here are three ways to do this Tutorial:

1• Print this page and follow along.

Click on the Goto Button to print this page

2• Launch InternetMemory and switch back and forth.

3• Use the "Tutorials" Apple Guide from within IM.

The Apple Guide files are available from the Help menu, found

immediately to the right of the InternetMemory menu. They are only

listed when IM is the front most application.

NOTES:
• The steps to Write-Protect an Address Book are almost exactly the same. In step 2, click in the "Write-Protect" column instead of the "DES Column".
• A section of Background Information about DES Encryption follows this Tutorial.

If it isn't already running, launch the InternetMemory Application.

1• Click on the "Open Address Book..." button
It's the second button in the first section. Find "CircleDream Software Addresses" from Tutorial 1 and click the "Okay" button.

2• Click in the "DES Column" of "CircleDream Software Addresses"
The "Password" dialog will appear.

• Enter a Password
This password will be needed to later unencrypt the Address Book. Don't forget your password! See the section after the Summary for more information on choosing a good password.

4• Type the Password again.
This is done to ensure that you entered the password you intended and not a typo.

5• Click "Okay" to accept the Password
The Address Book will be encrypted the next time it's saved.

6• Choose "Close" (âŒ˜W) from the "File" menu
Make sure you save the changes. InternetMemory will run your Address Book through a DES Encryption Algorithm and save it so that no one can read it. You will need your password to open the Address Book again.

Summary

In this Tutorial, you have:
• Opened an existing Address Book
• Encrypted the Address Book with a Password that you wisely chose
• Saved the Address Book to encrypt it

Choosing a Good Password

Do…
• …choose something you can remember.
• …try and come up with a combination of letters and numbers (it's harder to guess).

Don't…
• …write down your password anywhere.
• …make your password anything personal (i.e.: birthdate, mother's maiden name, address, etc.)
• …choose a word that exists in any language (an easy way to break passwords is to do a dictionary search until something matches up).

Tutorial 3: Insertion

Click on the Goto Button to proceed to Tutorial 3.

Background Information About DES Encryption

This information comes from RSA Laboratories' FAQ about Modern Encryption. RSA Labs is a Cryptographic Research and Consultation facility, and a division of RSA Data Security, Inc. They can be reached on the WWW at: http://www.rsa.com/rsalabs/faq/faq_des.html

"What's DES?
DES is the Data Encryption Standard, an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard; the details can be found in the official FIPS publication (NIST ref #59). It was originally developed at IBM. DES has been extensively studied over the last 15 years and is the most well-known and widely used cryptosystem in the world.

DES is a secret-key, symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography was invented to solve this problem. DES operates on 64-bit blocks with a 56-bit key. It was designed to be implemented in hardware, and its operation is relatively fast. It works well for bulk encryption, that is, for encrypting a large set of data.

NIST has recertified DES as an official U.S. government encryption standard
every five years; DES was last recertified in 1993, by default. NIST has indicated, however, that it may not recertify DES again.

Has DES been broken?
DES has never been "broken", despite the efforts of many researchers over many years. The obvious method of attack is brute-force exhaustive search of the key space; this takes 2^55 steps on average. Early on it was suggested (Diffie-Hellman ref #28) that a rich and powerful enemy could build a special-purpose computer capable of breaking DES by exhaustive search in a reasonable amount of time. Later, Hellman (ref #36) showed a time-memory trade-off that allows improvement over exhaustive search if memory space is plentiful, after an exhaustive precomputation. These ideas fostered doubts about the security of DES. There were also accusations that the NSA had intentionally weakened DES. Despite these suspicions, no feasible way to break DES faster than exhaustive search was discovered. The cost of a specialized computer to perform exhaustive search has been estimated by Wiener (ref #80) at one million dollars.

Just recently, however, the first attack on DES that is better than exhaustive search was announced by Eli Biham and Adi Shamir (Biham-Shamir ref #6 and #7), using a new technique known as differential cryptanalysis. This attack requires encryption of 2^47 chosen plaintexts, i.e., plaintexts chosen by the attacker. Although a theoretical breakthrough, this attack is not practical under normal circumstances because it requires the attacker to have easy access to the DES device in order to encrypt the chosen

plaintexts. Another attack, known as linear cryptanalysis (Matsui ref #51), does not require chosen plaintexts.

The consensus is that DES, when used properly, is secure against all but the most powerful enemies. In fact, triple encryption DES may be secure against anyone at all. Biham and Shamir have stated that they consider DES secure. It is used extensively in a wide variety of cryptographic systems, and in fact, most implementations of public-key cryptography include DES at some level."