Politics and Techniques of Data Encryption

by Dr. H.B. Wolfe

Introduction

Cryptography is the art or science, depending on how you look at it, of keeping messages secure. It has been around for a couple of thousand years in various forms. The Spartan Lysander and even Caesar made use of cryptography in some of their communications. Others in history include Roger Bacon, Edgar Allan Poe, Geoffrey Chaucer, and many more. By today's standards cryptographic techniques, through the ages right up to the end of World War I, have been pretty primitive. With the development of electro-mechanical devices cryptography came of age. The subsequent evolution of the computer has raised the level of security that cryptography can provide in communications and data storage.

How Does it Work?

Most modern cryptographic systems make use of two basic techniques: substitution and transposition. Substitution refers to substituting one character for another. The method of substitution can involve sophisticated mathematics in order to accomplish that transformation. Transposition refers to changing the physical position of characters within a message according to some predetermined scheme. The exact combination of these techniques is referred to as a cryptographic algorithm. The key is a unique instruction (normally devised or created by a user) which is used to drive the algorithm.

Cryptographic algorithms are further divided into two categories: symmetric and asymmetric. Symmetric describes an algorithm that uses a single key to both encrypt or decrypt (encode or decode). Asymmetric defines an algorithm that uses different keys for the two functions of encrypting and decrypting (sometimes referred to as public key systems).

Encrypted data has the property of being meaningless, however, through crypt-analytical techniques these encoded messages can be attacked and may or may not be able to be decoded. The level of confidence and implied security that a given algorithm can provide is usually based upon the cryptographic community's scrutiny and testing of that algorithm. Within the past twenty years several new mathematical attack strategies have been devised rendering heretofore secure algorithms useless.

Short History Lesson

Modern cryptography really came into its own in the mid 1970's. In 1975 the U.S. Government invited proposals for a data encryption standard that could be certified to provide a given level of protection. One of the algorithms submitted was called Lucifer (devised by IBM). It was a block cipher with a key length of 128 bits (this attribute is often confused as the ONLY gauge by which the relative strength of an algorithm can be judged). The National Security Agency (NSA) is the code making and code breaking agency for the U.S. It is the largest single user of computers, and largest single employer of mathematicians and cryptographers in the world. They had a great deal of influence in the creation of the final algorithm today known as the DES (Data Encryption Standard). This algorithm is one of the most commonly used encryption algorithms in use in business today.

The final DES consisted of a symmetric block cipher with a 56 bit key. The 56 bits can be described as follows: the total number of possible permutations of any given message encrypted using the DES algorithm is 2^{56}. That's a lot of different messages considering that only one of those is the real one. At the time of its creation it was estimated that with all of the available computing power in the world it would take hundreds of years to find the key. Things have changed since then, It is currently estimated that NSA can decrypt such a message in a few minutes or less with the equipment that they have available.

The DES has been shrouded in controversy ever since its certification. NSA has been accused of designing a "back door" into the algorithm. It has also been accused of deliberately diminishing the DES's level of security by reducing the possible number of permutations (56 bit key instead of the 128 bit key in the original Lucifer design). Of course all of these allegations have been denied, however, this introduces politics into the equation of privacy.

The Politics of Encryption

War has taught us that knowing what the enemy intends to do gives us an advantage. WW II was influenced dramatically by cryptography - some say that it determined the outcome. The Allies were, from the very beginning and throughout the war, able to decode the communications of both the Axis powers and the Japanese. The United States has considered data encryption and its tools the domain of the intelligence community and has legislated that (under the ITAR regulations) cryptographic hardware and software fall into the classification of munitions. As such they strictly regulate the export of items that fall into that category. Moreover, there is a strong conviction on the part of the U.S. Government and law enforcement that they and only they should have the right and authority to be able to decode any and all communications. The rationale apparently is that without that ability law enforcement cannot deal with crime prevention effectively. The intelligence community rationalize it by using the "threats to national security" argument for their justification.

Since both sectors wield significant influence and power, a new concept in cryptography has emerged. It's called escrow encryption. The U.S. Government is actively pursuing the notion that no one should be allowed to have strong encryption (meaning that they can't break it) and should "trust them" not to abuse their power. This from a government with a chronic history of the abuse of power.

Addressing what the U.S. does may not seem particularly relevant to what we do in New Zealand or the rest of the world but that couldn't be further from fact. The U.S. is currently in the process of attempting to hijack the Committee for Information, Computer and Communications Policy specifically set up by the **OECD** to establish cryptographic standards amongst OECD nations (New Zealand is a member). When I say hijack, I mean load the committee with like minded individuals so that their agenda can be carried out. It is the position of the U.S that only law enforcement and intelligence professionals should be members of this committee. Of course with no input from other sectors strong encryption for the masses will ultimately be outlawed. That means us.

Escrow Encryption

The current initiative in escrow encryption is generally referred to as Clipper, however, that is really only the name given to the chip in which the escrow algorithm called Skipjack is implemented. Its computer counterpart is the Capstone algorithm implemented in the Fortezza chip. The way it works is that encryption between parties is carried out in the normal way, however, lodged with two escrow agents (both are arms of the U.S. Government) is the escrow key or more precisely each escrow agent possesses one half of the key. If government or law enforcement decided that they wanted to have access to your communications or encrypted files, they would obtain a court order and take it to the escrow agents to obtain the two halves of your key and proceed to decode your communications or files. The escrow key is a secondary key that unlocks the algorithm to them.

For the reader that assumes that law enforcement or government should be able to view any and all communications that everyone might engage in, this type of encryption presents no problems. For those of us who believe strongly that **privacy is one of our most basic human rights**, this presents a big problem. One of the attitudes that I have noticed during the seventeen years that I have lived in New Zealand is that most folks seem to believe that anything that is secret is bad and/or illegal. For the reader who ascribes to that view, I direct your attention to the book by Sissela Bok called *SECRETS: Concealment & Revelation.* It is an excellent exposition of why each and every one of us needs privacy and secrecy in our day to day lives and dispels the notion that it is automatically bad or in some way illegal.

Newer Algorithms

Concurrently, from the time that the DES was certified by the U.S. Government, cryptographers in the public sector have engaged in continuous development. Several notable approaches have emerged, been tested and continue to provide strong encryption. There are a couple of symmetric block ciphers of note. The first is the 128 bit IDEA (International Data Encryption Algorithm) developed around 1990 by Xuejia Lai and James Massey. This is thought to be one of the most secure today. To give you an idea of exactly what that means: if you had a computer capable of doing one billion encryptions per second AND you could array one billion of these machines to work in concert, a brute-force attack, on a single message encrypted using IDEA, **would take 10^{13} years to find the solution**. By anyone's standards that's a long time. In cryptographic terms it is considered computationally secure. The interesting thing about IDEA is that it is not owned or controlled by the U.S. and can be licensed through Ascom, a Swiss company.

The second is a variable key length (up to 448 bits) block cipher, called Blowfish, developed in the last couple of years by Bruce Schneier. It's pretty new and has been scrutinized but thus far no one has been able to defeat it.

Another that is currently being used is called Triple DES. This uses the DES algorithm but does the encryption in three passes. Using two different keys. This improves the apparent security of the DES to 112 bits or 2 to the 112 power different possible permutations of any single message.

Public Key Crypto-Systems

In the late seventies another approach was developed called public key cryptography. Instead of having only one key to perform the functions of encryption and decryption public key systems require two keys. One with which you encrypt and another with which you decrypt. The idea being that you could publish your public key so that anyone could communicate with you privately without having to exchange keys (in cryptography key management, including the key exchange, is vitally important to its proper and effective use). Not having to worry about compromise during the exchange required in a symmetric system makes public key systems very desirable.

There are a few such systems that have emerged as being stable and secure. The first to receive attention is the RSA algorithm developed by Ron Rivest, Adi Shamir and Len Adleman. They issued a challenge in August 1977 to decrypt a message encoded with a 429 bit key. They predicted that it would take 40 quadrillion years with the technology of the day to crack the code. In April 1994 after eight months of effort using 1600 computers the message was solved.

You may have noticed earlier in the paper that I described the computational security of IDEA and it only had a 128 bit key as compared to the 429 bit key cited above. It is important to understand the difference in approach between a symmetric block cipher and a public key cipher. Solving the public key cipher does not depend on a brute-force attack strategy. In the case of the RSA algorithm the two keys are based on very large prime numbers. The attack strategy is to factor these prime numbers and then derive a solution. The symmetric block cipher does not depend on large prime numbers for any part of its activity and therefore this attack strategy does not work with them. A simple guide to comparative levels of computational security is as follows:

Symmetric		**Public Key**	
56	is equivalent to	**384**	**size of**
112	is equivalent to	**1792**	**keys in**
128	is equivalent to	**2304**	**bits**

What is to be learned by the solving of the RSA-429 message is that the RSA algorithm must be used with large key sizes - 512 bit keys or larger - preferably 1024 or greater in order to provide strong protection.

Another public key system is Pretty Good Privacy (PGP). It was developed and introduced by Phil Zimmermann in 1991 and has become the world de facto standard for ordinary citizens of all nations. This is a hybrid system which incorporates three different algorithms to provide sufficient computational security for the common man. These include RSA (used to protect the randomly generated keys used with IDEA to encrypt the main body of the message), IDEA (used to encrypt the main body of the message) and MD5 (a one way hash function developed by Ron Rivest and used in this incarnation to create an authentication signature for the message). PGP has become freely available from Internet sites around the world. If you're outside the U.S. and try to download a copy from MIT, for example, that download will be stopped and in fact constitutes an offense under U.S. law.

Unfortunately for Phil, the U.S. Government has viewed PGP's proliferation very negatively. In fact the FBI and other agencies investigated Phil with the intent to prosecute him for exporting encryption outside the U.S. without the required export approvals. They have spent the past four years on that investigation and in January of this year decided not to proceed. During that time Phil has had to put up with a lot of Government harassment. In fact, we were returning to the U.S. from Curacao in 1994 through Miami after speaking at a conference. I proceeded through Customs with no problem - it took 5 minutes. Eight hours later Phil emerged somewhat bedraggled to continue his trip home. Of course he'd missed his flight by then.

New Zealand has a community of interest in cryptography. There are at least two public key systems that have been developed here in New Zealand. The LUC system was developed by Peter Smith of Auckland. It makes use of Lucas functions in the generation of primes. It's too new to determine how secure the algorithm is at this point. There is some talk of an unpublished paper describing how to break at least some implementations of it. Another is RPK developed by Bill Raike of Auckland. Dr. Raike's system is based upon the mathematics of finite Galois fields. Once again it is too new to be certain of its real level of computational security but it does show promise.

Another firm in Christchurch (CES) has developed an analog stream cipher and implemented it in hardware form (called SignalGuard). It does not consider data in any way. It transforms the analog signal once it has left the modem for transmission over a telephone line. This is a unique approach to encryption and offers a level of security which is at this time unknown to the writer.

Available Products

Data encryption is available in many of the computer products that we may be using. For example, Word Perfect offers the facility to be able to encrypt documents that we believe to be sensitive. The fact is that the product cannot protect your privacy from anyone that knows about WPCRACK and is willing to use it against you. This is a program readily available from the Internet which derives the key from the encrypted file. There are many other examples of products offering an encryption facility which is only cosmetic and actually does not provide the expected nor advertised security.

Conclusion

Cryptography is an extremely specialized field. There are many political agendas that would hope to dictate the availability of strong encryption to anyone other than law enforcement and intelligence. If you believe that privacy is one of everyone's basic human rights then it is important to understand that encryption for everyone is now under attack. That governments will involve themselves in dictating what we are able to keep private and what will not be able to be kept private. Cryptography and strong encryption algorithms afford the common man the ability to communicate privately without risk of discovery of the contents of that communication. We ultimately have the last word as to whether or not to divulge the key(s) necessary to decode such communications.

Additional Sources of Useful Information:

Cryptography:

Schneier, Bruce, *Applied Cryptography*, 2nd Edition, New York, John Wiley & Sons, Inc., 1996, **ISBN 0-471-11709-9**.

Schneier, Bruce, *E-MAIL SECURITY: How to Keep Your Electronic Messages Private*, New York, John Wiley & Sons, Inc., 1995, **ISBN 0-471-05318-X**.

Stallings, William, *PROTECT YOUR PRIVACY: A Guide for PGP Users*, Englewood Cliffs, New Jersey, Prentice Hall PTR, 1995, **ISBN 0-13-185596-4**.

Bamford, James, *The Puzzle Palace*, Harmondworth, England, Penguin Books, Ltd., 1983, **ISBN 0-14-006748-5**.

Kahn, David, *THE CODE-BREAKERS: The Story of Secret Writing*, New York, MacMillan Publishing Company, 1967, **ISBN 0-02-560460-0**.

Periodicals:

Cryptologia, Terre Haute, Indiana, Rose-Hulman Institute of Technology, 4 issues per year, **ISSN 0161-1194**.

Computers & Security, Oxford, England, Elsevier Advanced Technology, 8 issues per year, **ISSN 0167-4048**.

General:

Bok, Sissela, *SECRETS: Concealment & Revelation*, Oxford, England, Oxford University Press, 1986, **ISBN 0-19-286072-0**.

Internet Sites of Interest

http://ciac.llnl.gov/
CIAC Security Web Site

http://www.sei.cmu.edu/technology/cert.cc.html
CERT Coordination Center

http://www.cdrom.com/pub/security/coast/
F-PROT Zip files

http://www.ifi.uio.no/pgp/download.shtml
How to download PGP 2.6.3I

http://www.ifi.uio.no/pgp/PGPfone.shtml
PGPFone

http://www.tscm.com/
TSCM.COM Counterintelligence and CounterTerrorism Home Page

http://www.enter.net/~chronos/cryptolog.html
Welcome to Crypto-Log: Internet Guide to Cryptography

ftp://ftp.win.tue.nl/pub/security/
Directory of /pub/security

http://www.thecodex.com/
The Codex

http://www.nwfusion.com/
A Flurry of Firewalls

http://www.isecure.com/newslet.htm
SECURE NEWS

http://www.netsurf.com/nsf/v01/03/nsf.01.03.html
Netsurfer Focus on Cryptography and Privacy

http://www.engin.umich.edu/~jgotts/underground.html
The Internet Underground

NOTE: The Internet is a fluid living thing. What is valid today may not be valid tomorrow. One or more of these addresses may no longer active but give them a try.