iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.57144

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

A Comprehensive Overview of the Unequivocal Influence and Evolution of Cryptography on Security

Aadya Jain
Student of Fountainhead School, Surat

Abstract: ***As this society unfolds into a conundrum of new possibilities and technical advancements, it simultaneously sets ground to several unprecedented challenges for its users. What today's digitally ensnared society doesn't understand is its vulnerability to malicious software, cyber attacks, and innumerable privacy violations that come their way as they mold themselves into this digital realm. For a country like India, that well adapts to the newer technologies invented across the globe, it is astonishing to see almost 1.3 million cybersecurity breaches being recorded in 2022, a hideous spike from 2019. Current internet users feel the need to be active on such delusional platforms every minute of their day, exposing themselves at every stage. This empowers unethical practices and practitioners to lure unsuspecting candidates into their traps and obtain private information linked to several sensitive, especially monetary affairs of the individual, consequently resulting in severe financial losses. Ironically, the very technological influence that facilitates security breaches is one that helps in its deterrence and prevention. One of the most predominant and recent technologies that have empowered its influence over such prevention is cryptography and encryption. Traditionally, prior to the widespread awareness about cryptography, companies and individuals used Access Control Lists(ACLs) that work on the basic principle of restricting or revoking access on certain administrative grounds offering data confidentiality and security on the internet. Apart from these companies, in the ancient times, there was significant use of Caesar Cipher, a way of encryption that works on the principle of substitution by a shift of some number down the alphabet. These traditional methods lacked transparency, had increased complexity, were insufficient for rapidly growing networks such as online social media, and also lacked scalability. In order to compensate for these challenges, a newer technology concatenated with cryptography is to be made prevalent in society so that it can offer more scalable and trustworthy encryption and security prevention from online security breaches across the globe. With this ideology, prevention and awareness both can be obtained and a better and safer society can be established in this generation.***
Keywords: Access Control Lists (ACLs), Cryptography, Encryption, Cybersecurity, and Caesar Cipher.

I. INTRODUCTION

Cryptography is the science behind securing communication employs codes and ciphers that help encrypt and decrypt a particular message. Cryptography ensures data confidentiality and data integrity serving as two integral parts within its broader application and has been applied in real life situations concerning warfare, digital security, etc since numerous preceding decades. As today's society is ensnared in the wrath of technological vulnerabilities that violates the privacy of an individual to an enormous extent, cryptography emerges as one of the most viable solutions that incorporates transparency, trust, ethics, and simplicity as it continues to develop in recent times. Although the scientific community began to embrace cryptography predominantly in recent decades, the application roots back to the millenia where it helped Romans under Julius Caesar, Germany under Adolf Hitler during the World War II, and England with the help of experts like Alan Turing, Gordon Welchmen, Harold Keen, etc at the Bletchley Park. Furthermore, its lesser-known yet significant historical uses include the first World War, featuring tools like the Vigenère disk, code books, and manual transposition ciphers. However, it is crucial to note that as these cryptographic modules need to be evaluated on a variety of ethical, economical, social factors in order to coherently understand their mechanism in the real world.

II. TIMELINE OF EVENTS (EVOLUTION)

The evolution of cryptography has been simultaneous to several other inventions across ancient history as physicists and mathematicians worked in unison to benefit this interdisciplinary field for a greater accomplishment. The initial uses of cryptography revolve around inscription done by the Romans, Egyptians, and several other civilizations to carve their sentimental artifacts.

©IJRASET: All Rights are Reserved

Following this were its applications in the first and second World Wars where both parties used these resources for subterfuge, secret communication, and strategy discussion with their armies up front. As the World Wars terminated, technological advancements embarked upon an unprecedented course, becoming increasingly demanding across universities, foundations, and centers that were then established for mathematics and sciences across the globe. Below is the explicit timeline categorized into 4 main categories that are the Pre-computing age(ancient times), War-time Communication, Modern Computation, and Contemporary Computation.

A. Pre-computing Age (ancient times)

The exploration into the dawn of cryptography unveils an intricate tapestry of developments along history, beginning from the hieroglyphics of the Egyptians to the Caesar Ciphers of the Romans. Primarily, recorded history of the Egyptian nobleman's tomb in 1900 BC showed inscriptions replacing ordinary text with hieroglyphics, associated with pictorial writing during the Egyptian civilization. These hieroglyphics were replacements against ordinary text that were then carved upon Egyptian entities such as tombs and several artifacts across their civilizations. The primary reason for such encryption revolved around secret communication since the decryption to these elements were only known to a few. Up until the end of the 18th century, no reputed Egyptologist was able to decrypt the Egyptian hieroglyphics. However, several conclusions were determined by two of the famous Johan Akerblad and Thomas Young who were able to achieve partial success in deciphering the Rosetta Stone. Rosetta stone, a stone accidentally found on Napoleon's expedition to Egypt in 1799, near Rashid on the Mediterranean coast.

The Rosetta Stone was an accumulation of three scripts, hieroglyphic, demotic, and Greek. The cumulative partial success was presented on the study of the demotic texts from the Rosetta stone and in the presumption of the false hypothesis that stated these hieroglyphics to be symbols rather than elements of pictorial writing. Thomas Young later rectified his wrongdoings and further succeeded in identifying the fact that demotic texts were essentially curated from these hieroglyphics which further led him to isolate single consonant hieroglyphics. After 21 years of extensive research, where every Egyptologist failed to fully decipher the Egyptian inscription, a Frenchman Jean-Francois Champollian was finally able to decipher the encoded writing in 1822. He was able to achieve complete success in his dissertation since he was able to identify the fact that these hieroglyphic writings were not symbols but a phonetic script, a script corresponding to speech sounds. Champollian later died in 1832, however, was considered one of the greatest minds in the field of Egyptology. After the Egyptian Civilization, advancements in ancient technologies were profoundly prevalent during the Roman period under Julius Caesar that introduced the Caesar Cipher in 100 BC. The Caesar cipher was introduced by Julius Caesar during his Gallic Wars as he intended to communicate with his besieged Cicero. This was when Julius Caesar used the basic principle of substitution replacing the Greek alphabet with the Roman alphabet. This basic substitution helped him deceive his opponents and successfully communicate with his allies all along. The Caesar cipher then introduced was an invention that substituted the letters in the message with a shift of a particular number down the alphabet. This was widely recognized as one of the primary applications of cryptography in ancient history. While the Caesar Cipher was profoundly recognized, another method through which cryptography was performed in the ancient times was the Scytale Cipher invented by the Greeks in 400 BC. This worked on the principle quite opposite to one that the Caesar Cipher used. The Scytale jumbled the message into an anagram for each of the words. Here, the characters of the plaintext are ciphered in a way that the encrypted version has the same characters but are scrambled; it operates as a transposition cipher.

Additionally, as the Caesar Cipher gained ubiquity, a device called the Secret Decoder Ring was introduced in society that acted as a cultural emblem resonating to the concept of cryptography in ancient history for the Romans. The Secret decoder ring was used as a popular tool in movies and online cinema that portrayed the ancient warfare and history of several civilizations. Although no real time implementations have been prevalent in the chronology of cryptographic development, the secret decoder ring acted as a cultural symbol to several communities across society.

B. War-time Communication

The lives of people prior to the invention of the internet in 1983 was an accumulation of discovery and struggle as the 1900s embarked upon the two crucial world wars one from 1914 to 1918 and the other from 1939 to 1945. Even though these world wars were lethally agonizing for humankind, it resulted in the inventions and discoveries of several components that are currently one of the most crucial parts of society. In the field of cryptography, these two world wars incorporated a series of inventions and revelations that changed the course of history internally within the warfare as well as externally for the society. Primarily, in context to World War One, the use of cryptography was accentuating in fields of telecommunications that was exceptionally paramount with the armies upfront.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Moreover, there was perceptive use of cryptography and encrypted communication, the invention of the radio was what played a crucial role in shaping the chronology of events across the war. The invention of the radio allowed military intelligence to effectively communicate with its allies, and their commanders, however, due to loose wireless communication, it had these parties potentially vulnerable to interception by the enemy. Although the use of cryptography did help both the parties, the speed at which radio was being adopted, encryption wasn't paced very well with the same.

There were several events across the war powered by cryptography that led to the war taking an unprecedented course several times. One of the most predominant examples of the same is the entry of the United States in the war, merely because of the British decryption of the Zimmermann Telegram by the Germans to Mexico. This led to the formation of the Crypto Arms race, a series of code breakers that had the advantage in the field of warfare at that time. Another predominant cryptographic application during the first World War was through the Vigenère disk that employed several substitution ciphers rather than just one like in the Caesar Cipher. The Vigenère disk comprises the plaintext being partially concealed within the ciphertext using monoalphabetic substitutions. The use of Vigenère disk was again used for secure communication across the parties and their allies due to the shortcomings of the radio. Apart from this, another predominant application of cryptography was the Navajo Code that used Native American Languages as their primary language of communication to and fro their allies. The use of the Navajo language presaged the use of the same encrypting technique even in World War Two later.

Following world war one, the second world war was one that was geographically, politically, and technologically the most widespread war in history. This was primarily because it showcased predominant differences in the technology used during the early 1900s or even the first world war compared to the ones used during the second world war in the 1940s. Additionally, this war was one that effectively pursued unprecedented communication in context to an explicit use of encrypting technologies. The First World War was one that hit several milestones as soon as Bletchley Park was introduced in England. Bletchley Park was an English country house located in Milton Keynes which was further pronounced as the principle house for allied code-breaking against German encryption. Bletchley Park is one of the most profound places that was termed as the birthplace for electronic computing. The establishment of Bletchley Park was initiated when the infamous computer scientist and mathematician Alan Turing along with his colleagues wrote a letter to Winston Churchill in pursuit of gathering resources that were required for the preparation of the following World War. As in when the letter was approved, Bletchley Park became the hub of secrecy and decryption against the German forces.

One of the most predominant applications of cryptography in the second world war was the usage of the modified Enigma Machine by the Germans as a way to establish operational communication across their allies and armed forces. With Enigma in the works, experts at the Bletchley Park including the ones from Poland that were able to crack the exceptionally difficult course on cryptography at the University of Poznan who were Rejewski, Rjoyski, and Zygaliski. The Polish had already created a code-breaking/decrypting device named BOMBA before, however, they believed that the Germans would modify the way Enigma would function ahead of the war which is why they sent their mechanisms and external support that spurred the works at Bletchley Park. As the Polish provided the working of BOMBA, Alan Turing perceptively understood the weaknesses in the same, resulting in a creation of a crib based mechanism that further allowed the decrypters to identify inconsistencies in the machine as possible matches of the converted plaintext with its corresponding ciphertext. As Alan Turing succeeded in this, he further contacted Keen through which they could cumulatively create BOMBE, an improved version of the Polish BOMBA. Turing required Keen's help in order to identify the potential stops, a term associated with possible matches that were priorly scrambled into ciphertext. Simultaneous to the creation of BOMBE, Alan Turing even focused on identifying the loop holes in Enigma until he figured out that the Enigma wheels never encoded a letter as the same letter alongwith the fact that Enigma had a 250 characters limit, making many messages to be sent in packets.

As Keen and Turing created BOMBE, Bletchley Park was successfully able to decrypt all of the messages across their communication lines. The parties were internally prohibited from using wireless communications fearing interception which is why there was an initial installment of such mechanisms. As the decryption increased, Adolf Hitler presented an unprecedented machine that he called Gheimschribers, Lorenz S242 that used teleprinted codes for communication. For a long time Bletchley Park couldn't deduce the reason for increased traffic in the communication lines they initially decrypted messages from, however as they did, they introduced another, the first electronic computer named Colossus. Colossus was built on a deadline by Thomas Flowers who was told to have it completed by the 1st of June 1944, 4 days prior to the D-Day for Operation Overlord(Battle of Normandy). The quick assemblage of Colossus helped the parties against Germany critically identify that Hitler had fallen for the subterfuge regarding the invasion which according to him was now on Pas De Calais and not Normandy. This intelligence was further provided to General Eisenhower who then claimed the success wouldn't have been possible without Bletchley Park.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

C. Modern Computation (Post-war)

As the war ended during the mid 1940s, there was a sudden change in the educational system across the West. It was when the countries understood that the safest country is the one with the smartest people. With this notion, the countries further established science and mathematics centers while the Bletchley Park shut and the scientists from there moved to several universities as professors. Since the works at Bletchley park were a secret until recent times, they were prohibited from sharing their works about electronic computation and decrypting machinery, however their assistance and presence at these universities paved the way for the creation of several computers and supercomputers including Manchester Baby, Ferranti Mark I, Harvard Mark I, and US Army ENIAC. Although these computers kept on getting invented, there was scarcity of resources and a surplus of intelligent minds across the globe. To solve this, significant individuals such as Larry Smarr contacted Peter Lax to create a Lax Report in pursuit of resource availability (supercomputers) in universities and other hubs for better technological development.

The introduction of supercomputers caused an increase in the prevalence of cryptography as it helped experts test their decryption algorithms, identifying weaknesses, and further rectifying them. Apart from this, supercomputers even made newer cryptographic techniques to be available such as lattice-based cryptography and several others that were possible due to the extremely quick tests through supercomputers. Ahead of the post war computation, there was the invention of the internet that further expanded the influence of cryptography in society. Post-war computation resulted in two major breakthroughs known as the public/private key confidentiality and the cryptographic hash. Both of these are profound methods of encryption that became ubiquitous as other technologies simultaneously grew. Primarily, in context to the public/private key cryptography, the private key scheme is symmetric cryptography where the key used for encryption is what is used for decryption. While this is a great way for encryption, it showcases issues in secure key distribution without external interception.

On the other hand, public key cryptography is when there are two keys used and is considered asymmetric. Public key cryptosystems are ones that have keys mathematically related to one another wherein the public key is provided to all interested parties, while the second key, the private key is the ones that needs to be kept secret and to be provided to those who the message is for. To generate these keys, it is necessary to keep them in pairs, which is why it is essential to choose huge prime numbers and multiply them. Following this, there is a need for computation via the larger number generated as the product to obtain the public and private key. Furthermore, following the post war computations, the last breakthrough was the cryptographic hash function which revolves around an online programming function that converts a huge block of plaintext into a series of numbers as a string as its digest. The cryptographic hash function checks the integrity of the ciphered text in context to whether or not it has been tampered with. It is important to note that the input for the cryptographic hash function is variable in size however the digest generated is of a fixed size.

D. Contemporary Computation (Early 21st Century, Current)

As the 20th Century came to an end, one of the most breakthroughs that took place in the late 1990s was the invention of quantum computation that spurred extensive growth of cryptography all across the globe in the early 21st Century. The beginning years of the 21st century encountered intellectual theories being presented at an international level on a daily basis with hypotheses enough to change the course of technology all across the world. Quantum computing was invented in 1998 by Issac Chung of Los Alamos National Laboratory, Neil Gershenfeld of MIT, and Mark Kubinec of the University of California at Berkeley. Although this initial invention wasn't applicable for problem solving and merely incorporated nanoseconds of coherence, it was one that effectively demonstrated the basic principles of quantum computation in early history. Throughout the history of cryptographic evolution, there have been three major revolutions that changed its being enormously. It started with the Kings and Queens using basic shift ciphers that was then revolutionized into the shared key system up until very recently which was now, in the 21st century again revolutionized into a scheme that operates on asymmetric cryptographic function involving a different key for encryption and a different one for decryption. This solved the issue of secure key distribution since the public key required zero protection.

With asymmetric key cryptography being one of the most prominent ones in society currently, it is extremely important to understand that with the extensive research and development currently underway for quantum cryptography, within the next decade, it is highly likely for quantum computation to take cryptography up an unprecedented level. Currently, there are several algorithms associated with cryptography that have helped technology to grow exponentially such as Homomorphic encryption, RSA(Rivest-Shamir-Adleman), Obfuscation, Format-preserving encryption(FPE), Attribute-based encryption(ABE), Elliptic Curve cryptography (ECC), and Advanced Encryption Standard(AES). Primarily, homomorphic encryption is a kind of encryption that works as an extended version of traditional encryption and decryption.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Using homomorphic encryption, an individual can encrypt a message using any traditional asymmetric encryption, however, it can also compute and perform different operations on the encrypted message without having to decrypt it at any point in time; this happens via homomorphic encryption. This kind of encryption was first introduced in 2009 by Craig Gentry and is currently applicable for several governmental activities such as E-voting and E-cash systems.

Apart from homomorphic encryption, another predominant encryption algorithm prevalent in society revolves around RSA(Rivest-Shamir-Adleman). This is one of the oldest modern cryptosystems which was first published in 1977. This kind of algorithm works on the mathematical principle of asymmetric key encryption. The next predominant recently prevalent cryptographic technique is Obfuscation. Obfuscation works on the means of an obfuscator that can potentially convert straightforward program code or revealing metadata into one that is rather difficult to comprehend where classes and variables are switched to meaningless terms that otherwise would make no sense in a programming software/code. To reverse obfuscation, just like any other encryption algorithm, incorporates of several deobfuscating techniques including slicing that cuts out unimportant bits from the code into the most relevant lines of code within the program or compiler optimization and program synthesis that even help deobfuscate the programming code. Additionally, these obfuscating techniques even include adding redundant code, packing, etc that can increase code secrecy and data security against hackers.

Apart from these, are two other cryptography techniques known as Format-preserving encryption(FPE) and Attribute-based encryption(ABE) that revolve around data security. Attribute based encryption predominantly revolves around a generalization of public key cryptography, however, the private key for decryption is often associated with certain attributes technically. This can primarily be applied to store customer information on the database in a way that within the company only certain management can view it. In a similar manner, format-preserving encryption(FPE) is one that revolves around data conversion for confidentiality in a manner that keeps the format the same. For instance, the most appropriate application of FPE is in the security against credit card numbers. When a customer enters a credit card number for storage, it converts into a different set of numbers that still look like a credit card number but in reality is just a random set of numbers stored. This allows data confidentiality in several of these banking activities and systems. Lastly, another exceptionally predominant algorithm in the field of cryptography is ECC, Elliptic Curve Cryptography that works as an alternative to RSA as another predominant algorithm under public-key cryptography. ECC is a rather growing public key algorithm since it has a relatively smaller key size and is mathematically more difficult to crack than RSA, making it more secure and efficient to work with. The uses of ECC are predominant in fields of digital signatures and several others.

III. POSITIVES AND NEGATIVES (IMPLICATIONS)

There are a range of implications associated with all stages of electronic computing that gave rise to several cryptographic techniques that have had multiple applications for data security, cybersecurity, etc in the technological field. Herewith is the detailed analysis of Economical, Ethical, Political, and Cultural implications of cryptographic applications on all the 4 stages discussed in the timeline aforementioned.

A. Pre-computing Age (Ancient Times)

The pre-computing age ranges back to early civilizations like the Egyptian and the Roman period that incorporated basic methods of cryptography for purposes of secret communication between the royals in society during that time. The pre-computing age gave birth to a series of cryptographic methods such as the Caesar cipher, hieroglyphics, etc that each had their socio-cultural sentiments associated with. These methods outline a range of economic, cultural, ethical, and political implications that need to be evaluated.

Primarily, in terms of the Caesar Cipher that was very well introduced during the Roman period highlighted a series of economic implications predominantly outlining the wheel's main purpose to secretly communicate during warfare and other military activities. The introduction to the Caesar cipher paved a way for secure communication that further led to military gains in the form of gold, silver, and slaves. These economic gains expanded the trade route back in that period for the Romans. The introduction to the Caesar cipher even spurred the development of cryptography in the following decades as scientists and mathematicians spent years working on the foundational cipher wheel in order to develop the modern ways of cryptography and encryption that offers stringent data security and confidentiality. Apart from the economic implication, another predominant implication revolves around the ethical perspective. While the Caesar cipher was rather a great tool to maintain security and effective communication, it was one that could've resulted in the shift of the power dynamics against the opponent parties, giving them an undue advantage. Although this can be viewed on a positive note, the question of ethics is predominantly based on the perspective of the individual.

Furthermore, the introduction of the Caesar Cipher gave rise to several cultural significance that are still prevalent in society today.

One of the most predominant cultural significances of this simple substitution cipher revolves around the birth of the Secret Decoder Ring, a concept introduced in the late 1960s as a playful tool replica of the Caesar cipher wheel. This ring was an emblem associated with the tool invented by Julius Caesar in remembrance of him and his doings that flourished the epithet of the Roman Empire. Apart from the caesar cipher, the pre-computing age even accounted for the Egyptian hieroglyphics which can be classified as the epitome of cultural significances as these hieroglyphics were prominently used on their tombs, temples, and other religious destinations in order to convey prayers and sacred text. Each phonetic symbol represents an intricate Egyptian heritage decorated around their monuments and sentimental artifacts predominantly portraying a positive cultural implication of these Egyptian hieroglyphics back during the Egyptian civilization. Apart from this, Pharaoh and other sacred individuals of Egyptian culture often used to document their achievements using hieroglyphic symbols on tombs and other artifacts again portraying significant relation with Egyptian culture which was further extended for secret communication and encryption.

B. War-time Communication

War-time communication incorporated itself of several extensive breakthroughs in the field of cryptography including the invention of the internet, the first electronic computer, new improvisations on Polish machinery, Adolf Hitler's new encrypting device apart from Enigma, establishment of the Bletchley Park, and several others that cumulatively questioned technology in terms of economics, ethics, and politics.

Foremostly, the primary breakthrough was during world war one wherein both parties spent significant money on the simultaneous research and development in order to build telegrams, and basic machinery that can accommodate secure and secretive communication. While the world war one was alongside the invention of radio that incorporated wireless communication but with easy interception, there was significant expenditure by the Germans as well as the other allied parties about the Zimmerman telegram, or even the Vigenere disk for monoalphabetic substitutions, a predominant extension of the previously established Caesar Cipher. These encrypting and decrypting tools cost primarily on the basis of the characters sent, however, as an overview, as both parties effectively used these devices for communication on a daily basis, the monetary costs would've been rather significant. Additionally, following the first world war, the second one that extensively changed the course of technology incorporated extensive labor costs, machinery cost, and even the cost of its implementation. Starting right from the Bletchley Park, its establishment alone costs millions of dollars that were initially approved by Winston Churchill. Apart from this, Bletchley Park hosted 10,000 workers on a mundane basis for the span of the entire war, again generating labor expenditure to an extensive extent. Moreover, the expenses associated with the creation of machinery and computers such as BOMBE and Colossus were yet another significant economic implication that although helped the tech society paramountly resulted in a great deal of economic expenditure by the State.

Furthermore, in terms of the ethical implications of using these devices it again highly depends on the perspective it has been viewed from. For instance, the Allied forces against Germany used, from their perspective, subterfuge against Hitler's armed forces, directing them towards a fake attack on Pac de Calais instead of the Battle Of Normandy as Operation Overlord. In order to check whether Hitler had believed the deceit, experts at Bletchley park along with the guidance of Tommy Flowers created the first Colossus to break into the ciphertexts communicated via Lorenz S242 Gheimschribers of Hitler. Such an act might turn out to be ethical from the perspective of Bletchley Park but can also be deemed as political propaganda and ruthless deceit in a neutral battlefield from the opposition parties. Another predominant ethical dilemma revolves around the argument of whether decrypted information gave rise to unprecedented war crimes and atrocities or prevented them which again differs according to perspective. Additionally, simultaneous to these ethical implications, these war-time encrypting technologies even gave rise to a set of political implications that extensively changed the course of the first world war.

World War One used the Zimmerman Telegram to secretly converse with Mexican intelligence which was further intercepted by the British Signals before it reached its destination cumulatively resulting in the active involvement of the United States in the war henceforth. This unprecedented political shift in the first world war was further accompanied by several other political breakthroughs that perceptively shows the flipside to cryptography and its applications in the real world.

C. Modern Communication (Post-war)

As both the world wars came to an end, the demand for technology spurred extensively giving rise to supercomputers, and several other inventions such as the internet and other encryption technologies that made tedious work easy for experts and scientists that tested algorithms on a daily basis. These post-war communications again highlighted significant implications economically and ethically as these inventions paved a way for security as a double edged sword.

Primarily, as the wars ended, Peter Lax and Larry Snarr, two highly appointed individuals created a Lax report that requested important resource availability at several destinations across the West, especially in universities that had intellectual professors and inventors who had their inventions at a halt due to the unavailability of resources. In a similar manner, in order to deliver and produce these supercomputers, it costs millions of dollars to gather labor, have a workplace, and further find appropriate tools for the supercomputers. Another predominant economic gain from modern communication was the invention of systems such as symmetric/asymmetric cryptography alongwith cryptographic hash functions that ensured data confidentiality and integrity pertaining to temperament with the encrypted data.

Apart from the economic benefits and drawbacks of these inventions and technologies, one of the most questionable implications of these technologies is the ethics associated with the same. In terms of the symmetric key cryptography, it is one that while is really efficient in encrypting information, its key circulation across systems that are highly dangerous to the secured data is one that questions the ethics of symmetric key cryptography. However, in terms of cryptographic hash functions or asymmetric cryptography, it is one that is considered rather ethical unless a hacker uses it to defend its own information for its purposes. One of the most prominent examples of the same revolves around the recent argument of government interference in citizen communications. This argument perceptively discusses the pros and cons of government authorities listening to every bit of information and communication amongst citizens in hopes of crime and terrorist prevention from society. This was applicable after the lethal terrorist attacks in Mumbai in the 2000s that had the terrorists communicating using cryptography(unethical) which further compelled all kinds of communication to be centrally disabled for days in the city causing havoc across the place.

D. Contemporary Communication (Current)

The last and the current phase computation and communication is yet evolving but is one that has the most extensively technical resources viable for a secure future. However, from the scratch in the early 21st century to the current developments, they highlight a range of economic and ethical concerns that need to be addressed and evaluated for better coherence to understand the dawn of electronic computing, communication and more.

Primarily, current methods of cryptography are within each and every aspect of an individual's life. Starting minimally from a video call where sound waves are transmitted across systems as analog and digital is the basic form of cryptography in the current modernized world. However, in an attempt to introduce such softwares in society, it profoundly encounters several economic benefits pertaining to future investment and consumer based data security although it is important to note that the expenditure associated with producing these technologies are also equivalent to the economic benefits it had monetarily on society and these scientific fields.

Apart from the economic implications, one of the most important implications of these cryptographic modules revolves around its ethics. These mechanisms are considered ethical up until malicious softwares use similar kinds of encryption techniques to safeguard their purposes from cyber experts that further result in breaches or the fact that these cryptographic breakthroughs have taken over society at an extent that if a company fails to safeguard their information even minimally it causes a havoc to their digital security. In order to assess these ethical dilemmas there are two predominant incidents that surfaced online in the recent years revolving around the Flipkart data breach and the 2020 Solar wind Data breach. Primarily, in terms of the Flipkart data breach, it was due to the lack of using cryptography which on one hand might impose as the company's carelessness while it might also be assessed as the superiority of cryptography in society. The Flipkart data breach revolved around malicious software entering the databases of Flipkart and comprising their customer's private information including phone numbers, names, addresses, pin codes, etc that might cause a risk to their privacy and private life. This coherently assesses the nature of cryptography and the ethics associated with it.

Furthermore, apart from the Flipkart Breach, another predominant breach in the United States revolved around the 2020 Solarwind breach pertaining to the cybercriminals using obfuscation, a predominantly used encryption technique for e-voting and other ethical practices, for their means of extracting data and comprising the privacy and safety of citizens. This 2020 breach involved a supply chain attack where these hackers entered into the Orion Framework on the Tulsa Company, Solarwind who had more than 30,000 companies using this framework as their IT infrastructure.

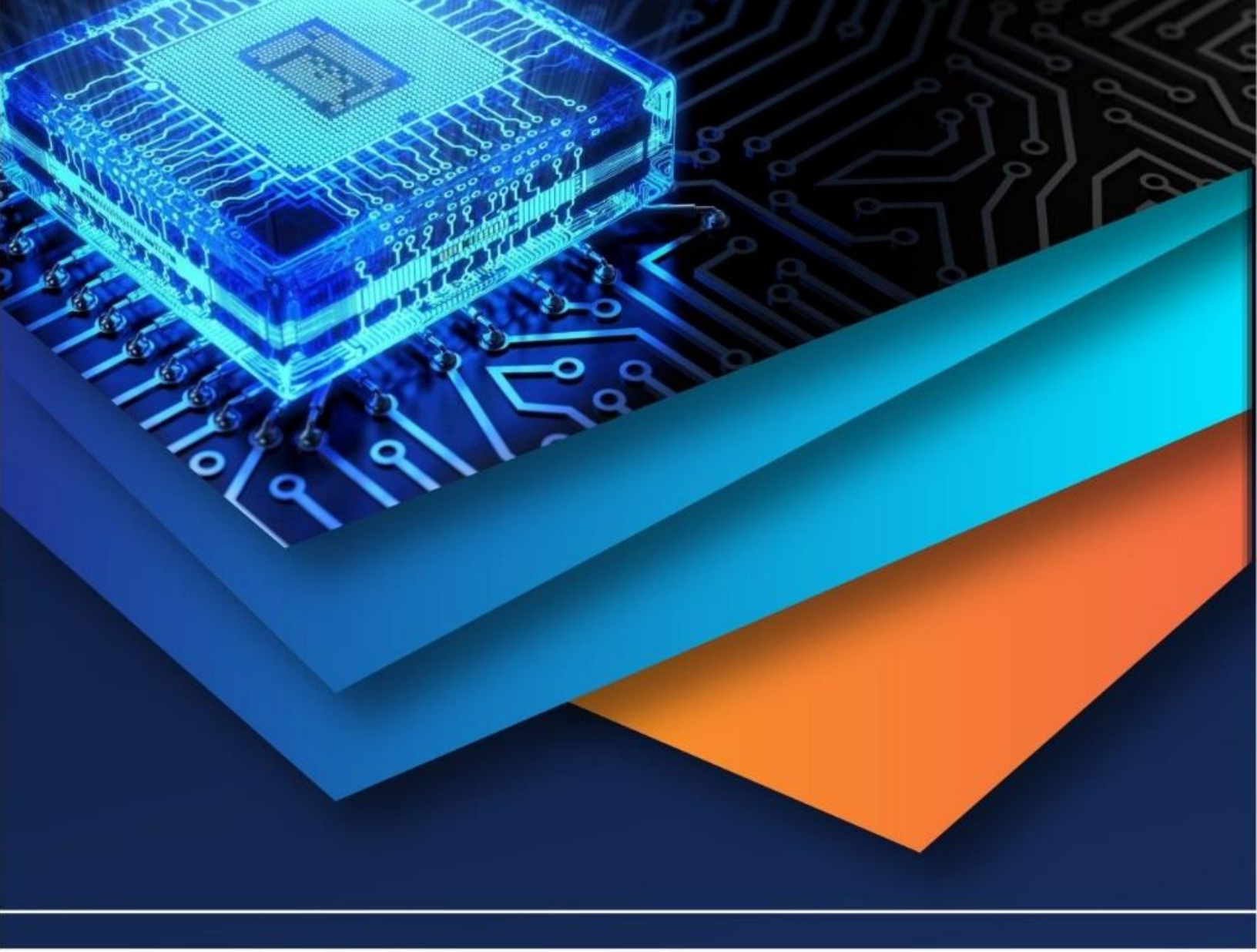
This used obfuscation in a way that it changed their means of hacking into gibberish using an obfuscator confusing the management who primarily monitored these data breaches and prevented them. Other prominent uses revolved around stealthy communication which made the entire breach look subtle and secretive using the tools of cryptography that were previously used for ethically being discreet about private information.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

V. CONCLUSION

Thus, to conclude, the ever-evolving scientific technology of cryptography is one that enunciates over basic and complex data confidentiality and integrity that needs to be thoroughly maintained in order to be digitally secure and communicate in a way through which external malicious software isn't able to intercept and gather information they shouldn't be aware of. Moreover, it is crucial to understand that like every other important scientific and mathematical breakthrough, this is also one that will have its own positives and negatives in terms of economics, ethics, politics, and even culture. At its core, cryptography is something that is viable, required and of utmost cruciality in the current times and without cryptography no data security can be possible. Keeping this in mind it is again necessary to note that with these emerging technologies are even newer platforms such as artificial intelligence and Internet of things(IoT) that are currently gaining ubiquity across society which can cumulatively result in a much larger breakthrough in terms of the foreseen quantum computation to an unprecedented course of events that may be possible in the upcoming years. Therefore, it is extensively paramount for individuals to understand that their vulnerability towards technology has reached to an extent that minimal mistakes can create havoc while minimal carefulness and awareness in this digital society will digitally protect a significant chunk of one's private information.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)