HISTORY OF CRYPTOGRAPHY

Cristian GRUBÎI, Liviu CHIRTOACĂ*, Augustin PLOTEANU

Department, of Software Engineering and Automation, Group FAF-233, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova, Chișinău, Republic of Moldova

*Corresponding author: Liviu Chirtoacă, liviu.chirtoaca@isa.utm.md

Abstract. *Cryptography represents the usage of ciphers to hide a certain message ensuring that only the intended recipient can read it. This paper provides an overview of the history of cryptography spanning from its ancient origins to modern-day encryption methods. It goes through important turning points like Polybius Square in Greece, the invention of the scytale in Sparta, and the development of rotor-based electromechanical machines, such as Enigma and SIGABA, during World War II. It goes over the ongoing fight for information security, from the weaknesses of antiquated techniques to the intricate machinery of World War II and the ultimate necessity for higher encryption standards. With the development of the Data Encryption Standard (DES) and its successor, the Advanced Encryption Standard (AES), the investigation carried into the Cold War era. The final section of the paper focuses on modern cryptography, emphasizing the importance of public key algorithms and the ongoing search for safe communication techniques. The paper emphasizes how public key cryptography replaced conventional symmetric ciphers, but it also discusses the difficulties in establishing safe key exchanges and the ongoing search for perfect encryption. Through an analysis of the historical evolution of cryptography, the paper underscores its relevance historically, the progress made in technology, and the ongoing search for safe means of communication.*

Keywords: *Cipher, Decryption, Encryption, Key, Security*

Introduction

Cryptography is the practice of concealing information through the use of ciphers, ensuring that only the intended recipient can access the original information. This process safeguards sensitive information from unauthorized access or interception, facilitating secure communication channels. The creation of cryptographic algorithms for encoding data and the analysis of these algorithms for potential vulnerabilities, known as cryptanalysis, collectively form cryptology, the broader study of secure communication methods.

During its six-millenia known history, cryptography has evolved in many ways, adapting to the progress made in technology. This evolution underscores cryptography's indispensable role in safeguarding sensitive information from ancient times to an ever-changing digital landscape [1, 2].

Ancient Cryptography

The first traces of cryptology date back to about four millennia ago, when an accomplished scribe, in a town from ancient Egypt called Menet Khufu, inscribed hieroglyphs detailing his lord's life. The inscriptions were completed in the main chamber of nobleman Khnumhotep II's tomb, which is depicted in Fig. 1. There was no intention of secrecy, nor was it intended to be difficult to read, however it did introduce a transformation of writing, another element of cryptography, with the aim of bestowing a sense of nobility and sovereignty. In other words, the common symbols were replaced with unique hieroglyphs [3].

Figure 1. Inscriptions in the main chamber of the tomb of the nobleman Khnumhotep II

As the Egyptian society evolved, writing in transformed manners became more complicated, but also more common. In the end, some of these transformations replaced the original letters. Intention for secrecy increased, especially for religious texts. Impressing the reader became one of the main goals of such writing, yet the effect was the opposite: a total lack of desire from the reader. Therefore, the start of cryptology is a form of quasi cryptology, meaning that it lacked the properties of security, but it did include 2 of its main elements: secrecy and transformation [3].

The next example of cryptography comes from ancient Assyria (~1500 BC), where merchants used intaglio, a carved stone tablet with images and text to identify themselves in trading transactions. Today this is known as a "digital signature". The public knew that a particular "signature" belonged to a particular trader, but only he had the intaglio to produce it [4].

The first system of military cryptography was introduced in Sparta, from as far back as the 5th century B.C. The Spartans used a device known as scytale, a cylindrical staff around which narrow ribbons of parchment were winded. The message was then inscribed on the parchment and the ribbon was unwound. The message could be read only after being rewrapped on a cylinder of exactly the same size, so that the letters would appear in their initial order [3, 5]. The device is shown in Fig. 2.

Figure 2. Spartan Scytale

A century prior to Caesar's Cypher, a Greek historian named Polybius formulated a tool which is broadly classified as a form of cryptographic manipulation, called the "Polybius Square". It consists of a two-dimensional table filled with letters, for which a pair of numbers: the indexes

of the row and column, are assigned. The junction of these numbers represents the position of the letter in the table [3, 6]. Table 1 is a representation of the original square, which used the Greek Alphabet. As an example, the plaintext "ΗΙΣΤΟΡΥ" would be converted to 22 24 43 44 35 42 45.

Table 1

Polybius Square

	1	**2**	**3**	**4**	**5**
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

An ancient cryptographic technique which might not be widely used today, but it is still well-known is Caesar's Cipher. It is a kind of monoalphabetic substitution cipher, where each plaintext letter is replaced by a ciphertext, consisting of letters situated three places further down the alphabet. For instance, A is substituted by D, B by E, and so on.

Renaissance Cryptography

After the Roman Empire's fall, cryptology was seldom used until the Renaissance era. One of the first popular examples is Leon Battista Albert's cipher disk. Alberti, in his paper about cryptanalysis, introduced the concept of frequency analysis, claiming that it is entirely his own idea, however, the theory was considered too developed for this to be the case. His text on cryptanalysis expressed that ciphers are solved based on letter characteristics in the Latin language. The main idea is that vowels are essential in forming syllables, and they individually outnumber the consonants.

Following an explanation of cipher solving, Alberti designed a device to prevent decoding of ciphertext – a cipher disk. This is the first occurrence of the concept of polyalphabetic ciphers, where multiple substitution alphabets are used. The disk is formed from a larger stationary disk, containing the plaintext letters, and a movable inner disk, including their ciphertext meaning. The message sender and receiver must possess identical devices and agree on an index for the inner ring, which is to be placed against the corresponding outer ring letters. In addition, Alberti mentioned that after a few words, the index may change, and therefore provide "new meanings" [3].

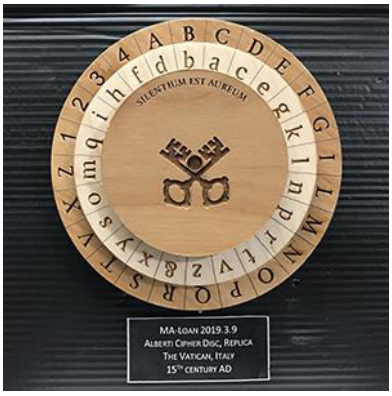

Figure 3. Alberti Cipher Disk

In the 16th century, Gerolamo Cardano, an Italian mathematician, invented the first "autokey" system. He used the plaintext as a key to encode itself, starting it over for each word. In spite of this being a brilliant concept, it contained significant flaws, such as multiple potential decipherments for the same ciphertext letter and vulnerability due to an adversary's ability to obtain the plaintext without difficulty after deducing the first word [3].

Several decades later, French diplomat Blaise de Vigenère, introduced another form of an autokey system, with notable improvements to Cardano's version. The first key letter, known to message sender and receiver, called "priming key", was used to determine the first plaintext letter. The decipherer could then use the obtained plaintext letter as the key for the following letter, and so on for each letter. In contrast to Cardano, Vigenère did not start over the key for each word [3]. The cipher text was obtained using a table similar to the modern version presented in Fig. 4. Each ciphertext letter is determined by the intersection of two coordinates: key and plaintext letters.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 4. Vigenère Table

Cryptography after WWI

Following World War I, the nations involved wanted a faster, more efficient and more secure way of ciphering and deciphering messages. This led to the development of rotor-based electromechanical machines which would cipher text using several substitution ciphers. An electromechanical rotor is a disk with 26 electrical contacts on both sides. These contacts are interconnected randomly, so when an electric current is applied to one contact, it emerges at another, creating a monoalphabetic substitution cipher. To increase security, rotors are designed to rotate after each letter, presenting a different substitution alphabet. This rotation, combined with multiple rotors, significantly increases the complexity of the cipher. For instance, pairing two rotors produces 26^2=676 mixed cipher alphabets, while three rotors yield 26^3=17,576, and so on, making the message much harder to decrypt [6].

These kinds of machines were used by both sides during World War II. All branches of the German armed forces started using the Enigma machine in the 1920s. The Enigma is a self-inverse machine, meaning that the same procedure is for both encryption and decryption, this being one of its weaknesses. In addition to the set of three rotors, the machine had a half-rotor which connects 13 electrical contacts on one side of the rotor to the other 13 contacts, preventing any letter from encrypting to itself. Finally, it contained a plugboard which connects 6 to 10 pairs of letters, adding about 150 trillion combinations to the period. When a key is pressed, the signal passes through the plugboard, rotors, reflector, plugboard again, and finally illuminates a lamp to display the ciphertext or plaintext letter.

To operate the Enigma, two or three operators were needed. In cases where three operators were involved, one would read the plaintext, the second would type and announce the cipher letter, and the third would record the ciphertext for transmission via Morse code.

The Enigma required two keys to be set up for use: the day key and the message key. The day key consists of five parts: the position of the rotors, the plugboard settings, the turnover positions of each rotor, the identification of the network and the starting position of each rotor. This key was changed monthly. The message key is the rotor setting for the current message. Operators set the day key, encrypt three random letters as the first three message letters, then reset the rotors accordingly. On the receiving end, operators set the day key, type the first three message letters to recover the message key, and reset the rotors to decrypt the rest of the message [6].

In September 1932, Polish mathematicians began working on breaking the German Army Enigma. By early 1933, they could read increasing numbers of German Army Enigma messages. Their breakthrough was based on using the mathematical theory of permutations for key recovery and the daily keys sold by a German traitor. In September 1938, the Germans changed Enigma settings, rendering the Poles' decryption methods ineffective. In December of the same year, they added two more rotors, increasing complexity tenfold. This change expanded rotor position possibilities from six to sixty. Additionally, they increased plugboard connections from six to ten, further complicating decryption. In the summer of 1939, the Poles shared their knowledge with the Allied countries [6].

In November 1939, British mathematician Alan Turing proposed a new approach to cracking the Enigma code. Rather than focusing on finding specific rotor settings and positions, Turing devised a method to eliminate incorrect possibilities more efficiently. He designed a machine called a bombe, inspired by the Polish version, which used probable words in ciphertext, called cribs to identify rotor settings, rotor order, and plugboard settings. The bombe checked if the crib and ciphertext could be transformed into each other, reducing the number of key possibilities for manual testing. The first bombe was delivered in March 1940, and soon dozens were operational at various sites. This breakthrough significantly accelerated the recovery of Enigma's daily keys, aiding in decrypting messages throughout the war [6].

SIGABA, also known as ECM Mark II, is a multi-rotor electromechanical cipher machine which was developed in 1934 and used by the US Army and US Navy during World War II. There is no publicly known successful cryptanalysis of the machine during its service lifetime.

It contains five cipher rotors, five control rotors, and five index rotors. The cipher and control rotors, interchangeable, have 26 contacts and are inscribed with the alphabet. The index rotors, with 10 contacts each, are labelled with sequential numbers 10-59. When a key is pressed, an electric current travels through a contact in the cipher rotors, producing the ciphertext letter as the output signal. Depending on the outputs of the control and index rotor groups, one or more of the cipher rotors will then rotate. The control rotors accept four signals and can output up to four signals, which are then gathered into ten groups serving as inputs to the index rotors. Among the five control rotors, the two outer ones remain stationary, while the inner three rotate similarly to a three-rotor Enigma.

The ten groups connect the output contacts using logical OR to generate the signal in the following manner 1: A 2: B 3: C 4: D, E 5: F, G, H 6: I, J, K 7: L, M, N, O 8: P, Q, R, S, T 9: U, V, W, X, Y, Z 0: is grounded.

The index rotors accept the ten signals and direct them through the five rotors. These index rotors remain stationary, and their outputs are combined logically in pairs. The output signals from the index rotors trigger the rotation of the cipher rotors. Following each key press, at least one cipher rotor and up to four may rotate. The control rotors dictate the number of steps taken by each cipher rotor.

This irregular stepping of the rotors is the key to SIGABA’s security because it eliminates the predictable succession of cipher alphabets that machines like the Enigma produce. Once the rotor wiring of an Enigma is known, the next alphabets can be predicted. That is much more difficult to do with a SIGABA [6].

Cryptography after WW2

A new era in cryptography began during the Cold War, when the USSR and the US acknowledged the vital need of information security. The establishment of agencies devoted to information security and warfare resulted in the creation of the Data Encryption Standard (DES) in 1979, which was utilized for confidential communications until 2005. However, by today's standards, the 56-bit DES key became insecure.

With block lengths and key lengths up to 256 bits, the Advanced Encryption Standard (AES) superseded the Data Encryption Standard (DES) in 2000, providing enhanced security. Because of AES's dependability and quickness in online communication, it has become the industry standard for encryption.

Secure key exchange is difficult because symmetric ciphers like DES and AES require the sender and recipient to have the same key. Diplomatic pouches were used by diplomats as a secure means of exchanging secret keys. This is consistent with the Kerckhoffs principle, which states that the key, not the algorithm, should be the only factor determining a cryptosystem's security.

The maximum level of security is offered by the one-time pad, which generates ciphertext that looks like random noise and has a key as long as the message. The tricky part is actually safely trading the key.

Whitfield Diffie and Martin Hellman's invention of public key cryptography in 1976 was a significant advancement. By using two distinct keys for encryption and decryption, this method enables users to keep the decryption key secret while publishing the encryption key. The invention of RSA by Rivest-Shamir-Adleman made public key cryptography far more advanced. Key exchange methods were further revolutionized with the introduction of elliptic curve cryptography, which provided faster and smaller key sizes.

The flexibility with which public and private keys can be applied to enable digital signatures is an intriguing feature of public key algorithms. By utilizing their private keys, users can sign documents, and anyone can use the matching public key to validate the signature. Therefore, the evolution of cryptography from the Cold War to modern times highlights the constant quest for secure communication methods. As technology advances, cryptography continues to play a pivotal role in ensuring the confidentiality and integrity of sensitive information [7].

Conclusions

Throughout history, wars and conflicts have played a crucial role in driving advancements in cryptography. The necessity to conceal sensitive information from adversaries has led to the development of various encryption techniques. Ancient civilizations used rudimentary forms of cryptography, such as substitution ciphers, to protect military communications. With the rise of technology, cryptography became increasingly reliant on machines. While the traditional methods generally presented basic forms of encryption, and were often lacking security measures, the techniques which rely on computers are not perfect, since with the evolution of technology comes the development of the tools and techniques available to those attempting to breach encrypted systems. Despite the relentless efforts to create foolproof encryption, vulnerabilities can still emerge. This is not necessarily a failure of the encryption methods themselves but often a result of unforeseen weaknesses.

Bibliography

[1] W. L. Hosch, "Britannica," Encyclopaedia Britannica, 18 February 2024. [Online]. Available: https://www.britannica.com/topic/cryptography. [Accessed 11 March 2024].

[2] G. J. Simmons, "Britannica," Encyclopaedia Britannica, 07 December 2023. [Online]. Available: https://www.britannica.com/topic/cryptology. [Accessed 11 March 2024].

[3] D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, New York, NY: Scribner, 1996.
[4] M. Jackob, "History of Encryption," p. 9, 2001.
[5] [5] L. D. Smith, Cryptography: The Science of Secret Writing, New York, NY: Dover Publications, 1955.
[6] J. F. Dooley, History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms, New York, NY: Springer, 2018.
[7] M. Fries, "The Unencrypted History of Cryptography," North Dakota University System, 20 September 2022. [Online]. Available: https://dda.ndus.edu/ddreview/the-unencryptedhistory-of-cryptography/. [Accessed 03 March 2024].