ENCRYPTION

of the

PAST and PRESENT

Written By:
Kimberly D. Greenizan
Internet Lodge of Research
Grand Lodge of Alberta
26 August 2000

ENCRYPTION of the PAST AND PRESENT!

The necessity to maintain secrecy has been a requirement for military leaders and the ability to intercept an enemy's message and understand the value of the information his vice. On the one-hand he wants to be able to ensure that his information, such as the placement of his troops and the next strategic move in the battle is not know to the opposing forces until it is too late for them to react while on the other hand he wants to know what the opposing forces plan to do so that he can make best use of this information in his own strategies. Therefore placing spies to gather information is a major military tactical advantage and encryption is one of the most important tools to prevent the spy from being successful.

We can see the value of the cipher from the very fact that the US government restricts the export of anything to do with encryption that they do not already have the means to intercept and successfully analyze. Encryption has now moved from the military environment to the industrial one as we become more aggressive in a competitive and shrinking world. This was exemplified in their attempt to insert key escrow into their legal system in support of "law enforcement".

Why encrypt any message? That is the question that has faced every leader in every walk of life since time immemorial. Is our information of such importance that someone would cause harm or injury to obtain it? Will the release of this information lead to disruption or loss? Will our real objectives become known too early if we permit our plans to become known to the enemy? In many instances of military planning the information on the battlefield has a limited life span. If this critical information becomes known to the enemy in sufficient time for them to react to it then the planning is for naught and the battle can be placed in danger of loss.

Information must be received by the intended recipient in sufficient time for them to properly prepare for what is to come. This information may be of great value to the opposing forces if it is received in a timely fashion. Every military leader has had informants in the enemy camp for just this purpose.

Therefore concealing information from opposing forces must also include concealing it from these informants. As such the leaders use cipher to conceal their tactics and plans from those who did not have a need-to-know. The leaders hold information from the followers so that objectives do not become confused. The troops that are being used as bait, or being sacrificed for the safe withdrawal of others is necessary in certain battle situations, however, for those troops it is best that they do not know this. Such concealment of information has existed for multiple millennia.

Concealing a message has been termed to write in cipher. The following definition has been extracted from the Encyclopaedia of Freemasonry:

> "Cipher writing – cryptography, or the art of writing in cipher, so as to conceal the meaning of what is written from all except those who possess the key, may be traced to remote antiquity [Hughan and Hawkins, 1924]."

Hughan further goes on to state that De la Guilletiere attributes its origin to the Spartans, and Polybius says that more than two thousand years ago Aeneas Tacitus had collected more than twenty different kinds of cipher which were then in use. It is common knowledge that kings and generals communicated their messages to officers in distant provinces. To do so in an open and easily readable fashion would prove to be fatal on a battlefield so they did this by means of a preconcerted cipher. The use of a cipher and an encryption system has always been employed

wherever there was a desire or a necessity to conceal from all but those who were entitled to the knowledge the meaning of a written document.

Dorothy Denning has identified cryptography as follows:

> "Cryptography is the science and study of secret writing. A cipher is a secret method of writing. Plaintext (or clear text) is transformed into ciphertext and the process is called encipherment or encryption. The reversal of this process is called decipherment or decryption. The whole process is dependent upon a key – that which when applied by a method of process (algorithm) transforms the plaintext to ciphertext or vice versa. Thus encryption is controlled by a key [Denning, 1982]."

We can look at many religious organizations and see the dilemma of concealing their most private beliefs from the slanted interpretations of the non-believers and those whose only interest is to denigrate them with disparaging rumours and fictitious information. The druids were not permitted by the rules of their order to commit any part of their ritual to ordinary writing. In order for them to preserve the memory of this most important work it became necessary to conceal it through the use of the letters of the Greek alphabet. The Kabbalists also developed their own method of concealing their works. They documented many words by writing them backwards and this method is reported to be in use by some French Masons to this day.

The old alchemists also made use of cipher writing, in order to conceal those processes the knowledge of which was intended only for the adepts. You may think that present day doctors use a cipher of their own in that only a pharmacist can actually read what they write on a prescription. Perhaps Roger Bacon was a doctor in disguise, for when he discovered the composition of gunpowder, it is said he concealed the names for the ingredients under a cipher made by a transposition of the letters.

Before we go into the evolution of cryptography we should review some of the basic components of cryptography. First we must have a message that needs to be sent. This message in a normal readable state is termed a plaintext message. In order to keep it a secret it has a code applied to it and the resulting message is encrypted or ciphertext.

The process of applying a key is known as the algorithm or procedure. There are many different algorithms and they have become more complex with time. As the strength of any encryption rests with the validity and secrecy of the key the actual algorithm or process becomes common knowledge. This is especially true today as we proceed further into a technology-based society. Today all of the security is based on the key; none is based in the details of the algorithm. Thus today's algorithms are published and analysed. Products using the algorithm can be mass-produced. It doesn't matter if an eavesdropper knows your algorithm, if she doesn't know your particular key, she can't read your messages.

Symmetric Algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms the encryption key and the decryption key are the same. These algorithms also called secret-key algorithms, single key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely [Schneier, 1996]. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret the key must remain secret.

For the most part the symmetric algorithm is the type of process that was used in the early centuries to provide protection to critical information. Such algorithms are believed to have been in use prior to the Roman Empire. We know that they were common during the successful reign of the Romans over most of the then known world.

00BC or thereabouts - Caesar Cipher

In the times of Julius Caesar or perhaps even earlier a cipher was used to pass messages to the legions afar. The overall control of the encryption key was maintained by the Roman Senate and the Caesars of the day. It was a very simple cipher and was used extensively during the times of the Roman Empire.

This cipher consisted of having the alphabet offset by a number of positions [Denning, 1982]. The number of positions taken was known as the cipher key and with the correct key you could decrypt or encrypt any message. Depending on the sender you would have to apply the correct key for the communication to be understood. By the same token, only those individuals who held your key would understand your messages. They would be able to use your key to decrypt messages you sent to them. For example if the key is 3 then A = A + 3 which is D; B then becomes E, C becomes F, etc. Each message used a single key for the entire process and made the cryptoanalysis fairly easy.

If you were to encrypt a simple message such as “head for Jerusalem” you would get the following:

Key = 3	KHDG IRU MHUXVDOHP
key = 6	NKGJ LUX PKXAYGRKS
key = 9	QNJM OXA SNADBJUNV

The whole point of cryptography is to keep the plaintext secret from the eavesdroppers. Eavesdroppers are assumed to have complete access to the communications between the sender and the receiver. **Cryptoanalysis** is the science of recovering the plaintext of a message without access to the decryption key. Successful cryptoanalysis may recover the plaintext message or the key. It may also find weaknesses or vulnerabilities that can be exploited which eventually lead to the previous results.

1200’s

Cornelius Agrippa tells us, in his Occult Philosophy, that the ancients accounted it unlawful to write the mysteries of God with those characters with which profane and vulgar things are written; and he cites Porphyry as saying that the ancients desired to conceal God, and divine virtues, by sensible figures which were visible, yet signified invisible things and therefore delivered their great mysteries in sacred letters, and explained then by symbolic representations. Prophyry here undoubtedly, referred to the invention and use of hieroglyphics by the Egyptian priests; but these hieroglyphic characters were in fact nothing else but a form of cipher intended to conceal their instructions from the uninitiated profane [Hughan and Hawkins, 1924].

Peter Aponas, an astrological writer of the thirteenth century, gives us some of the old ciphers which were used by the Kabbalists, and among others one alphabet called “the passing of the river,” which is referred to in some of the high degrees of Masonry.

But we obtain from Agrippa one alphabet in cipher which is of interest to Masons, and which he says was once in great esteem among the Kabbalists, but which has now, he adds, become so common as to be placed among profane things. He describes this cipher as follows: The twenty-seven characters (including the finals) of the Hebrew alphabet were divided into three classes of nine in each, and these were distributed into nine squares, made by the intersection of two horizontal and two vertical lines, forming the following figure:

3	2	1
6	5	4
9	8	7

In each of these compartments three letters were placed; as, for instance, in the first compartment, the first, tenth and nineteenth letters of the alphabet; in the second compartment, the second, eleventh and the twentieth, and so on. The three letters in each compartment were distinguished from each other by dots or accents. Thus the first compartment, or shape (shown as box 1) ⌞ represented the first letter, the same compartment with a dot represented the tenth letter, or with two dots the nineteenth letter. This pattern followed with the other

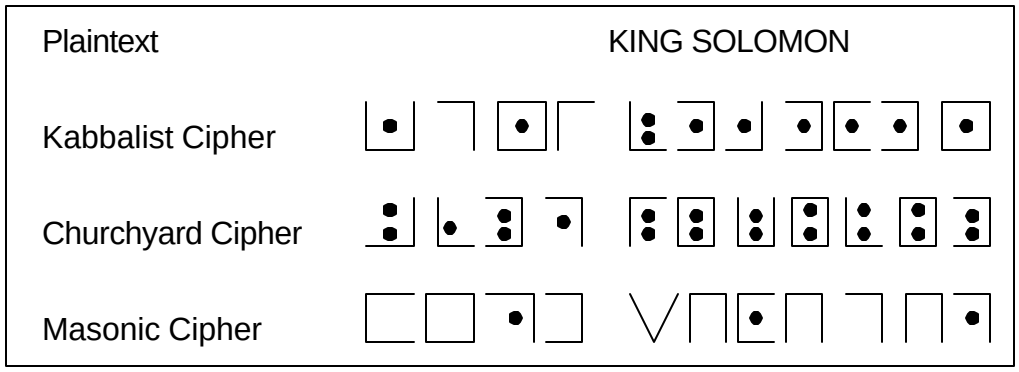
⌝

compartments; the ninth or last representing the ninth, eighteenth, and twenty-seventh letters, accordingly it was figured (shown as box 9) with zero, one or two dots in the center.

This process was used by a number of different groups in a number of different ways. In more current times it has been referred to as the "Churchyard cipher". The process was changed somewhat in that the letter A was in box 3 instead of box 1 and had one dot and the letter T in the same box had no dot [Denning, 1982]. In essence the boxes were reversed with 1 on the left and 3 on the right, the first set of letters held one dot, the second set two dots and the final set no dots. Also I and J shared a square leaving two blank squares in the last set.

We have seen a similar, cipher which follows the same pattern as the Churchyard cipher, with two letters per box, the second holding a dot. For example, box 1 would hold the letters a and b, box 2 the letters c and d, box 3 the letters e and f, etc. The remaining letters were placed in a large X where s and t were at the top, u and v to the right and the remaining letters following the pattern clockwise around the X [Pick and Knight, 1955]. This cipher was referred to as the "Masonic cipher" although Pick does not refer to the time in which it was most commonly used. Hughan does refer to the use of the St. Andrews cross variation and that it was considered to be so common by the middle of the 19th century as to be listed among those profane things and of no further significance.

Let us look at a couple of examples of the above ciphers.



Although this cipher has limitations in its use and the validity of the security of the message over time, it still has seen use as late as the early 20th Century [Denning, 1982]. As in many instances of the need for encipherment, the message is only good if the information is known when it is needed most. Therefore if a message takes an hour or a year to decipher it could still be valid to use. A cipher is good if the information it is concealing can be recovered by the intended recipient within a reasonable period of time. A reasonable time period would be one in which the recipient had enough time to respond in a positive manner to the information received. For example, if the information has a shelf life of one hour and the cipher takes two hours to decrypt then the cipher has done its job by denying the opposition the information for the critical time period of one hour. The failure of the cryptoanalyst to discover the key makes the opposition unable to act upon it.

1568 Leon Battista Alberti

Alberti published a cipher disk that defined multiple substitutions. The plan included two disks one inside the other with the outer disk containing 20 plaintext letters, [H, K and Y were not used and J, U and W were not part of the Latin alphabet] and numbers 1 to 4 for special codes. In the center ring he randomly placed the letters of the Latin alphabet plus the "&" sign. Depending on

the position of the rings you then had 24 possible substitutions from the plaintext letters in the outer ring to the cipher text letters in the inner ring. Alberti's important insight was his realization that the substitution could be changed during encipherment by turning the inner disk thereby increasing the key variable.

This changed the value and mode of encryption to a faster paced and more dynamic algorithm. If the key is randomly chosen and works in a random fashion then the ability of the cryptoanalyist to discover the key is lessened. The longer it takes to discover the key, the longer the secrecy of the message is upheld. With today's computer technology the keys are becoming more random in selection and longer for added strength.

Vigenere Cipher

This cipher used the process of shifting the alphabet similar to the Caesar cipher but using multiple keys in a single message. In this method the key could start as K=d then the alphabet would be substituted starting from d such that a=d, b=e, c=f, etc. But your could use a key word such as hilt. In this instance the first letter enciphered would use the key k=h, the second letter would use the key k=I, the third would use k=l and the fourth would use k=t. Then the process would repeat itself with the fifth letter being k=h again. For example:

Plaintext would be	T o r o n t o
Key would be	h i l t h i l
Cipher text would be	A w c h u b z

You only need to have a matrix of the possible keys with the plaintext and you can easily encrypt and decrypt messages. Again the length of the key is the crucial part for the longer it is the less chance it has for repetition and subsequent cryptoanalysis.

Beaufort Cipher

Identical in principle to the Vigenere cipher it reverses the alphabet such that for a key of d then a=d, b=c, c=b, d=a, e=z, f=y, etc. It also recommended a multiple key process to strengthen the cipher. Thus it was recognized that the strength of the encryption lay in the length of the key being used and the ability to keep this key secret.

Beale Cipher

A group of adventurers lead by Thomas Jefferson Beale was said to have buried a treasure in Virginia around 1820. The location of the treasure was purported to be identified in an encrypted message that used the declaration of Independence as the key. The process was to number each word and then take the corresponding numbered word and use the first letter of it. For example the first line “When, in the course of human events, it becomes necessary” the cipher would be as follows 1=W, 2=I, 3=t, 4=c, 5=o, 6=h, 7=e, 8=I, 9=b, and 10 = n. You will notice that some numbers will have the same value such as number 2 and 8. Beale left three ciphers the second of which was solved by James Ward in the 1880s. It described the gold, silver and jewels worth millions today that was hidden n the treasure and that the first cipher would give directions on where to find it [Denning, 1982]. The second cipher used the Declaration of Independence as the key however no one has been able to solve the first cipher.

Some feel that the whole existence of the treasure is a hoax left by Beale but in any event it shows the value of a strong key in the encryption process.

1854 Playfair Cipher

This is a diagram substitution cipher invented by Playfair's friend Charles Wheatstone and was used by the British in WWI. It consists of a 5 X 5 matrix of 25 letters, (J was not used). Plaintext letter pairs were encrypted or decrypted based upon a complex set of rules for character pairs. This process was based upon the premise that the cipher square was in the possession of both sender and receiver. Such cipher pads needed to be closely guarded and handled with extreme secrecy.

This process is still in use today within NATO organizations. The diagrams each have a validity period where the diagram is considered to be effective and they are destroyed after this time period expires.

1861 Ritual Cipher

In the late 1800's it was believed that the clarity and standardization of Masonic work was missing. In an effort to build a standard for uniform work it was permitted to record the ritual, but such records had to be done in a cipher. This cipher required that only a true mason who is knowledgeable in the craft could understand what was transcribed. To achieve this end Robert Morris designed a ritual cipher that was put into practice where it was lawfully supported by the appropriate Grand lodge. The cipher consisted of recording the first letter of each word with a dash between the letters. Therefore "Betty had a little golden sheet" would read b-h-a-l-g-s.

Such a line would be meaningless to a casual observer. It could mean anything like “be happy and love God’s sunshine.

Most Grand Lodges thought that such a cipher would enable the various lodges in the multitude of Grand Lodges to be able to follow the same ritual and at the same time safeguard the true words and meanings of the ritual itself. Unfortunately as not all of the lodges followed the same work as that which was transcribed it provided little or no guidance and failed to achieve its objective. In addition to that many Grand Lodges did not permit the use of ciphers and did not institute the standardization of the work.

Late 19th Century Running Key Ciphers

In this instance the key is as long as the message itself. Using the Beaufort method the message is encrypted but the key to the cipher is a second message, letter or extract from a book. The key is specified by the title of the book or document and the actual starting place.

Take into consideration the cipher purported to be left by Thomas Jefferson Beale. He only used the first letter of each word. What if he had actually used every letter of each word from a given starting place in the document? Then each letter of the plaintext message would be encrypted with a different letter from the key document. This would make cryptoanalysis more difficult as repetition in the message could not be used successfully to determine the key. You would have to know which document was being used as the key and where in this document the start point for the key was located.

The Rail Cipher

The Rail Cipher is a transposition cipher which uses the process of having the words written down in a pattern resembling a rail fence then removing them by rows. The key is the depth of the fence, for example:

FACILITY MANAGER

F				L				M		G
	A		I		I		Y		A	
		C				T				

FLMG

AIIYAAE

CTNR

Would give you the following cipher text

FLMGAIIYAAECTNR for the words Facility Manager. The key to this rail cipher is three (3) as it is three rails deep.

1917 One Time Pads

If a key is a random sequence of characters and is not repeated, there is not enough information to break the cipher. Such a cipher is called a “one-time-pad”, and is used only once. The one-time pad was designed by Gilbert Vernam in 1917 for AT&T. He designed a cryptographic device for telegraphic communications based on the 32 character Baudot code of the new teletypewriters developed at AT&T [Denning, 1982].

The value of a one-time pad has been revisited may times over the years and implemented in various forms. The management of the pad and the distribution of the keys has been the greatest

hurdle to overcome. This process was further implemented by means of punched cards in the early development days of computers.

1920's Hagelin Machines

Invented by Boris Hagelin in the 1920's and improved in the 1930's it was a series of key wheels with pins. The C48 for example had 6 wheels with 17, 19, 21, 23, 25 and 26 pins respectively. The pins can be pushed either left or right and the combined settings of the pins and the positions of the wheels determined the key. The encipherment is that of a Beaufort substitution and after each character is enciphered all the wheels are rotated one position forward. These machines have been used as late as 1983 with much success, however slowly, but the keys are not as random as they might seem and are therefore subject to cryptoanalysis.

WWII

Substitution ciphers were established with numerical values. These values had four or five digit values and the words or dictionary was contained in a book referred to as a code book. You then selected the appropriate word from the code book and used the numbers associated with it.
The key was given to the team at point of departure however sometimes it was passed by a trusted courier. The key to receive a message usually differed from that to send a message in the case one of the code books became compromised (fell into the hands of the enemy).
An example of the code book could look like the following:

Europe	1234	France	1345
brigade	1456	infantry	1567
Spy	2345	gun emplacement	2456

Church	2567	panzers	2678
Have	2789	courier	2890
Sent	3124	tonight	3245
West	4356	coming	4578
Bridge	4213	machine gunners	4798

Therefore the following would mean:

26784578324543564213 panzers coming tonight west bridge.

WWII Rotor Machines

These machines, which implement polyalphabetic substitution ciphers with a long key period, consisted of a bank of rotors or wired wheels along the lines of the Hagelin machines. The perimeter of each rotor had 26 electrical contacts on both its front and rear faces. The plaintext letter enters the bank of rotors at one end , travels through the rotors in succession and emerges as ciphertext at the other end.

The wirings plus initial positions of the rotors determine the starting key. As each plaintext letter is enciphered, one or more of the rotors move to a new position, changing the key. A machine with *t* rotors does not return to its starting position until after 26^t successive encipherments, thus a machine with 5 rotors has a period of 26^5 or 11,881,376 letters.

The Enigma, invented by Arthur Scherbius and used by the Germans in WWII used an odometer rotor motion cycling the rotors like an odometer on an automobile [Denning, 1982].

Today we are in a different world when it comes to encryption and key management. Information has become the life's blood for many an organization and their very survival rests with its security and secrecy. At the same time we share information readily and want to permit every customer, and potential customer, to have instant access and gratification with doing business with us. We rely heavily, perhaps too heavily, on the suppliers of software to protect our systems and do not retain anyone in our employment who can manage or decipher how the programs work. Who then is really in control of our information and will it remain accessible to us when we need it most?

The security professionals have a base in physical security and can understand only too readily the difficulties of securing something that is unseen, has no physical presence and is of instant value. The hackers also recognize the value of information that can be easily intercepted and/or redirected without the intended recipient even knowing. Therefore to encrypt our information and have very tight security on the key management is the objective of technology today. This brings into play several different types of algorithms where which key management can be successfully achieved.

Symmetric Algorithms

Sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms the encryption key and the decryption key are the same. These algorithms also called secret-key algorithms, single key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key;

divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret the key must remain secret.

Before computers, algorithms generally operated on one character at a time. Today we work on multiple characters at a time. We have two categories of symmetric algorithms. One that operates on the plaintext a single bit (or byte) at a time; they are called stream algorithms or stream ciphers. The other operates on the plaintext in groups of bits. The groups are called blocks, and the algorithms are called block algorithms or block ciphers.

Public-Key Algorithms

These are designed so that the key used for encryption is different from the key used for decryption. Furthermore the decryption key cannot be calculated from the key used for encrypting the message. The algorithms are called public key because the key used for encryption can be made public. A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems the encryption key is often called the public key and the decryption key the private key. The private key can also be referred to as the secret key.

The level of complexity of encryption algorithms and key management advanced rapidly with the advancement of computer technology. The faster and smarter terminals and communications technologies improved the ability for cryptoanalysis. It led to the production ciphers such as the Lucifer cipher by IBM and the Data Encryption Standard (DES) which became the defacto industrial standard for years.

1976 DES

In 1976 DES was evaluated during a series of intensive workshops. On conclusion of these workshops DES was accepted as the industrial standard for financial institutions. The National Bureau of Standards in the United States reinforced it as the industrial standard. A now well-known group of cryptographers, Diffie, Hellman, Morris, Sloane and Wyner, who were specialists at the time, had participated in these workshops. They identified two main weaknesses with the DES algorithm. First the key size of 56 bits may not provide adequate security, and secondly there may be hidden trap doors which could provide for quick decipherment if discovered.

1978 - Exponentiation Ciphers

In 1978 Pohlig and Hellman published an encryption scheme based upon computing exponentials over a finite field. Rivest, Shamir and Adleman published a similar scheme with a slight twist which gave the MIT group, for which thye worked, a method for realizing public-key encryption as put forth by Diffie and Hellman in 1976.

Both schemes encipher a message block by computing the exponential. The enciphering and deciphering processes are separate and consist of three components. Two can be readily released and one is coveted. The two being released form together as what is now know as the public key and the coveted one is the private key.

1980's - RSA Encryption

The development of the exponentiation cipher led to the development of the public and private key conventions. Such a convention is the foundation of RSA encryption and the advent of the Public Key Infrastructure (PKI). PKI has led to the development of methods for such areas as non-repudiation, authentication, data integrity checks, the secure socket layer (SSC) and internet protocol security (IPSec).

We go even further than this when if comes to accessibility and ease of movement of information through out networks. There are a number of trends that have worked together to make the threat of computer crime greater than ever before. Because these trends are likely to continue in the foreseeable future, the threat to organizations will only become more serious.

What are these trends you may ask? They are :

The rise of distributed computing;

The trend toward mobile computing;

The emergence of the Internet for business communications;

Better hacker tools; and

Widespread computer literacy.

So what are we asking for in the security of our systems? We are seeking to be able to verify the authenticity of users, establish a means for identification, protect the privacy and integrity of our information on and beyond the network and prevent validated parties in transaction or exchange from denying the actions they have taken. In short form we want authentication and identification (I&A), Integrity and non-repudiation of others actions.

Most of this is being achieved by means of encryption systems where keys can be used to positively identify an individual, provide a signature that the owner can nor refute is his and limit the access to our information by compartmentalizing it with different key accesses for different areas. The challenge?

How do you secretly and securely distribute the keys to the necessary people without compromise at one stage or another. This has lead to the advent of what is now termed PKI, or Public Key Infrastructure. Digital certificates are provided by a certificate authority who confirms the identity of the owner to the level and degree of the certificate requested. These certificates provide private and public keys to support non-repudiation. It supports non-repudiation of the origin of the message, non-repudiation of the submission of the message (like a postage mark), and non-repudiation of the receipt of the message proving that the other party actually received the sent message.

But even with this development and the universal standards that are being accepted by industry today, we still face the fact that technology is advancing. Privacy is a major issue and as one devises a means to protect another will devise a method to break that protection.

Steganography

This serves to hide secret messages in other messages, such that the secret's very existence is concealed. Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. Historical tricks include invisible inks, tiny pin punctures

on selected characters, minute differences between handwritten characters, pencil marks on typewritten characters, grilles which cover most of the message except for a few characters, etc.

More recently people are hiding secret messages in graphic images. Replace the least significant bit of each byte of the image with bits of the message. The graphical image won't change appreciable – most graphics standards specify more gradations of colour than the human eye can notice – and the message can be stripped out at the receiving end. You can store a 64-kilobyte message in a 1024 X 1024 grey scale picture this way. Several public domain programs do this sort of thing.

Keys today are a minimum of 128 bits but should be progressing towards 256 bits. Eventually we may have a running key to work on the computer which actually incorporates a truly random, one-time key.

The art of deciphering has been brought to so great a state of perfection that there is no cipher so complicated as to bid defiance for many hours to the penetrating skill of the experienced decipherer.

As we become smarter in the use of technology we also become wiser in how to deceive it. Information is the source of income and can make or break a company. It pushes scientists to devise new ways to secure information and others the challenge and thrill to break the security so developed. But even with this state of technology available today there is no greater protection than a one-time key pad used only once and for a single purpose.

Cryptoanalysis

I have alluded to cryptoanalysis in a couple of places in this paper. Let us look at the meaning of the word. Cryptoanalysis is the process of determining the cipher key that was used for a message by analyzing the encrypted message. For example in 1863 the Prussian military officer Friedrich W. Kasiski used the method of analyzing the repetitions in the cipher text to determine the period of the cipher. For example take the phrase BACON AND EGGS OR EGGS AND BACON ina Vinegere cipher with a key of PIG:

Plaintext	BACONANDEGGSOREGGSANDBACON
Key	PI G P I GP I GP IG PI GP IG PI G P I GP I
Ciphertext	QI I D V GCLKVOYDZKVOYPVJQ I IDV

You will notice that the ciphertext holds two repetitious sequences, one of IIDV and the other of KVOY. Repetitions in the ciphertext occur when a plaintext pattern repeats itself as a distance equal to a multiple of the key length. For IIDV the sequence is 21 characters apart and for KVOY it is only six. this leaves a definite key length of three. [Note that you count the letters of one of the repeated sections.] This method, called the Kasiski method, has been used successfully in many instances through both world wars. It is also the basis for many automated "code cracking" systems.

This then is the basis for the need for continued vigilance in security for automated systems. The constant management of keys, their period of use, the length and frequency of change will determine the overall effectiveness of the procedures in place. We must always face the fact that encryption is there to temp, or challenge, the cryptoanalyist. To some it is a game of who can

outsmart whom, for others it is a avenue for test development, corporate espionage and/or revenue.

Forewarned is forearmed – so the saying goes. Be wise enough to know that if it is important enough to be kept secret then it should be stored in cipher and the key changed on a regular basis or use a one-time-pad. My interpretation is that if you don't want it to become common knowledge then you must put some protection on it. If you put it in an open area then someone will find it, even if it is only by accident.

Where the future will take us is anybody's guess but we can be assured that if there is a challenge then someone will take it up. The best security is a one-time-pad, for even today with all of the technology available to us we still do not know the results of the first and third cipher left by Thomas Jefferson Beale, or the true interpretation of some of the carvings left around the world on ancient stones.

Edgar A. Poe has justly said in his story of The Gold Bug, that "it may well be doubted whether human ingenuity can construct an enigma of the kind, which human ingenuity may not, by proper application, resolve" [Hughan and Hawkins, 1924].

REFERENCES

Denning, D.E.R. (1982) Cryptography and Data Security. Reading Massachusetts, Addison-Wesley Publishing Company

Entrust Technologies Limited (1998) Guide to the Business Impact of PKIs. Ottawa, Entrust Technologies Limited.

Hughan, W.J. and Hawkins, E.L. (1924) An encyclopaedia of Freemasonry and its Kindred Sciences. Chicago, The Masonic History Company pp150-151, 191, 490

Industry Canada (1998) A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society. Ottawa, Industry Canada

Pick, F.L. and Knight, G.N. (1955) The Freemason's Pocket Reference Book. London, Frederick Muller Limited p58

RSA Security Inc. (1999) A Guide to Security Technologies: A Primer for IT Professionals. Bedford Massachusetts, RSA Security Inc.

Schneier, B. (1996) Appllied Cryptography, Protocols, Algorithms and Source Code in C. 2nd Edition Toronto, John Wiley & Sons, Inc.

The Masonic Service Association (no date) Ritual Ciphers. Silver spring, Maryland, The Masonic Service Association

Tudhope, G.V. (no date) The Discovery of Francis Bacon's Cipher Signatures in James Anderson's Constitution of the Freemasons. Montana, Kessinger Publishing Company

Web Sites

Entrust Technologies www.entrust.com
Industry Canada Strategies http://strategies.ic.gc.ca/crypto
RSA Security www.rsasecurity.com
Jaws Technologies www.jawstech.com