Blowfish

Blowfish is a 64-bit symetrical block cipher that employs a variable length key of up to **448 bits**. **There are no known attacks against Blowfish**. It is a relatively new cipher invented by noted cryptographer Bruce Schneier. It is **extremely fast**. It has been analyzed considerably, and is widely accepted as a strong encryption algorithm.

Blowfish is a symmetric block cipher that encrypts data in 8-byte blocks. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several subkey arrays totaling 4168 bytes. Blowfish has 16 rounds. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Contents

Copyright/License/Warranty

License Agreement

You should carefully read the following terms and conditions before using this software. Unless you have a different license agreement signed by Aslan Software, Inc. your use of this software indicates your acceptance of this license agreement and warranty.

For information on distributing the evaluation version of CryptSafe see the section titled Evaluation License.

Registered Version

One registered copy of CryptSafe may either be used by a single person who uses the software personally on one or more computers, or installed on a single workstation used non-simultaneously by multiple people, but not both.

You may access the registered version of CryptSafe through a network, provided that you have obtained individual licenses for the software covering all workstations that will access the software through the network. For instance, if 8 different workstations will access CryptSafe on the network, each workstation must have its own CryptSafe license, regardless of whether they use CryptSafe at different times or concurrently.

Governing Law

This agreement shall be governed by the laws of the State of Texas.

Disclaimer of Warranty

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the various hardware and software environments into which CryptSafe may be put, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

Good data processing procedure dictates that any program be thoroughly tested with non-critical data before relying on it. The user must assume the entire risk of using the program. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

CryptSafe combinations (passphrases) should be written down and stored in a safe place. The user must assume the entire risk of not being able to access data in the safe if the combination is lost. THERE IS NO WAY TO RETRIEVE DATA FROM A CRYPTSAFE SAFE IF THE COMBINATION IS LOST.

CryptSafe Encryption Standards Compliance

DES has been implemented as per:

ANSI X3.92, "American National Standard, Data Encryption Algorithm", 1981.

FIPS PUB 46-2, "Data Encryption Standard", 1994.

FIPS PUB 74, "Guidelines for Implementing and Using the NBS Data Encryption Standard", 1981.

ISO/IEC 8731:1987, "Banking - Approved Algorithms for Message Authentication - Part 1: Data Encryption Algorithm (DEA)".

The DES modes of operation are given in:

ANSI X3.106, "American National Standard, Information Systems - Data Encryption Algorithm - Modes of Operation", 1983.

FIPS PUB 81, "DES Modes of Operation", 1980.

ISO/IEC 8372, "Information Technology - Modes of Operation for a 64-bit Block Cipher Algorithm".

The DES code has been validated against the test vectors given in:

NIST Special Publication 500-20, "Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard".

Blowfish has been implemented as per:

"Description of a New Varible-Length Key, 64-bit Block Cipher (Blowfish)", Bruce Schneier, "Fast Software Encryption", Lecture Notes in Computer Science No. 809, Springer-Verlag 1994.

The Blowfish modes of operation are given in:

ISO/IEC 8372, "Information Technology - Modes of Operation for a 64-bit Block Cipher Algorithm".

The Blowfish code has been validated against the Blowfish reference implementation test vectors.

CryptSafe Features

- **Easy to use** WinZip like interface enables you to create safes to hold your private files. Onced locked using your combination, only you can open the safe and access the files inside.

- You can lock safes using DES and/or Blowfish (registered version) encryption. Blowfish is one of the strongest encryption algorithms available and is extremely fast.

- The registered version enables you to select multiple encryption methods for **multi-layered encryption**, strengthening the already strong encryption available.

- **Completely removes files** that are moved to the safe by “wiping” them from your disk, making them unrecoverable by anyone else.

- **File Compression** can be used at different levels to reduce the storage footprint of your safe and provide greater portability. This is the same compression used by PKZIP and WinZip.

- **File associations** are maintained within the safe so you can open and update files without having to extract them from the safe.

- You can **Drag & Drop** files onto the safe for easy adding.

Data Encryption Standard (DES)

DES is a strong encryption algorithm that features a **56-bit** key length. **There are no know attacks against DES except brute force attacks**. DES has been a standard cipher used extensively by the banking and finance communities over the years, and **is probably the most well known and common algorithm in use today**. It was developed by IBM and endorsed by the U.S. government in 1977 as an official standard. It is a block-cipher symmetric algorithm, and has been a worldwide standard for at least 20 years.

Although efforts are underway to replace it with a newer, stronger algorithm, DES has held up well against cryptanalysis for many years. Due to recent advances in computer technology, **some experts no longer consider DES secure against all attacks**. A chosen-ciphertext attack using the technique of linear cryptanalysis can break DES in 2^43 steps. However, unless you're encrypting data that you want to be safe from governments DES will be fine.

DES operates on a 64-bit block of plaintext. This block is permuted according to a set regimen, then broken into a left and right half. Then 16 rounds of identical operations (called Function f) are performed, where the data is combined with the key. After the sixteenth round, the data is joined back into a single 64 bit block, then permuted a final time (this second permutation is the inverse of the first).

In the DES key, every eighth bit is ignored. In each of the 16 rounds, the 56 bits remaining are circular shifted left either one or two bits, depending on the round. Then 48 bits are selected for the Function F. First the right 32-bits is expanded to 48 bits through an expansion permutation, then combined with the 48 selected bits of the key through an XOR. These 48 new bits are broken into 6-bit groups and sent through 8 substitution-boxes, that 6-bit group to 4 bits. The final part of Function f is the permutation of the 32 remaining bits. The output of Function f is combined with the left half via another XOR. The result of this operation becomes the new right half, and the old right half becomes the new left half. DES also has the property that the same algorithm can be used for decryption, only the 48-bit subkeys used in each round for encryption must be used in the reverse order.

Encryption Methods

With the registered version of CryptSafe, you can use both DES and Blowfish for methods for multi-layered encryption.

Data Encryption Standard (DES)

Blowfish (registered version only)

Introduction To Encryption

Encryption is a way of altering or scrambling data so that only those who know how to unscramble it can use it. The basic concept of encryption is that it makes your information private and secret.

Cryptography ("hidden writing") involves the translation of a message in plain language into one in a secret language and back again.

Children use cryptography in its simplest form when they send secret messages that are scrambled and unscrambled using a "decoder ring." These decoder rings were based on a substitution algorithm - one letter of the alphabet is substituted for another. The message writer uses the substitution method to encode, or encrypt, his message, and the receiver uses the same method to decode, or decrypt, the message. The problem with these simple forms is that they are easy to break - as evidenced by the fact that people often solve "cryptogram" puzzles in newspapers just for fun.

With the advent of computers, more complicated forms of cryptography were developed. These systems use a key, derived from a password or passphrase. The key, which is a computer generated pattern, is used to encrypt and decrypt the data. "Single key" systems use the same key to encrypt and decrypt. CryptSafe uses single key encryption. A "two key" system uses one key for encyrpting and a separate key for decrypting, such as is used by PGP and other Public Key encryption programs.

Why is encryption necessary?

Encryption provides primarily one thing: **Privacy!** Whether storing information on a computer at work, on a portable computer, or sending it over the Internet, most likely you want some or all of this information to be kept private. Political, financial, or sensitive personal information that falls into the wrong hands can be used against you.

There are many points along the Internet where data and messages can be intercepted, copied and re-routed. Depending on your browser configuration, a Web site can even read information off of your PC. Because of these weaknesses, the need for strong encryption is greater than ever before. One must assume that all information (personal, financial, or otherwise) that is not encrypted, can be intercepted and used by a third party. It is analogous to talking on a shared phone line. You never know who is listening, or when they are listening. The nature of the Internet and electronic medium allows effective scanning of message contents using sophisticated filtering software. Electronic mail is gradually replacing conventional paper mail and messages can be easily and automatically intercepted and scanned for interesting keywords. The CIA and NSA are reported to engage in this kind of activity.

In addition to the dangers of the Internet, the proliferation of laptop computers poses an even greater danger. Many people risk having their sensitive financial and business information stolen and used by criminals.

If use a computer at work, most likely you have information on it that you want to keep private from your co-workers. This may include resumes, business plans, and contacts.

Opening Files In The Safe

You can open files in the safe without extracting them by **double-clicking** on the file, or highlighting the file and selecting **File | Open** from the menu. Files are opened using the application associated with the file type in the system registry.

In order to open a file in the safe, the file is extracted to a temporary directory. The file is then passed as a parameter to the associated application. When the associated application is closed, the safe is updated with latest revision of the file, if applicable, and the extracted version of the file is wiped from the disk. This process prevents anyone from accessing data in files that have been opened from within the safe.

Ordering Information

Phone: PsL's operators are available from 8:00 a.m. to 6:00 p.m. Monday-Friday at 800-242-4775 Ext. 15532 or at 713-524-6394 Ext.15532 (Orders ONLY)

Internet: http://www.integrityonline2.com/asi/cryptsafe.htm

Fax: 713-524-6398 (include product #15532 and please type or block print clearly)

Email: 15532@pslweb.com

Mail: Mail credit card orders to PsL at
P.O.Box 35705, Houston, TX 77235-5705.
(Please reference product #15532)

THE ABOVE NUMBERS ARE FOR CREDIT CARD ORDERS ONLY.
THE AUTHOR OF THIS PROGRAM CANNOT BE REACHED AT THESE NUMBERS.

Any questions about the status of the shipment of the order, refunds, registration options, product details, technical support, volume discounts, dealer pricing, site licenses, non-credit card orders, etc, must be directed to:

asi@integrityonline2.com

Aslan Software, Inc.
P.O. Box 261657
Plano, TX 75026-1657

To insure that you get the latest version, PsL will notify us within one business day of your order and we will ship or e-mail the product directly to you.

CryptSafe Pricing:
(guaranteed through December, 1998)

Single Copy:	$25 each	= _____
Site License:		
2 to 10 machines:	$20 each	= _____
11 to 49 machines:	$15 each	= _____
50+ machines:	$10 each	= _____
	Total Payment	= _____