Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

Contribution of Muslims and European in the Evolution of Cryptology: A case Study

Dr. Asma Aziz (Principal Author)[1*], Suneeza Hameed(Corresponding Author)[2*], Dr. Hasan Baig[3], Madiha Kanwal [4], Farhana Mustafa, [5] , Hamza Sattar[6], Maimoona Ajmal [7]

[1] Department of Islamic Studies, Government College Women University Faisalabad, Pakistan

[2,4,] Department of Information Technology, Government College Women University Faisalabad, Pakistan

[3] Department of Interfaith Studies, F/O AIS, Allama Iqbal Open University, Islamabad, Pakistan

[5] Department of Islamic Studies, Govt. College University, Faisalabad, Pakistan

[6] Department of Mathematics Govt. College University Faisalabad, Pakistan

[7] Department of IT, Govt. College Women University Faisalabad, Pakistan

Abstract:

Some of the greatest technological achievements in human history, like as computers, the internet, and the digital world, have been greatly influenced by cryptography. Keeping secrets has always been vital, which is why people and governments have come up with strategies to protect important data. This need lead to the development of methods for coding, hiding, and creating codes as well as improvements in methods for obtaining intelligence and cracking codes. Muslims have long made contributions to the study of cryptology, using their knowledge to improve security and create advanced cryptographic techniques. This paper examines the important contributions Muslims have made to the field of cryptology.

Keywords: Cryptology, Cryptography, Cipher text, Plaintext, Encryption, Decryption, History, Origin, Role of Muslims, Arabs born Science.

* **Corresponding Authors:** Dr. Asma Aziz, Department of Islamic Studies, Government College Women University Faisalabad, Pakistan,
Suneeza Hameed, Department of Information of Technology, Government College Women University Faisalabad, Pakistan,

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

Introduction:

The Internet is a massive global network that links millions of computers and allows for quick communication and information sharing. Although email facilitates communication, the Global widely Internet supports online commerce, data exchange, advertising, investigation, and education. Because it eliminates the possibility of fraud or deceit, cryptography is essential to building confidence and security in the digital sphere. Numerous people connect electronically on a daily basis via email, e-commerce, ATMs, and mobile phone, which adds to the increasing need on encryption. Cryptography protects the three essential components of data protection: confidentiality, integrity, and authentication. This controls to attempt at theft, fraud, and unauthorized entry. It ensures the security of websites, permitting safe online banking, trading, and credit card transactions without putting personal information at risk. The vital role that encryption plays in protecting digital assets and fostering user confidence is critical to the sustainability of the Internet and electronic commerce. [i]

Cryptography is the process of encrypting data during transmission in order to protect its confidentiality. Its primary goal is to restrict unauthorized access to the data being communicated, so enabling parties to communicate safely. In addition to confidentiality, cryptography is utilized for data integrity, authentication, and non-repudiation. It's an intriguing area of computer science where the majority of the work is devoted to maintaining the confidentiality of methods and algorithms. The two major forms of encryption are symmetric (also referred to as secret key encryption) and asymmetric (which is also known as public key). Applying a secret key to the message modifies its content through symmetric encryption, which is the more conventional approach. A public key and a private key are two related keys used in asymmetric encryption, on the other hand.[ii]

Information security is critical in today's technology environment, particularly when it comes to online communication and e-transactions. Although some may believe that increased security is superfluous, the truth is that it is essential to protect the enormous amounts of data that millions of people exchange every day. A variety of techniques that are essential for guaranteeing safe online shopping, secure money transactions, confidential correspondence, and password security are provided by cryptography. However, it's important to understand that encryption cannot provide security on its own. This field of study focuses on creating and evaluating safe communication strategies in the face of potential dangers. This includes creating and evaluating techniques that are susceptible to the impact of adversaries, among other information security-related topics. The

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

intersections of modern cryptography with mathematics, computer science, and electrical engineering demonstrate its comprehensive approach to resolving security issues.[iii]

The goal of network security and cryptography is to protect data transfers and network structure, especially when they occur across wireless networks. Multiple layers of defense are used by a comprehensive network security system, which consists of a variety of hardware, appliances, security software, and network monitoring tools. Collectively, these elements improve the computer network's overall security condition. This is where data security techniques like cryptography arrive into play, making them an increasingly vital part of network security. Network security can be improved through the potential that comes with combining neural networks and encryption. Strong security protections are provided by a proposed model for a cryptosystem using neural networks. Neural networks are used to generate cryptographic keys that are very difficult to decrypt. These keys take the shape of weights and neuronal functions. Information data is used as input for cryptography in this architecture, which makes it unreadable to would-be attackers and maintains its security. Numerous applications of cryptography can benefit from the ideas of reciprocal learning, self-learning, and random behavior included in neural networks and related algorithms. These include encoding and pseudo-random number generation, as well as public-key cryptography, which uses neural network mutual synchronization to solve the key distribution problem.[iv]

Information protection has always been an essential part of being human. Because society is becoming more and more dependent on technology in the digital era, information security has become crucial. Strong security measures are increasingly needed as a result of the constant inflow of new, developing technology. Particularly, cryptography is an essential method for protecting sensitive data and guaranteeing secure message transmission. The applications of this technology cover a wide range of industries, such as business transactions, Pay-Tv, electronic communications (such as private emails and mobile messaging), e-commerce, transmission of financial information, ATM card security, and computer passwords. By using mathematical methods to disguise sensitive information, cryptography helps to provide both privacy and security for that information.[v]

Purpose and Function of Cryptography:

Data encryption and decryption are key components of cryptography, which has its roots in mathematics. It makes it possible to transfer or keep private data securely through open

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

networks, like the internet, so that only the intended receiver can access and understand it.[vi]

Cryptoanalysis is the study and interpretation of encrypted communication, while cryptography deals with data protection. A fascinating combination of analytical reasoning, mathematical methods, pattern identification, persistence, resolve, and luck is involved in classical cryptanalysis.

Cryptology, which includes both cryptography and cryptanalysis, is the thorough study of covert communication techniques. Message cracking is the area of expertise for cryptanalysts, sometimes known as attackers. Cryptography comes in different strengths; strong cryptography generates ciphertext that is very hard to decrypt without the right key. For comparison, deciphering strong encryption would take longer than the universe's age, even with all of the computing power available today, including billions of machines doing billions of checks each second. Certain security standards must be fulfilled in each application-to-application communication.[vii]

There are five basic purposes for cryptography.

i) Authentication: The process of demonstrating one's identity is known as identity verification. Despite both having serious flaws, name-based protocols are still the most widely used technique of host-to-host verification on the worldwide web.

ii) Privacy / Confidentiality: preventing undesired access and guaranteeing that the communication is only accessible by the intended sender.

iii) Integrity: Presenting the sender with the assurance that the text they have obtained has not been changed or tampered.

iv) Non-repudiation: A procedure to confirm that the communication was actually sent by the person listed as the sender.

v) Key exchange: The procedure that allows senders and recipients to trade cryptographic keys.[viii]

Definition of Cryptology:

Data encoding and decoding using mathematical concepts is known as cryptography. Sensitive data can be securely transmitted or stored via unprotected networks, like the Internet, with the assurance that only the intended receiver can access it. Cryptanalysis is

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

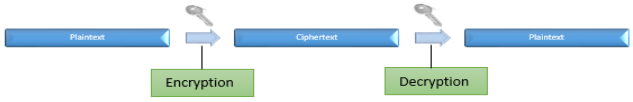
the study of examining and decrypting encrypted communication, whereas cryptography is primarily concerned with data security. Analytical reasoning, mathematical methods, pattern identification, persistence, and a small amount of luck are all necessary for classical cryptanalysis. Attackers are the term used to describe those who specialize in cryptanalysis. Cryptography and cryptanalysis are both included in cryptology.[ix]

The art of writing and decoding codes is known as cryptology, and it dates back more than 4,000 years. The discipline of cryptology had its first formal recording in the ninth century CE, thanks to the work of Arab cryptologists who not only created new codes but also carefully described methods for cracking them, a process known as cryptanalysis.[x]

Different kinds of Cryptography:

Three various kinds of cryptography exist.

- Symmetric-key Cryptography
- public-key cryptography
- Hash function.



(a)Symmetric-key Cryptography: A single key for both encryption and decrryption.

(b) Public-key Cryptography: A pair of keys, one for encryption and the other for decryption.

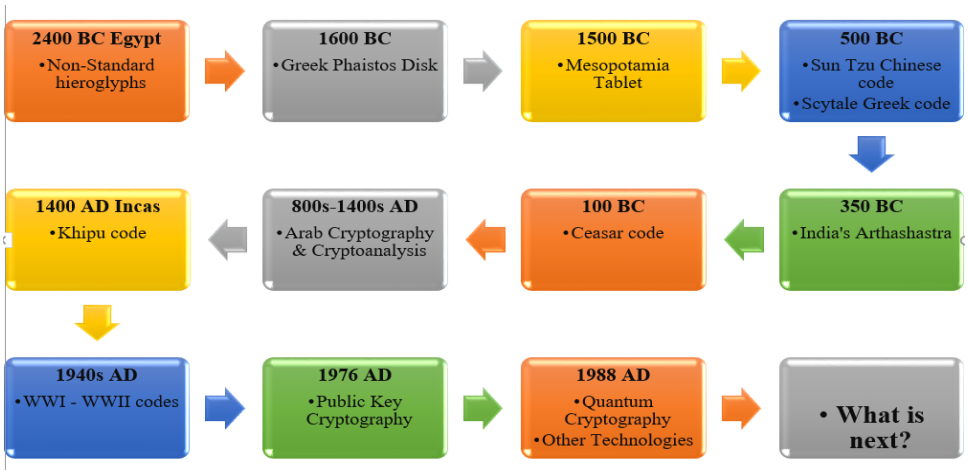
(c) Hash Function (one-way cryptography): Hash Functions have no key since the plaintext is not recoverable from the ciphertext.

Muslim Contribution in Cryptology

Various civilizations, including the Egyptians, Chinese, Indians, Mesopotamians, Greeks, and Romans, have used cryptography to conceal signals from ancient times. The Spartans are credited with using a cipher device called the scytale for clandestine communication

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

among military leaders about 400 BC, which is the earliest known usage of encryption in letters. The writing medium for the scytale was a tapering rod that had a strip of parchment or leather twisted spirally around it. The letters were scrambled when they were opened, creating the cipher. But when the strip was rewrapped around a comparable rod, the first message surfaced once more. As a result, the first transposition cipher is assigned to Greek invention. Aeneas Tacticus wrote a piece of literature called "On" in the fourth century BC.[xi]



These civilizations were all purely focused on cryptography; none of them worked in cryptanalysis. Shortly after the Arab-Islamic empire was established, the Arabs developed cryptology, which comprises both the creation of ciphers (cryptography) and their deciphering (cryptanalysis). Several Arab academics have advanced both fields of cryptology. The information is as follows.

i) The book "“مفتاح الكنوز في إيضاح المرموز Miftah A-Kunuz fi Idah Al-Marmuz" (Key to Treasures on Clarifying Ciphers) was written in 1353 AD by Ali ibn ad-Durayhim and was a major cryptology reference book.

ii) The extensive guidebook for secretaries "صبح العشى في صناعة النشاء Subh Al-A’sha fi Sina’at Al-Insha" (The Dawn of the Blind in the Writing Industry) was written in 1412 AD by Shihab al-Din al-Qalqashandi and included a section on cryptology. He added to this handbook a section on codes, mainly based on ibn ad-Durayhim's writings.

iii) In 1963 AD, Clifford Bosworth from the University of St Andrews translated "The Section on Codes" from al-Qalqashandi's Subh al-a‘shā and included a commentary on Arabic cryptology in an article.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

iv) "Cryptology originated among the Arabs," according to renowned cryptology historian David Kahn, in his 1967 publication "The Code Breakers – The Story of Secret Writing." Al-Qalqashandi's 1412 CE encyclopedia "Subh Al-A'sha fi Sina'at Al-Insha'" contained sources that Kahn's allegation was based on. These allusions mainly came from a book called "Muftah Al-Kunuz fi Idhah Al-Marmuz" (The Treasures Key in Deciphering Cryptograms), written by Ali ibn ad-Durayhim in 1350 CE. Ibn ad-Durayhim was thought to have lost his manuscript at the time.

v) Scholars from the Arab Academy of Damascus, Dr. Mrayati, Y. Alam, and M. al-Tayyan, set out in 1979 to verify Kahn's claim by searching for the missing version of Ibn ad-Durayhim's work.

vi) Their investigation produced an amazing discovery! They discovered more than fifteen Arabic works on cryptology that date from the second to the eighth Hijri centuries, or the ninth to the fifteenth centuries CE, in addition to finding the manuscript of Ibn ad-Durayhim. The Suleymaniye Ottoman Archive in Istanbul, Turkey is where most of these books were found.

vii) After being thoroughly edited and examined by Dr. Mrayati and his group, the manuscripts were published in Arabic in 1987. Subsequently, the Arabic texts were translated into English and released in nine volumes.[xii]

viii) The oldest known cryptologic text is found in one of the manuscripts. It is called Risalah fi Istikhraj al Mu'amma (Treatise on Decrypting Cryptographic Messages) and was written by Ya'qub ibn Ishaq al-Kindi in 850 CE.

Al-Kindi's Treatise demonstrates the attraction Arab thinkers had with their native language, which inspired them to investigate fields that would later become important to cryptology, including combinatorics, linguistics, and statistics related to the Arabic language and alphabet. In his Arabic dictionary Al-Ayn, Mathematician Al-Farahidi used permutation and combination methods to create comprehensive listings of every prospective Arabic words, both with and without vowels. Letter frequency analysis was demonstrated by Al-Kindi about 1200 years ago as a means of breaking alternative numbers![xiii]

ix) According to recently discovered documents, the cryptography methods created by Ibn Adlan (666 AH / 1268 AD) and Ibn ad-Durayhim (762 AH / 1359 AD) were similar to those created by G. Porta (1535–1615 CE), Blaise de Vigenère (1523–1596 CE), and G. Cardano (1501–1576 CE).

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

x) Ahmad ibn Wahshiyyah (291 AH / 914 CE) included 93 alphabets and symbols, including Hieroglyphics, in his book "Shawq al Mustaham fi Ma'rifat Rumuz al-Aqlam" (Seekers Joy in Learning about Other Languages' Symbols). Ibn Wahshiyyah recorded his findings on the symbols and was able to decode almost half of the Hieroglyphic alphabet.

xi) Arab academics correctly decoded hieroglyphics around the ninth century CE, almost a millennium before Jean-Francois Champollion, according to the instructor Okasha El Castro from the Institute of History at the University of Cambridge.

The work that Arab academics did in the field of cryptology was not isolated; it formed a "School" of cryptology that thrived for centuries. Academics participated in collaborative learning, merging their distinct perspectives and sharing their discoveries with others. The freshly discovered documents corrected the course of Cryptology's history, reversing its origins by more than five centuries and supplying proof for Kahn's claim that "Cryptology was born among the Arabs."

European contribution to cryptology

It is impossible to consider the development of cryptology in Renaissance Europe in a vacuum. While it is true that the papacy and the Italian city-states gained power over time, the development of current cryptography techniques must be viewed within their historical context. It's also crucial to remember that over the Middle Ages, a lot of cryptographic techniques from classical antiquity were virtually lost. Newly found manuscripts from Turkey and the Middle East have revealed significant advancements in cryptology during the first three centuries of Islamic civilization, specifically between 700 and 1000 AD. Previously, classical cryptology had been largely forgotten in central Europe during the Middle Ages. Ibrahim A. AlKadi outlined a few of the elements that influenced the creation of cryptographic techniques in a recent article. The need for effective administrative structure in the growing Islamic empire, the advancement of translation and linguistic studies, the high degree of public literacy demanding the protection of sensitive information, and the substantial advancements in mathematics, including the development of algebra, were among these factors. The oldest known treatise on cryptology was written by the encyclopedic author Ismạl al-Kindï (801–873), who was among the first to contribute to the discipline of cryptology. Al-Kindí covered cryptanalysis techniques in his "Treatise on Cryptanalysis," which included the first documented explanation and use of statistical techniques to resolve cryptographic issues. The oldest known treatise on cryptology was written by the encyclopedic author Ismạl al-Kindï (801–873), who was among the first to contribute to the discipline of cryptology. Al-Kindí covered cryptanalysis

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

techniques in his "Treatise on Cryptanalysis," which included the first documented explanation and use of statistical techniques to resolve cryptographic issues.[xiv]

Methods of Cryptology

Cryptography techniques render the plaintext unintelligible to outsiders by implementing various modifications, rather than concealing the existence of a secret message. Transposition and substitution are the two main types of transformations. Transposition is the process of rearranging the plaintext's letters so that their normal sequence is broken. A transposition can be demonstrated, for example, by rearranging "secret" to "ETCRSE". In substitution, different letters, numbers, or symbols are used in place of the plaintext's letters. In a more complex design, "secret" might become "19 5 3 18 5 20" or "XIWOXY". Transposed letters lose their original locations but retain their original identities (e.g., the two "e's" in "secret" are still represented in "ETCRSE"). On the other hand, in substitution, the letters change in identity but maintain their original places. It is possible to mix substitution with transposition. When compared to transposition systems, substitution systems are more diverse and significant. They rely on the idea of the cipher alphabet, which offers a list of equivalents that may be used to change plaintext into an encrypted format. For instance, a sample cipher alphabet would couple the letters "a" through "m" in plaintext with the cipher letters "L" through "M" and the letters "n" through "z" with the cipher letters "H" through "P". This graphically represents the substitution of matching cipher letters for plaintext letters and vice versa. Therefore, "enemy" would become "CHCME" and "swc" would become "foe" in the encoding. The title "cipher alphabet" is retained for a set of correspondences in which the plaintext letters are missing or jumbled, since cipher letters are always equivalent to their plaintext counterparts. A cipher alphabet could sometimes provide more than one replacement letter. For example, the plaintext letter "e" may be replaced by any of the numbers 16, 74, 35, or 21, which are known as homophones, rather than always being replaced by a single figure like 16. Null symbols are symbols that are included in cipher alphabets sometimes just to confuse interceptors but have no actual meaning. When the above-described single cipher alphabet is used, the system is called monoalphabetic. The system becomes polyalphabetic when it employs several cipher alphabets in an organized fashion. Simplifying polyalphabetic substitution is as simple as placing a second cipher alphabet beneath the first and switching between them. For each plaintext letter, this means using the first alphabet, then the second, and so on, repeating the cycle. For the third plaintext letter, it means using the first alphabet, and so on. Modern cipher machines use millions of cipher alphabets to create polyalphabetic ciphers. There is a distinction drawn between code and cipher in the context of substitution

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

systems. A code consists of a huge number of words, phrases, letters, and syllables that are replaced with codewords, code-numbers, or more generally, codegroups, in place of these plaintext parts. For example, the codewords "DVAP" for "emplacing," "DVBO" for "employ," "DVDM" for "enable," and "DVEL" for "enabled" might all be used to represent these concepts.[xv]

Origin of modern cryptography:

Modern cryptography and cryptanalysis developed in the several tiny Italian states throughout the later Middle Ages as a result of competing demands. Protecting secret correspondence between ambassadors and their respective sovereigns was one thing; understanding and deciphering secret correspondence between foreign diplomats and their leaders was quite another. Investigations carried out recently at the State Archives of Venice have produced new information clarifying this historical trend.[xvi]

Phases of Cryptography:

There are three different phases to the history of cryptology in the modern era:

i) Manual Cryptography:

Manual cryptography dominated the first phase, which lasted from the beginning of the field's development in antiquity to the end of World War I. Cryptography efforts in this period were limited by the talents of code clerks, who utilized simple memory tricks. Because of this, ciphers were usually limited to a few pages long, or a few thousand characters. Although the basic ideas of cryptanalysis and cryptography were known, the amount of security that could be achieved was still limited by manual methods. Given enough time and effort, the majority of cryptographic systems from this era might be decrypted using cryptanalysis techniques. Essentially, if ancient civilizations had known about cryptography, they could have theoretically used any system developed during these two millennia.

i) Mechanization of Cryptography:

The second stage, which is still going strong now, is called the organization of encryption and started soon after the end of World War I. Technology during this time was mostly focused on calculating machines like the Brunsvigas, Marchants, Facits, and Friedens, which employed motors, cylinders, ratchets, pawls, and sensors, and telecommunication

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

systems like telephones and telegraphs, which used drilled paper clips, cellphone routers, and switches. Spinning devices first appeared around this time and were extensively used by all sides in World War II. Compared to manual methods, these machines allowed for much more sophisticated operations and provided faster and more accurate encryption and decryption processes. As a result, ciphers' capacity increased and several hundred of million letters could be encrypted and decrypted. This advancement was further sped up by the switch from electrical to digital technologies. In 1999, for example, the U.S. government developed and produced a one piece of silicon chip that could process 6.7 billion pieces per second as an application of the Data Encryption Standard (DES). Similar to this, an Internet backbone circuit can handle 10 gigabits per second (1010 bits per second) of traffic using a single silicon chip to implement the Advanced Encryption Standard (AES). Since the first manual encryption systems were able to decode hundreds of words per second, this represented a huge leap. Towards the conclusion of the twentieth decade, the amount of encrypted text processed over just one path has grown by almost a billion times, and this tendency is still growing exponentially.

ii) Public Key Cryptography:

The most significant change emerged during the third phase, which surfaced in the latter the final two decades of the 20th century and discussed the widespread adoption of cryptology in the digital era. During this time, digital signatures, authentication systems, and the dissemination of cryptologic function execution capabilities were introduced. However it is appealing to link this phase exclusively to the introduction of encrypted public keys, this viewpoint is unduly constrictive. Rather, the third period of cryptology emerged as a natural reaction to the need to find ways to let electronic information perform all the tasks that physical papers used to perform.

Conclusion:

The advancement of cryptology has been greatly aided by the cooperation and achievements of Muslims and Europeans. Muslims have advanced encryption and decoding techniques significantly throughout history, establishing the framework for contemporary cryptography. Muslim scholars have developed a vast body of knowledge and competence in the topic, as demonstrated by works like "Subh Al-A'sha fi Sina'at Al-Insha" by Shihab al-Din al-Qalqashandi and "Miftah A-Kunuz fi Idah Al-Marmuz" by Ali ibn ad-Durayhim. The discovery of manuscripts from the ninth century CE further highlights the significant contributions made by Arab scholars.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

The establishment of cryptographic systems and cryptanalysis have also seen significant advancements by European scientists. Cryptology has seen revolutionary changes thanks to inventions like the Enigma machine during World War II and resulting advances in computer-based encryption. The mutual influence and individual contributions of Muslim and European experts have resulted in the development of contemporary encryption systems that guarantee the security of digital communication in the globalized world of today.

The development of cryptology is evidence of the intellectual capacity and cooperative spirit of Muslims and Europeans. In an increasingly digital world, their efforts have changed the profession and continue to encourage innovation, protecting the security and privacy of information.

---

[i] Elnaim, B. M. E., & Al-Lami, H. A. S. W. (2017). Arab contributions in cryptography, case study: Ibn Dunaynir effort. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(1).

[ii] Sharma, S., & Gupta, Y. (2017). Study on cryptography and techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(1), 249-252.

[iii] Goyal, S. (2012). A Survey on the Applications of Cryptography. *International Journal of Science and Technology*, *1*(3), 352-355.

[iv] Savant, V. B., & Kasar, R. D. (2021). A review on network security and cryptography. *Research Journal of Engineering and Technology*, *12*(4), 110-114.

[v] Hiwarekar, A. P. (2013, July). Application of Laplace transform for cryptographic scheme. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 3-5).

[vi] Network Associates (1999), An Introduction to Cryptography, United States of America, p-11.

[vii] Gary C. Kessler (2010), An Overview of Cryptography, Available at https://www.garykessler.net/library/crypto.html#purpose

[viii] Ibid

[ix] Network Associates (1999), An Introduction to Cryptography, United States of America, p-11-12.

[x] Al-Suwaiyel, Muhammad, Dr. (2018), Arab Origin of Cryptology, Available at https://muslimheritage.com/arab-origins-of-cryptology/

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

[xi] History of Cryptology, https://www.britannica.com/topic/cryptology/Developments-during-World-Wars-I-and-II

[xii] Volumes 1 to 6 can be downloaded from: *https://publications.kacst.edu.sa/SystemFiles/Books_Pdf/302.pdf*

[xiii] Sami Eltamawy, (2022), The Arab Cryptanalysts and Al-Kindi's Method, King's College London, p-2-4.

[xiv] de Leeuw, K., & Bergstra, J. (2007). THE RISE OF CRYPTOLOGY IN THE EUROPEAN RENAISSANCE. The History of Information Security: A Comprehensive Handbook, 277.

[xv] Khan David, The Codebreakers, The Story of Secret Writings, The MacMillian Company, New York, p: 72-78.

[xvi] Dooley John F., (2018), History of Cryptography and Cryptanalysis, Springer International Publishing, p-20-29.