by Hugh Long, C.Tech

CRACKING THE CRYPTOGRAPHY CODE

WHEN YOU HEAR THE WORD CRYPTOGRAPHY you may think of James Bond breaking secret codes on a mission to a hostile country. Cryptography, however, goes much further than the domain of spies and intelligence agencies. It is also used in virtually all commercial transactions where data confidentiality is important. For example, credit information is encrypted prior to transfer over the phone lines or the Internet.

Cryptography is used to make data unreadable to anyone but the intended audience. We encrypt data using a computer with a cryptographic algorithm or cipher. A cipher is the mathematical function used for encryption or decryption. As a child you may have experimented with various codes or ciphers where you substituted the characters of a plaintext message (the text to be encrypted) with symbols or other characters. Runes in Tolkien's "The Hobbit" are an example of a code created by replacing plaintext characters with symbols from a pre-defined set.

A simple type of cryptography is the Caesar cipher. Each character in a plaintext string is replaced with a character three to the right. A variation commonly used by UNIX systems, ROT13, rotates each character 13 places to the right. Without knowing how the ciphertext was encrypted, it would be unreadable; these are examples of monoalphabetic substitutions.

Here is an example of the Caesar cipher:
Plaintext: abcdefghijklmnopqrstuvwxyz
Ciphertext: defghijklmnopqrstuvwxyzabc

To encrypt a message, simply apply the cipher to the plaintext message:
Plaintext: My Secret Code Is Better Than Yours
Ciphertext: Pb Vhfuw Frgh Lv Ehwwhu Wkdq Brxuv

A polyalphabetic substitution substitutes blocks of letters for individual characters. Be forewarned. Ciphers like previous examples are not secure by any means; they may keep your child from reading your e-mail, but a cryptanalyst could easily crack them with only a pen and paper.

Cryptography is used to make data unreadable to anyone but the intended audience.

A key, in cryptographic terms, is a random string of characters used to seed, or start, a computer-based encryption algorithm. There are two types of keys used in cryptography: secret or private keys, and public keys. In secret key cryptography one key is used to encrypt and decrypt data. Both parties must have access to the key prior to encrypting and decrypting the message. The difficulty lies in transmitting the key in the first place; if the two parties had a secure channel to transmit a secret key, they could just transmit the message.

In public key cryptography two complementary keys are used. A public key is first used to encrypt the message and a second secret key is used to decrypt the message. The public key can then be widely published. No one can read the encrypted message but the holder of the complementary secret key, not even the person who encrypted it in the first place. This makes public key cryptography much more practical.

You may want to try encrypting some of your personal e-mail. PGP for Personal Privacy 5.0 is a great shareware program that's compatible with several e-mail packages such as Eudora by Qualcomm. To get a copy of PGP 5.0, visit the Web site: www.pgpi.com

Take a virtual trip to the following Web site. It has excellent links and good information for beginners: www.ftech.net/~monark/crypto/main.hts

If you're interested in training, contact your local university math department. There is also a federal government agency, The Communications Security Establishment (CSE), that offers training to other government agencies. Courses such as "Introduction to Cryptography and its Applications" are also available to people in the private sector. Find out more on their Web site at www.cse.dnd.ca

References:

- Schneider, Bruce, Applied Cryptography - Protocols, Algorithms and Source Code in C, Toronto: John Wiley & Sons, 1994
- Zimmerman, Phil, PGP for Personal Privacy, Version 5.0, Users Manual, San Mateo, CA: Pretty Good Privacy Inc., 1997

The opinions expressed in this article are not necessarily those of my employer, nor is any endorsement implied of any product or company mentioned.

Hugh Long is a senior consultant at Cadence Design Systems, Inc. He can be reached at 613-726-8423 or hlong@cadence.com. Cadence is a supplier of software tools and professional services used to accelerate and manage the design of semiconductors, computer systems, networking and telecommunications equipment and a variety of other electronic-based products.