A Brief History of Cryptography

By Tony M. Damico
٢٠٠٩, Vol. ١ No. ١١ | pg. ١/١
KEYWORDS:
Cryptography Cyber Security Codes Cipher Communication Encryption

The earliest form of cryptography was the simple writing of a message, as most people could not read (New World, ٢٠٠٧). In fact, the very word cryptography comes from the Greek words kryptos and graphein, which mean hidden and writing, respectively (Pawlan, ١٩٩٨).

Early cryptography was solely concerned with converting messages into unreadable groups of figures to protect the message's content during the time the message was being carried from one place to another. In the modern era, cryptography has grown from basic message confidentiality to include some phases of message integrity checking, sender/receiver identity authentication, and digital signatures, among other things (New World, ٢٠٠٧).

The need to conceal messages has been with us since we moved out of caves, started living in groups and decided to take this civilization idea seriously. As soon as there were different groups or tribes, the idea that we had to work against each other surfaced and was proliferated, along with rank violence, secrecy, and crowd manipulation. The earliest forms of cryptography were found in the cradle of civilization, which comes as no surprise, including the regions currently encompassed by Egypt, Greece and Rome.

As early as ١٩٠٠ B.C., Egyptian scribes used hieroglyphs in a non-standard fashion, presumably to hide the meaning from those who did not know the meaning (Whitman, ٢٠٠٥). The Greek's idea was to wrap a tape around a stick, and then write the message on the wound tape. When the tape was unwound, the writing would be meaningless. The receiver of the message would of course have a stick of the same diameter and use it to decipher the message. The Roman method of cryptography was known as the Caesar Shift Cipher. It utilized the idea of shifting letters by an agreed upon number (three was a common historical choice), and thus writing the message using the letter-shift. The receiving group would then shift the letters back by the same number and decipher the message (Taylor, ٢٠٠٢).

The Caesar Shift Cipher is an example of a Monoalphabetic Cipher. It is easy to see why this method of encryption is simple to break. All a person has to do is to go down the alphabet, juxtapositioning the start of the alphabet to each succeeding letter. At each iteration, the message is decrypted to see if it makes sense. When it does appear as a readable message, the code has been broken. Another way to break Monoalphabetic ciphers is by the use of what is known as frequency analysis, attributed to the Arabs circa ١٠٠٠ C.E. (New World, ٢٠٠٧). This method utilizes the idea that certain letters, in English the letter "e," for instance, are repeated more often than others. Armed with this knowledge, a person could go over a message and look for the repeated use, or frequency of use, of a particular letter and try to substitute known frequently used letters (Taylor, ٢٠٠٢).

As for the Greek method of using a stick, once the method was known, it was a simple matter of trying out sticks of different diameters until the message became readable.

The art and science of cryptography showed no major changes or advancements until the Middle Ages. By that time, all of the western European governments were utilizing cryptography in one form or another. Keeping in touch with ambassadors was the major use of cryptography. One Leon Battista Alberti was known as "The Father of Western Cryptology," most notably due to his development of polyalphabetic substitution. His method was to use two copper disks that fit together. Each one of them had the alphabet inscribed on it. After every few words, the disks were rotated to change the encryption logic, thereby limiting the use of frequency analysis to crack the cipher (Cohen, ١٩٩٠). Polyalphabetic substitution went through a variety of changes and is most notably attributed to Vigenere, although Rubin claims that he in fact had nothing to do with its creation. Rubin further points out that the use of the cipher disks continued in the Civil War, with the South using brass cipher disks, although the North regularly cracked the messages (٢٠٠٨).

Gilbert Vernam worked to improve the broken cipher, creating the Vernam-Vigenere cipher in ١٩١٨, but was unable to create one of significantly greater strength. His work did lead to the *one time pad*, which uses a key word only once, and it proved to be near unbreakable (Rubin, ٢٠٠٨). Whitman reports that criminals used cryptography during prohibition to communicate with each other.

Additionally, it is important to mention the recently popularized "windtalkers." The Navajo's used their own language as a basis for cryptography (٢٠٠٥). The code was never broken and was instrumental in the victory in the Pacific Theatre during WWII. An argument could be made that the spoken language was not technically cryptography, but it should be noted that at every communication, the message was written down as a matter of procedure.

In modern times, the public key method of cryptography has seen wide adoption. The use of a common public key and a private key held only by the sender is in use today as a form of asymmetric encryption; one of the uses of this method is for the sender to use the private key to encrypt the message and then anyone who receives the message uses the public key to decipher it. In this way, the receiver knows who the message had to come from.

This method makes up the backbone of the Digital Signature. Problems arise when communications between multiple organizations require the use of many public keys and knowing when to use which one. No matter which method is used, a combination of methods applied one after the other will give the best result (Whitman, ٢٠٠٥).

In conclusion, it is somewhat surprising how limited the history of this very important topic is. No doubt cryptography and in a greater sense, cryptology, has played an enormous role in the shaping and development of many societies and cultures. While history may paint a different picture, the fact that the winners often write history is worth noting. If an army has a strong weapon that was instrumental in providing information that led to success, how apt are they to reveal it in the records of the wars? Instead, it may seem better to have idolized heroes than to reveal the cloak and dagger methods that actually led to success. Crpytography, by its very

nature, suggests secrecy and misdirection; therefore, the fact that the history of this topic is short and somewhat inaccessible is of no great surprise. Perhaps it is itself coded in what is has already been written.

References

Cohen, F (١٩٩٠). A short history of cryptography. Retrieved May ٤, ٢٠٠٩, from http://www.all.net/books/ip/Chap٢-١.html New World Encyclopedia (٢٠٠٧).

Cryptography. Retrieved May ٤, ٢٠٠٩, from http://www.newworldencyclopedia.org/entry/Cryptography

Pawlan, M. (١٩٩٨, February). Cryptography: the ancient art of secret messages. Retrieved May ٤, ٢٠٠٩, from http://www.pawlan.com/Monica/crypto/

Rubin, J. (٢٠٠٨). Vigenere Cipher. Retrieved May ٤, ٢٠٠٩, from http://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html

Taylor, K. (٢٠٠٢, July ٣١). Number theory ١. Retrieved May ٤, ٢٠٠٩, from http://math.usask.ca/encryption/lessons/lesson٠٠/page١.html

Whitman, M. & Mattord, H. (٢٠٠٥). *Principles of information security*. [University of Phoenix Custom Edition e-text]. Canada, Thomson Learning, Inc. Retrieved May ٤, ٢٠٠٩, from University of Phoenix, rEsource, CMGT/٤٣٢