GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

History of Encryption
Roger A. Prichard
January 26, 2002

Introduction:

One of the oldest forms of science that man has undertaken is Encryption. From prehistoric times to modern times it concerns the basic human desire to disguise, masquerade, or protect certain sensitive information from curious eyes. This is a trait that today is considered an absolute necessity to survive. This is normally achieved through substituting the characters, which make up the original message. This is accomplished by a method of characters prearranged by the sender and recipient so that, the message can be read only by the intended recipient, who possesses the correct key to unraveling its true meaning. The major problem with encryption is no matter how strong or complex the encryption scheme used is it all comes down to key management. The problem is and was with key exchange mainly its' securely and secretly. This paper will attempt to give a brief history of how and where encryption started and where it presently is and used in modern day.

Ancient Egypt:

There are several possibilities to exactly how encryption first started, but it is known that it did start in ancient Egypt. One of the beliefs of how encryption started is that the Egyptians wished to preserve the secrecy of the religious rituals from the casual observer or another reason is it might have been a political move to promote their religion. Then again it might have been to give their scripts/documents a formal appearance, unfortunately we will never know.

In the town of Menet Khufu a scribe, wanting to preserve his master's life, drew out the story of his master's life in hieroglyphics, and thus created the first form of Cryptography almost 4000 years ago. In 1900 BC a nobleman used a simple code of hieroglyphic substitution in the tomb of Khnumhotep, he did this by simply altering one symbol or character for another.[7] Since this was the first form of encryption the scribe only substituted hieroglyphs here and there instead of the entire document. As the civilization matured they continued to use transformed hieroglyphs in the writings and scripts, the only down fall was that they only changed certain characters instead of all of them. Since the encryption was so simple and primitive any viewer could figure out what the message read in a relatively short time and effort.

Greece:

One of the provinces in ancient Greece, Sparta used a form called the transposition cipher. This form incorporates changing the positions of the letters in the documents rather then changing the letters themselves.

In the fifth century BC the Spartans developed a system called Skytale, which did more than the simple transposition. The concept was very simple as compared to modern times, but was very complicated in their times. It consisted of a thin piece of papyrus wrapped around a round staff. The encryptor would simply write his message down the length of the staff when finished he would enwrap the papyrus. To any observer the message was unreadable and looked like scribble. The recipient of the message would first have to have an identical stick as the writer of the message, and would then rewrap the papyrus lining up the characters reviling the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

message. This method seems very simple to due since you only needed a round staff to break the message, but however in the fifth only a small percent of the population could read and write.

> The Greeks also provide one of the first literary references to cryptography. In "Iliad" by Homer, Bellerophon is sent to the king with a secret message telling the king to kill him. The king tried to send Bellerophon to his death by having him fight several mythological monsters, but he triumphed each time.[7]

Julius Caesar:

The first use of encryption for military purposes came when the Romans ruled the earth, over two thousand years ago. [8] Caesar needed a way to send communication documents to his troops in the field and thus developed a method called the substitution cipher. In this method he simply shifted the letters in the alphabet by three. Once again a very simple method by today's times, but very effective for its time.

Jefferson's Wheel Cipher:

One of America's greatest inventors was ahead of this time in 1795 when he came up with a cipher system that was later used in the United States Army from 1923 to 1942. However the odd fact concerning this was that the Army never knew about Jefferson's invention, they simply re-invented it calling it the M-64.

> This system used 26 wheels each with the letters of the alphabet arranged randomly around them. The key to this system was how the wheels were ordered around the axis. The users would then devise a code word, which corresponded to the ordering of the wheels. Once the order was devised, you can move the rows up and down until the message is spelled out. The recipient simply has to get the discs in the correct order, spell out the encrypted message, and then look around until he sees the plain message. [7]

Zimmerman Telegram:

In 1917 the British intercepted a German transmission that came across their communication lines. The British were able to decode the encrypted message and thus changed history more than any other cryptographer, past or present.

The telegram is now called the "Zimmerman Telegram" which was written by the German Foreign Minister Arthur Zimmerman to the German Minister of Mexico. The message contained an offer of United States Territory to Mexico if it joined the German cause. The telegram acted as a catalyst for the US as the British showed the telegram to the US in February 1917. On April 6, 1917 the U.S. Congress officially declared war on Germany and it allies.

Choctaw Codetalkers:

The United States in the end of WWI had a problem with their phone calls being intercepted by the German forces. To counterbalance this Captain Lewis a commander in the U.S. Army utilized the complex language of the Choctaw Indians. He employed eight Choctaw Indians, stationed them at certain command posts and any message that needed to be encrypted was encrypted in the native language of Choctaw. The German intelligence wasn't able to decrypt any of the messages, thus resulting in their retreat from the Mousse-Argonne campaign.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Never again was the Choctaw language used in any military effort, but then again there might be data that is still classified.

Trench Codes:

Following the massacre in the battle of Ovillers-la Boiselle in 1916, resulting in thousand of British soldiers, cause by a battlefield telephone call being intercepted by the enemy. General August Dubail of the French Army asked the cryptographers of that time to develop a kind of encryption to be used in the trenches of battle. The French office came up with a method that was called "carnet de chiffre". Any word that might give away troops positions or plans of an attack were in a notebook along with its code word.

> The Germans were about a year behind in developing these "trench codes," but they eventually caught up. In March 1917, the Germans, with a small code where certain bigrams, or combinations of two letters, replaced keywords or letters. These codes evolved into more notebooks, some of which were changed as often as every fifteen days towards the end of the war. The French referred to the codes as "KRUSA", since those were the five letters there invariably stated with. [7]

Superencipherment was a crucial difference between the French and German codes, which used encryption to encrypt something that was already encrypted. This form of encryption caused to the breaking of the German trench codes.

Enigma:

Developed by the Germans in World War II, the actual machine is built in a small wooded box that is small enough to be carried by a single soldier. When opened up the box reveals a small typewriter style keyboard. The actual encryption is completed by a set of three rotors, these rotors can be set to any letter of the alphabet, making the encryption key. The rotors are set to substitute one letter for any letter. By incorporating three sets of rotors this form makes it much stronger and more complicated then simple substitution.

In addition to the three rotors the machine had several additional security features to protect from being decrypted. There were five standard rotors, but only three could be used in the machine at one time, this result in a possibility of 60 different combinations. [10] The Germans would change the rotors and their stating positions every two days. There was also a plugboard included on the World War II version, this allowed the user to swap any letter for any other letter thus increasing the number of combinations of enigma settings by a factor of ten to the fifteenth power. The different branches of the German military used different types or versions of the enigma, thus creating add secrecy. If one version was compromised the other branches could still use theirs. An example of this is that the German Navy used four rotors instead of the standard three and instead of having only five rotors to choose from the Navy had eight rotors to choose from.

Cracking Enigma:

Every encryption involves math, and the Enigma system was very strong and very secure when used correctly. The only problem with the machine wasn't the machine itself but with the users becoming overconfident, thus giving away the ability to read their messages.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In 1930 the first advancements in cracking the enigma were made by the Polish. At this point in it's early history the enigma only used three rotors in six possible combinations. But once the Germans took control of its development in World War II the Polish were unable to crack it again. The first thing that the Germans did was to increase the total number of rotors to eight, which increase the rotor combinations to 60.

Alan Turning a young mathematician working for the British government took over where the Polish left off by building a machine called the Turing Bombe for deciphering the German version of the enigma. This machine is often called the foundation for the modern computer. The Bombe could crack the average enigma code in about fifteen hours as compared to several minutes with a modern computer. [10]

The Bombe took advantage of the weaknesses in the Germans to break the codes. One example of a mistake made by the Germans was that they seldom changed the wiring of the rotors. The rotor wiring is what determines which letter is substituted for which when the message goes through the encryption system. Another mistake was that the beginning of each message was often the same as the ones before.

Japan's Purple Encryption:

The PUPRLE as the United States cryptographers called it was a pure genius of ingenuity. As the British, Polish and French were busy in Europe, during World War II trying to crack the Engima of German, the United States was trying to decrypt the "PURPLE" as they called it. [7]

While the Engima used rotors the PURPLE used the stepping of telephone switches to due its' encrypting. By using the method of telephone switches, this allowed the encrypted message not to follow any traditional patterns of the modern day encryption schemes.

Without ever seeing the actual PURPLE machine or a single blue print but only seeing encrypted messages from it, William Friedman and his team developed an almost identical version of the PURPLE for decoding purposes only. A feat that on one thought was possible, since one of the most efficient things that the Japanese did was destroying their cryptographic equipment. To this date not one complete machine has been discovered.

SIGABA:

Often called the big brother of the German Engima the United States' version, called by the Navy ECM-Mark Two, incorporated fifteen rotors instead of three in the Engima. While the Enigma's rotors used a speedometer fashion, the used the "stepping maze" developed by Lt. Joseph N. Wenger of the United States Navy. This development made the movement of the rotors as close as random as they could be. What this method not only did one of the rotors move with each letter but four moved.

This machine was used in the closing days of World War II, about ten thousand of them were built and being used. One of the most amazing feats about this machine is that not one of these impressive machines fell into enemy hands. This was the only machine used to the war by any participant to remain totally unbroken for the duration of its use.

After the war the SIGABA remained in service until around 1959, and then was retired very slowly. These machines were systematically destroyed, and only a few exist today. The largest number is believed to belong to the National Security Agency (NSA). Compared to the secure methods in use in modern time, the SIGABA is extremely insecure. It would only take a matter of seconds for a modern supercomputer to break the SIGAMA.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Navajo Codetalkers:

During World War II people remembered the effectiveness of the enlisted Choctaw Indians and enlisted the Navajo Indians to speak important messages in their native language over insecure communications. The Navajo language is an unwritten language with no alphabet or symbols. The sound of the words makes it unintelligible to anyone who hasn't had the exposure to it. The Navajo language was only spoken in the Navajo lands of Southwest of America. At the time of the use of the Navajo language there was an estimated 30 non-Navajos who could understand the language and none of them were from Japan.

Philip Johnson was one of those non-Navajos that could speak and understand the language since he was raised on a reservation. During his service in World War I he learned how the military used the language of the Choctaw and was convinced that complexity and obscurity of the Navajo language could be utilized as well.

One of the amazing advantages to using the language was that it the Navajo people could do a task in twenty seconds that would normally take over 30 minutes to perform. [7] Encode, transmit and then decode a three-line message with a traditional encryption machine of the time. This speed was the convincing factor to use them for the Marine Corps. In all there were about 400 Navajos used as Codetalkers in World War II. It has been said that if it were not for the Codetalkers during the Battle of Iwo Jima the Marines would have never taken control of the island.

Despite the abduction of one of the Navajo Indians by the Japanese, who was not a Codetalker, the Japanese were never able to break the codes. They broke codes used by the Army, but were never able of crack the Marine Code. The abducted Indians were force to but could never translate the language, since the codetalkers used a special dictionary with their special military equivalents.

The program remained valuable much long after World War II, and was still classified. In 1992, an exhibit was opened in the Pentagon to commemorate the contributions of the Navajo to the allied victory in World War II.

National Security Agency:

Located near Washington D.C., this is the crypto logic organization of the United States Government. [8] In 1952 it was formed under presidential directive, and is charged with analyzing foreign transmissions and gaining intelligence and protecting United States information systems.

In the United States it's the largest employer of mathematicians. It's said that it has some of the most power computers in the world, it contains it's own chip fabrication planet for it's super powerful computers. These computers are used to achieve two main objectives: cracking enemy codes and protecting domestic secrets.

It's not known exactly how powerful and high tech these super computers are or what exactly they can do, but it is know that the NSA does have some limits to restrictions on what it can do and what it can't. They are not allowed to intercept domestic calls, if a NSA person is listening to a conversation and a citizen of the United States comes on line they must turn the monitoring equipment off immediately and log everything that had happened. Only with the FBI's permission can they monitor domestic calls for official investigations.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

National Institute of Standards of Technology:

It was until the 1960's before modern day companies starting getting into the act of creating and breaking codes. IBM's research group developed an encryption system called "Lucifer" which was a commercial success. The government felt that this was controversial since they believed that the public sector didn't need or deserve cryptography. It wasn't until 1973 that the government developed a National Bureau of Standards for encryption. Today it's better known as NIST, National Institute of Standards of Technology.

History of PGP:

It is a concept of where something is encrypted with one key and is decrypted with another. In 1976 two men by the names of Martin Hellman and Whitfield Diffe devised a new encryption scheme. [12] In the past it didn't matter how strong or complex the encryption scheme used was, all that mattered was the key management. Before 1976 the same key was used to encrypt and decrypt the message.

Then in 1977 a team of researchers from MIT developed an advance in the public key system called RSA, which stood for their initials Ron Rivest, Adi Shamir and Len Adleman. [11] One in which a user generated both keys, one of them a public key, which is distributed openly. Anyone can than use this key to send encrypted email to the key's owners. He would in turn use the second key, owned by him, as the private key to decrypt the message. When the NSA heard of their accomplishment they warned them not to publish the result as they dimmed it could be a significant threat to national security. They still published their document titled "New Directions in Cryptography".

Phil Zimmerman in 1991 was prompted to write PGP version one due to the fact the he was frightened by the restrictions of a bill that the United States Senate was busy trying to pass, Bill 266. The would have required all makers of encryption systems of insert trap doors into their systems so that the government could intercept and read communications.

What this PGP version did was to allow people to have two distinct keys, one that was kept secret and one that would be given away. If a message was encrypted with one it can only be decrypted with the other. This is one of the basic elements in key encryption and is also used in conjunction with an algorithm to determine how the possible communication will be encrypted and decrypted. It also allowed two new freedoms,

- To "sign" a message, guaranteeing to a recipient that in come from them. This is accomplished by encrypting the message with a private key, which only the sender knows. The only code that can decrypt the message is the public key, which the recipients know belongs to the sender. [7]

- To send someone a message so that only the recipient could view it. If it was intercepted, and the spy knew the public key used to encrypt the message, it could not be decrypted. Only the private key can be used to decrypt a message encrypted with the public key. The key used to encrypt a message cannot be used to decrypt it. [7]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The algorithm determines the over all plan for the way in which the encryptor will alter the original message, and then a key is used to select the actual pattern of encryption that will take place for the particular message.

The cryptography revolves once again around a math theory, no surprise here, that all non-prime numbers can be represented as a product of a unique set of prime numbers. All you have to do in order to break the system is find the prime factorization key. Sounds pretty simple doesn't it? That's when you get into key length. The key length pretty much represents how much effort an attacker must put in to find the correct key to decrypt a message, with a brute force attack. The larger the key the more combinations the attacker will have to try. The key length is usually described in bits and a 128-bit key allows for 300,000,000,000,000,000,000,000,000,000,000,000 different combinations give or take a few. [6]

Cryptography:

This is the study of encryption, which includes two types: symmetric and asymmetric. Symmetric cryptosystems use the same secret key to encrypt and decrypt a particular message and asymmetric systems use one key to encrypt the message and a different key to decrypt the message. Another name for this type is also public key cryptosystems.

There is one major problem with symmetric systems: how do you transport the secret key from the sender to the recipient in a secure fashion. This fix for this simple but in theory you shouldn't need to do anything since, if you could send the secret key securely then you wouldn't need the symmetric cryptosystem. The real solution to the problem is to use trusted couriers. This is why asymmetric is a more efficient and reliable solution.

In January of 1997 the National Institute for Technologies announced that it was in the need for a new Encryption Standard to replace the Date Encryption Standard (DES) as it was called. NIST challenged the public for submissions for new algorithms. In total 15 algorithms were submitted but after expert analysis they were narrowed down to 5 finalist, MARS, RC6, Rijndeal, Serpent and Twofish. After much debate and review of the finalists the experts selected Rijndeal for further review for the new adoption standard.

Issues of Protection of Data:

The American government had its real first view of the potential power of encryption in large-scale confrontations in World War II. Only then did we really begin to understand why governments were so keen upon monitoring the public. In 1987 the United States Congress passed the Computer Security Act. It didn't take many years before citizens of the US were criticizing the Government of violating their human rights. Some saw this as a political motive, while others saw this as a threat to science.

In other parts of the world as in Europe, it does not seem to be a potential concern. Take for example the "Euro-Encryption" which was being discussed in 1994 by the European Union to coordinate the interests of the state authorities for the scientific freedom to pursue intellectual research into encryption.

The other parts of the world have not seemed to pay as much attention or concern to the use of encryption. This maybe attributed to the fact that there has not been the significant localized development of encryption techniques in their area or the level of computer use where the governments should start the action of regulating encryption.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Summary:

This paper attempted to give you a brief history of the beliefs of how and why encryption started and where it is in present day, from the Ancient Egyptian form of simple substitution to the complexity of modern day algorithms with over billions of codes to try.

Although many non-computer people still think is was developed form the explosion of the Internet for shopping purposes, this is not the case. Over the worlds history encryption was needed for many reasons: to preserve someone's history, hide secret documents from the enemy's eyes, plan invasions, and of course for the personal security of one's credit card for shopping on the Internet.

For cryptographic innovation, wartime has always been and will be the leader in this field, from the Romans to our current day military. The military/government will continue to remain one of the main users of encryption on a regular basis.

Currently the government, privacy rights activists, and the computer industries are trying to decide the future of encryption. What path should be taken next? With the explosion of the Internet and e-commerce, it's critical that personal and government information be made secure from evil eyes. How secure is the question being asked, also what standards should be improved or developed, and for PGP how long should the key be? With the ever-increasing speed of computers for hackers and attackers to use, new schemes and plans need to be developed and deployed. Also should the government have access to keys that would allow them to decrypted messages/information for criminal purposes? All these and many more questions like this are currently being asked, but whatever the decisions are they will undoubtedly impact the privacy world wide in the 21st century.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. "The Advanced Encryption Standard" URL: http://www.cescomm.co.nz/cryptinfo/aes.html

2. "A Brief History of Encryption" URL: http://www.earthlink.net/internet/security/encryption/history.html

3. "History of Encryption" URL: http://www.cescomm.co.nz/cryptinfo/history.html

4. http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/akdeniz.htm#3.1

5. "Ethical Issues" URL: http://www.geocities.com/arudyanto/encrypt/ethics.html

6. "Questions About Cryptography" URL: http://www.cescomm.co.nz/cryptinfo/cryptoFAQs.html

7. "Introduction of Data Encryption" URL: http://www.geocities.com/arudyanto/encrypt/history.html

8. Clark, Brian, "Crytography" URL: http://www.trincoll.edu/depts/cpsc/cryptography/index.html

9. Clark, Brian, "Caesar" URL: http://www.trincoll.edu/depts/cpsc/cryptography/caesar.html

10. Clark, Brian "Enigma" URL: http://www.trincoll.edu/depts/cpsc/cryptography/enigma.html

11. Clark, Brian "RSA" URL: http://www.trincoll.edu/depts/cpsc/cryptography/rsa.html

12. Clark, Brian "PGP" URL: http://www.trincoll.edu/depts/cpsc/cryptography/pgp.html

13. Clark, Brian "Substitution" URL: http://www.trincoll.edu/depts/cpsc/cryptography/substitution.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.