Radha Munver
06/02/2022

Ancient European and Arabic Cryptography: Evolution of Ancient and Medieval Ciphers

Introduction

As it is today, communication was an integral part of the ancient European and Arabic worlds. Many leaders sought to send messages to specific people without having them read by others. As people sent messages inscribed on parchment, leaves, and tablets, the issue arose that the messages were being intercepted and read by enemies, thus not allowing the intended message to reach the destination with the desired privacy and security. Oftentimes, these messages contained confidential information or plans regarding certain political affairs or military plots – words meant only to be read by specific people. This led to the creation of cryptography, the art of creating ciphers[1] to encrypt[2] messages such that they are no longer legible unless decrypted.[3] The creation of new methods for the codebreaking of ciphers forced new, more complex ciphers to be devised to ensure the security of the message. The field began very simply with the use of steganography[4] and transposition[5] ciphers; however, as they were very new and experimental, they were therefore filled with flaws, and people were not focused enough on keeping the key secret. This led to the creation of monoalphabetic substitution[6], pioneered by Julius Caesar, and was very successful until the creation of frequency analysis.[7] Arabic cryptography gained a lead over Europe with their invention of frequency analysis to break the monoalphabetic substitution cipher. For many years, cryptanalysts[8] were ahead of the cryptographers[9] until the conception of polyalphabetic substitution[10] cipher. Many plots were resultantly foiled due to the knowledge of frequency analysis. The

[1] *cipher* - a method or code for encrypting text
[2] *encrypt* / *encryption* - using the cipher's instructions to disguise or make the original text appear differently
[3] *decrypt* / *decryption* - the act of reverting encrypted text back into its original, legible plaintext form
[4] *steganography* - secret communication achieved by hiding the existence of a message; derived from Greek word, "*steganos*," which translates to 'covered'
[5] *transposition* - when letters of the message are rearranged (scrambled), generating what is called an anagram
[6] *monoalphabetic substitution* - when every letter of the alphabet is consistently replaced by another letter
[7] *frequency analysis* - a method of using the percentage occurrence of letters to decrypt monoalphabetically substituted text
[8] *cryptanalysts* - people who were trying to break and find ways to decrypt ciphers
[9] *cryptographers* - people devising new ciphers and people who encrypted messages
[10] *polyalphabetic substitution* - when every letter is replaced by another letter according to multiple cipher alphabets

evolution of cryptography in ancient Europe carries a lengthy history, mainly with the driving factor being the desire to send messages in a secure manner.

Transposition & Steganography:

One of the earliest records of cryptography was used in ancient Greece through the use of a scytale to create an encrypted transposition of a message; this early form of a cipher laid the foundation for the field of cryptography and greatly impacted the path of future transposition ciphers as a whole. The process of the scytale cipher can be described through the following:

> Early forms of secret writing were used by the Spartans of Greece about 400 BCE. Employing a type of transposition cipher called 'scytale,' they would take a strip of parchment and wrap it around a rod. A scribe would then write the message on the parchment. After unwrapping it from the rod, the message became a meaningless set of random letters. Only a person with the correct size rod could reconstruct the message.[11]

This method represents the first meaningful interaction in the field of cryptography. The introduction of a process which is able to secretly send a message without it being left in plain sight was revolutionary to history; information could then travel without the risk of being read by common people or enemies, allowing only the person with the key, the scytale radius, to decrypt the message. The aspect of the scytale cipher which is specifically unique is its feature of transposition, allowing the encrypted text to appear as a random scramble of letters. On the other hand, the scytale cipher is only relatively secure; an interceptor of the ciphertext[12] may test scytales of various radii until the key and plaintext[13] is revealed. This process challenges the security of the scytale cipher in that as soon as people can recognise the transposition as scytale, it is relatively easy to decrypt the message through brute force. However, this only holds true if a common radius is chosen as the key; if an extremely precise and large radius is chosen, for instance of

[11] Roberts, Larry. "Information: Cryptology." Tech Directions, 10, 2001, 11, https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/magazines/information-cryptology/docview/218511253/se-2?accountid=35837.

[12] *ciphertext* - the encrypted text

[13] *plaintext* - The text prior to being encrypted or the text after being decrypted; legible text in original language

2.23 meters, brute force becomes a gamble. If the messenger is found carrying the scytale or if the radius and key is revealed, then the message's security is guaranteedly in jeopardy. Although this cipher was successful in many messages during ancient times, its failures during other encounters show its imperfections and the deficiencies which make its security unreliable, ultimately leading to a shift away from transposition ciphers.

Another path of cryptography which did not involve changing the forms of the letters was steganography, which merely concealed the message and thus eliminated the need for a shared key. Its security, however, is questionable since if anything goes wrong and the message is revealed, it can be easily read without any shield. During ancient and medieval times, there were many methods of steganography; for instance, some wrote their messages on fabrics which would be crumpled into a small ball, covered in wax, and then swallowed by the messenger. Others chose to write with invisible ink, and Pliny the Elder introduced the idea that an invisible ink could be created from the nectar of a tithymalus plant, which dries transparent but turns brown when put in contact with heat.[14] Superficially, steganography seemed to carry a high level of security with its discreet hiding of the information. It was sufficient for unimportant matters which did not carry consequences if by chance revealed; however, as society began to learn these various methodologies, it probably became common practice to check people for any steganographic messages when crossing borders or entering into significant locations. This would have sabotaged plans for those who were hoping to conquer territories or commit murder. Ultimately, it is clear it was inadequate to merely hide a message of significance through steganographic techniques; it seems that a greater level of security could have been achieved with the encryption of the letters along with steganography. This would have required the interceptor of the message to attempt decryption of the text should it have been revealed. Essentially, steganography offers an additional branch of cryptography or an alternative to encryption, but is most effective when combined with encryption to ensure optimal security.

[14] Singh, Simon. "The Evolution of Secret Writing." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 10. New York: Doubleday, 1999.

The thought-process of transposition ciphers contained a fundamental flaw, as would be proven by Kerckhoffs' Principle in the 19th century. It was unclear to the people that a more rigid mindset would need to be enforced regarding the protection of a cipher's key in order for successful security. With the introduction of transposition ciphers, it was believed that the security of the message was dependent on the amount of protection held by the cipher's algorithm. However, Kerckhoffs presented an alternative perspective:

> If the cipher alphabet, the key, is kept a closely guarded secret between the sender and the receiver, then the enemy cannot decipher the intercepted message…It was definitively stated in 1883 by the Dutch linguist Auguste Kerckhoffs von Nieuwenhof in his book *La Cryptographie militaire*: "Kerckhoffs' Principle: The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key."[15]

People were likely so preoccupied with ensuring that the algorithm was not revealed, when they were truly missing the importance of the key. In transposition ciphers, using brute-force can take an enormous length of time. So if the algorithm is revealed, an interceptor or enemy cannot do anything to decrypt a random transposition of letters if they do not have the key. In the case of

the scytale cipher, the parchment appears to contain a random string of letters, but when the strip of paper is wound over the scytale of appropriate radius, the text can be easily read. For most keys which are chosen for the scytale radius, it is still simple enough to decrypt the cipher since rods of various radii may be checked until the the letters line up; if the person encrypting the message is smart, they would choose a very large radius, thus making an interceptor clueless as to how many letters need to pass when testing a given radius. Using this knowledge, Kerckhoffs' Principle becomes very relevant and applicable in the sense that it would not matter whether an interceptor is aware of which cipher has been used so long as the key is never exposed. It is probable that a basic idea of this was formed as new ciphers were created and was taken into consideration when choosing ciphers for encrypting messages; the invention of new ciphers for which the key was difficult to expose was crucial to ensure the desired secrecy. This idea,

[15] Singh, Simon. "The Evolution of Secret Writing." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 16. New York: Doubleday, 1999.

however, would not become clearly and formally defined until Kerkhoffs' time, although the basic idea was likely already grounded in cryptography due to the many failures of transposition ciphers.

Monoalphabetic Substitution Ciphers

As vulnerabilities in the transposition cipher were discovered and there was a push for creating a more complex cipher, the concept of monoalphabetic substitution was formed during the times of Caesar around 60 BC; its success allowed this concept to continue without hazard for many centuries. The British and scientific author, Simon Singh, described the use of Caesar's cipher as such:

> He [Caesar] simply replaced each letter in the message with the letter that is three places further down the alphabet. Cryptographers often think in terms of the plain alphabet, the alphabet used to write the original message, and the cipher alphabet, the letters that are substituted in place of the plain letters. When the plain alphabet is placed above the cipher alphabet,…it is clear that the cipher alphabet has been shifted by three places, and hence this form of substitution is often called the *Caesar shift cipher*, or simply the Caesar cipher.[16]

Based on this description, it can be inferred that monoalphabetic substitution ciphers involve replacing plaintext letters with a different ciphertext letter contingent on a specific key. As this cipher became more popular, the term 'Caesar shift' became used more broadly in the sense that it began to be viewed as a shift of any number between one and twenty-six. This is probably a result of the desire to make the key more complex and less guessable. If someone could discern that a message was encrypted with the general Caesar cipher with simply a shift of three, it would be incredibly easy to decrypt. However, if an interceptor did not know what the specific shift was, using brute-force would become much more difficult and far more time consuming. This use of substitution was revolutionary as people began to construct different substitutions other than just Caesar shifts. When calculated, it turns out that there are 26! different ways to scramble the alphabet, which is equivalent to a little over 400 septillion, which is 400 followed by 24 zeros. In context, this enormous amount of keys would take several lifetimes to decrypt, thus providing a great blanket of security. With the creation of substitution, people could easily encrypt

[16] Singh, Simon. "The Evolution of Secret Writing." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 14. New York: Doubleday, 1999.

messages knowing that it would be near impossible to decrypt should an interceptor sort through every possible key. In this regard, the monoalphabetic substitution cipher seemed near perfect for centuries, allowing leaders to send safely-communicated messages to conquer other kingdoms or win battles. If there had been a simpler, more efficient codebreaking method during this time period, history plausibly would not have followed the same course. However, as it will be seen, once an easier approach was created, historical events began to take a different route. The ability to use substitution rather than steganographic techniques or tools such as scytales allowed the Caesar cipher and other substitution ciphers to be successful in encrypting the message; this also eliminated the risk of the message being revealed prior to reaching the intended reader, especially due to the vast combinations of keys.

Arabic Cryptography & Frequency Analysis

Although the substitution cipher was perceived as unbreakable for many centuries, al-Kindī's breakthrough in ancient Arabia in 815 AD regarding cryptanalysis allowed substitution ciphers to be deciphered easily without a key, thus revolutionising the field of cryptography. Al-Kindī's invention of frequency analysis as a subsector of cryptanalysis can be simplified into the following as recorded in his famous manuscript:

> "One way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. We call the most frequently occurring letter the 'first,' the next most occurring letter the 'second,' the following most occurring letter the 'third,' and so on, until we account for all the different letters in the plaintext sample.
>
> Then we look at the ciphertext we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the third most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve."[17]

[17] Singh, Simon. "The Evolution of Secret Writing." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 22-23. New York: Doubleday, 1999.

Essentially, frequency analysis involves sorting through the occurrences of every letter present in a given encrypted message and recording the percentages. Then, these percentages can be compared with the percentage frequencies of letters in a specific plaintext language to determine what shift or substitution was used during the encryption. Since letters do not appear with the same frequencies across different languages, finding the frequency of cipher letters would allow for the matching of distributions via a specific pattern. This was critical to cryptography and history in that codebreakers and interceptors now had an easy method of reading messages prior to the intended recipient, allowing them to more easily defeat enemies. This presented a dilemma in the continuity of use of monoalphabetic substitution ciphers as they were no longer secure. This discovery's occurrence in Arabia rather than in Europe had an interesting impact; since the Islamic territories now had access to the technique, they had a clear leg up over the Europeans. "Europe was firmly stuck in the Dark Ages. While al-Kindī was describing the invention of cryptanalysis, Europeans were still struggling with the basics of cryptography."[18] The Arabians were shielded from interceptors since the Europeans were not yet exposed to frequency analysis, but as the Europeans' own substitution ciphers would be deciphered, it became necessary for them to create something even stronger than a simple monoalphabetic substitution. Furthermore, this would have presented a greater challenge when frequency analysis spread to Europe since that would have more aggressively turned intracontinental countries against each other as well as between borders across different continents.

Monoalphabetic substitution had carried much success for many years as codebreakers were unable to decrypt substitution ciphers and thus did not demand the creation of an even more complex class of ciphers. However, as frequency analysis was a simple method for breaking substitution ciphers without a key, the security of substitution ciphers was jeopardized and contributed to the foiling of plots in history as it did with Mary Queen of Scots. Mary had been imprisoned by Queen Elizabeth I for many years, until she began exchanging messages with a friend, Babington, which were encrypted via a

[18] Singh, Simon. "Renaissance In The West." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 31. New York: Doubleday, 1999.

nomenclator substitution cipher. Mary planned to have Queen Elizabeth assassinated so that Mary would be the rightful heir to the throne due their being cousins. Queen Elizabeth's spy and secretary of state, Walsingham, keenly discerned the use of the basic substitution cipher, allowing him to use the simplicity of frequency analysis to decrypt Mary's messages.[19] For a great amount of time, codebreakers had been working tirelessly to come up with simple methods to break the monoalphabetic substitution cipher; however, al-Kindī's discovery completely changed the game. World leaders who were familiar with al-Kindī's work were able to decrypt enemies' messages without concern. An enemy of the sender would have wanted to be able to decrypt a message in time to foil a plot or gain higher ground in political and military affairs. This was true in the case of Mary and her attempt to break free from her prison and become the queen of England. Should Mary's plot have succeeded, world history as it is known could have followed a drastically different timeline; Mary could have become Queen of England and the entire hereditary circuit of power would have been altered. However, since Mary's message was deciphered and she was sentenced to death, her situation and legacy further seemed to have compelled cryptographers to work more diligently in creating an effective encryption process which could circumvent the use of frequency analysis.

Polyalphabetic Substitution Ciphers

As frequency analysis made the monoalphabetic substitution cipher obsolete, Leon Battista Alberti, a fifteenth-century Florentine polymath, recognised the issue and thereby created polyalphabetic substitution to better protect messages. "At the time, all substitution ciphers required a single cipher alphabet for encrypting each message. However, Alberti proposed using two or more cipher alphabets and

[19] Poole, William. "A LATE SIXTEENTH-CENTURY CRYPTOGRAPHIC AL TREATISE: JACOBUS COLIUS'S 'TRACTATUS DE FICTIS CHARACTERIBUS' (1584–86)." Journal of the Warburg and Courtauld Institutes 74 (2011): 213–39. http://www.jstor.org/stable/41418735.

switching between them during encipherment."[20] Alberti acknowledged that the issue with monoalphabetic substitution was the fact that each individual letter is substituted with a specific cipher letter which would not change as the message was encrypted. Alberti knew that if he could discover a way to encrypt a singular plaintext letter under multiple cipher letters while allowing the intended recipient to decrypt easily via the key, this would prove to be far more successful and secure compared to older methods. With Alberti's concept of using multiple cipher alphabets and alternating among them based on a shared key, this would thereby confuse cryptanalysts in their pursuits to decrypt a poly-alphabetically encrypted message as no letter would be encrypted the same. However, it can be noted that Alberti's discovery was not introduced until many years after the invention of frequency analysis; this was likely a result of the time taken for frequency analysis to spread from ancient Arabia and for Europeans to familiarize themselves with cryptographic techniques. The Arabians had first began their study in cryptanalysis as a result of their religious duty in achieving ilm, or knowledge, in all subjects, which meant translating texts from all different cultures.[21] The Arabians presumably did not devise a new cipher system due to cryptanalysis' relevance to their Islamic responsibilities; specifically, the Qu'ran required every Muslim to pursue knowledge in all of its states and forms rather than worrying about formulating new concepts. Europeans seemed to be more power focused, so the inventing of stronger ciphers would better fit their inclinations. Alberti's basic concept of polyalphabetic substitution would serve as a foundation for more complex polyalphabetic substitution ciphers to be invented in the future.

Following Alberti's breakthrough with polyalphabetic substitution, the Vigenère cipher cleverly incorporated and refined the concept to create a far more secure cipher, one that would not be broken for many centuries afterward, and thus provided sufficient protection for that time period. The Vigenère cipher, like Alberti's, used multiple cipher alphabets; however, the Vigenère cipher had a specific sequence in choosing which cipher alphabet with which to encrypt. This process can be described as such:

[20] Singh, Simon. "The Anonymous Codebreaker." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 51. New York: Doubleday, 1999.

[21] Singh, Simon. "The Arab Cryptanalysts." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 20-21. New York: Doubleday, 1999.

> Blaise de Vigenère, a French diplomat born in 1523, became acquainted with the writings of Alberti when, at the age of twenty-six … he examined Alberti's idea and turned it into a coherent and powerful new cipher, now known as the Vigenère cipher. The strength of the Vigenère cipher lies in its use of not one or two but twenty-six distinct cipher alphabets to encrypt a message. The first step in encipherment is to draw up a so-called Vigenère square,…a plaintext alphabet followed by twenty-six cipher alphabets, each shifted by one letter with respect to the previous alphabet. Hence, row 1 represents a cipher alphabet with a Caesar shift of 1, which means that it could be used to implement a Caesar shift cipher…Similarly, row 2 represents a cipher alphabet with a Caesar shift of 2, and so on. The top row of the square, in lowercase, represents the plaintext letters. You could encipher each plaintext letter according to any one of the twenty-six cipher alphabets.[22]

Even though the Vigenère square only showed the various cipher alphabets from A to Z, one would first need this table in order to decrypt. Furthermore, the cipher alphabet chosen would have been dependent on a keyword which had been agreed upon by the sender and intended receiver. This became problematic for an interceptor because it would seem nearly impossible to discover the keyword due to the fact that the same plaintext letter could be enciphered under different ciphertext letters. Specifically, this was likely the main aspect of the cipher which troubled cryptanalysts and led to the cipher's nickname being *'le chiffre indéchiffrable*,' which can be translated from French to 'the indecipherable cipher.' The Vigenère cipher was clearly more advanced and complicated in both the algorithm and key when contrasted against the basic transposition cipher and original Caesar cipher. The complexity of the Vigenère cipher whose polyalphabetic substitution hindered the use of frequency analysis showed great improvement compared to the thus simple monoalphabetic substitution cipher. This drawback for cryptanalysts was probably what assisted in the success of many plots in history and allowed governments and countries to communicate without fear of their messages being intercepted and decrypted. The success of this cipher is demonstrated by the fact that this cipher was not broken for another 250 years after its creation.

[22] Singh, Simon. "The Anonymous Codebreaker." Essay. In The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 53-54. New York: Doubleday, 1999.

Conclusion

The evolution of cryptography was greatly driven by the cryptanalysts' constant creation of new codebreaking methods, forcing cryptographers to create more complex ciphers to ensure sufficient protection. Given that transposition and steganography proved ineffective because the key or steganographic message could be revealed, cryptographers had to adapt to this deficiency with the creation of the monoalphabetic substitution cipher. When the monoalphabetic substitution cipher became inpotent due to the creation of frequency analysis, it became necessary for something even more difficult to decrypt to be created, which turned out to be the polyalphabetic substitution cipher.

Not only did this evolution of ciphers in ancient Europe impact the general structure and format of the ciphers, but it also played an integral role in the specific course of history. It seems that the increased use of encryption and the spread of information of its uses resulted in its profound function in history. The desire for the sending end to maintain secrecy in conjunction with the enemy's impulse to intercept and decrypt the message made the use of ciphers evermore important. This has been translated into modern society as cryptography has travelled great lengths to be as secure as it is today. The fact that it has been integrated into the Internet through the use of binary and modular arithmetic is astounding with its simplicity in encryption yet immense complexity for decryption. The mere idea that public-key cryptography is what runs modern internet security is difficult to comprehend given Kerckhoffs' Principle, which further exhibits a continued evolution in cryptography. As people continue to desire privacy in their communication, it can be concluded that cryptography will undoubtedly continue to evolve and complexify as hackers discover new decryption methods.

Additional Sources:

Holzmann, Gerard J. "Tales from the Encrypt." Inc, Nov 18, 1997, 168, https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/magazines/tales-encrypt/docview/214516394/se-2?accountid=35837.

Roberts, Larry. "Information: Cryptology." Tech Directions, 10, 2001, 11, https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/magazines/information-cryptology/docview/218511253/se-2?accountid=35837.

Gualtieri, Devlin M. "Keeping Secrets." Phi Kappa Phi Forum 83, no. 2 (Spring, 2003): 6-7. https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/scholarly-journals/keeping-secrets/docview/235180614/se-2?accountid=35837.

"NATIONAL CYBERSECURITY AWARENESS MONTH: TACKLE IT TOGETHER." US Fed News Service, Including US State News, Oct 20, 2018. https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/newspapers/national-cybersecurity-awareness-month-tackle/docview/2123094160/se-2?accountid=35837.

Jones, Kevin. "The Puzzling Mr Elgar." New Scientist, Dec, 2005, 56-58, https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/magazines/puzzling-mr-elgar/docview/200450046/se-2?accountid=35837.

Sánchez-Ávila, Carmen. "Some Notes on a Formal Algebraic Structure of Cryptology." Mathematics 9, no. 18 (2021): 2183. doi:https://doi.org/10.3390/math9182183. https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/scholarly-journals/some-notes-on-formal-algebraic-structure/docview/2576442332/se-2.

Zeller, Tom. "Of Hiding and Seeking." New York Times, Sep 08, 2002, Late Edition (East Coast). https://ezproxy.d-e.org:2443/login?Citation=https://www.proquest.com/newspapers/hiding-seeking/docview/432196969/se-2?accountid=35837.