Encryption: “A History of Secret Communication”

Introduction

Encryption is almost as old as writing itself. From its earliest beginnings over 4,000 years ago humans have attempted to conceal information that may be used by others. The use of encryption for military purposes has been one of the most significant driving forces in its development. The history of cryptology can be seen as a battle between cipher designers and analysts, as over time one gains the upper hand before the other retaliates. The advent of computers and the associated increase in processing power has seen many breakthroughs in the world of encryption and today encryption of sensitive data is an essential part of the business world as much as it is in military applications.

This essay will briefly examine the history of encryption from the ancient world to modern times and will highlight historical issues as they relate to today’s modern computing environment.

Ancient Egypt

Almost four thousand years ago in Egypt, a scribe drew out the story of his master’s life in hieroglyphics. At the same time though, he also brought into the world the first documented use of Cryptography (Kahn, 1996). The scribe used a simple code of hieroglyphic substitution, changing one symbol for another that was not as well known. The Egyptians had several letters that were often transposed in written communications and this fundamental form of encryption became more common as their civilisation matured.

The ancient Egyptian’s reasons for encryption are not known, but speculation has provided some possibilities. One possibility is that they simply wanted to give their documents a more formal appearance in a similar way that legal documents are formatted today. It is also possible that the Egyptians wanted to preserve the secrecy of certain religious rituals from the casual observer. By making the religious texts difficult for an outsider to read, they would make their religion enigmatic, but not forbidden. Since the mysterious usually provokes curiosity, encrypting texts could have been a political move to promote their religion.

Ancient Greece

In Sparta, one of the provinces of ancient Greece, one of the few uses of a transposition cipher can be found. In the fifth century BC, they used a system that consisted of a thin sheet of papyrus wrapped around a staff. This is now known as a “Skytale”. If a person wanted to send a message in secrecy, they could write it down the length of the staff so that when the papyrus was unwrapped, the message would be unintelligible. To read it the recipient would have to rewrap the papyrus with an identical stick. Only then would the letters line up.

Ancient Rome

“The earliest recorded use of Cryptography for a practical military purpose comes from Roman times during the Gallic Wars, over two thousand years ago” (Khan, 1996, pp83-84). The substitution cipher, or Caesar cipher is attributed to Julius Caesar
who shifted the position of letters by three, substituting the resulting letter for the original. By today’s standards Julius Caesar’s messages were not safe at all. Using modern computer technology, messages encrypted with the Caesar Cipher can be forcibly decoded in a matter of milliseconds.

The Middle Ages
Not much happened in Western culture during the dark ages although some use was reported by monks in the eighth to the tenth centuries (Brown, 2001). Roger Bacon is the only person known to have written about cryptography in his book "Secret Works of Art and the Nullity of Magic" in the mid thirteenth century. Moving into the middle ages one of the best-known names is Chaucer, who also included ciphers in his works.

Cryptanalysis was born amongst the Arabs with some early descriptions in 855, and a full discussion is in a fourteen-volume encyclopedia completed in 1412. The growth of diplomacy led to increasing use of, and attacks on, enciphered communications by the Spanish, Italians, Germans and others. Leon Alberti in the fifteenth century is regarded as the "Father of Western Cryptology" and is attributed with inventing polyalphabetic ciphers, the cipher wheel, and describing the principles of frequency analysis, which were documented in a number of manuscripts (Brown, 2001).

The Eighteenth Century
In 1795 Thomas Jefferson designed a cipher system that was later used by the United States Army from 1923 until 1942. In order to make his cipher Jefferson 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 user could devise a code word that corresponded to the ordering of the wheels. This system is considered quite secure against modern code breaking if the message is short and the code breaker does not know the ordering of letters and wheels.

The Impact of Radio on Encryption
In 1895 the first wireless radio was invented, giving rise to a new age in cryptography. Radioprovided military troops in World War I with much greater flexibility by eliminating the need to run telephone wires between camps and headquarters. However radio is public; anyone can intercept the signals. No longer was it necessary to tap a wire directly. Someone could simply put up a radio receiver and half the work was done. As a result cryptographers of World War One had to invent stronger systems of encryption to withstand an enemy’s best attack when a greater amount of encoded text is available.

In World War I, the French were the first ones to be prepared for the impact of radio on the breaking of enemy codes (Aaron, Christopher & Asher, 1999). By the time war broke out, France had established bases and outposts for the sole purpose of intercepting German communications. These outposts had been intercepting German messages during the peace and continued to do so into the war. Although they couldn’t decrypt them at first, the French stored all German transmission then, when decryption of messages became a reality, the French were able to decrypt the earlier messages and gain insight into what the Germans were thinking earlier in the war.

The French tackled the problem of where German troops were located in a very creative way. Although they had no idea what German messages said, they recorded
the strength of signal, the volume of messages, call signs, as well as any clear non-encrypted text that slipped through to determine the composition of the German forces. Their analysis resulted in a mostly accurate diagram of major German bases within two weeks of the outbreak of war.

Trench Codes
Thousands of British soldiers were injured in a battle of Ovillers-la-Boiselle in 1916, due to a commander’s battlefield telephone call being intercepted by the enemy (Kahn, 1996). Following that incident, a General of the French Army asked cryptographers to come up with some kind of encryption mechanism for telephone conversations to increase the security of battlefield telephone messages. The office of cryptography produced a notebook of ciphers. Any word that might give away troop positions or plans were in the notebook, along with a corresponding code. Whenever a telephone conversation would take place, the caller would be required to spell out these special words in code. The Germans started using trench code about a year later. A crucial difference between the French and German codes was something called superencipherment (encoding something already encoded). This gave the allies an edge, leading to the breaking of the German trench code.

American Indian Code Talkers
Towards the end of the First World War, the United States had an ongoing problem of phone calls being intercepted by German forces. One smart commander, Captain Lewis, realized that the languages used by American Indians were extremely complex and difficult to learn. He capitalized on the complexity as a code, employing eight Choctaw Indians during the final German push of the war. The Indians were stationed at command posts, and spoke important telephone calls in their native language, translating from and into English for their commanders.

In 1942, the Navajo Indians were used to speak important messages in their native language over insecure channels. The Navajo language is unwritten, and its syntax makes it sound unintelligible to anyone who hasn't had extensive exposure to it. It has no alphabet and no symbols. It was estimated at the time that there were only thirty non-Navajos who could understand the language. What convinced the Marine Corps to use Navajos though was the speed with which they could convey secure communications. Traditionally, with machine encryption, it would take thirty minutes to encode, transmit, and decode a three-line English message. The Navajos could perform the same task in twenty seconds (Aaron, Christopher & Asher, 1999).

Enigma
Quite possibly the most famous encryption device of all time, the Enigma Machine of World War II, was a German marvel of cryptography (Hinsley & Stripp, 1993). This electro mechanical device consisted of a complicated system of three rotors. The Enigma used by the German Forces during World War II included a plug board allowing the user of the enigma to swap any letter for any other letter at a location other than the rotors. The use of this plug board increased the number of combinations of enigma settings by a factor of ten to the fifteenth power.

Different branches of the German forces used different types of Enigmas. The Enigma used by the Navy was different from the Army, which was different from the Railway. Each branch had no idea what the other branch was using for its encryption.
This secrecy meant that if an enigma from one service were compromised, other branches would not have been overly concerned.

**Modern Times**

Modern systems can now have ciphers of vastly greater complexity than before, but are still built using the same foundations that can be traced back over four thousand years. The history of cryptology can be seen as a battle between cipher designers and analysts as over time one gains the upper hand before the other retaliates (Brown, 2001).

For e-mail encryption and signature, the current de facto standard is PGP (Pretty Good Privacy). PGP is also capable of local file encryption. During 1991, the United States Senate was working on Bill 266. If it had passed, this bill would have required makers of all encryption systems to insert trap doors into their systems so that the government could intercept and read all communications. Phil Zimmerman, alarmed by the restrictions this or a bill like it would place on the encryption community, was prompted to write PGP Version One.

In Australia, the major users of cryptography are those in government and business. In the business community, users are more likely to be found in larger businesses like banks, although there is no published data on usage. There is likely to be substantial growth in usage by small business and individuals, particularly as electronic commerce takes off (Pure & Taylor, 2001).

A number of widely available software applications include cryptographic routines. However, with the exception of banking applications, all software originating in the USA is crippled as regards crypto strength because of US exports restrictions.

Warfare has been the single biggest driver of developments in cryptology. The new look of war will be “bloodless, but deadly”. As Asia’s armies won’t be able to compete with the Western powers’ military might, they are preparing to fight wars via the Web, training crack teams of code-breakers with the skills to cripple nations. According to Desmond Ball, head of the Strategic and Defence studies Centre at ANU Canberra, “Intelligence budgets around the world have more than doubled in the last few years and much of that is electronic activity” (Bickers, 2001).

**Conclusion**

The beginnings of encryption can be traced back to Ancient Egypt over four thousand years ago and was widely used throughout the ancient world for many purposes but the need to protect sensitive military information was one of the main drivers in the development of this technology.

Developments during the middle ages were sparse, although writings about encryption began to increase leading to Leon Alberti, known as the “Father of Western Cryptology”, who published his works on encryption in the fifteenth century.

During the two World Wars, encryption became increasingly important as the human cost of sensitive data falling into the wrong hands became more and more apparent. The use of technology, such as the Enigma machine and innovations such as using
American Indians to code and decode messages, allowed significant advances and sophistication in military encryption.

With the advent of the computer age and the associated increase in processing power, encryption processes became even more powerful. The major uses for encryption still remains with the military but given the vast amounts of data that are now used by businesses around the world the need for encryption in industry and business is becoming more prevalent.

Warfare has been the single biggest driver of developments in cryptology. The new look of war will be “bloodless, but deadly” with battlefields created over the Internet rather than using mass force. The history of cryptology can be seen as a battle between cipher designers and analysts as over time one gains the upper hand before the other retaliates.
References


