International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Review on Ancient Cryptographic, Modern Cryptographic and Quantum Cryptographic Techniques

Mangala Sharma[1], Dr. Rajesh Boghey[2], Ritu Prasad[3]

[1]Research Scholar, Computer Science & Eng., TIT(Excellence), Bhopal, India
[2]HOD, Computer Science & Eng., TIT(Excellence), Bhopal, India
[3]Assistant Prof., Computer Science Eng., TIT(Excellence), Bhopal, India

Abstract

Cryptography has a long and fascinating history, evolving from ancient techniques to modern methods and now exploring the potential of quantum mechanics. This review paper provides a comprehensive overview of cryptographic techniques from past to present.

We begin by examining ancient cryptographic techniques, tracing their origins back to 2000 B.C. when the ancient Egyptians used "secret" hieroglyphics. We also discuss evidence from ancient Greece and Rome, such as secret writings and the famous Caesar cipher [1]. These early methods laid the foundation for the field of cryptography. Next, we delve into modern cryptographic techniques that have become increasingly complex and diverse in their applications. We explore how cryptography now makes extensive use of mathematical concepts from fields like information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics. We also discuss how the development of digital computers and electronics has revolutionized cryptography, allowing for the encryption of any kind of binary data and the design of much more intricate ciphers [2].

Finally, we examine the emerging field of quantum cryptography, which aims to harness the principles of quantum mechanics to achieve new cryptographic functionalities beyond classical information alone. We survey some of the most remarkable theoretical uses of quantum information for cryptography, as well as the limitations and challenges faced by cryptographers in this new paradigm [3].

By tracing the evolution of cryptography from ancient times to the present day and beyond, this review paper provides valuable insights into the rich history and promising future of this critical field of study.

Keywords: Cryptography, Quantum cryptography, Modern Cryptography

1. Introduction

Across thousands of years, cryptography has developed from basic means of covert communication to the intricate algorithms that support contemporary digital security. This article intends to investigate the history of cryptography, starting with prehistoric traditions that paved the way for modern approaches, continuing through modern cryptography's advances, and concluding with the revolutionary advancements of quantum cryptography.

Cryptography was mostly used in antiquity as a means of protection against enemies and secrecy. The ear-

liest documented application of cryptography dates to approximately 1900 BC in Egypt, where scribes used strange hieroglyphs to obfuscate messages. Julius Caesar and other historical personalities helped to popularize cryptography by using straightforward substitution ciphers to transmit confidential military communications. Even though these early systems were simple by today's standards, they laid the groundwork for encryption and secrecy, two concepts that still shape modern cryptography techniques.

Cryptographic systems became more complicated and powerful as technology developed. With the introduction of algorithms like the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), modern cryptography emerged in the 20th century, signaling a dramatic change. These technologies changed information protection in the digital age by introducing concepts like symmetric and asymmetric key cryptography, in addition to improving data transmission security.

With the advent of quantum cryptographic techniques, we are at the cusp of a new era in cryptography. Utilizing the ideas of quantum mechanics, quantum cryptography develops impenetrable encryption techniques. Quantum cryptography promises to safeguard data against possible risks posed by quantum computing, providing a fundamentally different approach to secure communication than classical cryptographic systems that rely on mathematical complexity.

This review will examine how cryptography has evolved historically, assess how modern cryptography is doing, and consider how quantum cryptography may affect data security in the future. We may better appreciate the crucial role that encryption plays in protecting our digital environment by being aware of these advances.

One method to ensure message confidentiality is using cryptography. The Greek translation of the phrase is "secret writing." These days, however, high-level cryptography ensures that information delivered is safe enough that only the authorized recipient may access it, protecting the privacy of people and organizations [4]. Cryptography has a long history and is still being researched as an ancient method. Examples date back to 2000 B.C., when the Egyptians employed "secret" hieroglyphic writing. Other pieces of evidence include the well-known Caesar cipher from ancient Rome and hidden manuscripts from ancient Greece [5]. Every day, encryption is used by billions of individuals worldwide to safeguard data and information, even though the majority are unaware that they are utilizing it. Although cryptography is very helpful, it is also quite brittle because even a single programming or specification error can lead to a cryptographic system being compromised [6].

2. Basic Terminology of Cryptography

A cryptographic system's fundamental idea is to encrypt data or information in order to safeguard its confidentiality by making it impossible for an unauthorized individual to understand. Two prevalent applications of cryptography include data transmission via unsecure channels, like the internet, and information tampering to prevent unauthorized individuals from understanding what they are viewing after they have gained access to the data. Within the field of cryptography, the information that is hidden is commonly referred to as "plaintext." The act of hiding the plaintext is called "encryption," and the resultant encrypted plaintext is called "ciphertext." "Encryption algorithms" are a set of rules that facilitate this operation. " An "encryption key," which is supplied to the encryption algorithm as input along with the data, is typically used in the encryption process. The receiving side can obtain the data by employing the relevant "decryption key" in conjunction with a "decryption algorithm" [12].

The process of transforming legible and fluid statistics into a form that is unchangeable for protecting information is known as cryptography. The Greek words "Kryptos" (meaning unknown and invisible) and

"graphikos" (meaning writing) are the origin of the word cryptography. The process of converting regular plain language into incomprehensible text and vice versa is similar to cryptography. It is a method of keeping and sending data for a predetermined amount of time so that the people who are meant to see it and process it can do so most efficiently. Cryptography can now be used for customer authentication in addition to safeguarding data from loss or tampering. The data that needs to be covered is referred to as legitimate textual content. It could consist of characters, numbers, executable programs, images, or other types of quiet information. Crypher text is the term used to describe records that are meant to be translated; it's a term used to describe a sequence of "worthless" or meaningless records. It is the data intended to be sent specifically via a network; numerous methods are required to convert plaintext into encrypted text.

3. Historical/Ancient Algorithms

A few historical algorithms will be explained in this section, along with examples for a nonmathematical reader using pencil and paper. These algorithms predate the idea of public key cryptography by several years.

3.1. Casear Cheaper: During the Gallic Wars, Rome's emperor Julius Caesar created one of the earliest known instances of encryption. This kind of method encrypts the letters A through We by using the letters three positions ahead of each letter in the alphabet to represent them, and using X, Y, and Z to represent the remaining letters A, B, and C. This indicates that a "shift" of 3 is used, while we could achieve a comparable result on the encrypted text by using any number between 1 and 25. As a result, a shift is now frequently considered a Caesar Cipher [12]. One of the simplest cryptography examples, the Caesar cipher is easy to crack: to decrypt the ciphertext, one needs to shift the shifted letters three letters back to their original positions. This weakness may have been sufficient for Julius Caesar to use it during his wars, but since the Caesar cipher's shifted letter is always three, all that is needed to crack the ciphertext is to shift the letters [13].

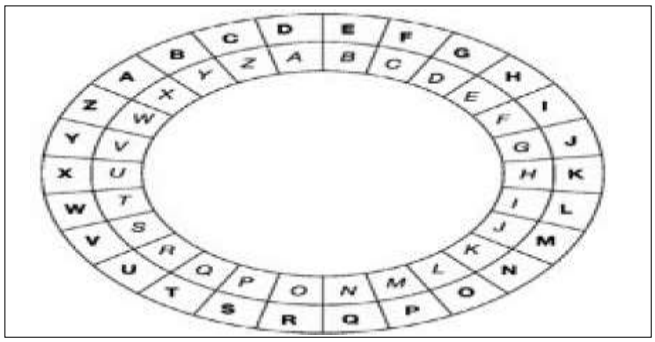

Fig. 1. Caesar Cipher encryption wheel

3.2. Simple Substitution Chipers: For example, consider the Simple Substitutions Cipher, also called the Monoalphabetic Cipher. In a Simple Substitution Cipher, the alphabet letters are placed in a random order beneath the alphabet that is written correctly, as demonstrated here:

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

The key used in encryption and decryption is the same. Here, "each letter gets replaced by the letter beneath

it" is the encryption rule; the decryption rule would be the opposite. For example, QDN is the matching ciphertext for the plaintext CAN [12].

3.3. Transposition Chiper: Another way that some cipher families operate is by using a key and a specific rule to order the plaintext's letters so that they can be transformed into cipher text. Transposition is the process of changing the plaintext's letters using rules and a key. One of the most basic types of transposition ciphers is the columnar cipher, which comes in two forms: "complete columnar transposition" and "incomplete columnar." Whichever form is employed, the written plaintext is represented horizontally by a rectangle whose width should match the length of the key. As many rows as are required to write the message can be present. The plaintext is written and all empty columns are filled with null to ensure that every column has the same length when complete columnar transposition is applied. As an illustration:

s e c o n d
d i v i s o n
a d v a n c
i n g t o
n i g h t x

The cipher text is then derived from the columns depending on the key. In this example, if we used the key “321654”, the cipher text is going to be:

cvdng eiaii sdncn donox nsatt oivgh

On the other hand, the null characters are omitted from an incomplete columnar transposition cipher since the columns are not necessary to be finished. Columns of varying lengths are the result, and this can make it harder to read the ciphertext without the key [14].

4. Modern Algorithms

4.1. Stream Chipers: The plaintext is encrypted by XORing the pseudorandom bits and the plaintext, which is how stream ciphers work. The pseudorandom bits are created from the key. In the past, people occasionally avoided using stream ciphers because they were more likely to be cracked than block ciphers. But now, after years of design development, the stream cipher is more reliable and secure, making it suitable for usage in Bluetooth connections, mobile 4G, TLS connections, and other applications. Every bit in a stream cipher is encrypted separately. There are two different kinds of stream ciphers: asynchronous and synchronous. In the former, the ciphertext depends on the key stream, whereas in the latter, the key stream depends on the key. We have a dotted line in Figure 3. The stream cipher would be asynchronous if it existed; synchronous otherwise. One type of asynchronous cryptography is the cipher feedback (CFB) [5].

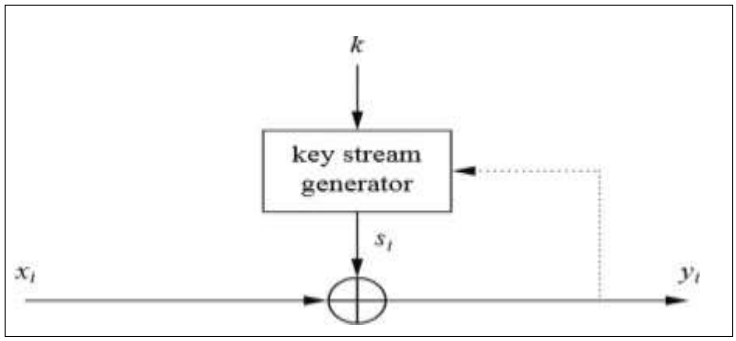

Fig. 2. Asynchronous and synchronous types of stream ciphers

4.2. Block Chipers: An encryption algorithm and a decryption algorithm combine to create such a type of cipher:

- The block of plaintext (P) and the encryption method (E) are given a key (K), and the product of a ciphertext block and C is C. The formula for the encryption process is C = E (K, P).
- The ciphertext is decrypted for the plaintext, P, in the preceding step. This is the inverse of the decryption procedure (D). The formula for it is P = D (K, C).

For added security, a pseudorandom permutation (PRP) is employed in the block cipher. Accordingly, an attacker will be unable to decrypt the block cipher and calculate the output from any input if the key is kept secret. As long as K's confidentiality and randomness are guaranteed from the attacker's perspective, this is acceptable. This basically means that the values that are either input into or produced from the block cipher would not allow the attacker to identify any patterns.

Two numbers are typically mentioned in a block cipher: the block size and the key size. The worth of both determines the security. A 128-bit or 64-bit block is used by many block ciphers. The length of the cipher-text and the memory footprint are short since it is important that the blocks not be too big. In terms of the length of the ciphertext, a block cipher processes blocks rather than bits. In other words, in order to encrypt a 16-bit message and its blocks using 128-bit blocks, we must first convert the message into 128-bit blocks. The block cipher will not begin processing and produce a 128-bit ciphertext until this need is satisfied.

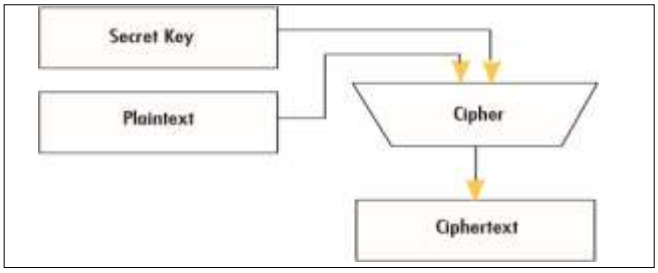

Fig. 3. Block cipher diagram

In terms of memory footprint, in order to operate and process a 128-bit block, we require a minimum of 128 bits of memory. Most CPUs have tiny enough registers to fit. Otherwise, this can be achieved using specialized hardware circuits. In most situations, a block of 68 bits, 128 bits, or even 512 bits is still small enough for effective implementation. However, the cost and performance of the implementation might be significantly affected when the blocks increase bigger, or kilobytes long [13].

4.4. Public Key Systems: One could argue that the development of public key encryption represented a revolution in cryptography. It is clear that general cryptography and encryption remained exclusively the domain of the military and intelligence services even in the 1970s and 1980s. Only public key methods and systems allowed cryptography to proliferate into new domains. Since the public key can be disclosed without ever being concerned about, public key encryption allows us to communicate without relying on secret channels. The public key's characteristics are outlined as follows:

1. Key distribution over public channels are permitted when public key encryption is used. This could simplify the system's initial deployment and make it easier to maintain when parties join or depart.
2. Less secret keys need to be stored when using public key encryption. Every party has the option to store their own private key securely, even in situations when everyone wants to be able to communicate

securely. It is possible to keep other parties' public keys in an insecure manner or to retrieve them when required.

3. Public key cryptography works better in open situations, particularly when parties that have never communicated before wish to interact and communicate safely. When a business wants to encrypt credit card information, for instance, they could be able to disclose their public key online, and anyone looking to make a transaction can obtain the merchant's public key as needed [6].

4.5. Digital Signature: Digital signatures were nonexistent prior to the development of computers, in contrast to cryptography. Since the advent of computer communications, there has been a need to talk about digital signatures, particularly in business settings when several parties are involved and each needs to promise to uphold their statements and/or proposals. Centuries ago, people first pondered the idea of unforgeable signatures—but those were handwritten signatures. In a paper titled "New Directions in Cryptography," Diffie and Hellman originally presented the concept of digital signatures [15]. Consequently, authentication by alone is unable to bridge the confidence gap between a sender and a recipient in this scenario. In a manner akin to the handwritten signature, something further is needed, namely the digital signature [16].

Digital Signature Requirements: The "digitalization" period that we are presently seeing and living in gave rise to the interaction that established the connection between encryption and signature. An unforgeable signature schema would need to meet the following requirements:

- Every user should be able to create their own signature on any document they choose.
- Every user should be able to quickly ascertain whether a given string is actually the signature of another user.
- On documents that the original owner does not sign, no one should be able to create signatures [17].

Digital Signature Principle: It is crucial to demonstrate that a message originated from a user or individual both inside and outside of the digital sphere. This is accomplished in the modern world by using handwritten signatures. Public-key cryptography is used to generate digital signatures. The fundamental notion behind this method is that the person signing a document or communication uses a private key, also referred to as the private-key, while the person receiving the message or document needs to use the matching public-key. Figure 7 illustrates the digital signature scheme's basic idea.

5. Quantum Cryptography

The way traditional computing works is that operations are carried out in the form of bits. At any given time, these bits can have a value of 0 or 1. The quantum physics concept of superposition is used in quantum computing. When anything, such as a bit, is in two states at the same time, it is called a superposition. This means that quantum bits, also known as qubits, can be in both the 1 and 0 states at the same time. Because the bits might be set to 00, 11, 01, or 10, doing computation on a set of two classical bits takes four calculations. Because qubits can be in all four states at the same time in quantum computing, the quantum computer can execute calculations on all four states. This creates a slew of problems for today's encryption technologies. The private key for some encryption algorithms, such as RSA, which is used in the majority of eCommerce transaction encryptions, is obtained by factoring a number that is the product of two large prime integers. This is incredibly difficult to achieve with traditional computers, and with a long enough key length, it may take thousands of years to break. The usage of qubits in quantum computers, on the other hand, greatly reduces the time it takes to crack an algorithm like RSA. Although

the key length can be increased for added security, a 256-bit key is now only as secure as a 128-bit key in the face of quantum computing.

Using what we currently know about physics, quantum cryptography creates an unbeatable cryptosystem that is impenetrable that is, one that cannot be compromised without the sender or recipient of the messages knowing about it. The term "quantum" itself describes the most basic properties of the tiniest matter particles and Energy: Nothing can be in violation of quantum theory, which explains everything that exists. It differs from conventional cryptography systems in that a major component of its security concept is based more on physics than on mathematics [19].

In classical information, a bit is a base that can be either 0 or 1.A unit of quantum data is called a qubit. In quantum cryptography, there are two distinct processes that are used: conversion and polarization. Conversion involves converting data into bits of 0s and 1s, which are then conveyed via polarized photons. These amazing achievements are made possible by quantum cryptography, which takes advantage of the characteristics of tiny particles like photons. There are three selected bases of polarization for the photons, and the following are the likely outcomes of the measurement based on the bases:

- Rectilinear (horizontal or vertical)
- Circular (left-circular or right-circular)
- Diagonal (45° or 135°).

Even though there are three bases, only two of them are typically used. In order to determine their orientation relative to each of these bases of polarization individually, photons are used. Conventionally, one would expect the photon to have a certain polarization that is measurable but unaffected by the measurement. In any case, photons are quantum objects; a property is assigned to them automatically upon measurement. The type of measurement affects the object's property. This implies that a photon's polarization must be taken into account after measurement and that the polarization will depend on the premise chosen for the estimation.

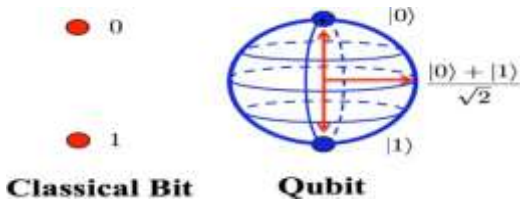

Fig. 4. Classical bit vs Quantum bit

5.1. Quantum Key Distribution - "BB84" is the current name for the first quantum key distribution technique, which was developed in 1984[20]. In 1991, Artur Ekert advanced the field of hypothetical quantum cryptography by proposing that the security of a quantum cryptography convention based on Bell's inequalities may be achieved by the use of "entangled" two-molecule states, as described by Einstein-Podolsky-Rosen (EPR) [21]. Bennet, Brassard, and a collaborator carried out the first experiment on QKD in 1989 while developing a BB84 protocol prototype system. A real-world example of quantum cryptography is demonstrated at a distance of roughly 30 cm [22].

Data protection is a continuous challenge because hackers steal information on a regular basis. Information encryption technology available today has been compromised and will become outdated in a matter of years. The principles of physics demonstrate that Quantum Key Distribution (QKD) technology can help safeguard the sensitive data we deliver, both now and in the future. A secure communication technique called quantum key distribution (QKD) uses quantum mechanical concepts to construct a cryptographic

protocol. With its help, two people can generate a shared, randomly generated secret key that only they know, which can be used to encrypt and decode messages [23]. The only technology that can truly deal with this long-term security concern is QKD.

This is a basic example of how keys can be distributed safely using quantum cryptography. Here, "Eve" is a stand-in for an eavesdropper, "Bob" is a receiver, and "Alice" is the sender. Usually, a single photon contains all of the information. In four distinct polarization states—vertical, horizontal, or diagonal—and in the opposite direction (0°, 45°, 90°, and 135°—Alice starts messaging Bob. Bob then takes a measurement of the polarization state, which might be diagonal (45° or 135°) or rectilinear (0° or 90°). His response will be deemed random and disregarded if the base he measures differs from the one Alice used to prepare; but, if they select the same base, the results will be precisely correlated.

Inaccurately measured photons are discarded, and accurately measured photons are converted into bits using their division. These images are now the foundation of a one-time pad that transmits encrypted data. Since the key will be the result of both random selections, Bob and Alice will not be able to decipher it, making the cryptography technique excessively safe.

In order to break into the system, let's assume that there are eavesdroppers on the network. Eve, the attacker, attempts to eavesdrop and chooses at random a rectilinear or diagonal filter to measure each photon that Alice emits. Eves will have an equal chance of choosing the right or incorrect filters when breaking the framework, and they won't be able to figure out which filter Alice was using at the time of the transmission. Even Eve manages to obtain accurate information while Bob verifies with Alice the photons he obtained; nonetheless, Eve won't be able to use the information until she knows the precise polarization state of each and every photon. If Eve cannot recognize the polarization state, she cannot create the final key.

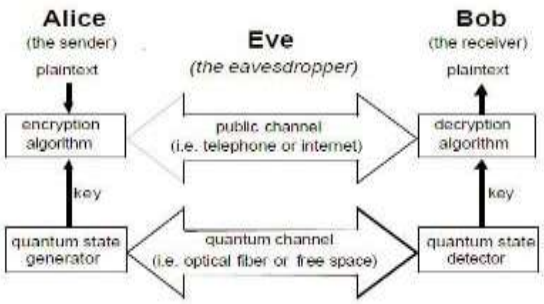

Fig. 5. Quantum Key Distribution Model

6. Conclusion

Classical cryptography has a long history dating back thousands of years, with early examples of substitution ciphers like the Caesar cipher used by Julius Caesar. Over time, more advanced techniques were developed, such as the Vigenère cipher in the 16th century. However, these classical ciphers rely on the secrecy of the encryption system itself rather than just the key, violating Kerckhoffs's principle.

In the modern era, cryptography has become a rigorous science. The Data Encryption Standard (DES) was introduced in 1973 as the first US government standard for encryption. However, DES was later broken due to its small key size. The Advanced Encryption Standard (AES) replaced DES in 2000 and is now widely used for symmetric encryption.

Quantum cryptography offers a fundamentally new approach by exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example is quantum key distribution (QKD),

which allows two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. QKD is information-theoretically secure, meaning it is secure even against an attacker with unlimited computational power.

However, quantum cryptography has mainly focused on key distribution so far. In response, post-quantum cryptography (PQC) aims to develop cryptographic algorithms that are secure against quantum computers. In 2016, NIST began a process to solicit and evaluate PQC algorithms. Four finalists were announced in 2020.

In conclusion, cryptography has evolved from simple substitution ciphers to a sophisticated science. While classical and modern cryptography rely on computational security, quantum cryptography offers information-theoretic security. However, challenges remain in applying quantum cryptography beyond key distribution. Post-quantum cryptography is a promising approach to protect against future quantum computers. The field of cryptography continues to advance rapidly to meet new security challenges.

List of References

1. Twinkal, Mohit Sharma, “Review and Analysis of Cryptography Techniques”, International Journal of Creative Research Thoughts (IJCRT), Volume 10, Issue 6 June 2022 | ISSN: 2320-2882.
2. https://en.wikipedia.org/wiki/Cryptography
3. Anne Broadbent, Christian Schaffner, “Quantum cryptography beyond quantum key distribution”, Springerlink.com, Published online: 21 December 2015.
4. N. Sharma, Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.
5. B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
6. J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.
7. S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.
8. O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.
9. N. Jirwan, A. Singh and S. Vijay, "Review and Analysis of Cryptography Techniques," International Journal of Scientific &Engineering Research, vol. 3, no. 4, pp. 1-6, 2013.
10. S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 763-770, 2017.
11. A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672,2014.
12. F. Piper and S. Murphy, “Cryptography: A Very Short Introduction”, London: Oxford University Press, 2002.
13. J. P. Aumasson, “SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption”, San Francisco: No Starch Press, Inc, 2018.
14. J. F. Dooley, “A Brief History of Cryptology and Cryptographic Algorithms”, New York: Springer, 2013.

15. W. D. A. M. E. HELLMAN, "New directions in cryptography," IEEE Transactions on Information Theory, Vols. IT-22, no. 6, pp. 644-654, 1976.
16. W. Stallings, “Cryptography and Network Security Principles and Practices”, New York: Prentice Hall, 2005.
17. O. Goldreich, “Foundations of Cryptography Basic Tools”, Cambridge: Cambridge University Press, 2004.
18. Laxman poudel, “A Review on Quantum Cryptography” International Journal of Recent Research and Review, Vol. XIII, Issue 3, September 2020.
19. https://searchsecurity.techtarget.com/definition/quantumcryptography.
20. https://en.wikipedia.org/wiki/BB84
21. https://en.wikipedia.org/wiki/EPR_paradox
22. Richard J. Hughes*, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux,,George L. Mokgari; Jane E. Nordholt, and Charles G. Peterson,”Quantum Cryptography For Secure Satellite Communications”
23. https://en.wikipedia.org/wiki/Quantum_key_distribution