ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

The History of Cryptography and Its Applications

Huixin Li[1], Yubo Wang[2]

[1]School of Guangzhou Foreign Language School, Guangzhou, 511455, China

[2]School of Zhengzhou Foreign Language School, Zhengzhou, 450001, China

Abstract

Cryptography paved the way for making communication more secure by hiding information in a communicated message or making it incomprehensible, which has evolved since ancient times, with each era embracing technological advancements that make encryption and decryption more complex and secure. The application of Cryptography also varies with each era. The technology was primarily used in military and religious communication during ancient and medieval times. The governments and religious institutions found it secure to share sensitive information such as military campaign communication as encryption. The modern era also embraced a similar trend with most Cryptography usage experienced during World War II. Such also influenced the introduction of a cipher. The contemporary era paved the way for the introduction of cryptocurrency widely used, given the advantages involved. The transformation of cryptography captures the historical relevance of the technology across different settings. This essay focuses on reviewing the history of cryptography and its applications.

Keywords

Cryptography; Ancient times; Modern times; Contemporary; Encryption; Decryption.

1. Introduction

The application of cryptography in the modern environment sometimes evokes different perceptions, including espionage, and secretes communication between agents and governments. The perceptions extend to internet users who view cryptography elements as a representation of technological walls that could withstand tampering. However, science is all about making communication messages incomprehensible to those accessing them except the sender and the targeted recipient. Cryptography in this context paves the way for encryption to help conceal the secrecy in such messages (Damico, 2009) [1]. Cryptography is a technological tool that has been around for centuries, with efficiency and application in concealing secret messages varying with every era. Therefore, this essay evaluates the history and application of cryptography in ancient, modern, and contemporary times.

2. History and Application

Humans have been focusing on communicating messages with a protective approach from preying eye ever since. The idea of protecting the message is all about encryption, where the person communicating a message moves some of the characters around to hide the intended message. The idea of keeping communication messages a secret tends to involve two approaches, including hiding the information's existence or making it unintelligible. Cryptography as science has helped with such measures (Damico, 2009), including ensuring information communicated between agents and governments remains secure and out of reach of unintended audiences [1]. Cryptography has been advancing over the years, with every era

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

presenting new approaches that help make cryptography more advanced and reliable. The history and application of cryptography are as follows:

2.1. Ancient Times

Cryptography was in use during the era of antiquity and medieval times. During antiquity, cryptography was widely used in Mesopotamia, Egypt, and ancient Greeks in various capacities. One of the ancient cryptographies was the non-standard hieroglyphs used during the 1900Bc by the old Egyptian kingdom (Damico, 2009) [1]. The cryptography focused on alphabetic, syllabic, and sometimes logographic factors with up to over 1000 characters. The cryptography was in different forms with the cursive elements used in communicating religious literature on wood. Besides, cryptography developed from Egypt's embrace of the proto-literate system associated with the Early Bronze era dated 32nd century BC. Part of the first decipherable statements using cryptography involved using the Egyptian language, which also paved the way for the transformation of the hieroglyphs into a more advanced writing and communication system [1]. The system also accommodated several distinct signs which continued to the Persian Period with the late survivals evident in the Roman Period, which extended to the era of the 4the century AD.

Furthermore, the application of cryptography happened in different contexts. One of the contexts was the carvings in tomb walls to help with secret communications. In this regard, the approach proved to be an unsolvable mystery for some, but the sender and receiver of the information shared could decrypt the message (Damico, 2009) [1]. Such made the process of decrypting message characters and establishing meaning easy for the people associated with the communicated message while outsiders found it strange. Cryptography also involved a combination of logographic, alphabetic, and syllabic factors in communicating leadership and military messages. The use involved focusing on distinct characters that the elements represented in the communication [1]. Besides, the leading application of the cryptographic in the setting was to hide and conserve religious communication intended for specific Egyptian recipients such as the leadership and staunch followers.

Secondly, the ancient Greeks also used the scytale cipher design of cryptography. The cryptography tool had a cylindrical shape wrapped in a parchment strip with the written message. The Greeks and the Spartans used the toll in sending and receiving secret information in the military. The tool helped conceal secret messages during their military campaigns [1]. The clear indication of the introduction of the tool during the ancient era was through Apollonius of Rhodes poet who was also a Homeric scholar. According to the description of the skytale, admirals or generals were sent out during the military campaigns with the scytale tool with one left with the ephors. The two corresponded in dimensions. The secret information could be relayed through a parchment scroll wind around the scytale and written. The parchment was then set off, leaving the tool with the commander. The receiver then placed the received parchment scroll on another scytale. The message could be read with the spiral course restored in a perfect way around the scytale.

Moreover, the usage of the cryptography tool indicates that only the receiver with a scytale with similar dimensions could read the communicated message. The approach made it challenging for the enemy spies to read or alter the communication between military commanders (Lanase, 2019) [6]. The strength of the cryptography in message encryption was the random characters on the leather strip and the wooden tool used in decrypting that was of a specific size with letters aligned into distinct words. In this regard, the encryption of messages involved writing across the leather strip so that the ciphertext could read in special characters. Decrypting the message involved raping the sent message around the exact rod and reading across (Lanase, 2019) [6]. Such is an implication that skytale played a fundamental role as a transposition cipher in transmitting and reading encrypted messages during the Greek era. The usage of

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

cryptography became an essential approach in physically concealing communications during military campaigns [6]. Therefore, this made cryptography a critical weapon in every Greek military engagement.

Additionally, cryptography science was used during medieval times in hiding information and making communications unintelligible. The invention of the technique created an avenue for ensuring safe communication and message got to the intended audience. For instance, medieval England used the tool in different settings, such as the scribes in enciphering notes, riddle solutions, and colophons [1]. In this regard, this science ensured the ciphers were fairly straightforward for the intended audience but a deviation from the standard communication patterns and complex for the rest of the people who managed access. The sophistication involved ensuring cryptographic experimentation worked during the Period, thereby paving the way for the advancement of science to the timeframes that followed.

The effort made cryptography science more important in Europe, with an extensive religious revolution and political campaigns. For example, one of the science applications in Europe was during Elizabeth I's reign as the queen (National Archives, n.d), where cryptography ciphers were used to communicate the Babington Plot [2]. The information communicated in the cryptographic effort was the planned assassination of the queen, which eventually led to the execution of Queen of Scots. Therefore, this proves the significance of the introduction of cryptography during the ancient and medieval eras.

2.2. Modern Times

Cryptography significantly developed from the 1800s to the First World War. The era saw the transformation of cryptography science from the complex system used in the ancient phase to a more sophisticated system (Sahinaslan & Sahinaslan, 2019) [3]. In this regard, the cryptography science advancement came with changes also in encryption as most of the entities that embraced the technology focused on developing ciphers that could help understand some of the information relayed. The cryptography advancement paved the way for the developments during the First World War. Countries used the tool to establish ways of reading military or religious messages communicated during the event. For instance, the government, such as the British, managed to introduce cryptanalysis tools such as Room 40 developed from cryptography science to help break naval codes such as that of the Germans [3]. In such context, it played a fundamental role in understanding some of the intended naval engagements of the wars that involved the British and the Germans, especially the detection of battle advancements.

One of the essential applications of the cryptography tools was the decryption of the Zimmermann Telegram, which was a critical cable communication between the German foreign office and an ambassador to Mexico [3]. Americans using the cryptography advancement in deciphering the communication contributed to the ignition of war. The modern settings also allowed the development of cryptography in the 1920s before the Second World War. Countries like the Polish used the technology to assist other governments with cipher development [3]. In this regard, such governments focused on assisting with cipher development to help strengthen their participation in the war, such as the Polish officers working for the naval assisting the Japanese military in developing a cipher that could help intercept and translate military communications.

Furthermore, Worlds War II paved the way for the advancement of cryptography science. One of the developments that helped demonstrate the advancement of cryptography technology is introducing and using the Enigma tool between the early and mid-20th centuries (Sahinaslan & Sahinaslan, 2019) [3]. The invention enabled the mechanization of encryption besides foiling frequency analysis. The machine resembled a typewriter with three components. The critical components included the input keyboard, output lamp-board, and the scrambling device between the keyboard and the lamp-board. In this regard, the scrambling device enables letters

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

typed in respond differently, such as typing A triggering lighting of M on the device's lamp-board [3]. Besides, the scrambling aspect of the Enigma machine presented a dynamic moment with an opportunity for the scrambling mode to change after typing in every letter. Therefore, the electromechanical machine connecting the input and output through an electrical circuit which changed constantly, helped communicate concealed information.

Additionally, Arthur Scherbius was behind the invention of the Enigma machine in the post-first world war, with Germany as the most prominent user before and after the war. In this regard, most of the entities involved in using the invention in communications were the army, civil service, navy units, and the railway stations that played a pivotal role in the war (Sahinaslan & Sahinaslan, 2019) [3]. The entities needed to communicate secret messages through encrypting and decrypting through the machine. Part of the strength of the cryptography was the concealed key or setting, which thereby did not worry countries using it, such as Germany, from the machine falling into the wrong hands. Such include the sender and the receiver of information having the similar setting of the machine, which made encryption and decryption an easy process but a challenge to the others. Besides, the Nazi cryptographers using the machine also believed in the impossibility of working out the cryptography key [3]. The case led to assumptions about the safety of communication.

Moreover, the machine came with varying applications, specifically the encryption of crucial messages to prevent allied hands from access. In this regard, the introduction of the system enabled an avenue for protecting commercial, military, and diplomatic information (Sahinaslan & Sahinaslan, 2019) [3]. The country that mostly used science in Nazi Germany in the Second World War believed in secure communication, which guaranteed an advantage. The countries participating in the war believed that the system was secure so that even the top-secret communication could be enciphered. The Nazis managed to improve the system over the years, thereby limiting decryption development [3]. Part of the development was the plugboard setting which proved to be fundamental in the key to message encryption and decryption.

The plugboard setting enabled the machine users, such as the German Nazis, to swap letter pairs when communicating. In this case, the plug cable that connected letters A and W implied that an individual typing the letter triggered a signal that followed a path where W, when typed, follows [3]. The process was the same when typing the letter W. The sender and the receiver using the machine to communicate military plans could have a similar plugboard setting to enable the process to be smooth. The approach enabled the Germans to track military communication such as the Atlantic convoys, which enabled them to sink some warships. However, Allied codebreakers such as the Polish used cryptography technology to crack the system [3]. The weakness enabled allies to exploit some of the enigma-enabled messages and use such communication as intelligence.

2.3. Contemporary

The further advancement of cryptography has been seen in the contemporary setting. The objective behind cryptography usage remains similar, which is the prevention of interference with a communicated message between parties. Algorithms have enabled the achievements with the key for encryption and decryption of information. The encryption and decryption keys facilitate a framework for converting communication messages into a digital context that could be transformed into an original form once it reaches the intended audience (Abbod & Guirguis, 2018) [4]. The objective of cryptography in the contemporary setting was to enable authentication, confidentiality, data integrity, access control, and non-repudiation. Besides, some of the entities using the cryptography science in encrypting messages tend to consider the longer keys, which help makes it challenging to crack the code. According to Abbod & Guirguis (2018), one of the cryptographic algorithms which made a difference upon the introduction in the contemporary setting is the DES introduced by IBM in 1972 to help with

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

securing crucial financial databases [4]. The advancement was efficient in the encryption of communication in the financial sector. The tool was adopted in the US and used at a national standard. However, it had its drawbacks, such as the minor encryption key that exposed information incrementally increased computing power, making it easy to brute-force an all-out attack.

Moreover, the encryption algorithm also involved the 3DES, which became the DES upgrade developed to help overcome some of the drawbacks experienced with the earlier version. The tool became operational during the late 1990s and made communication harder to crack (Abbod & Guirguis, 2018). The application was mostly in areas including payment systems in the finance industry. The tool also had its drawbacks, such as the security holes, which influenced the security industry's weaknesses and facilitated the embrace of other efficient cryptography tools. The other encryption algorithm developed from cryptography science is the Advanced Encryption System, developed as a DES alternative approved in 2001 (Abbod & Guirguis, 2018) [4]. The cipher is comprised of distinct vital lengths. The advantages associated with the tool include safety, speed, and flexibility compared to the previous cryptography tools, thereby making it most preferable in wireless security, Wi-Fi security, and mobile app encryption.

Furthermore, one of the encryption algorithms developed in the contemporary setting is the RSA introduced in 1977 by Ron Rivest, Leonard Adleman, and Adi Shamir [4]. The usage of this tool is wide based on the potency, which lies on the prime factorization. The advantage associated with the tool is the scalability as it comes with different encryption key lengths, including the 1024-bit and 4096-bit (Seth, 2021) [5]. The tool also embraces a less complex mathematical strategy, which makes the public keys infrastructure efficient. The second asymmetric tool is the Elliptic Curve Cryptography introduced in 1985 by Victor Miller and Neal Koblitz [5]. The encryption involving this tool focuses on an elliptic curve representing points capable of satisfying a mathematical equation. The advantage associated with this tool includes greater security compared to the other tools, given the complexity.

Additionally, one of the contemporary applications of the encryption algorithm tool is cryptocurrency. The technology involves using cryptography science in encryption and decryption where there is an involvement in advanced mathematical codes in the storage and transmission of data values using secure formats [5]. The approach ensures that the financial values are communicated to the targeted audience to receive and process the data. The case also involves ensuring transaction authenticity. The cryptography approach makes it challenging to counterfeiting or altering spending. Besides, most cryptocurrencies operate as decentralized networks driven by blockchain technology which involves a distributed ledger enforceable through a computer network. The cryptocurrency's lack of association with a central authority also makes them efficient based on immunity from manipulation cases or government interference.

The cryptography application takes different approaches. First, symmetric encryption involves using a secret key in encrypting the cryptocurrency message at a source before transmitting it to a recipient [5]. The decryption of the message then happens at the destination. Such ensures that the unauthorized parties receiving the message as encrypted cannot make sense of the transaction values unless the encryption method is in play. Secondly, the cryptocurrency aspect of cryptography involves asymmetric encryption where there is an involvement of two distinct keys: private and public. The keys help with encrypting the communicated transaction message (Seth, 2021) [5]. In this regard, the dissemination of the public key is open, including the recipient's address. The private key is only available to the owner. The method involves encrypting messages through the public key, with decryption only possible with the private key (Flori, 2019) [7]. Therefore, the cryptography method is significant when it comes to authentication and transaction encryption in cryptocurrency.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

Cryptocurrency also works in different ways. In this regard, there are different alternative cryptocurrencies with specifications serving distinct functions. One of the globally embraced and valuable forms of cryptocurrency is Bitcoin. The cryptocurrency was established in 2009 through Satoshi Nakamoto, considered a pseudonym. The world currently has over 18.8 million bitcoins circulating as of 2021 (Frankenfield, 2021) [8]. The bitcoin in circulation has a market cap of approximately $858.9 billion and continues to update regularly. The financial market also has only 21 billion bitcoins in existence (Frankenfield, 2021) [8] as a measure of prevention of possible inflation or manipulation. Cryptography has also helped reinforce the measure by allowing safe encryption and decryption of bitcoin transactions. Besides, bitcoin has competition from other cryptocurrencies, including Litecoin, Ethereum, and Namecoin, thereby making the aggregate value of existing cryptocurrencies hit up to $1.8 trillion, with Bitcoin taking the largest share of 46.5% [8]. Therefore, this indicates the level of impact cryptography has enabled through cryptocurrency.

Moreover, the wide embrace of the cryptography tool is due to the advantages involved. In this case, one of the advantages is the strength of making it easier and safer to transact with funds between entities (Bunjaku, 2017) [9]. The cryptography technology ensures a safety process through encryption and decryption of data, thereby eliminating the involvement of third parties such as banks and credit card companies that could increase risks. The transfers in this process have enough security through the involvement of public and private keys. Besides, the modern cryptocurrency system involves users having public keys through their account addresses, with the private key only left with the owner for signing transactions [9]. Such indicates the function of cryptographic tools where the key helps encrypt the cryptocurrency message from the source before transmission, with the decryption happening at the reception. The other strength is the minimal fees associated with the processing of transfers (Sharma & Sharma, 2018) [10]. Such allows users to prevent specific changes incurred when using financial institutions in wiring transfers.

However, cryptocurrency also comes with advantages that users consider when embracing cryptography technology. One of the disadvantages is the semi-anonymous concept of the transactions, making it appropriate for entities to conduct illegal activities, including tax evasion (Jeripothula, 2021) [11]. Some entities also take advantage of cryptocurrency to launder money. However, the cryptocurrency providers emphasize the need for anonymity in ensuring privacy for entities operating in harsh environments such as the activists affected by repressive governments. Besides, some cryptocurrencies, such as Bitcoin, have measures to help prevent illegal activities (Nadeem et al., 2021) [12]. The technology creates an avenue for forensic analysts with cryptography skills, especially for blockchain technology, to track illegal transactions. The approach helps authorities access and prosecute involved cryptocurrency criminals thereby improving the efficiency of the tool (Giudici, Milne & Vinogradov, 2019) [13]. Therefore, cryptography technology creates a safe avenue for transacting online but has weaknesses that should be considered to ensure its efficiency.

3. Conclusion

Cryptography remains one of the technologies with historical significance. The advancement of cryptography started during ancient times with the introduction of tools such as the scytale cipher, helping make a difference in secure communication. The modern era, such as World War II, also saw the significance of cryptography, especially in the secure exchange of military communication. However, the contemporary era has made a difference by facilitating a more advanced cryptography encryption and decryption approach. The most common example of cryptography advancement is the cryptocurrency widely used in the financial market. The cryptography system ensures the security, complexity, and efficiency of cryptocurrency.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202203_5(3).0056

Therefore, the advancement of cryptography has created avenues for safe and secure encryption and decryption of information, thereby facilitating the reliability and efficiency of some of the technological communication or transactions.

References

[1] Damico, M. T. (2009). A Brief History of Cryptography. Inquiries Journal, 1(11), 1.

[2] Lanese, N. (2019). What is cryptography? Live Science, Jun 06, 2019. Available at: https://www.livescience.com/65648-cryptography.html

[3] Sahinaslan, E. & Sahinaslan, O. (2019). Cryptography Methods and Development Stages Used throughout History. AIP Conference Proceedings, 2086(1), 1-4.

[4] Abbod, O & Guirguis, S. (2018). A Survey on Cryptography Algorithms. International Journal of Scientific and Research, 8(7), 495-516.

[5] Seth, S. (2021). Explaining the Crypto in Cryptocurrency. Investopedia, Aug 4, 2021. Available at: https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

[6] National Archives (n.d). "Ciphers Used by Mary Queen of Scots." National Archives. Available at: https://www.nationalarchives.gov.uk/education/resources/elizabeth-monarchy/ciphers-used-by-mary-queen-of-scots/

[7] Flori, A. (2019). Cryptocurrencies in finance: Review and applications. International Journal of Theoretical and Applied Finance, 22(5). Available at: https://doi.org/10.1142/S0219024919500201

[8] Frankenfield, J. (2021). Cryptocurrency. Investopedia, Aug 9, 2021. Available at https://www.investopedia.com/terms/c/cryptocurrency.asp

[9] Bunjaku, F. (2017). Cryptocurrency- advantages and disadvantages. Journal of Economics, 2(1).

[10] Sharma, P.R. & Sharma, A. (2018). Using cryptocurrency and associated advantages and disadvantages. International Journal of Economics & Finance Research and Applications, 2(2), 18-22.

[11] Jeripothula, S. (2021). Cryptocurrency part 3 of 3: Disadvantages, investment and future. The UIS Journal, May 7, 2021. Available at: https://uisjournal.com/top-stories/2021/05/07/cryptocurrency-part-3-of-3-disadvantages-investment-and-future/

[12] Nadeem, M.A., Liu, Z. Pitafi, A.H., Younis, A. & Xu, Y. (2021). Investigating the adoption factors of cryptocurrencies – A case of Bitcoin: Empirical evidence from China. SAGE Open, 11(1). Available at: https://doi.org/10.1177%2F2158244021998704

[13] Giudici, G., Milne, A. & Vinogradov, D. (2019). Cryptocurrencies: market analysis and perspectives. Journal of Industrial and Business Economics, 47(1), 1-18.