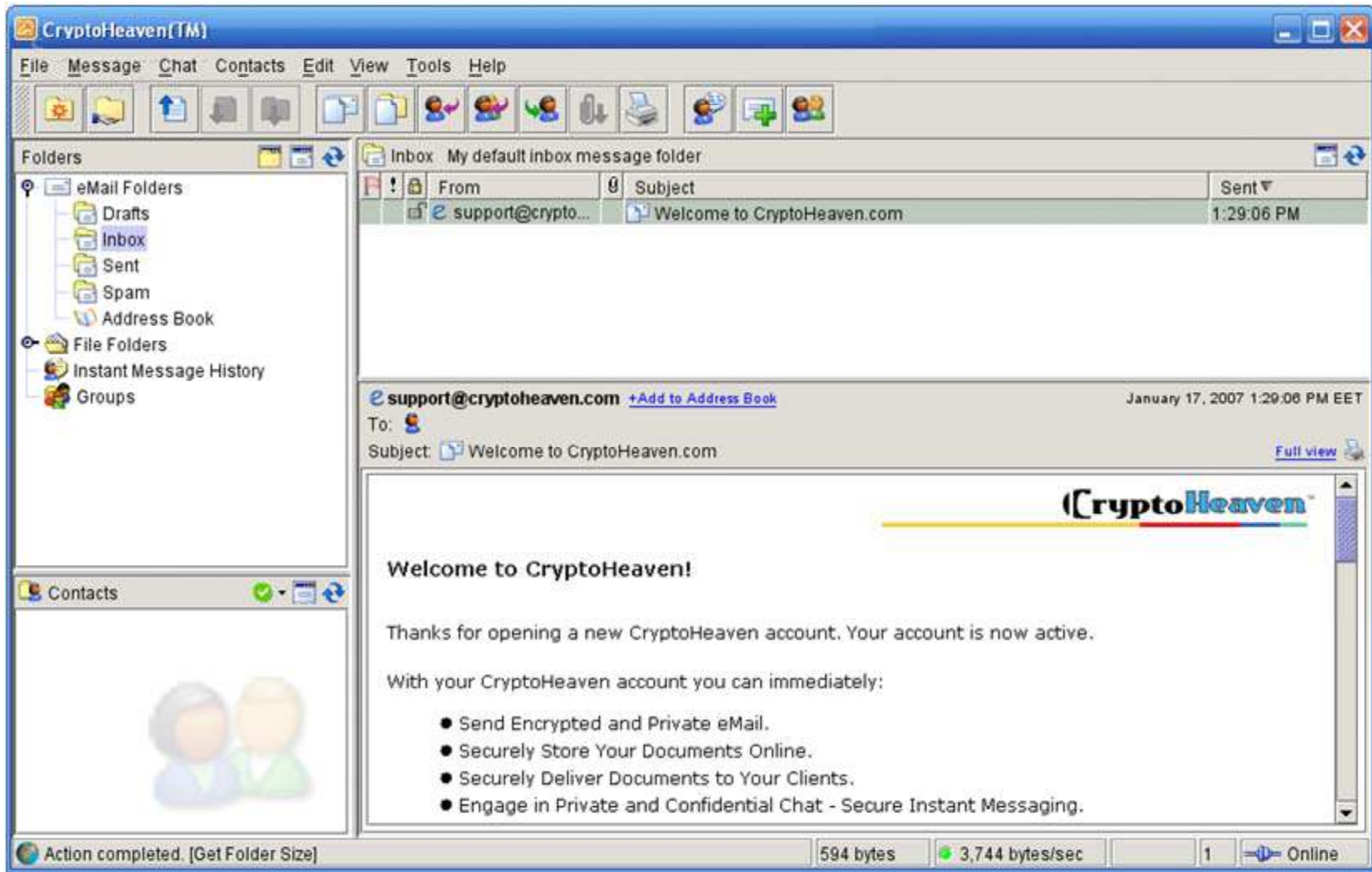
- Secure document storage
- Secure document sharing and distribution
- Secure message boards
- Secure email and secure instant messaging



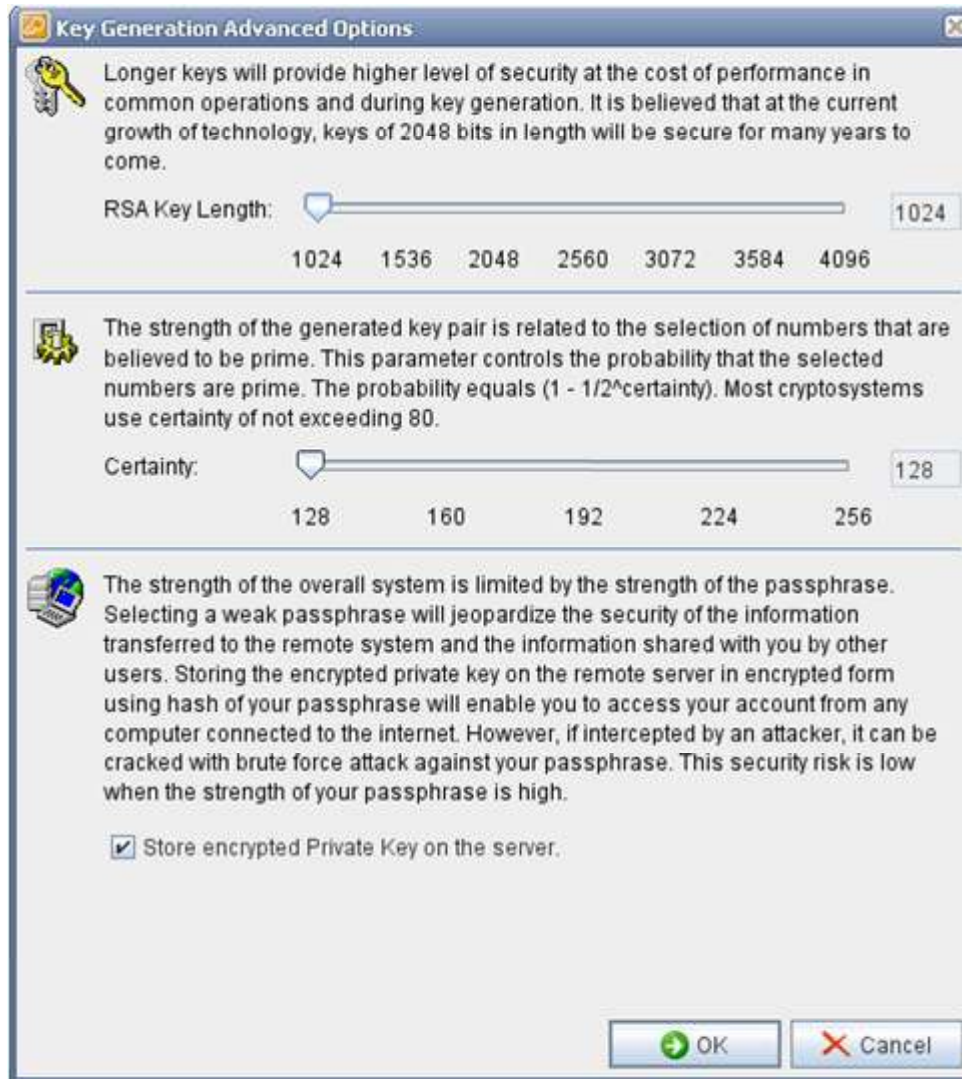
# CryptoHeaven: Screenshot 1



# CryptoHeaven: Screenshot 2



# CryptoHeaven: Screenshot 3



# Hacking Tool: PGP Crack

PGP crack is a program designed to brute force a conventionally encrypted file with a PGP, or a PGP secret key

The file pgpfile cannot be ascii-armored

The file phraselist should be a file containing all of the passphrases that will be used to crack the encrypted file





# Magic Lantern

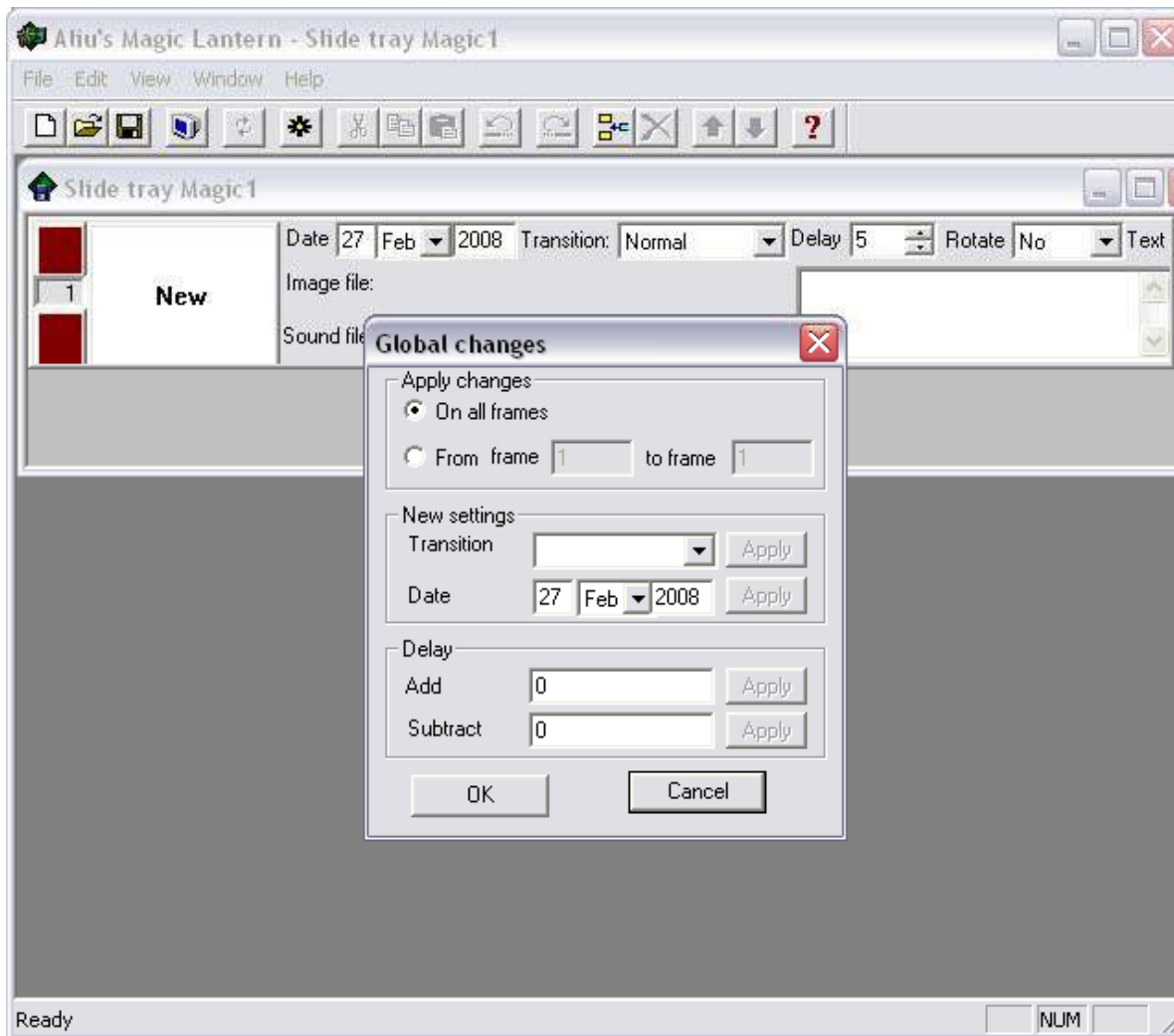
Magic Lantern is a new surveillance software that allows agents to de-code the hard-to-break encrypted data of criminal suspects

Magic Lantern works by infecting a suspect's computer with a virus that installs keylogging software – a program that can capture the keystrokes typed into a computer





# Magic Lantern: Screenshot



# Advanced File Encryptor

Advanced File Encryptor is a tool to encrypt and secure most important files like banking information, e-mail documents, and any other file with special personal value

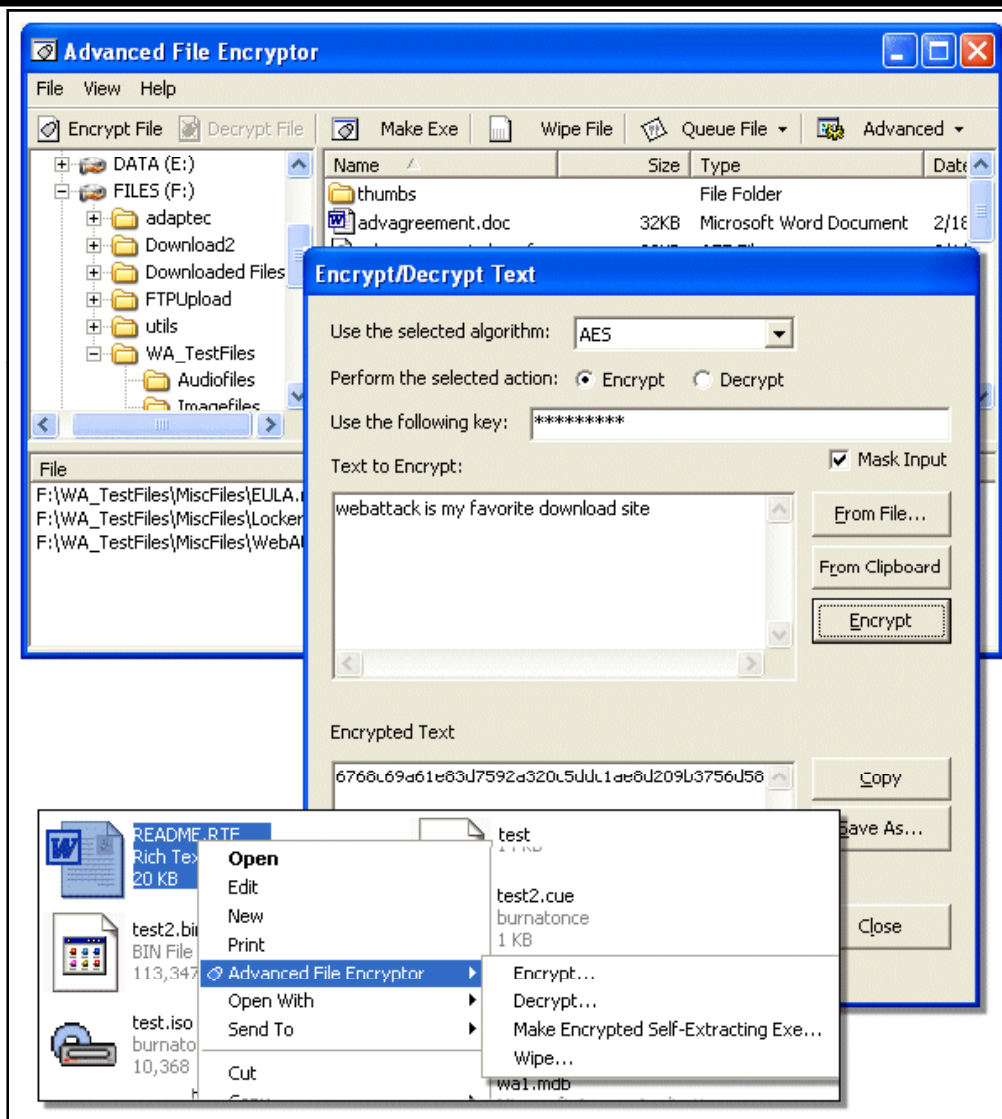
This program uses unbreakable 256-bit AES encryption and provides a peace of mind that data is safe

It can also create self-decrypting archive files that require a password when opened and will extract the protected documents

It allows to encrypt typed text or clipboard content using AES, Twofish, or RSA encryption, which allows you to protect email or chat conversations as well



# Advanced File Encryptor: Screenshot



# Encryption Engine

Encryption Engine allows to protect the privacy of sensitive files and folders by encrypting them with a strong encryption algorithm and a password

Once encrypted, the files or folders cannot be viewed without the original password with which they were encrypted

Encrypted files can be stored on any unsecured devices or can be sent through email without worrying about the security of the data

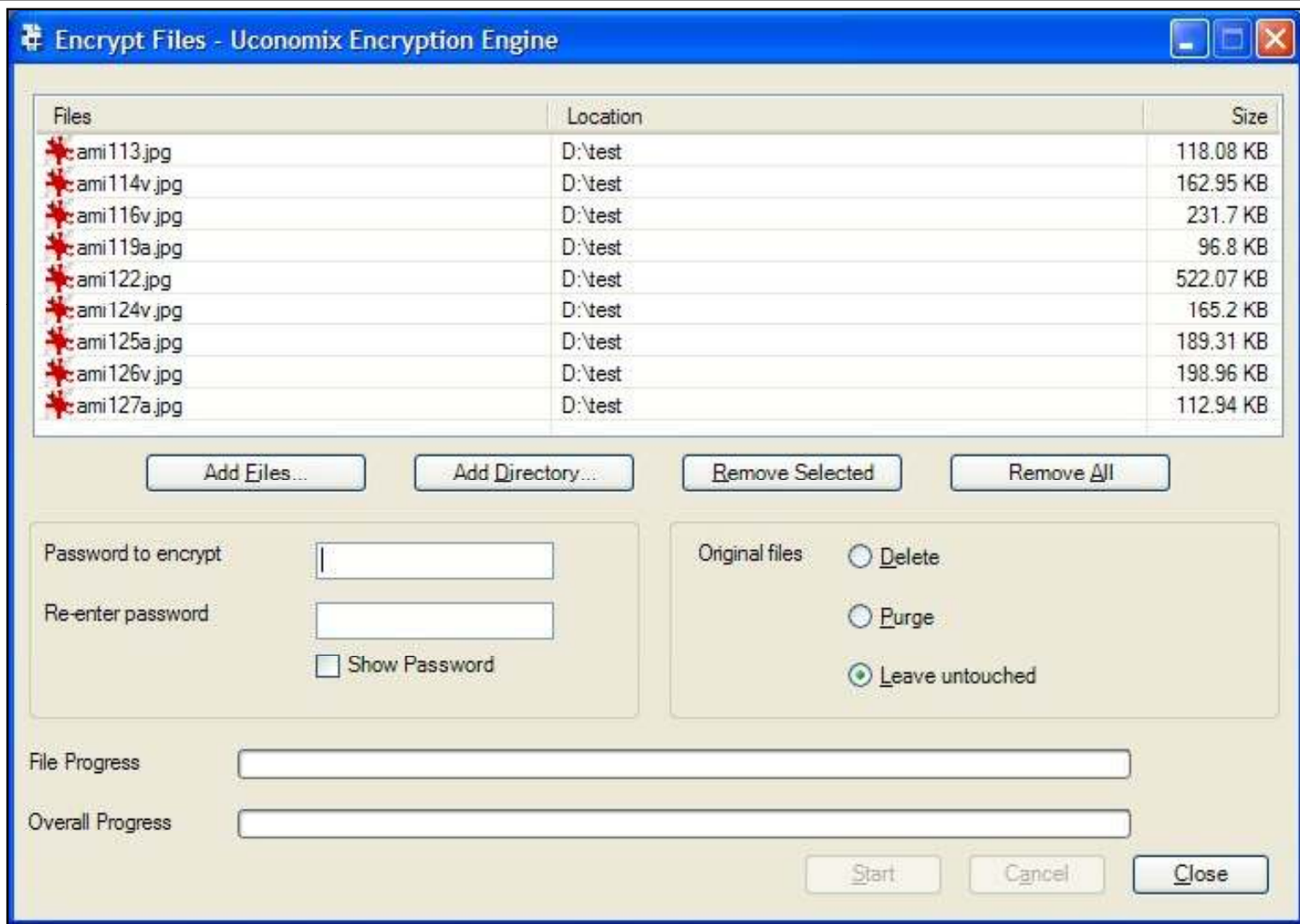
It can encrypt any type of file, be it a Word document, PDF document, PowerPoint presentation, Excel worksheet, MP3 song, Video clip, image, plain text file, or any other data that is in binary format



# Encryption Engine: Screenshot 1

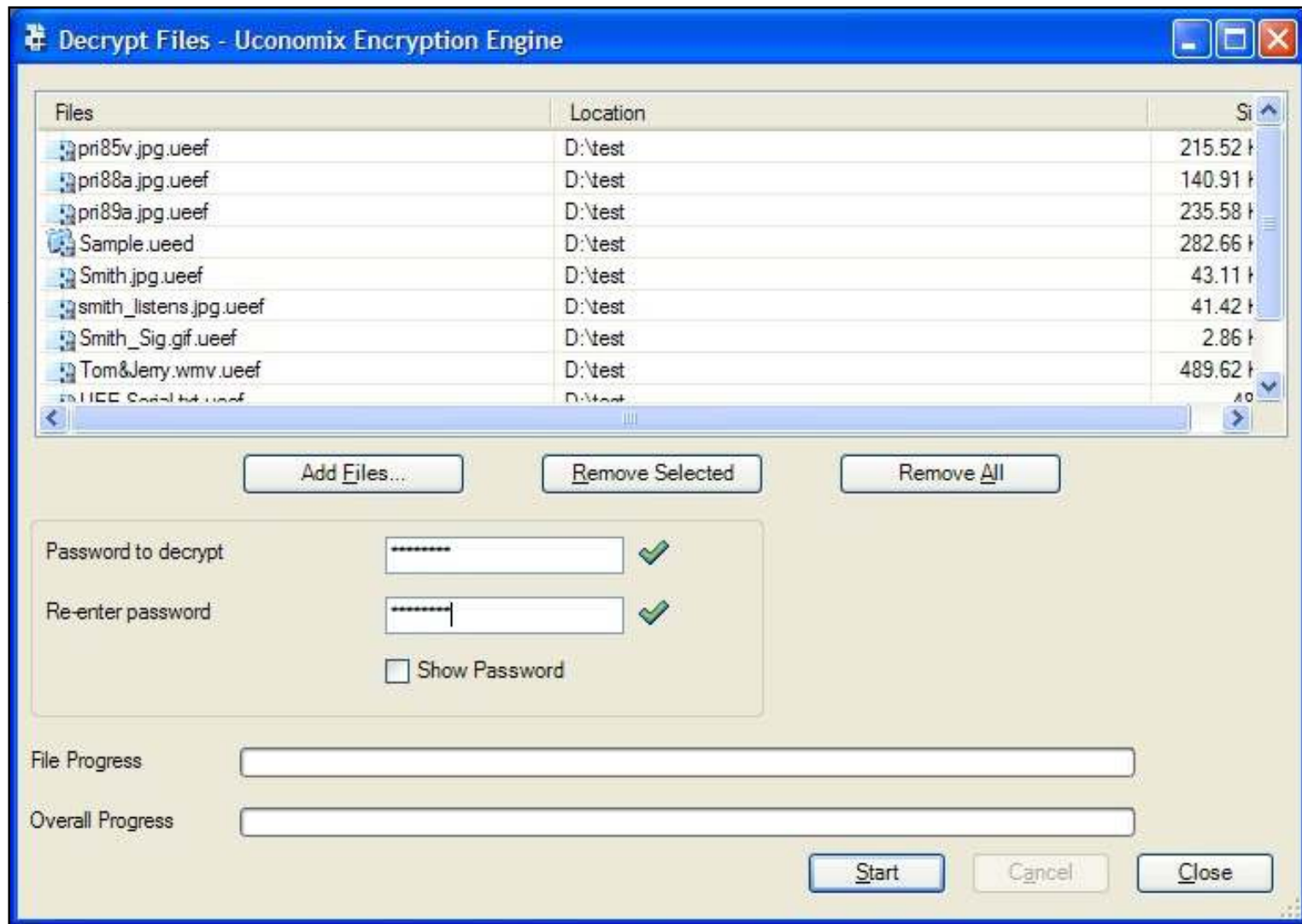


# Encryption Engine: Screenshot 2





# Encryption Engine: Screenshot 3



# Encrypt Files

Encrypt Files is an encryption desktop computer software

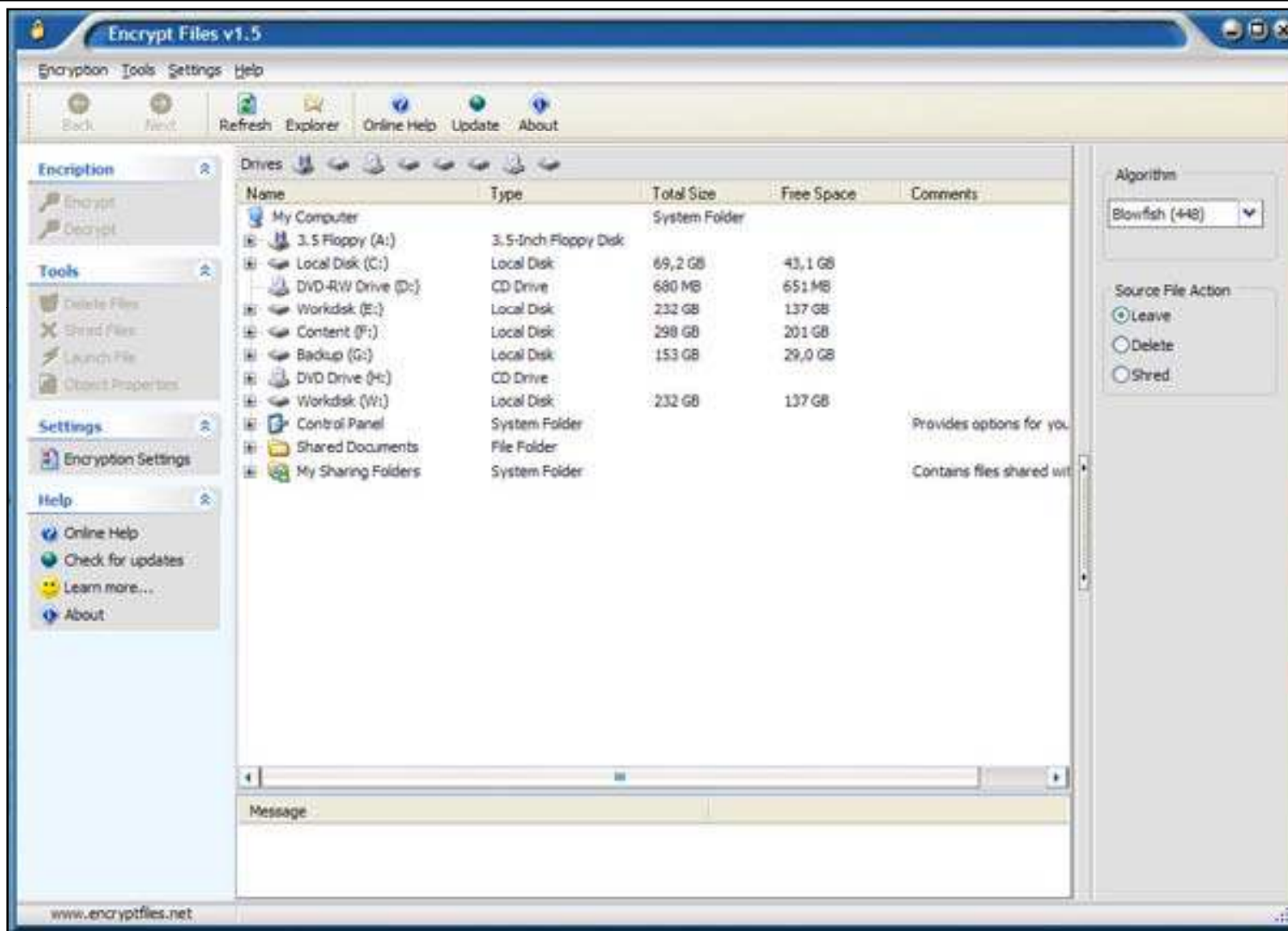
It is a desktop application that supports 13 advanced encryption algorithms including Blowfish, Cast, Ice, Mars RC 2,6 and 4, Rijn Dael, Tripple Des

This powerful program will allow to encrypt files and folders and password protect them





# Encrypt Files: Screenshot



# Encrypt PDF

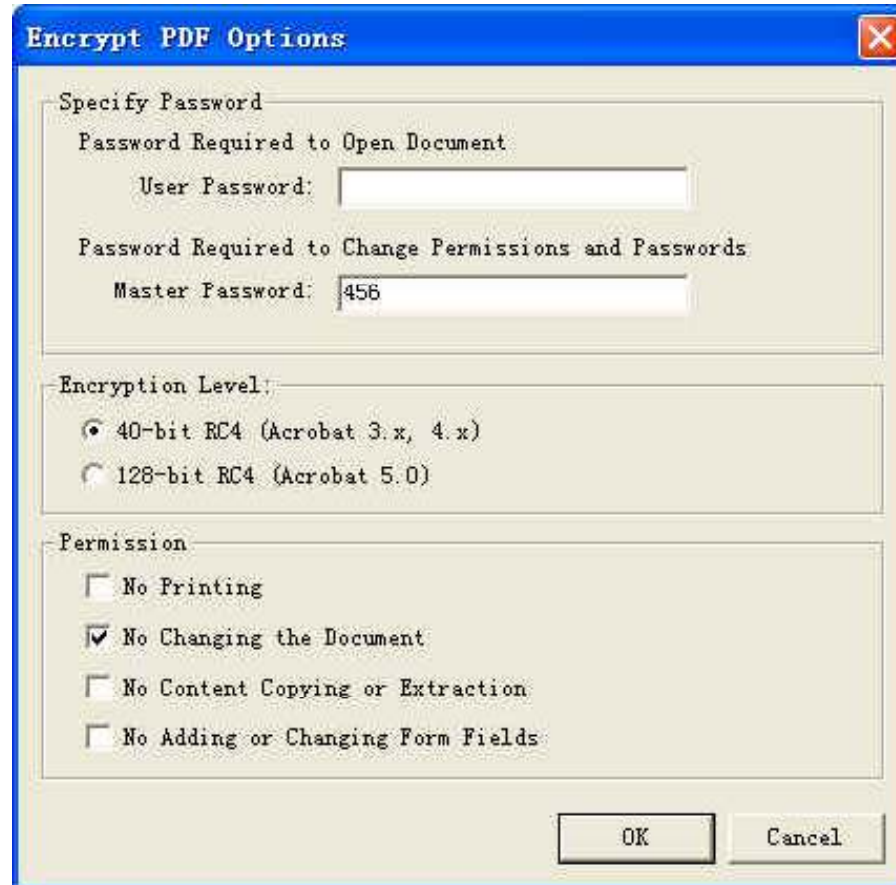
Encrypt PDF software allows to encrypt (using standard 40-bit or 128-bit supported by Acrobat Reader 7.0 and up) existing PDFs, set permissions, add user, and owner password

Button to print the file will be disabled in Acrobat Reader application, it can encrypt a PDF allowing the user to read it only if he knows the correct password

Two passwords can be applied to the PDF: they are owner and user password



# Encrypt PDF: Screenshot



# Encrypt Easy

Encrypt Easy is a file encryption program enabling one-click encryption and decryption of single files, folders, and entire directory trees

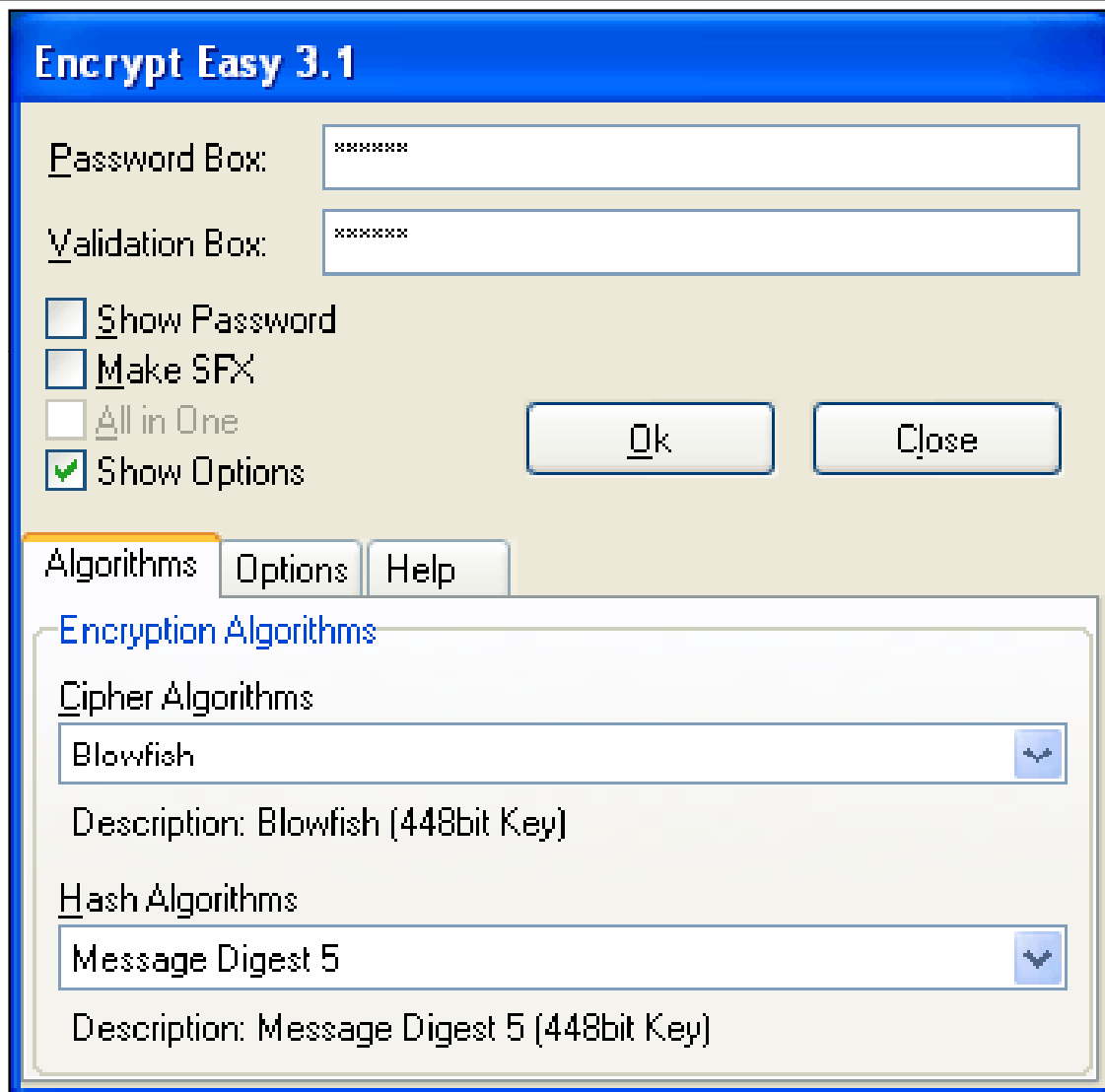
It uses the best and most proven cryptographic algorithms such as 448-bit Blowfish, Hash, Des, and Triple Des

Files can be only decrypted using the password

Encrypt Easy contains self extracting; it can send encrypted files through Internet and decrypt them without using Encrypt Easy program

File shredder function enables to remove files or folders containing sensitive data permanently from systems in such a way that nobody can recover them

# Encrypt Easy: Screenshot



# Encrypt my Folder

Encrypt my Folder is a new folder password protected software which can help to lock files, folders with personal password

Encrypting files, folders is the best way to guarantee that nobody accidentally or intentionally gets access to your private and confidential information

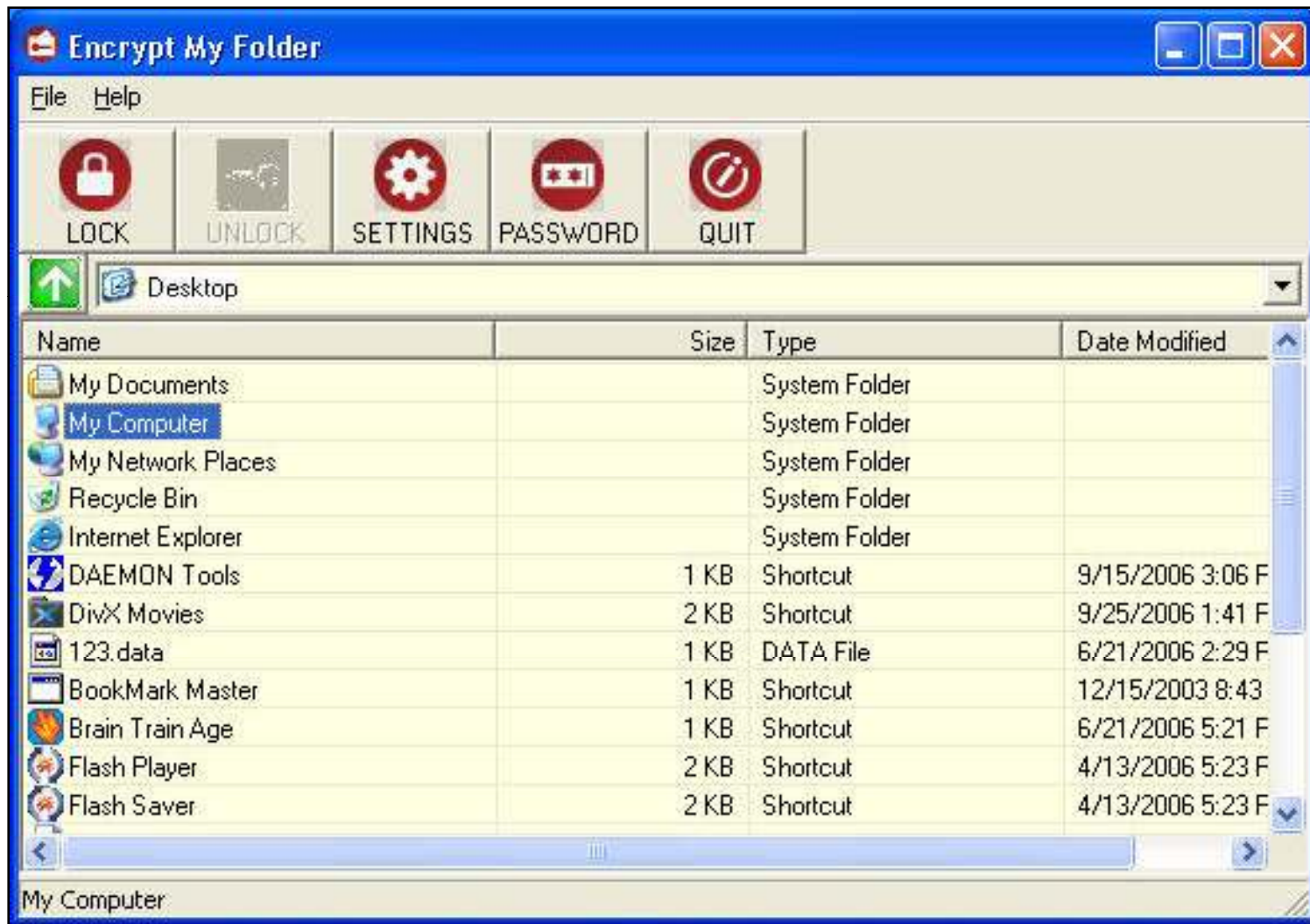
Encrypt my Folder enables folder security to be simple, intuitive, and dependable

## Features:

- Locks or unlocks file, folder
- Locks local directory and subdirectory
- Works perfectly on disk types like NTFS/FAT
- No need to run Encrypt my Folder at all time; it supports lock all items when exit



# Encrypt my Folder: Screenshot



# Advanced HTML Encrypt and Password Protect

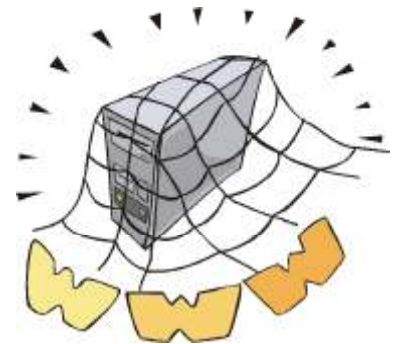
Advanced HTML Encrypt and Password Protect allows to encrypt HTML pages with strong encryption algorithms and protects them with a password

This program will prevent anyone from viewing the source code or stealing art work

Encrypted pages will have the same look as the original ones and can be viewed in all modern web browsers

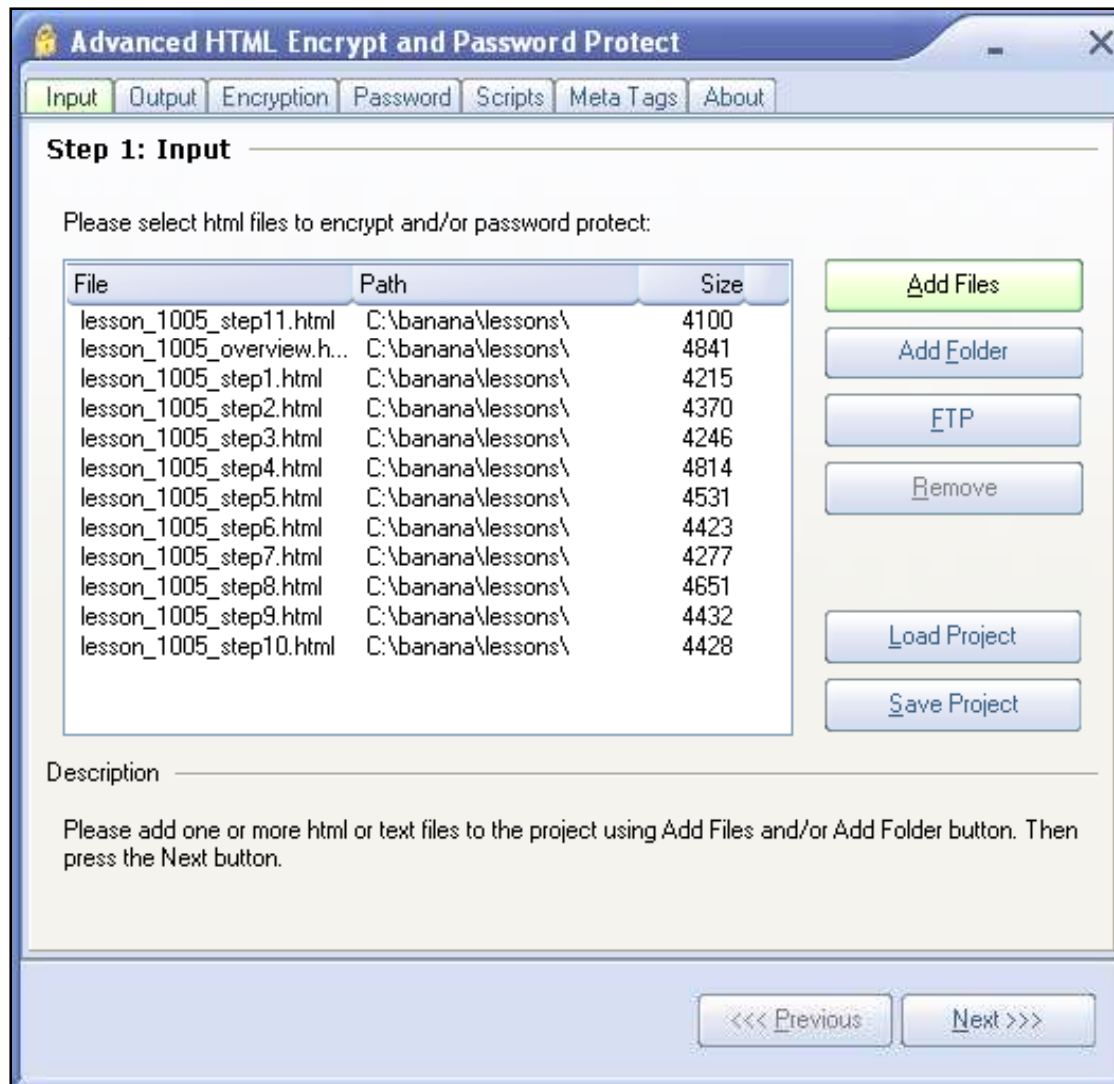
It can stop spam robots from extracting email addresses from pages

It can prevent people from using automated downloader to save the entire website to their hard drive

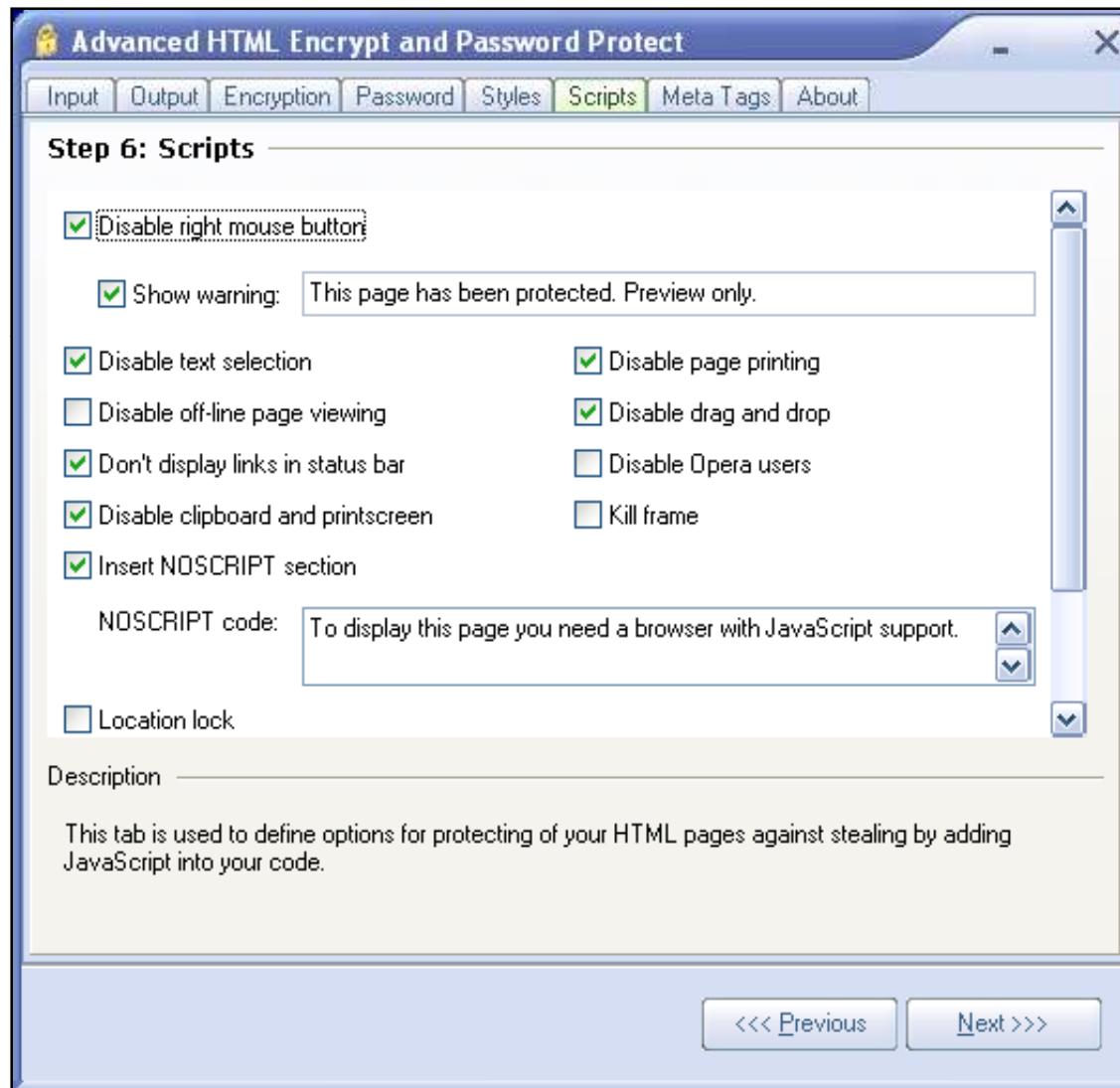




# Advanced HTML Encrypt and Password Protect: Screenshot 1



# Advanced HTML Encrypt and Password Protect: Screenshot 2



# Encrypt HTML Source

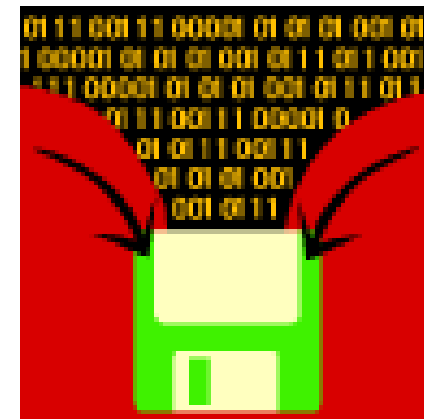
Encrypt HTML source is a solution for full web site protection

It will encrypt HTML, ASP, JavaScript, VBScript, SHTML, and CSS source code and will make it impossible to steal and reuse it in other websites

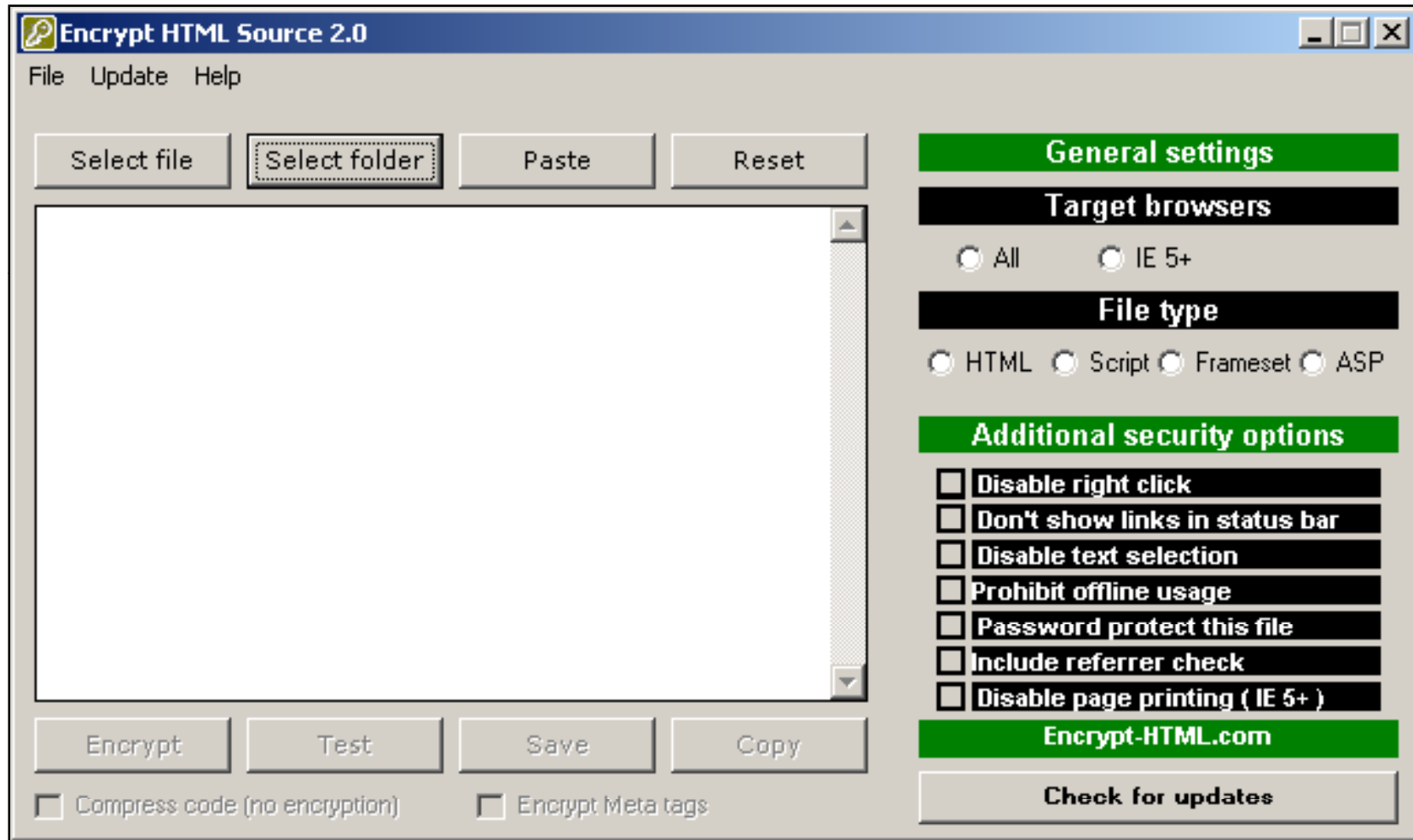
Password protects web pages

Advanced web site images protection

Security options available such as disable right-click, page printing, text selection, copying, clipboard, and offline usage of encrypted files



# Encrypt HTML Source: Screenshot



# Alive File Encryption



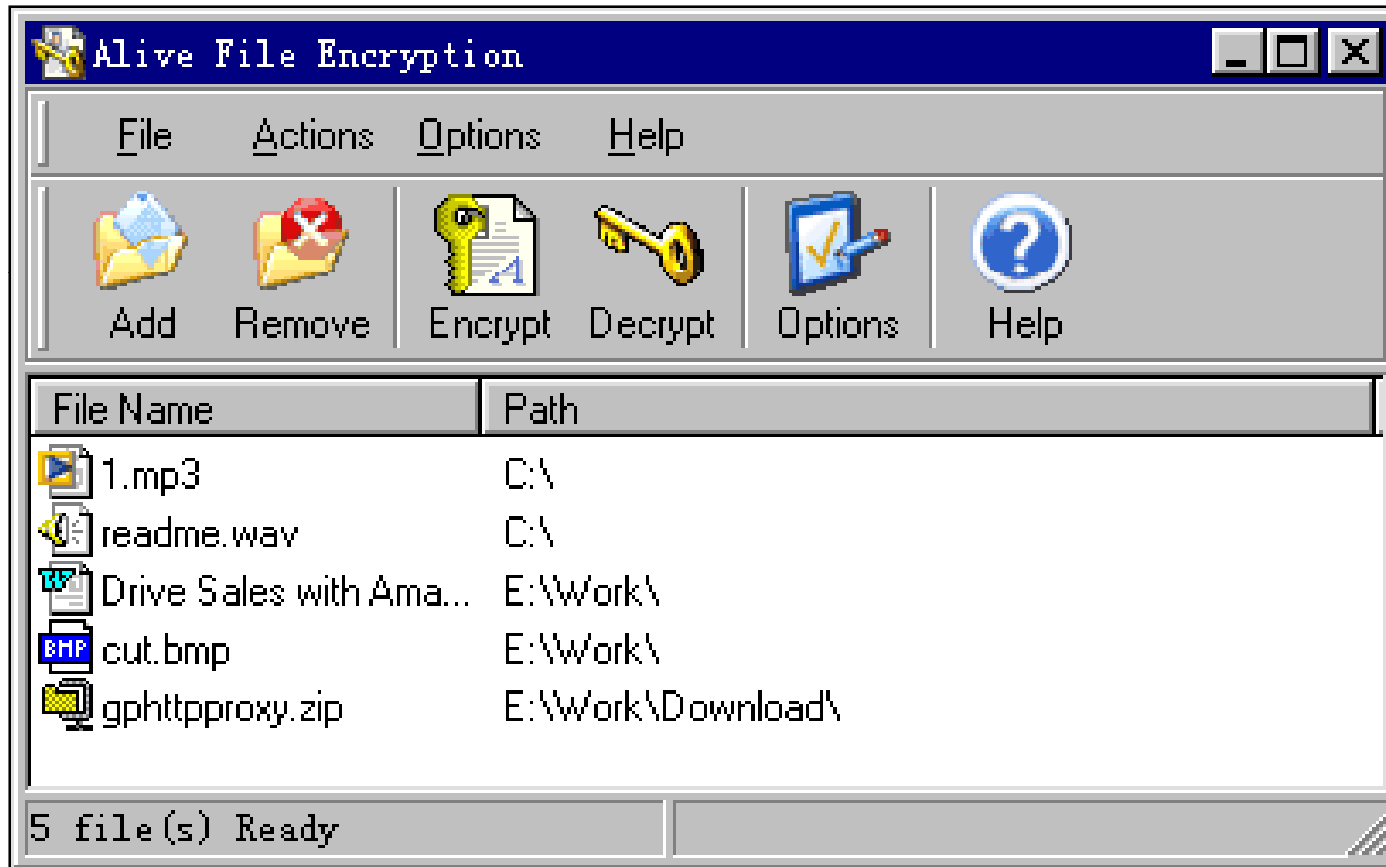
Alive File Encryption is a program that encrypts files and folders

It is integrated with Windows Explorer; it can secure any file with a simple right click

Just right click the files or folders you would like to encrypt or decrypt, and then enter a password to encrypt or decrypt them

It can also encrypt the file into an executable file (EXE-file), which can be decrypted without Alive File Encryption

# Alive File Encryption: Screenshot



# Omziff

Omziff is an encryption utility that uses various cryptographic algorithms to encrypt and decrypt textual files

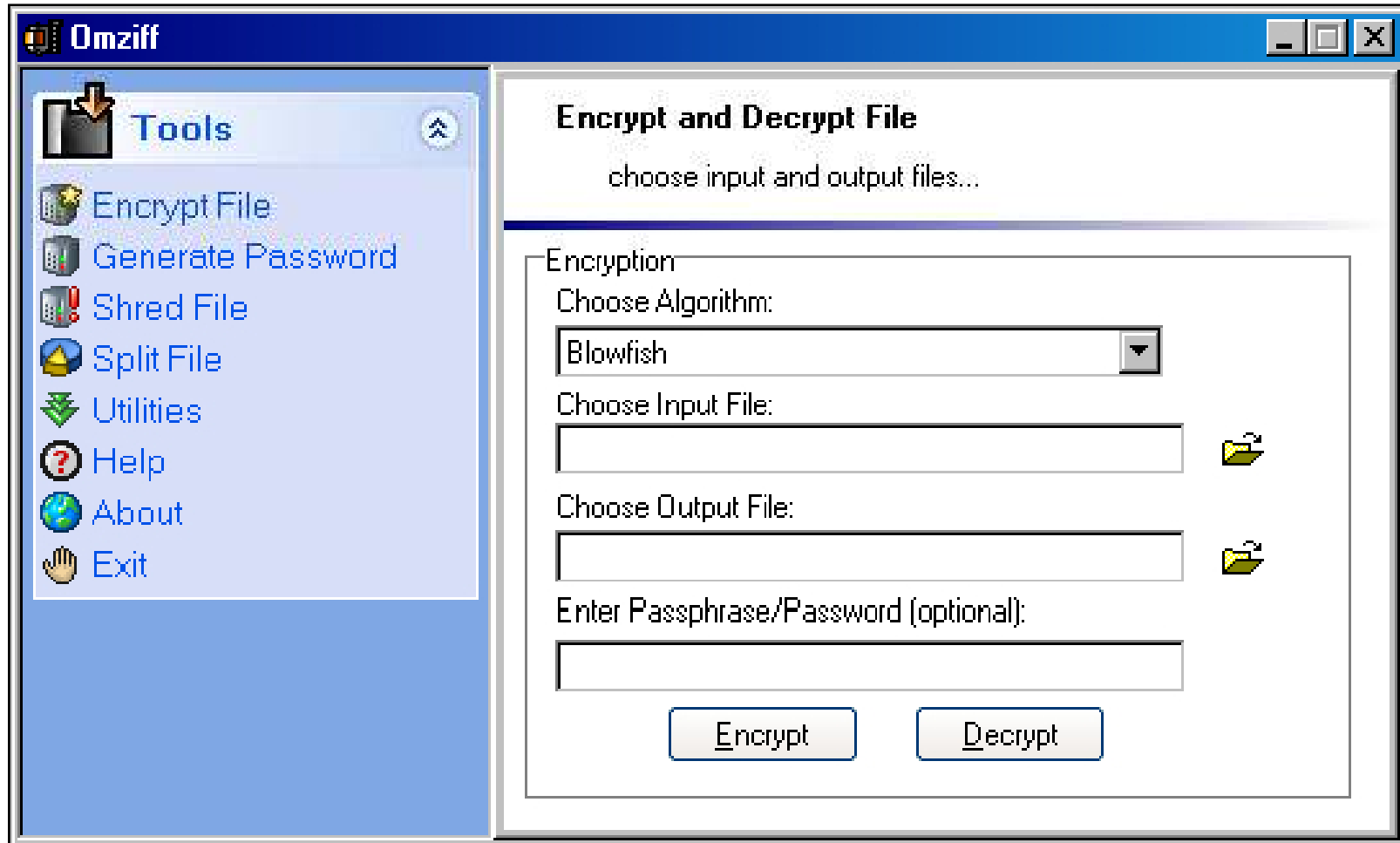
These algorithms include Blowfish, Cast128, Gost, IDEA, Misty1, AES/Rijndael, and Twofish

Omziff also generates random passwords, splits files, and deletes secure file according to DOD Standards

It is freeware, comes in a standalone executable file with no dependencies and is a completely USB portable application



# Omziff: Screenshot





# ABC CHAOS

ABC CHAOS easily encrypts files into the personal data archive and can be confident that the data is safely secured

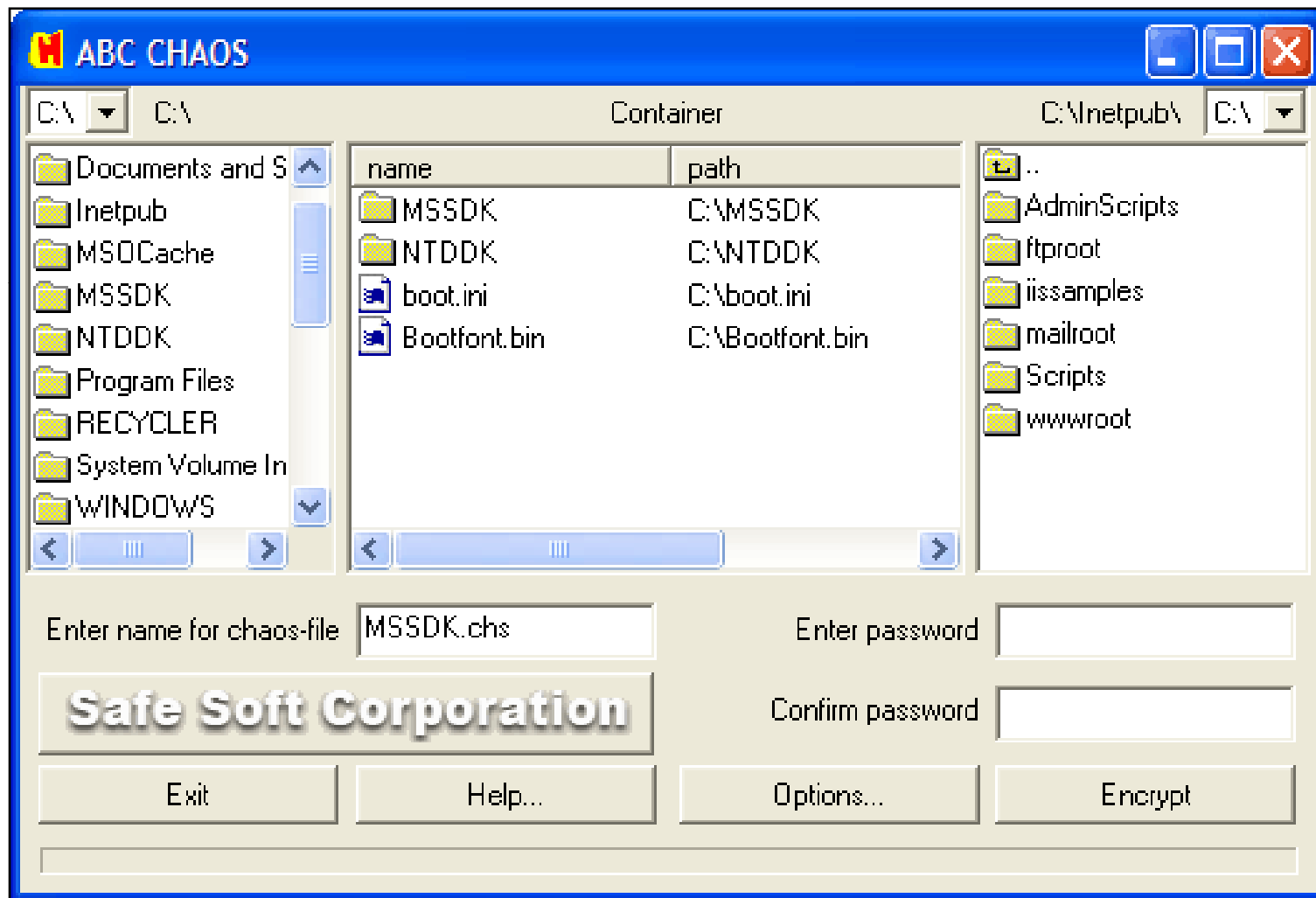
Additional special protection completely excludes an opportunity to select the password of the encrypted information which is used by the password and the key generator

ABC Chaos uses Blowfish algorithm and 128 bit keysize

Length of the password may be upto 7 symbols



# ABC CHAOS: Screenshot



# EncryptOnClick

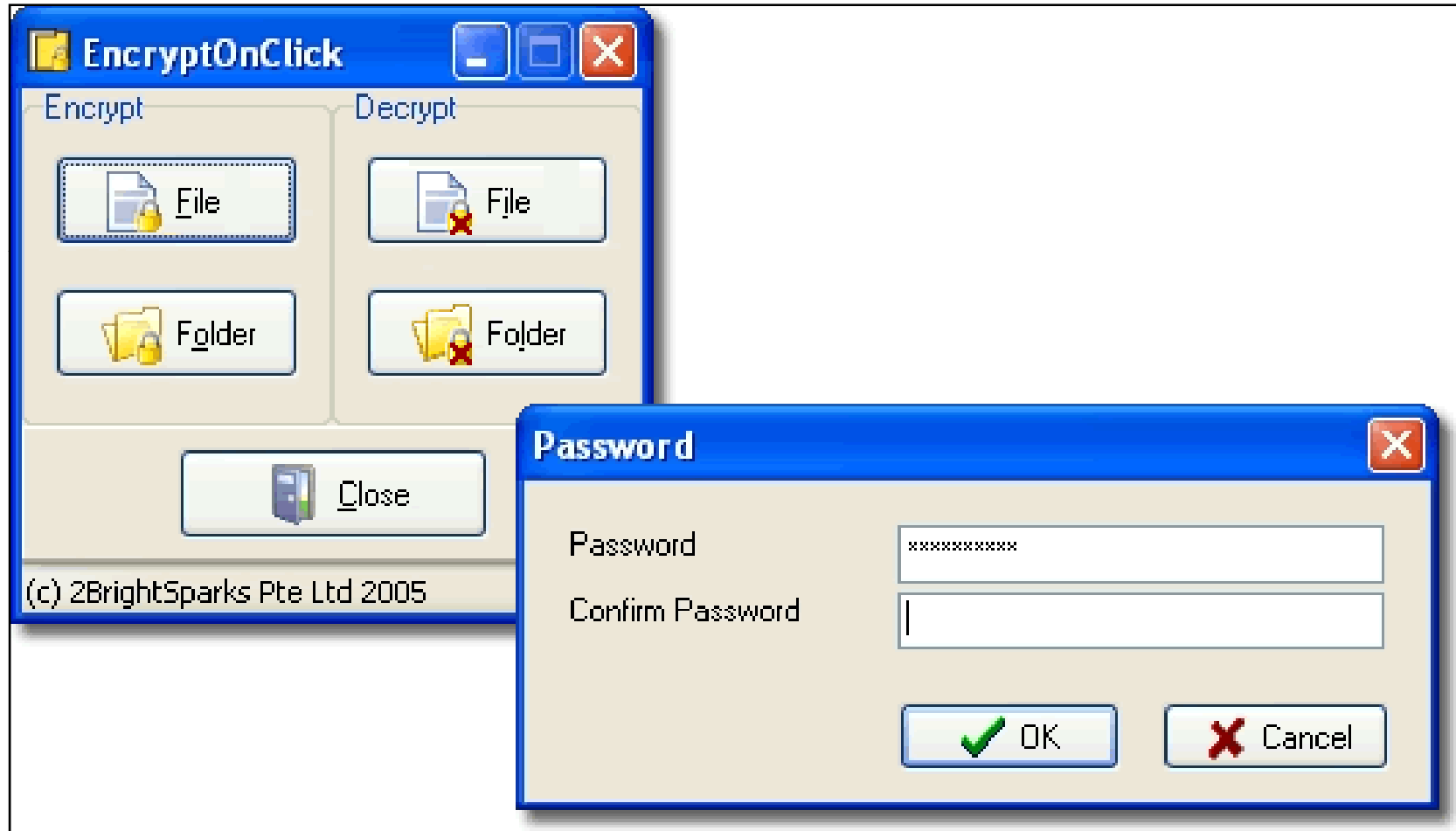


EncryptOnClick is a program that securely encrypts and decrypts files

It is like hiring own highly experienced data security guard which ensures the safety of the files and keeps them out of view from others

This program is very simple to use and features military grade 256-bit AES encryption

# EncryptOnClick: Screenshot



# CryptoForge

CryptoForge is an encryption software for personal and professional security

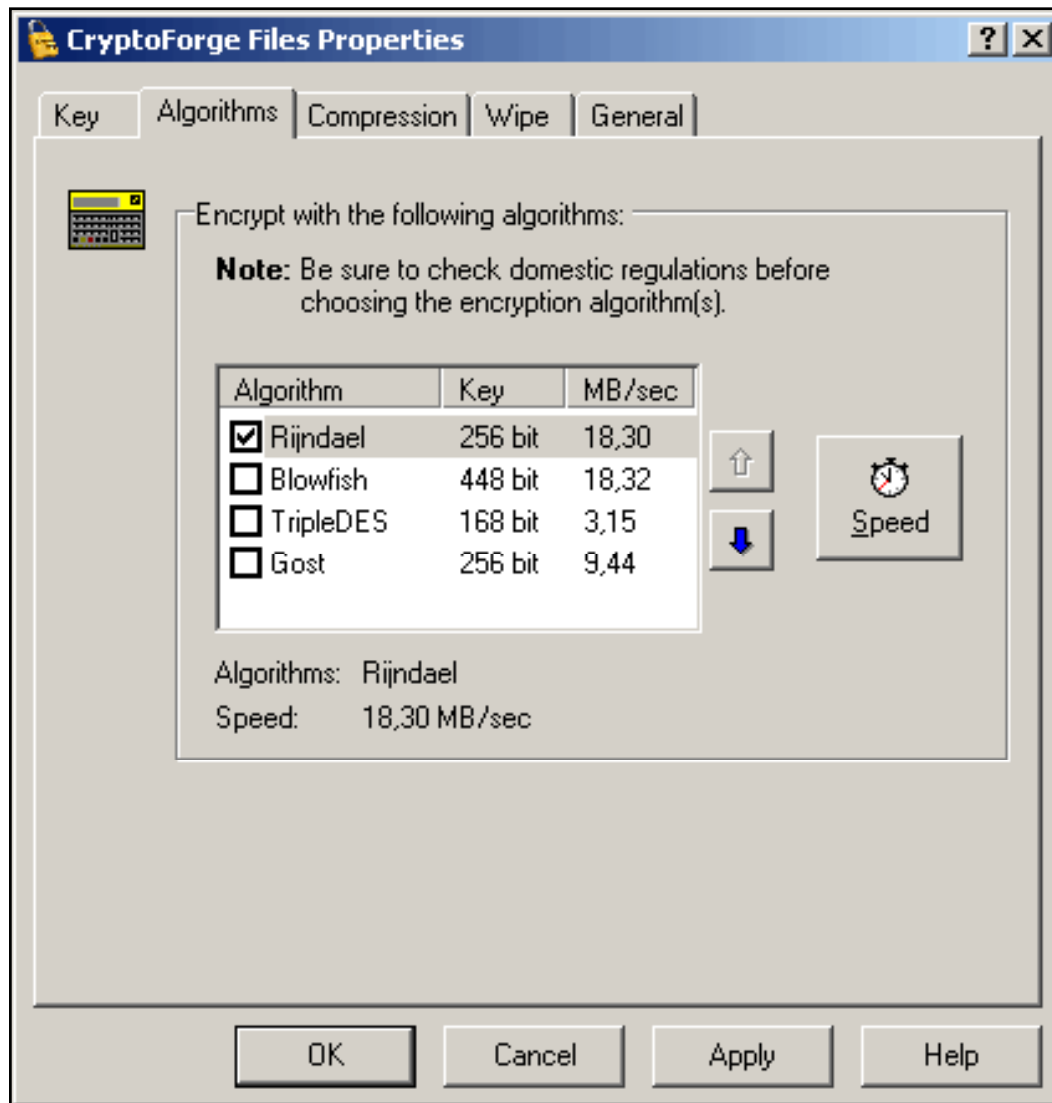
It allows to protect the privacy of sensitive files, folders, or messages, by encrypting them with upto four strong encryption algorithms

Once the information has been encrypted, it can be stored on insecure media or transmitted to an insecure network like the Internet

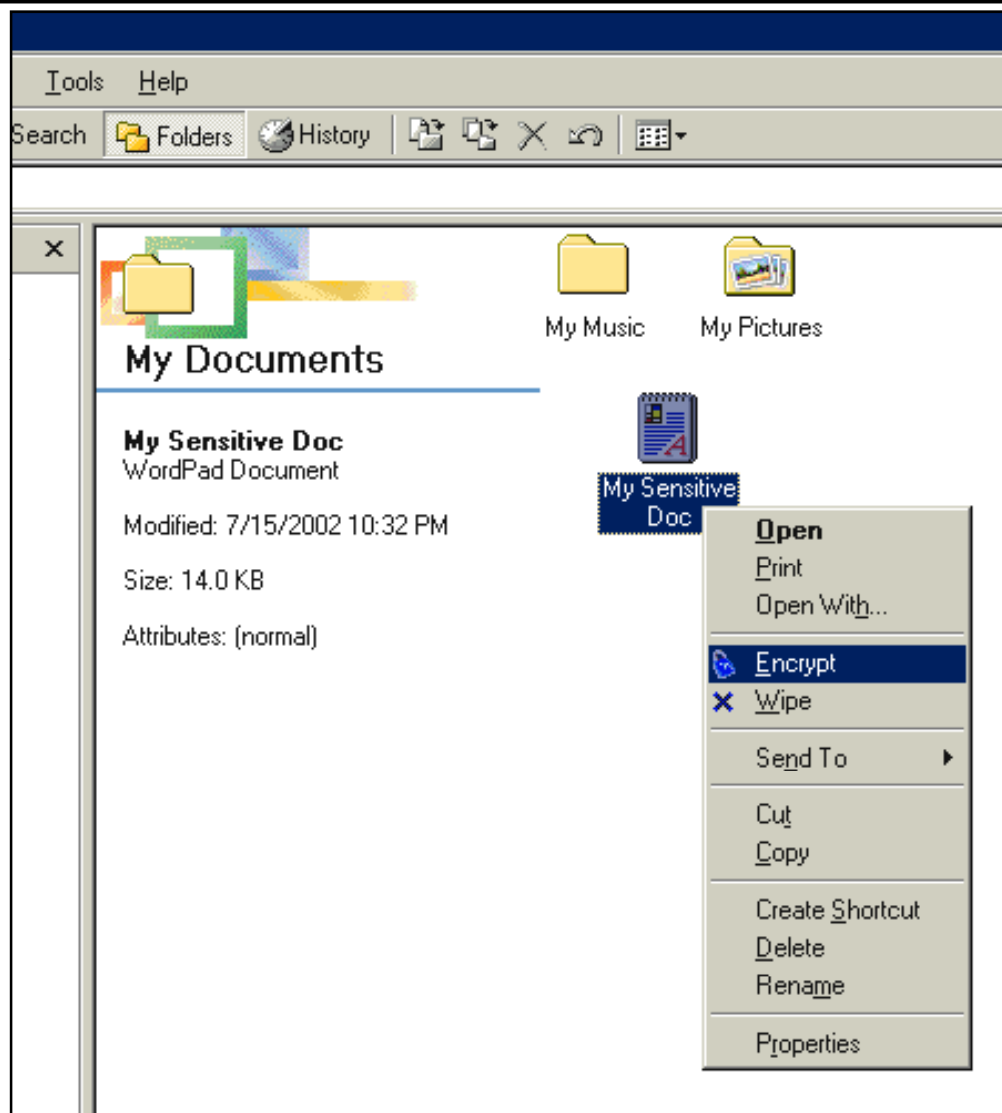
Later information can be decrypted into its original form



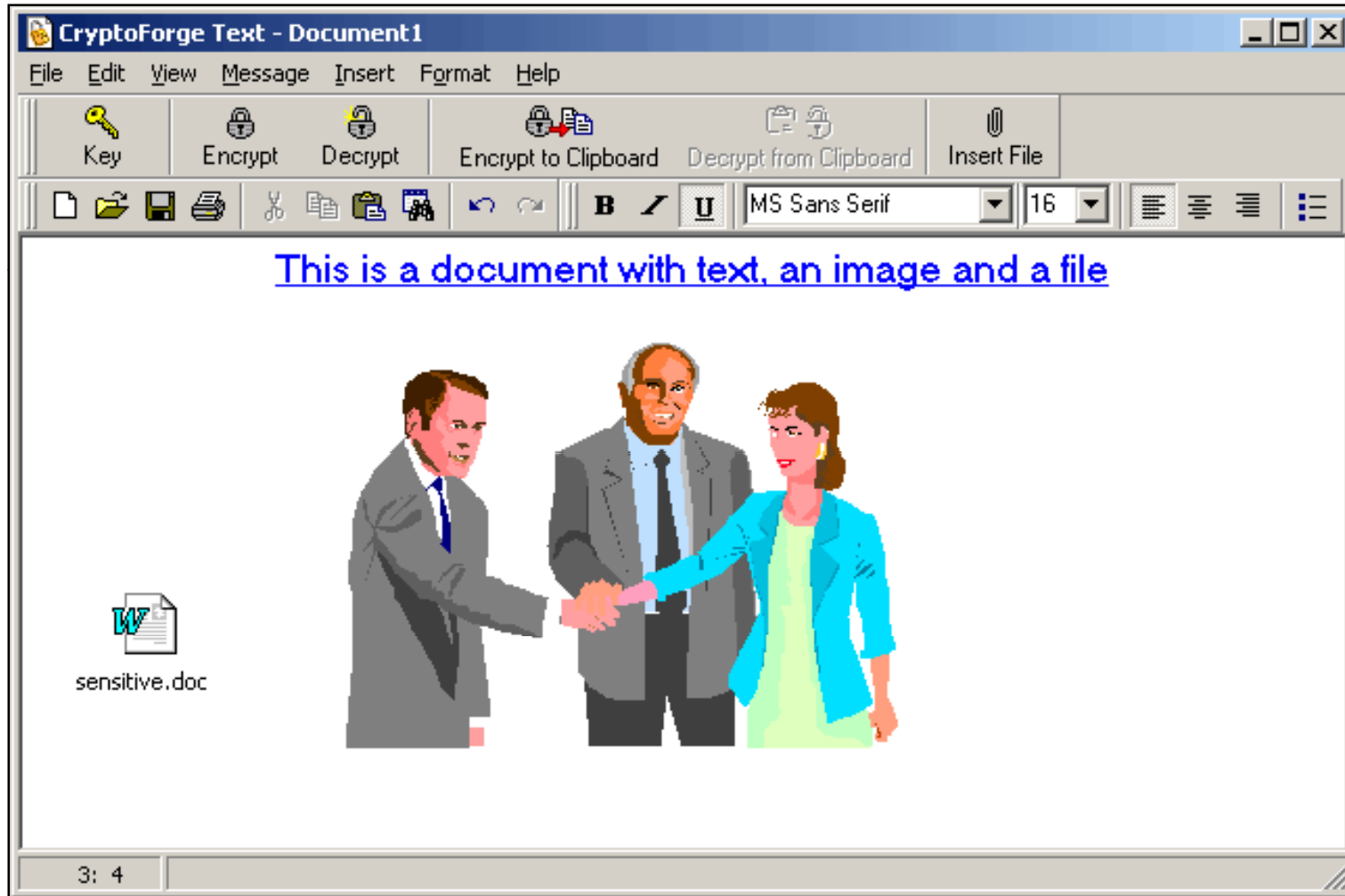
# CryptoForge: Screenshot 1



# CryptoForge: Screenshot 2



# CryptoForge: Screenshot 3



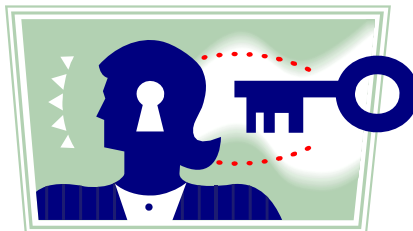


# SafeCryptor

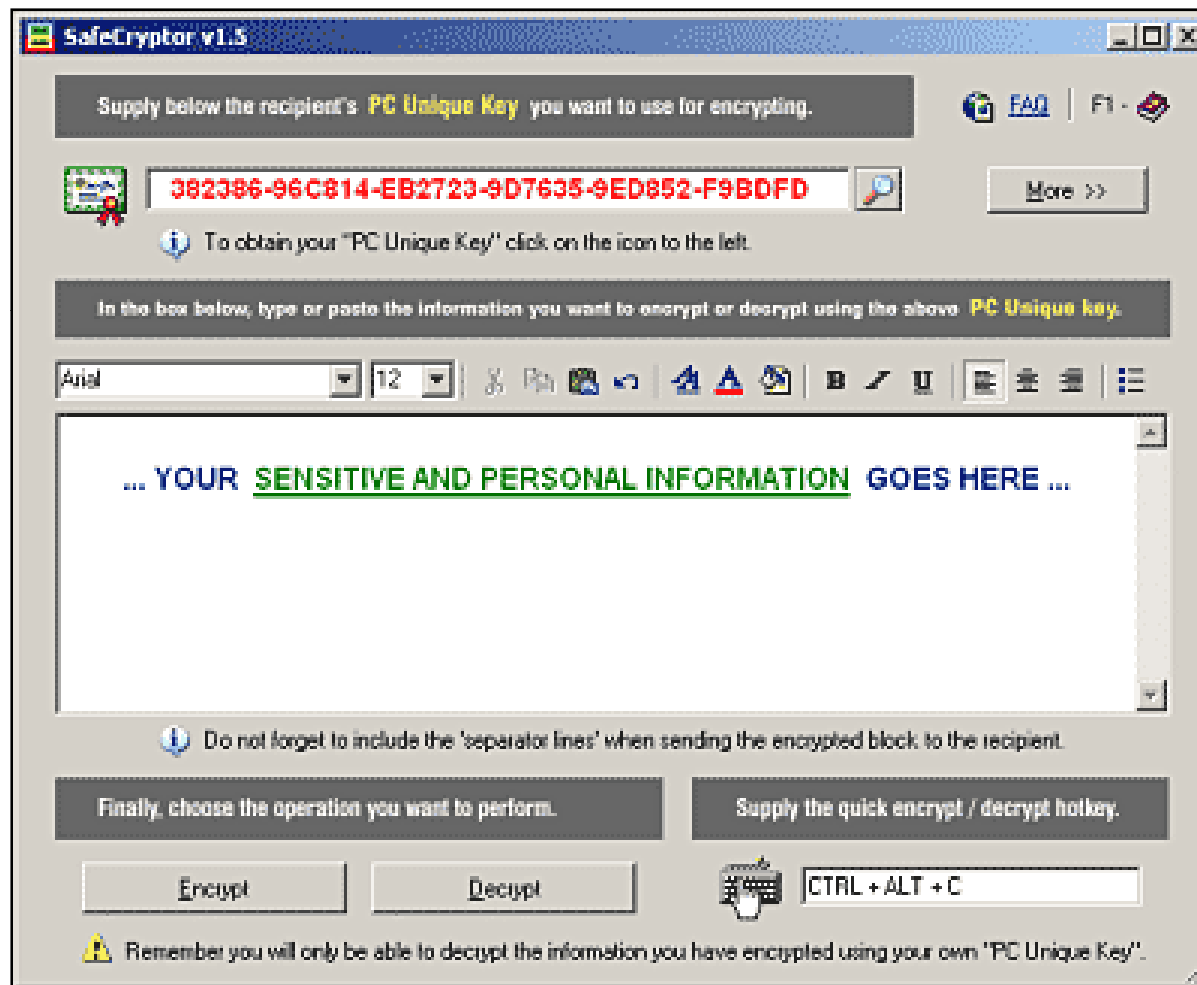
SafeCryptor provides you with safe, fast, and reliable text encryption anywhere, anytime, and lets you securely and quickly send all of your sensitive and personal information via e-mail or chat session to your partners, customers, friends, or family

It is the encryption system where your own computer is your unique key, especially suitable for the secure transfer of passwords between two computers

Recipients just need their own computers for decrypting the information; their computers are their unique keys



# SafeCryptor: Screenshot



# CrypTool

CrypTool is a program which enables to apply and analyze cryptographic mechanisms



It contains exhaustive online help, which can be understood without extensive knowledge of cryptography

If any document is encrypted, the result will be shown in a separate window, title of the resulting window contains both the name of the original document and encryption key used



CrypTool can display a histogram of the document, determine the statistics for any N-grams, and calculate entropy and autocorrelation

# CrypTool: Screenshot 1

CrypTool 1.3.00 beta 9 - ASCII Histogram of <CrypTool.txt> (1708 characters)

File Edit View Key Management Indiv. Procedures Options Window Help

CrypTool.txt

algorithms. The methods available include both classic methods (e.g. the Caesar encryption algorithm) and modern cryptosystems (for example, the RSA and DES algorithms, as well as algorithms based on elliptic curves). The symmetric AES algorithms are very topical. One of these is the Rijndael algorithm, which on 2 October 2000 was

ASCII Histogram of <CrypTool.txt> (1708 characters)

Autocorrelation of <english.txt>

Autocorrelation of <english.txt>

Number of characters that agree

Autocorrelation of <Rijndael encryption of <english.txt>, key <AB CD 12 34>

Autocorrelation of <Rijndael encryption of <english.txt>, key <AB CD 12 34>

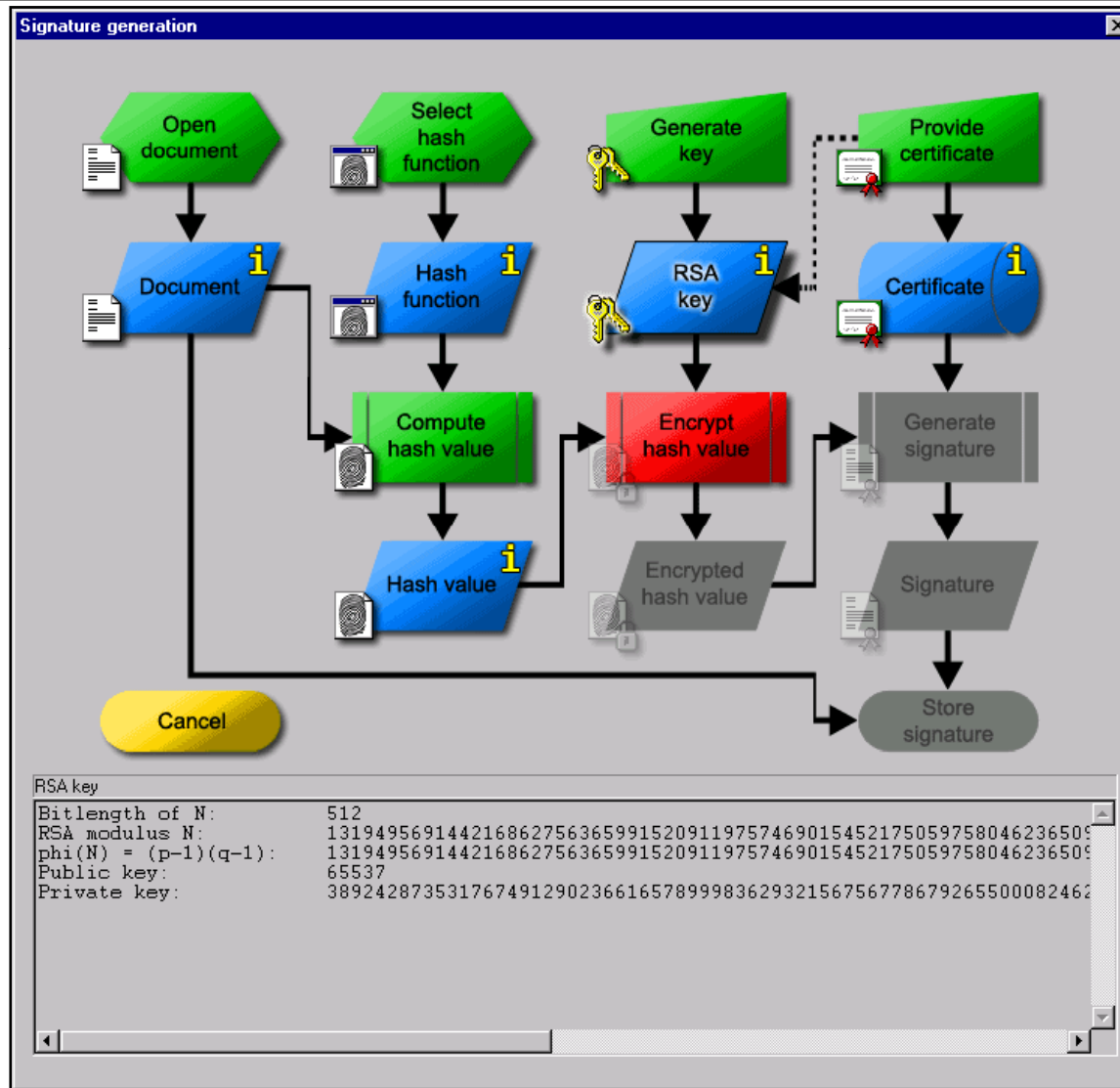
Number of characters that agree

english.txt

0008F	4A	61	6E	65	69	72	6F	2C	20	6F	6E	Janeiro
0009A	20	4A	75	6E	65	20	31	34	2C	20	31	June
000A5	39	39	32	2E	20	54	68	69	73	20	64	992. Th
000B0	6F	63	75	6D	65	6E	74	20	77	69	6C	ocumen
000BB	6C	20	62	65	20	66	75	72	74	68	65	l be f
000C6	72	20	65	64	69	74	65	64	2C	20	74	r edit
000D1	72	61	6E	73	6C	61	74	65	64	20	69	ranslated i
000DC	6E	74	6F	20	74	68	65	0D	0A	6F	66	nto the .of
000E7	66	69	63	69	61	6C	20	6C	61	6E	67	ficial lang
000F2	75	61	67	65	73	2C	20	61	6E	64	20	uages, and
000FD	70	75	62	6C	69	73	60	65	64	20	62	ublished b
00108	79	20	74	68	65	20	55	6E	69	74	65	y the Unite
00113	64	20	4E	61	74	69	6F	6E	73	20	66	d Nations f
0011E	6F	72	20	74	68	65	20	47	65	6E	65	or the Gene

Press F1 to obtain help.

# CrypTool: Screenshot 2



# CrypTool: Screenshot 3

The screenshot shows the CrypTool 1.3.00 beta 9 interface. The main window displays the 'Generation of Asymmetric Key Pair' dialog box. The 'Algorithm' section has three radio buttons: **RSA** (selected), **DSA**, and **Elliptic curves**. The 'Bit length of RSA modulus' is set to 512. The 'Bit length of DSA prime number' is also set to 512. The 'Identifier (bit length and curve parameter)' is set to 'prime239v1'. Below this, the 'Domain parameters of elliptic curve 'prime239v1'' are listed in a table:

Parameters	Value of the parameter
Elliptic curve E described through the curve equation	
a	88342353238919216479164875036030888531447
b	73852521740699241734859608803878172416486
p	88342353238919216479164875036030888531447
Point G on curve E (described through its (x,y) coord	
x	11028200374954885647634853354118620457790
y	86907840743550937874735187379305886850021

At the bottom, there are radio buttons for 'Base for presentation of numbers': **Octal**, **Decimal** (selected), and **Hexadecimal**. There are two buttons: 'Generate new key pair...' and 'PKCS#12 import'. A hex dump is visible at the bottom of the dialog box:

```

00201 6C 20 68 65 61 6C 74 68 20 61 6E
00214 74 65 72 61 63 79 2C 20 61 6E 64
00227 74 69 6E 75 69 6E 67 20 64 65 74
0023A 6F 6F 20 6F 66 20 74 68 65 20 65
  
```

The help window, titled 'CrypTool-Anwendungshilfe', is open on the right. It contains the following text:

**Dialogue box "Generation of asymmetric key pair"**

This dialogue box is used to specify the parameters to be used to [generate an asymmetric key pair](#). It is accessed by selecting the menu option [Key management / Key generation](#). Asymmetric [key pairs](#) can be generated for the following cryptosystems:

- RSA
- DSA
- methods based on [elliptic curves](#)

[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 curve](#) keys are generated):

1. Choice of **algorithm**:  
 For RSA and DSA keys, the [length of the key](#) must be specified (in bits). The **RSA** modulus  $n$  ( $n$  is the product of two approximately equal-sized prime numbers) must be between 301 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 1024 are already pre-defined and can be selected with the mouse. The **DSA** prime number  $p$  - 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 among a set of "parameter identifiers" (also known as "curve identifiers"). Every parameter 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 defined through  $Z[p]$ . See also Elliptic Curves [tutorial](#), section entitled Elliptic Curves in Cryptography.)
1. User information:  
 There are fields in which to enter user-relevant data by means of which it is possible to distinguish the different [keys](#). Entries in the fields **Last name**, **First name**, **PIN-code** and **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 identifier, no special characters (for example, \/: \* ? " < > | \) may be used: if they are, an

# Microsoft Cryptography Tools

Publishing tools and the signing DLL are installed in Bin directory of Microsoft SDK installation

They include the following files:

File name	Remarks
Cert2SPC.exe	Creates an Software Publisher Certificate (SPC) for testing purposes only
CertMgr.exe	Manages certificates, CTLs, and certificate revocation lists (CRLs)
MakeCat.exe	Creates an unsigned catalog file that contains the hashes of a set of files along with the associated attributes of each file
MakeCert.exe	Creates an X.509 certificate for testing purposes only
MakeCTL.exe	Creates a CTL
SetReg.exe	Sets registry keys that control certificate verification
Signer.dll	Required only by the tools in Internet Explorer 4.01
SignTool.exe	Signs and time stamps a file additionally, checks the signature of a file

# Polar Crypto Light

Polar Crypto Light is an ActiveX control which seamlessly adds encryption features to Windows applications

It incorporates full strength, upto 256-bit key, symmetric AES encryption

It uses public and private RSA keys for encryption and decryption

It encrypt strings, buffers, and files

It allows Error Reporting and Password Property





# Polar Crypto Light: Screenshot



# CryptoSafe

CryptoSafe provides on-line encryption of files saved in protected directories

Encryption and decryption of a selected file proceeds by simply copying or saving into or out of protected directory

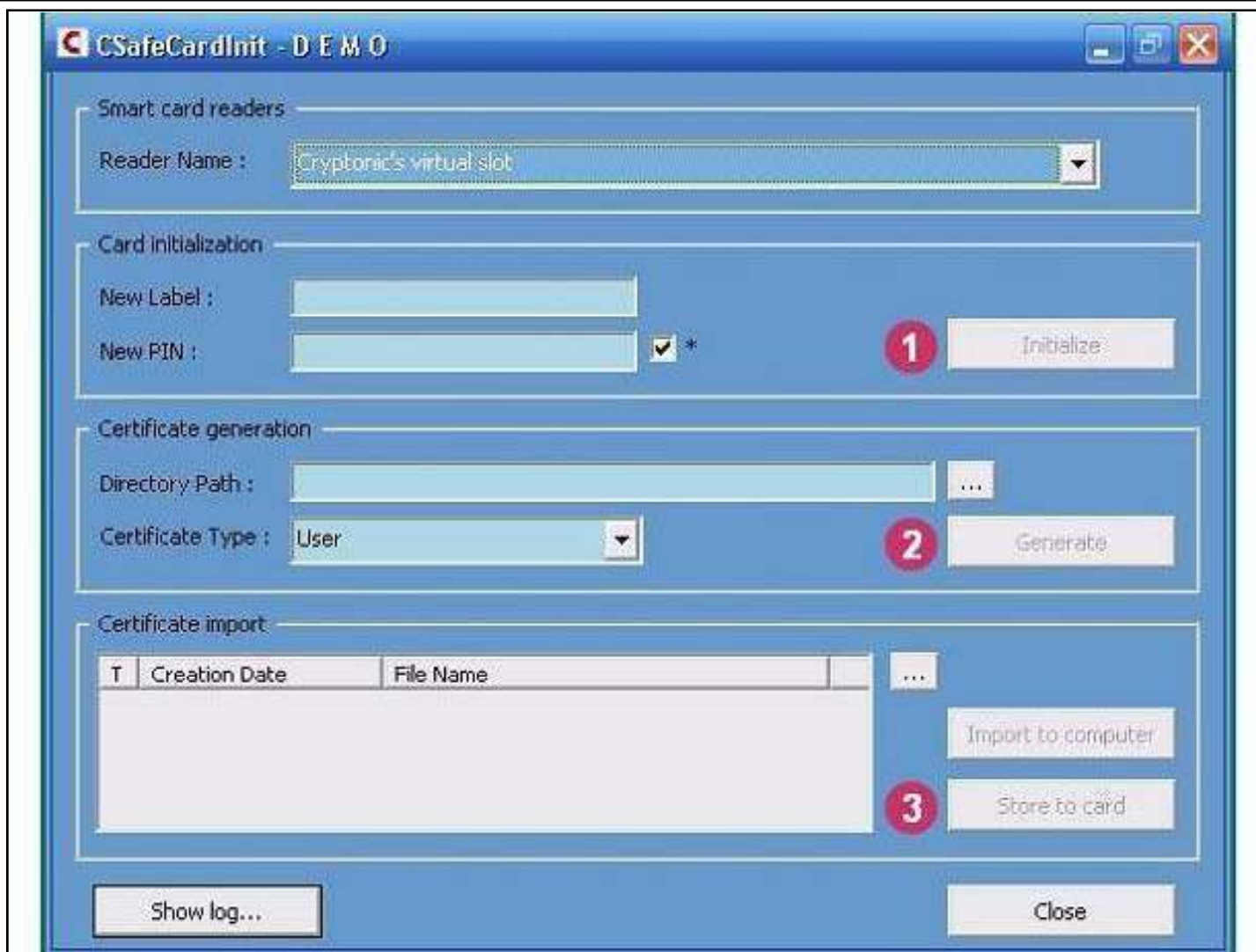
It is impossible to open a protected directory without the proper smart card

Cipher keys are securely saved on cryptography smart cards

CryptoSafe enables to encrypt only selected directories and files, without the necessity to encrypt the whole hard disk, so process is fast



# CryptoSafe: Screenshot



# Crypt Edit

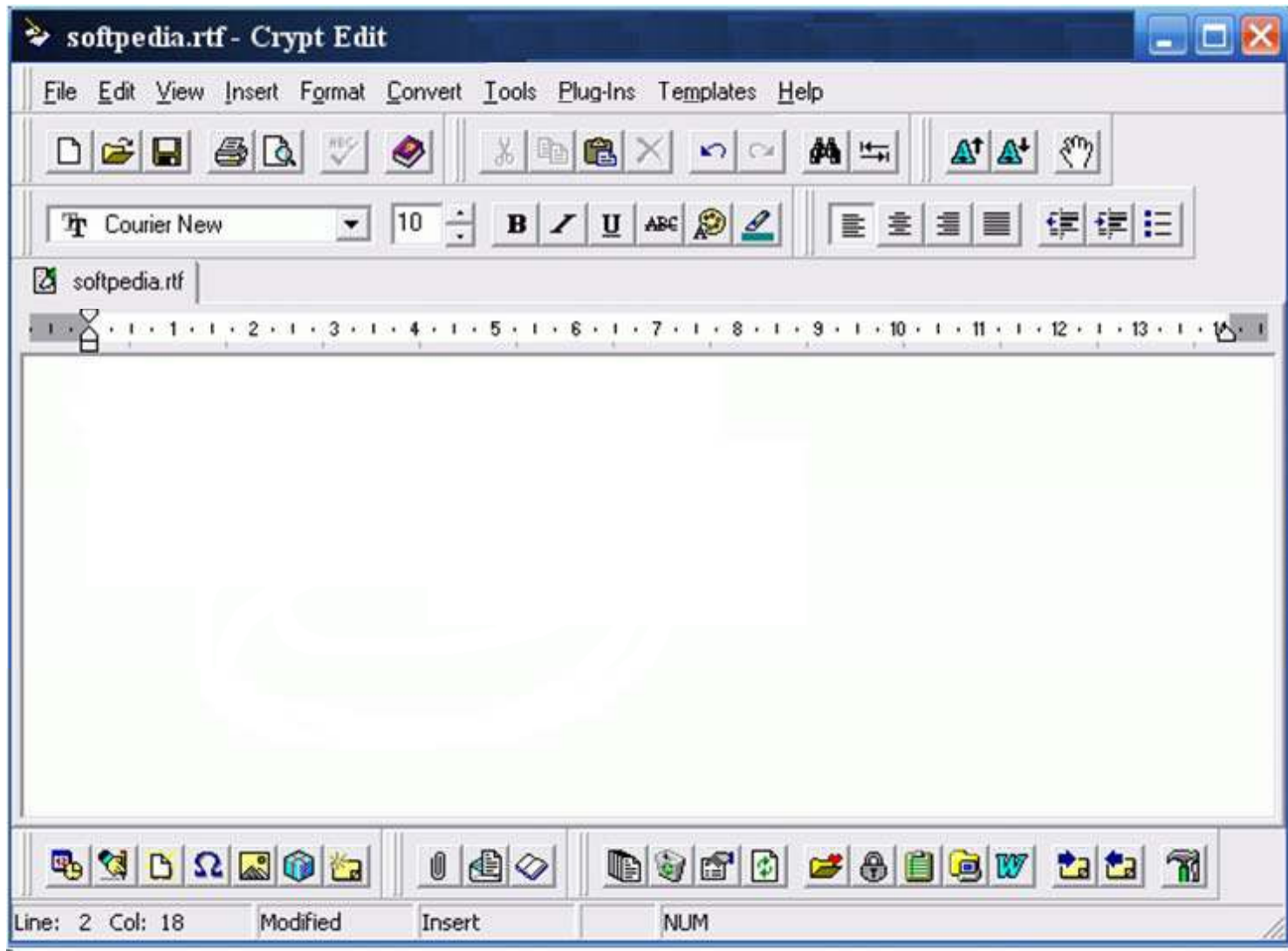
Crypt Edit is a powerful multi document word processor with enhanced cryptography features

It can easily save texts as HTML, DOC, RTF, ASCII (DOS, WIN, UNIX, MAC), WRI, UNICODE, and PRT

Encrypt and decrypt binary files with compression

Program includes an advanced e-mail client with an address book, a spelling checker, a built-in clipboard viewer, various converters, a character map, an auto format tool, and much more

# Crypt Edit: Screenshot



# CrypSecure

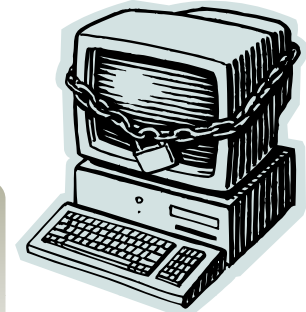
Encrypt files and whole folders with a right click of the mouse

Protect encrypted files with a password

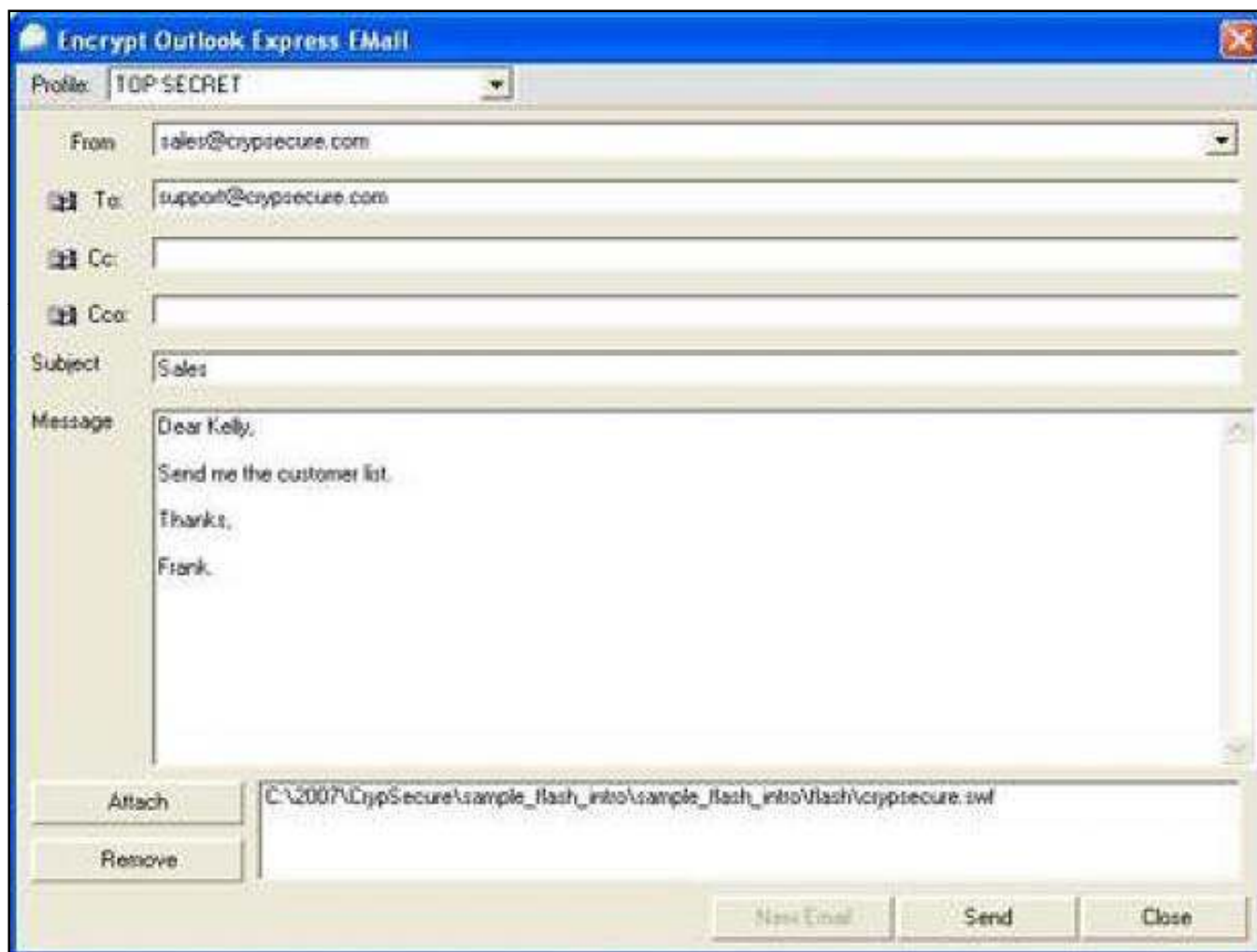
CrypSecure can create many profiles for many people or group of people

It sends encrypted messages or texts to FTP server easily

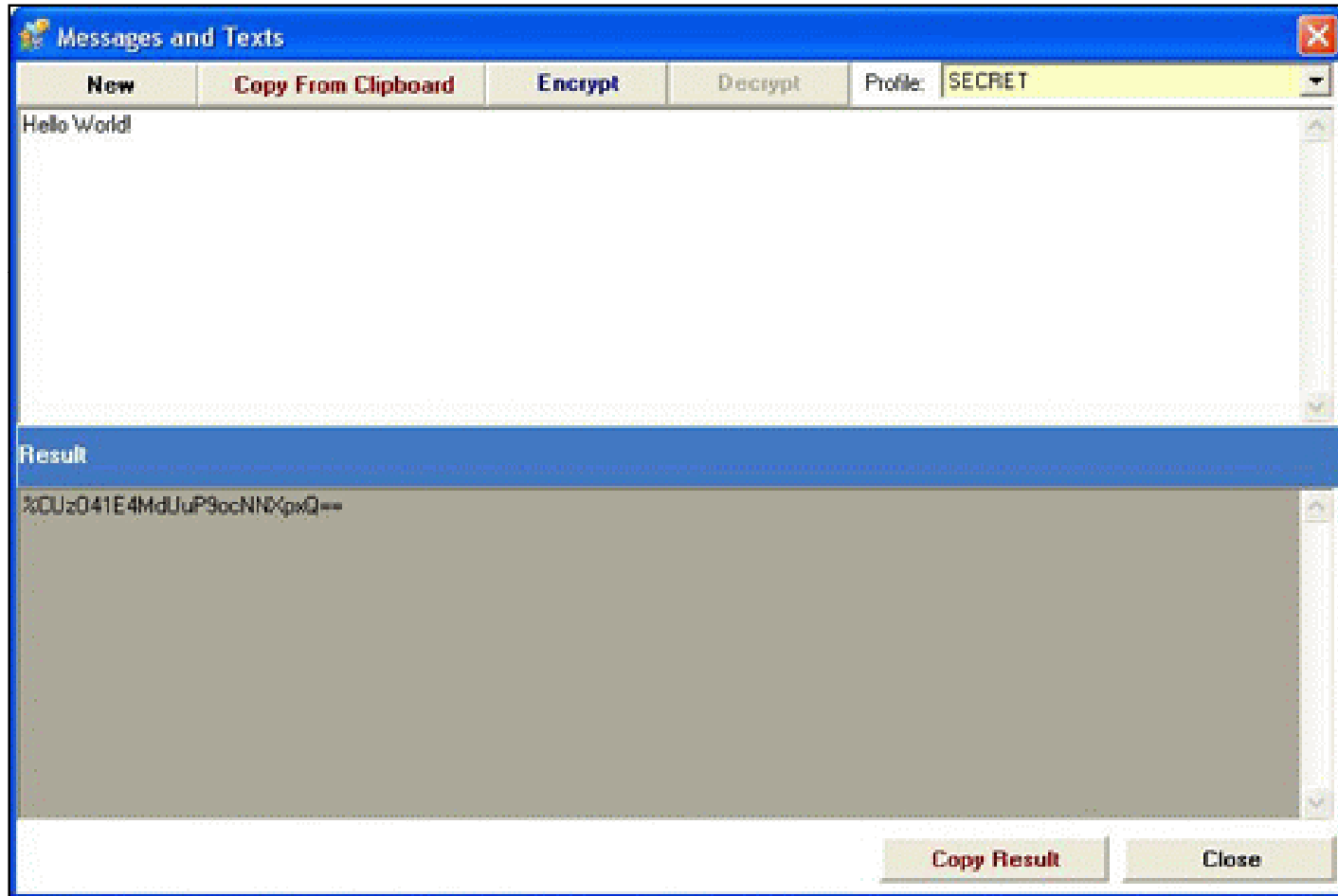
It sends encrypted Outlook Express email with a single click



# CrypSecure: Screenshot 1



# CrypSecure: Screenshot 2





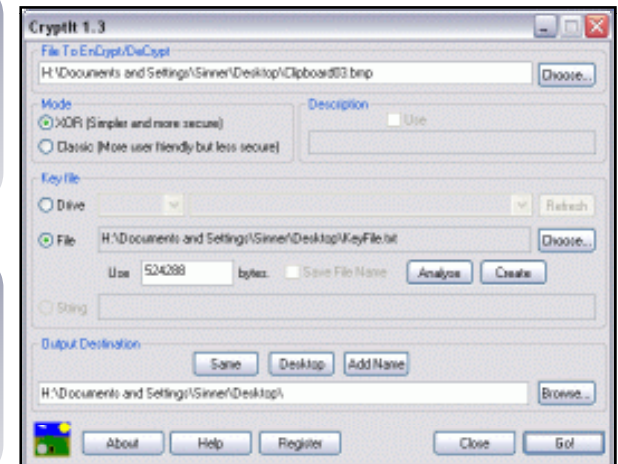
# Cryptlib

Cryptlib allows even inexperienced crypto programmers to easily add encryption and authentication services

It allows email, files, and EDI transactions to be authenticated with digital signatures and encrypted in an industry-standard format

It provides an extensive range of other capabilities including full X.509/PKIX certificate handling

It can make use of the crypto capabilities of a variety of external crypto devices such as hardware crypto accelerators, Fortezza cards, PKCS # 11 devices, hardware security modules, and crypto smart cards



# Crypto++ Library

Crypto++ Library is a free C++ class library of cryptographic schemes contains the following algorithms:

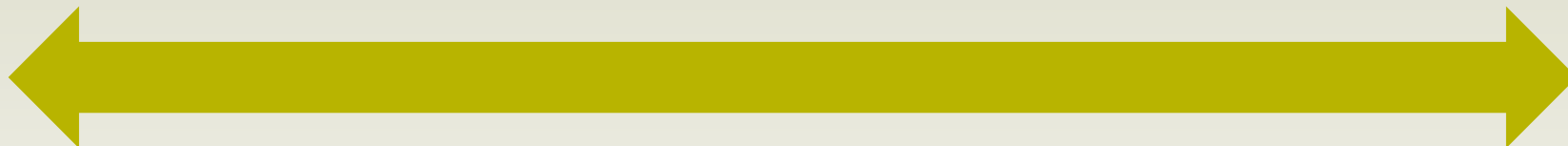
Algorithm type	Name
High speed stream ciphers	Panama, Salsa20, Sosemanuk
AES and AES candidates	AES (Rijndael), RC6, MARS, Twofish, Serpent, CAST-256
Other block ciphers	IDEA, Triple-DES (DES-EDE2 and DES-EDE3), Camellia, RC5, Blowfish, TEA, XTEA, Skipjack, SHACAL-2
Block cipher modes of operation	ECB, CBC, CBC ciphertext stealing (CTS), CFB, OFB, counter mode (CTR)
Message authentication codes	VMAC, HMAC, CBC-MAC, DMAC, Two-Track-MAC
Hash functions	SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, and SHA-512), Tiger, WHIRLPOOL, RIPEMD-128, RIPEMD-256, RIPEMD-160, RIPEMD-320
Public-key cryptography	RSA, DSA, ElGamal, Nyberg-Rueppel (NR), Rabin, Rabin-Williams (RW), LUC, LUCELG, DLIES (variants of DHAES), ESIGN
Padding schemes for public-key systems	PKCS#1 v2.0, OAEP, PSS, PSSR, IEEE P1363 EMSA2 and EMSA5
Key agreement schemes	Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF, XTR-DH
Elliptic curve cryptography	ECDSA, ECNR, ECIES, ECDH, ECMQV
Insecure or obsolescent algorithms retained for backwards compatibility and historical value	MD2, MD4, MD5, Panama Hash, DES, ARC4, SEAL 3.0, WAKE, WAKE-OFB, DESX (DES-XEX3), RC2, SAFER, 3-WAY, GOST, SHARK, CAST-128, Square

# Code Breaking: Methodologies



The various methodologies used for code breaking are:

- Using brute-force
- Frequency analysis
- Trickery and deceit
- One-time pad



# Cryptanalysis

Cryptanalysis is the study of methods for obtaining the meaning of the encrypted information without accessing the secret information

Typically, this involves finding the secret key

In non-technical language, this is the practice of codebreaking or cracking the code

It is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general

However, cryptanalysis usually excludes attacks that do not primarily target weaknesses in the actual cryptography methods such as bribery, physical coercion, burglary, keystroke logging, and so on

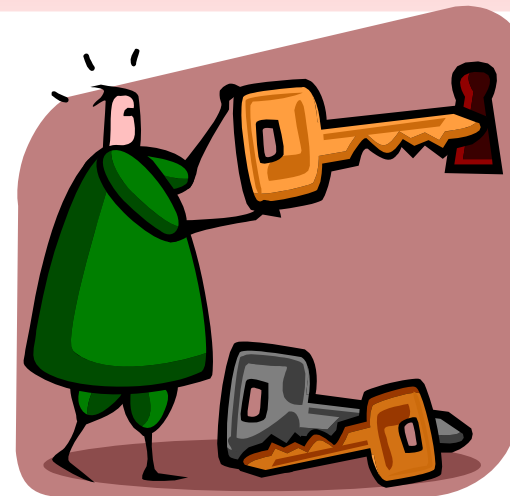
These latter types of attack are an important concern in computer security, and are often more effective than traditional cryptanalysis

# Cryptography Attacks

Cryptography attacks are based on the assumption that the cryptanalyst has knowledge of the encrypted information

There are seven types of Cryptography attacks:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext
- Adaptive chosen-plaintext attack
- Chosen-ciphertext attack
- Chosen-key attack
- Rubber hose attack



# Brute-Force Attack

Brute-Force Attack is a method of defeating a cryptographic scheme by trying a large number of possibilities

For example, exhaustively working through all possible keys in order to decrypt a message

The difficulty of a brute force attack depends on several factors, such as:

- How long can the key be?
- How many possible values can each component of the key have?
- How long will it take to attempt each key?
- Is there a mechanism which will lock the attacker out after a number of failed attempts?

# Brute-Force Attack (cont'd)

A Brute-Force attack is, however, more certain to achieve results

<b>Estimate Time for Successful Brute-Force Attack</b>				
<b>Power / cost</b>	<b>40 bits (5 char)</b>	<b>56 bits (7 char)</b>	<b>64 bits (8 char)</b>	<b>128 bits (16 chars)</b>
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10 <sup>20</sup> years
\$ 100 K (This can be achieved by a company)	2 sec	35 hours	1 year	10 <sup>19</sup> years
\$ 1 M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10 <sup>18</sup> years

# Cracking S/MIME Encryption Using Idle CPU Time

Tries to brute-force an S/MIME encrypted email message by translating an S/MIME encrypted message to RC2 format, and then trying all the possible keys to decrypt the message

This brute-force utility comes in two forms:

- Command line
- Screen saver





<http://www.distributed.net>

- ◉ distributed.net is an attempt to crack RC5 encryption using a network of computers worldwide
- ◉ The client utility, when downloaded from distributed.net, runs the crack algorithm as a screensaver, and sends the results to the distributed.net connected servers
- ◉ The challenge is still running

The screenshot shows the distributed.net website interface. At the top, there's a navigation bar with language options: 简体中文 | 繁體中文 | Deutsch | English | Español | Esperanto | Français | Italiano | Nederlands | 日本語 | Norsk | Svenska. Below this is a section titled "The Organization" which contains the following text: "distributed.net was the Internet's first general-purpose distributed computing project. Founded in 1997, our network has grown to include thousands of users around the world donating the power of their home computers to academic research and public-interest projects. Join us in this ground-breaking computing experience. We need your help...". To the right of this text is a small cow icon. Below the main text, there's another paragraph: "It's very simple to participate in our challenges. You only need to download a small program, which will talk to our network and begin to process parts of the current challenges. The program uses only the computer's idle time, so when you want to use your computer, the client will automatically get out of your way. Plus, there's that cute little cow icon...". At the bottom of the screenshot, there's a link: "There's more information on setting up the client, and about what our mission statement is." On the left side of the screenshot, there's a sidebar with a globe logo and a menu with the following items: Projects, - RC5, - OGR, Download, News, Help/Support.

# Use Of Cryptography

Cryptography is used to protect data from theft and alteration

It is used to provide secure communication on any untrusted medium such as Internet

It is used to authenticate the sender and the recipient

It is used to provide privacy and integrity

It is used to protect web transactions and e-commerce applications



# What Happened Next

The company was working on an important project and Larry's part of work was significant for the project's completion. Deadline for the project was drawing close, and when Larry's system was searched for his part of the work, nothing was found except encrypted data.

The project manager called his friend Jason who is a security advisor with a reputed firm. Jason examined the encryption pattern and used various encryption breaking methodologies to break the encryption. Finally he succeeded to decrypt the data by using tool 'Magic Lantern' and saved a large amount of resources and reputation for the company.

Company has initiated legal proceedings against Larry for breaching his agreement of service.

# Summary

Using Public Key Infrastructure (PKI), anyone can send a confidential message using public information, which can only be decrypted with a private-key in the sole possession of the intended recipient

RSA encryption is widely used and is a de-facto encryption standard

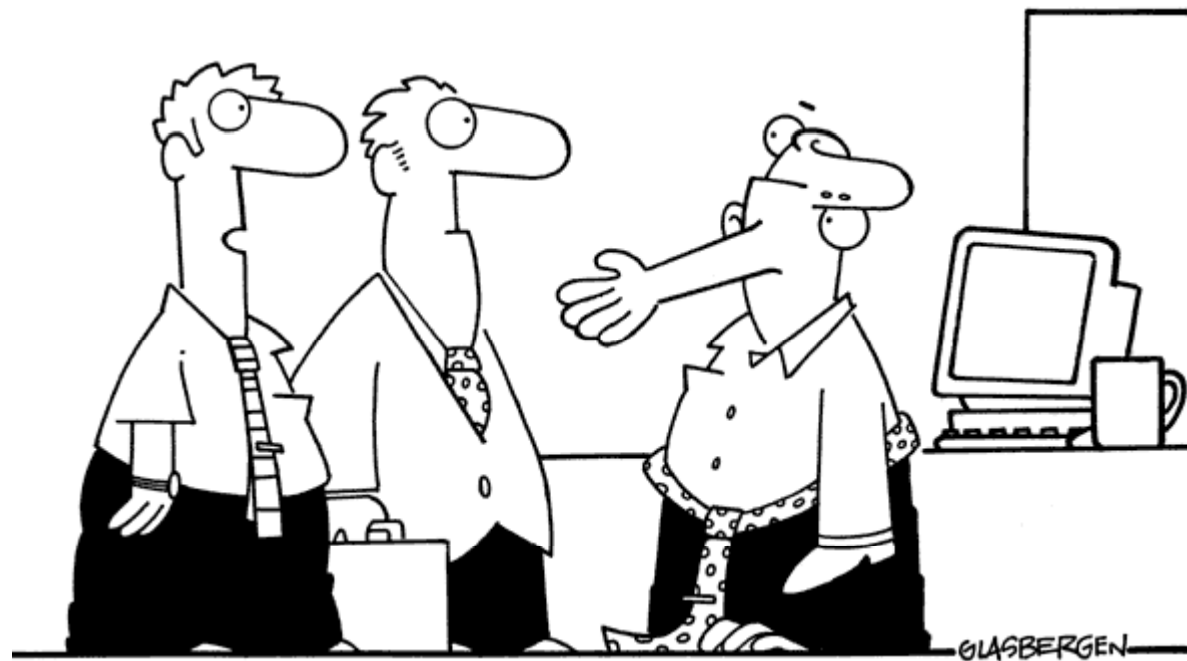
The MD5 algorithm is intended for digital signature applications, where a large file must be compressed securely before being encrypted

SHA algorithm takes, as input, a message of arbitrary length and outputs a 160-bit message digest of the input

Secure Sockets Layer, SSL is a protocol for transmitting private documents via the Internet

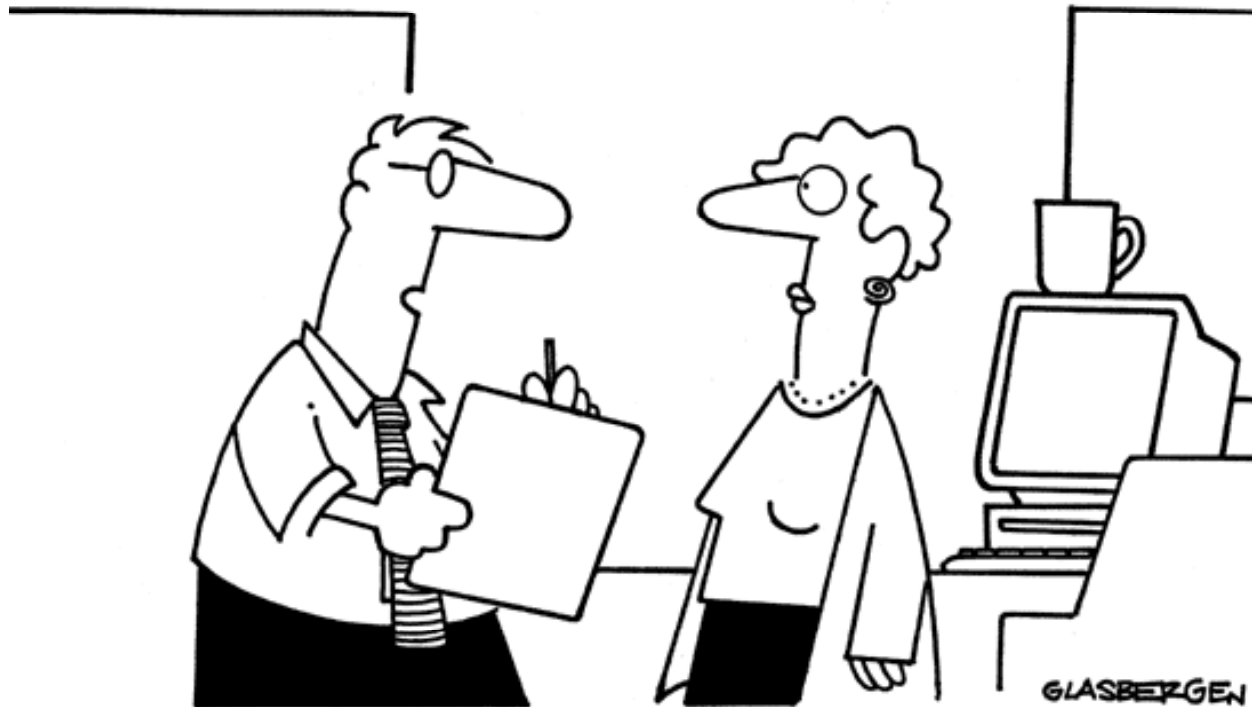
RC5 is a fast block cipher designed by RSA Security

Copyright 2002 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“That’s our CIO. He’s encrypted for security purposes.”**

Copyright 2003 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“I’m making a list of information that needs to be encrypted. Should I include your secret recipe for butterscotch brownies?”**