RESEARCH ARTICLE | APRIL 02 2019

Cryptographic methods and development stages used throughout history

Ender Sahinaslan ✉; Onder Sahinaslan

AIP Conf. Proc. 2086, 030033 (2019)
https://doi.org/10.1063/1.5095118

Cryptographic Methods and Development Stages Used Throughout History

Ender Sahinaslan[1, a)] and Onder Sahinaslan[2, b)]

Maltepe University, Information Technology, Istanbul, Turkey

[a)]Corresponding author: dr.endsa@gmail.com
[b)]ondersahinaslan@maltepe.edu.tr

Abstract. Throughout history the need for secrecy has been important. This need for secrecy brought about the invention and the art of concealment, coding and code making [1]. As early as 1900 B.C., Egyptian scribes used hieroglyphs in a non-standard fashion, presumably to hide the meaning from those who did not know the meaning [2]. Cryptography is the effect of designing privacy requirements systems in communication [3]. From the past to the present, many classical encryption methods such as Caesar, Vigenere, and Enigma have been replaced by more powerful modern new encryption methods such as DES, RSA, PGP, AES, and SHA-3.

This study aims to present chronologically together about major cryptography methods and developmental stages in the history of cryptology.

Keyword: History of cryptology, cryptography, steganography, cryptanalysis, data security, public-key
Mathematics subject classification: 97R40, 94A60, 11T71

INTRODUCTION

The basis of cryptology is mathematics, which is essential for ensuring communication security. The information that mankind shares with someone but wants to keep a secret against others has always existed. There will also exist. So how is this provided? When we make a study through history, we see that people have developed a number of cryptographic methods in the context of the possibilities in their time. The first was a set of signs and shapes used to describe a number of threats and dangers. In the course of time, the invention of writing, developments in mathematics and information technology have accelerated the change in encryption methods and devices and spread the usage.

HISTORY OF CRYPTOLOGY FROM PAST TO PRESENT

It can be seen from the date of cryptography that some information or documents have been transferred, whether official or informal. Probably since the first day of mankind, people have felt the need to hide some private information from someone else, even if it's not called 'password' on that day. Again, in the conditions of that day, according to their own knowledge and experience to develop and use a number of methods to meet this need.

Cryptology in pre-Christ Period

The history of cryptology dates back to BC 1900. One clerk used non-standard hieroglyphic signs in the inscriptions he wrote to tell the life of his master in Egypt. Although this system is not a 'secret writing system', some hieroglyphic symbols have never been used in the text. However, little is known about this oldest attempt in

International Conference of Mathematical Sciences (ICMS 2018)
AIP Conf. Proc. 2086, 030033-1–030033-4; https://doi.org/10.1063/1.5095118
Published by AIP Publishing. 978-0-7354-1816-5/$30.00

encryption. After that, it is observed that for centuries, cryptography has not shown much improvement, or there is still no healthy information reaching us.

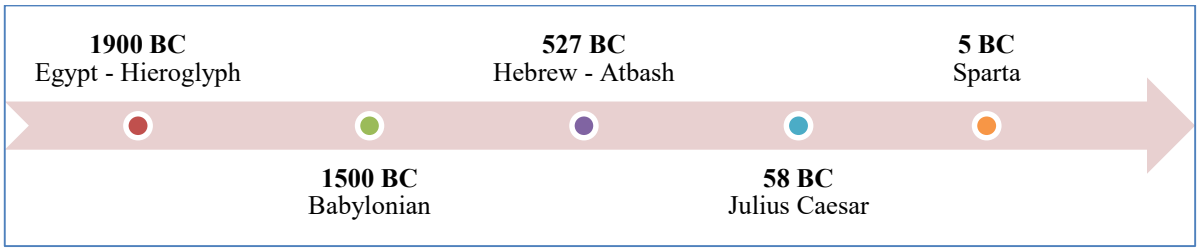

FIGURE 1. Cryptology timeline of the period before Christ

A Babylonian cuneiform tablet, dating from about 1500 BC, contains an encrypted recipe for making pottery glaze. This example more likely represents the occurrence of ciphers in this part of the world as this example would be fairly trivial [4]. B.C. In 527, Hebrew, when writing the book of Jeremiah, used a 'secret', sometimes known as 'Atbash', or a simple code to hide. This code was in the form of an alphabet changing the first letter and the last letter. This was one of the few Hebrew rules.

The first important use of cryptography is the relocation code. This was described by the Greek writer Polyibus as a substitution technique [6], but his military use was developed by the Roman Emperor Julius Caesar (58 BC). Caesar communicated with his commanders through this encryption method. Messages are encrypted by replacing the letter in the text with one of the three positions to the right. For example, the word ENDER was changed to HQGHU. This password method could easily be broken by the frequency analysis of the letters used in the text, but it was not known at that time. This method was used in the need of the Great Roman army and was used for hundreds of years. This method was broken with the frequency analysis of the alphabet by the Arabic mathematician of the famous Muslim philosopher Al-Kindi. So Al-Kindi is considered the first code breaker [7].

In the 5th century BC, the first displacement system was introduced by a method developed by Sparta. For this reason, the first nation to use cryptography in military communication is referred to as Sparta. The developed device consisted of a wooden roller of a certain thickness and a papyrus or a thin, leather band that was bent around the cylinder. The hidden message was written over the roll along the roll, and then the strip was unwound from the cylinder and transmitted to the desired target. Here, the diameter of the cylinder served as a key to the encryption and resolution of the text.

Classical Cryptology, Period before World War II

When the period after Christ is examined, a new study or work is not encountered for a long time. II. Important stages of cryptology from the period until the end of World War II are summarized in Figure-2.

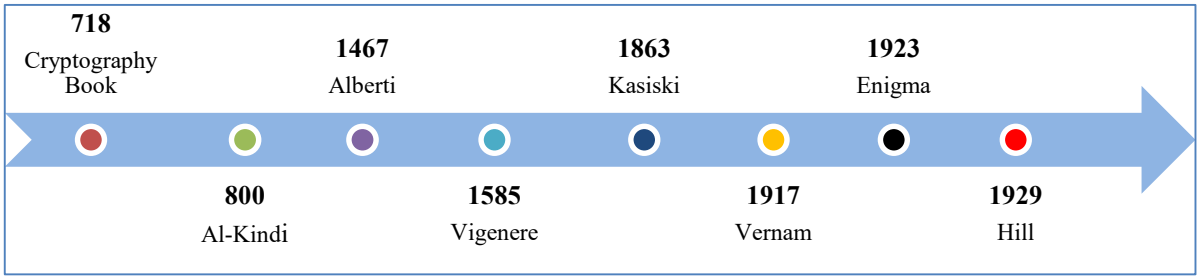

FIGURE 2. Cryptology timeline of the period before World War II

In Europe, no secret correspondence has been conducted until the Middle Ages on cryptoanalysis. The first serious cryptoanalysis studies were conducted by the Arabs. The Arabs began their studies of cryptography in literature and mathematics in the AD 600s. The English word 'cipher' and the French word 'chiffre' are used in Arabic (cifr or cifir). The first work of the Arabs on cryptography was written by Abdurrahman al-Khalil Ibn Ahmad by Kitab-ul Muamma in 718 AD. In this book, Abdurrahman al-Khalil gives the solution of a Greek cryptic letter

sent by the Byzantine emperor [8]. Ciphertexts produced by a classical cipher (and some modern ciphers) always reveal statistical information about the plaintext, which can often be used to break them. After the discovery of frequency analysis perhaps by the Arab mathematician and polymath, Al-Kindi (also known as Alkindus), in the 9th century, nearly all such ciphers became more or less readily breakable by any informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles. Al-Kindi wrote a book on cryptography entitled Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages), in which described the first cryptanalysis techniques [1, 9, 10].

In 1467, the Italian Leon Battista Alberti developed a cryptographic mechanism consisting of two intertwined disks, known as the father of cryptography. There were 24 cells in this mechanism and the device was the first example of the transition from single-alphabet encryption to alphabet encryption systems. In 1596, Anthony Babington wrote letters that he had encrypted using his personal password. However, after the deciphering of the password, learning about the assassination plan for Queen Elizabeth II caused Babington to be executed. This has prevented the use of cryptography for some time [11, 12].

In 1585 the Vigenère crypto method was invented by Frenchman Blaise de Vigenère. The encryption system using this standard alphabet is also known as Vigenère Frame. Two or more alphabets are used to encrypt data. In other words, letters are shifted in different amounts using a word or phrase as the encryption key. This method has been used in different ways for hundreds of years. In 1854, Charles Wheatstone developed a system that digraphic, that is, the letters are encoded in pairs and the result is dependent on both letters.

In 1863, Friedrich Kasiski developed a test that broke this method. This method, also known as Kasiski test in literature, is based on estimating the duration of the password key, starting from the distance between the syllables which are more frequent than expected in the encrypted text. In 1917, Gilbert Vernam invented the teleprinter cipher, which used a key on paper tape to be added with regular words to encrypt phrases. Praised by the NSA as one of the greatest inventions in cryptology, the Vernam Cipher is known as the world's first unbreakable cipher [12]. Perhaps the most famous cipher of the classical crypto era, the Enigma machine was developed by Arthur Scherbius in 1918. II. It was used by German Intelligence during World War II. The Enigma machine is an essentially complex substitution encryption machine. It consists of a plug board, light board, a rotor set and a reflector [13].

The Hill Cipher is a classical symmetric-key cipher that was published by Lester Hill in 1929 [14]. The Hill Cipher represents each plaintext as a vector of integer values, and encrypts this vector using a single multiplication by a square key matrix. This has the advantage of simplicity, but renders the cipher vulnerable to a straightforward known-plaintext attack based on linear algebra [15].

Modern Cryptology in the Computer Era

Advances in both computer and mathematics have led to the discovery of more secure and useful new methods in the field of modern cryptology. Figure 3 shows important improvements in this area.

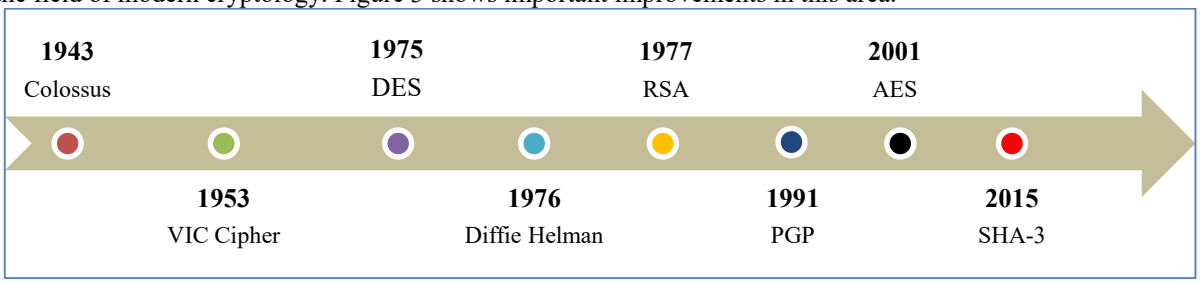

FIGURE 3. Cryptology timeline of the period after computer era

In 1943 two British inventors developed Colossus, the world's first digital electronic computer. It was intended to help the cryptanalysis of German messages during World War II, and by breaking the messages sent at that time, it reached its goal to a great extent. VIC Cipher is used by Soviet spies in the world since 1953. The VIC password is considered the most complex modification of the family of Nihilist passwords. It is considered to be one of the strongest passwords that can be used manually without a computer [16].

Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s. In recent times, IBM personnel designed the algorithm that became the Federal (i.e., US) Data Encryption Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm [17]. The RSA algorithm was published in 1977 in Martin Gardner's Scientific American column. Since then, encryption has been widely used in many areas such as communication, computer networks, information security, banking and e-commerce. Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics [10].

One of the modern cryptography systems produced by Phil Zimmermann in 1991, PGP is widely used to encrypt and decrypt e-mails especially over the internet. It can also authenticate messages. AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits[18]. SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. [19]. Although part of the same series of standards, SHA-3 is internally different from the MD5 -like structure of SHA-1 and SHA-2 [20]. Modern cryptology will continue with new methods and solutions.

CONCLUSION

Cryptology has always existed throughout history, changing shapes and methods, and then there will be. In order to understand and develop new generation methods, it is necessary to know the past and its development well. This study can be used initially as a reference source for researchers and developers working in this field.

REFERENCES

1. The Code Book. The Secret History of Codes and Code-Breaking. Simon Singh 1999
2. Whitman, M. & Mattord, H. (2005). *Principles of information security*. [University of Phoenix Custom Edition e-text]. Canada, Thomson Learning, Inc. Retrieved May 4, 2009, from University of Phoenix, resource, CMGT/432
3. Trappe, W. ve Washington, C., 2002. Introducing to Cryptography with Coding Theory, New Jersey: Prentice Hall
4. James J. Tattersall. Elementary Number Theory in Nine Chapters. Cambridge University Press. (|210|, 1999). ISBN: 0521585317
5. Kahn D., *The Codebreakers*, Macmillan, 1967, pp.82
6. Cohen F., Short History of Cryptography, 1995, retrieved 8 June 2010
7. Al-Ehwany, Ahmad Fouad. (1961). "Al-Kindi" in A History of Muslim Philosophy Volume 1. New Delhi: Low Price Publications. pp. 421-434.
8. Babaoğlu A., "Kriptolojinin Geçmişi", Bilim ve Teknik, TÜBİTAK, July 2009, N:500 , pp 24-27
9. Ibrahim A. Al-Kadi (1992), The origins of cryptology: The Arab contributions, Cryptologia 16 (2): 97–126
10. Al-Vahed A., Sahhavi H., An overview of modern cryptography, World Applied Programming, Vol (1), No (1), April 2011. 55-61, ISSN: 2222-2510
11. http://5010.mathed.usu.edu/Fall2014/KKing/sigmary.html, Date of access : July 2018
12. https://www.timetoast.com/timelines/the-history-of-cryptography, Date of access : July 2018
13. http://www.counton.org/explorer/codebreaking/enigma-cipher.php, Date of access : July 2018
14. L. S. Hill, "Cryptography in an algebraic alphabet," American Mathematical Monthly, vol. 36, no. 6, pp. 306–312, 1929.
15. W. Stallings, Cryptography and Network Security, 5th ed., Boston: Prentice Hall, 2011.
16. http://www.crypto-it.net/eng/simple/vic.html?tab=0, Date of access : July 2018
17. Diffie W., Hellman M., "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT- 22, Nov. 1976, pp: 644–654.
18. https://aesencryption.net/, Date of access : July 2018
19. Hernandez, P., (2015). "NIST Releases SHA-3 Cryptographic Hash Standard"
20. https://en.wikipedia.org/wiki/SHA-3, Date of access : September 2018