International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 14 Issue 5 May 2025 || PP 48-54

The Role of Cryptography in Cyber Security

Subhalaxmi Sabitri Das[1], Sachin Jena[2], H.Dipali Singh[3]
[1]*Assistant Professor in Mathematics, Basic Science and Humanities, Raajdhani Engineering College Bhubaneswar, Odisha, India*
[2]*Assistant Professor in Mathematics, Department of Mathematics, Nimina Brundaban Chandra College, Ganjam, Odisha, India*
[3] *Assistant Professor in Mathematics, Department of Mathematics, Gandhi Engineering College Bhubaneswar, Odisha, India*

Abstract: *One description of cryptography is the study and practice of information concealment. Cryptography intersects with fields like computer wisdom and mathematics. Among the terms used in this term paper are plaintext, or information to be conveyed, Cipher textbook, or ordinary textbook that has been made incomprehensible by an operation of a fine procedure, The key is a numerical value, formula, or procedure that establishes how a plaintext communication is translated or deciphered. The cryptographic algorithm, also, is a fine formula that's used to tousle the plain textbook to produce cipher textbook. Public crucial cryptography (PKC), hash functions, and secret crucial cryptography (SKC) are the three orders of cryptography. Each bone of them will be completely described.*

Keywords: *Cryptography, Secret key, Private Key, Public Key, Cipher Text.*

Date of Submission: 15-05-2025 Date of Acceptance: 26-05-2025

I. Introduction:

The field that deals with building cryptographic systems is called cryptography [1]. Modern electronic communication is directly related to cryptography. Note that the history of cryptography is fairly old; the earliest examples date back to around 2000 B.C., when ancient Egypt utilized non-standard "secret" the hieroglyphic Since the time of the Egyptians, cryptography has been utilized in one way or another in most, if not all, of the cultures that invented written language [2]. The science and practice of concealing information is known as cryptography. The fields of mathematics, computer science, and engineering are all impacted by modern cryptography. Computer passwords, ATM cards, and e-commerce are a few examples of applications of cryptography [3]. The art and science of creating encrypted or secured communications that are only understandable by the key holder is another way to describe it. The term "cryptography" relates to both refer to the art or method of communicating in or interpreting secret writings (also known as codes or ciphers) and to the use of codes to modify digital data so that only a designated receiver may read it with a key [3].Cryptography, in its broadest definition, encompasses the use of codes, ciphers, and hidden messages. The effectiveness of concealed messages, such as those written in invisible ink or concealed inside seemingly benign language, depends on their ability to go unnoticed. They are often straightforward to decipher once they are found. Without the key codebook, codes that use predefined words, numbers, or symbols to represent words and sentences are typically hard to understand. Using computerized encryption to secure data and message transmissions is an additional aspect of cryptography. Most communications nowadays leave some sort of documented trace. Communications via telephone lines, such as faxes and emails, for instance, generate a record of the phone number and time that was called. Credit card receipts or insurance records can track financial activities, medical histories, movie rental choices, and even dietary preferences. The phone provider or financial institution records the number contacted, the transaction amount, the location, and the date each time a person uses a credit card or the phone. As phone networks evolve to digital in the future, it's possible that actual conversations will be captured and saved. All of this adds up to a significant privacy risk. One tool that can provide greater privacy is cryptography. Encrypting data, conversations, and other information empowers people to regain their privacy [4].

But the importance of cryptography extends beyond privacy. The banking systems around the world are also protected by cryptography. Open networks, like internet, are used by many banks and other financial organizations to conduct business. If bank transactions and communications aren't protected, robbers could tamper with them and take money covertly.

II. Literature Review:

In 600 B.C. the soldiers of the Greek military used the cipher text mechanism to send the confidential military information. Later in ancient Rome Julius Caesar partially invented simple letter substitution to protect military communications by cipher text methodology and named it as Caesar cipher. After the rapid involvement of computers in communication in the modern world the methodology under cryptography also evolved. As cryptographic applications are basically dependent on the computer system. At that time everyone used computers to store their data and started online financial transaction ways. But at the end the sensitive data needed to be secure and exposure of that need to be controlled by some security levels. So onward some key-security systems were developed for code breaking factors, such as encryption and decryption of data. The valuable shared data is always at risk due to improper securities measures and leads to cyber-attacks, identity theft, and financial fraud. To secure them the evolution in technologies used in Cryptography was necessary. The modern era Cryptography had come with unbreakable cipher code that was under information theory applied principles. That was demonstrated by Claude Shannon in the 1940s in his seminal paper "Communication Theory of Secrecy Systems" .The foundation of his contribution was that secure communication was a right of everyone. In early 1970s, the evolution was highly fruitful by intention of keyed-security level by Whitfield Daffier and Martin Hellman and revolutionized as Public- Private Key methodology. The data was more secure by using the key locked procedure and the users could rely on them. At first only one key was used to lock the message and shared only between the sender and receiver. At that time Cryptography was being tested in fields to see the reliability of the security levels. To secure the data many data analytics used various mathematical algorithms that could lock the data and share only by the right key. Cryptography grounded by mathematical algorithms became an easy way to compute private keys by one-way mathematical functions-problems. Optimization techniques of mathematics allow cryptography procedures to relate real life communications. Although there were some drawbacks such as resource-limited devices and easily pattern functional. Later in 1977 at the Massachusetts Institute of Technology (MIT), the most widely used public-key cryptographic algorithm based on a mathematical principle was invented by **Ron Rivest**, **Adi Shamir**, and **Leonard Adleman** and named **RSA.** In that system there are two different keys used by sender and receiver for the encryption and decryption process. In the encryption process the key shared by the sender is called **Public key** and for decryption the receiver used a key called **Private Key**. As RSA has a strong mathematical foundation it can be developed as the long-standing reliable future factor toward public-private key structure. All things in this world need to be adequate with the flow. New technology comes with wide uses of artificial intelligence, IoT, cloud computing that can be the surface for any cyber threats. The security systems need to be strong and well-implemented that can guard against the cyber crimes that can steal anybody's identity and sensitive data. In order to develop more reliable techniques now-a-days the cryptography systems are practically based on curve related phenomenon. In 1985, a new form of public-key Cryptography was developed by using an ellipse curve equation over a finite field. It was developed by **Neal Koblitz** and **Victor Miller** and named as **Elliptic Curve Cryptography (ECC).** Like RSA it also offers the same security level but the keys size is smaller. This allows devices with less processing power and memory to be accessible from ECC. In the 2000s it was more standardized by using P-256 curves and developed by organizations like **NIST (National Institute of Standards and Technology).** The latest versions of ECC are widely used to enable secure communication along with digital signatures. ECC is now commonly used in TLS, SSH and Bit coins. The communication by ECC is reliable and keeps the data safe by exploit. In future the security levels are needed to be more effective as the data is widely imported on the internet. The more it is useful and variable it should be more protected and always at risk.

III. Important Terminologies:

The procedure of cryptography includes the following terms:

- Keys:

Two cryptographic keys are used in Elliptic wind Cryptography (ECC) a public key and a private key. The proprietor alone knows the private key, which is an aimlessly chosen number. The public key is generated from the private key using elliptic wind point addition, a one-way fine operation that's delicate to reverse computationally. These keys are employed in a number of cryptographic processes, including crucial exchange, digital autographs, encryption, and decryption. ECC is effective for operation in bias with limited processing power and memory because it may give high situations of security with significantly lower crucial sizes than further conventional ways like RSA.

- Cipher Text:

A communication that has been converted from plaintext using an encryption fashion and a key is called cipher text book. Without the proper decryption key, it appears as an arbitrary and ungraspable string of characters. The thing of cipher textbook is to guard information secretiveness by making sure that unauthorized

parties cannot decrypt the data, indeed if it's interdicted on transmission. The only way to restore the cipher textbook to its original, readable form — known as plaintext — is for someone to retain the necessary decryption key. In mainstream cryptography, cipher textbook is an essential part of safe communication.

- Encryption Process :

A piecemeal from maintaining confidentiality, the encryption process is essential for guaranteeing data security and integrity in online communication networks. Asymmetric encryption, which employs a brace of keys — public and private — for secure communication, and symmetric encryption, which utilizes the same key for both encryption and decryption, are the two primary forms of encryption. It's delicate to distribute keys when using symmetric encryption since the sender and the philanthropist must have the same secret key. Asymmetric encryption is more secure for some operations, similar as digital autographs and dispatch encryption, because the private key is kept hidden by the proprietor while the public key is participated intimately.

- Decryption Process:

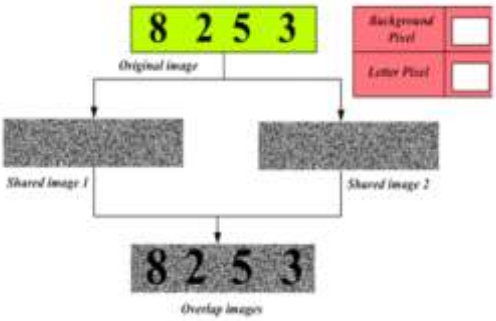
In the process of decryption, cipher textbook is converted back into plaintext, which is its original readable form. A crucial and a decryption algorithm are demanded for this procedure. Asymmetric encryption uses the private key to decrypt data that was translated with the matching public key, whereas symmetric encryption requires the decryption key to match the encryption key. Maintaining data security and confidentiality, decryption makes sure that only authorized druggies with the right key can pierce the original data. It's an essential element of secure communication systems, allowing druggies to pierce and comprehend translated or transmitted defended data. The translated data stays useless and unobtainable without applicable decryption.

IV. The Purpose Of Cryptography:

Elliptic Wind Cryptography(ECC) is essential to society because it protects sensitive data and allows for safe communication in our decreasingly digital terrain. As further individualities calculate on digital services,e-commerce, online banking, and cell phones, ECC helps guarantee that private dispatches, fiscal deals, and particular information are kept safe and private. Given that of its effectiveness and robust security, it may be used in a variety of common operations, similar as securing websites and mobile apps, as well as conserving data on smart bias and government systems. ECC helps insure the safety, sequestration, and responsibility of the digital structure that society relies on a diurnal base by promoting secure connections and digital trust. therefore, cryptography can be employed for stoner authentication in addition to securing data from loss or revision. These objects are generally achieved by three types of cryptographic systems, each of which is explained below hash functions, public-key (or asymmetric) cryptography, and secret key(or symmetric) cryptography. The original, unencrypted data is always appertained to as plaintext. The cipher textbook is translated and also (generally) decrypted into plaintext that can be used [3]. To guarantee that Elliptic wind Cryptography ECC) is successful in securing data and dispatches, certain security norms must be met. Important prerequisites correspond of

- Secure Key Generation: In order to keep bushwhackers from figuring out or anticipating the private keys, ECC has to induce strong, arbitrary keys. Secure elliptic wind operations must be used to directly decide the matching public key.
- Proper wind Selection: The elliptic wind selection is pivotal. In order to help vulnerabilities, only well-established and formalized angles, like those suggested by groups like NIST or SECG, should be employed.
- Applicable crucial operation cancellation, distribution, and safe crucial storehouse are essential to conserving ECC's security. At all times, private keys must be kept secret.
- Acceptable crucial Size While ECC provides robust security with lower keys, for long- term protection, it's pivotal to elect a crucial size that satisfies current security norms, which are generally at least 256 bits.
- Secure perpetration ECC must be enforced with tackle or software that's free of blights and impervious to side- channel attacks that could expose private crucial information, like timing or power analysis attacks. One key is employed for both encryption and decryption in secret crucial cryptography.

The sender encrypts the plaintext using a crucial or a set of rules before transmitting the cipher textbook to the philanthropist. To decipher the communication and recoup the plaintext, the philanthropist uses the same key (or rule set). Secret crucial cryptography is also known as symmetric encryption since a single key is employed for both purposes. It's clear that the secret in this type of encryption is that the sender and the philanthropist must both know the key. The dispersion of the key is, of course, the most challenge with this strategy.

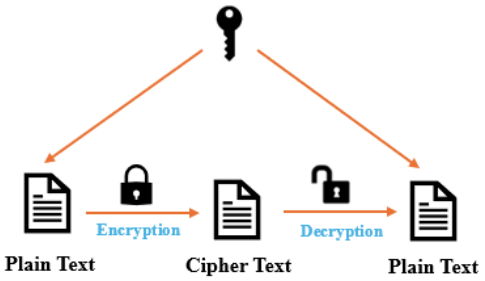


V. Types Of Cryptography:

Under Cryptography, the sender shares the information to the receiver locked by a key. The key must be shared between them so that only they can read or assess the data inside the information. This procedure is called key distribution. On the basis of key numbers or size Cryptography is divided into four basic branches. In this paper we are going to discuss only two of them:

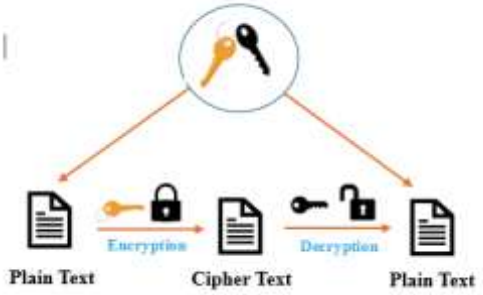
- Symmetric Cryptography:

The procedure in which there is a single key that is shared between sender and receiver for both encryption and decryption is called Symmetric Cryptography. For security purpose the key code in only share between them so that the data is secured and a cipher text code is displayed wherever the decryption process started. So it is also known as Private key Cryptography.



- Asymmetric Cryptography:

In asymmetric cryptography a pair of keys is used between the sender and receiver. The key that is used in encryption is called Public Key and locks the data shared by the sender and produces the cipher text and the other key used in decryption that converts the cipher text into plaintext is called Private Key. The public key can be shared with others but the private key can only be used by the receiver. So it is also known as Public key Cryptography.



Comparison between Symmetric and Asymmetric Cryptography:

As in symmetric cryptography only a single key is implemented in the process of encryption and decryption the process is faster than asymmetric. On the other hand asymmetric cryptography is much more

secure than symmetric as there are two different keys used in the whole process and leads to less risk of exposure of sensitive data.
The most commonly used asymmetric cryptography is:

- RSA (Rivest–Shamir–Adleman)
- ECC (Elliptic Curve Cryptography)

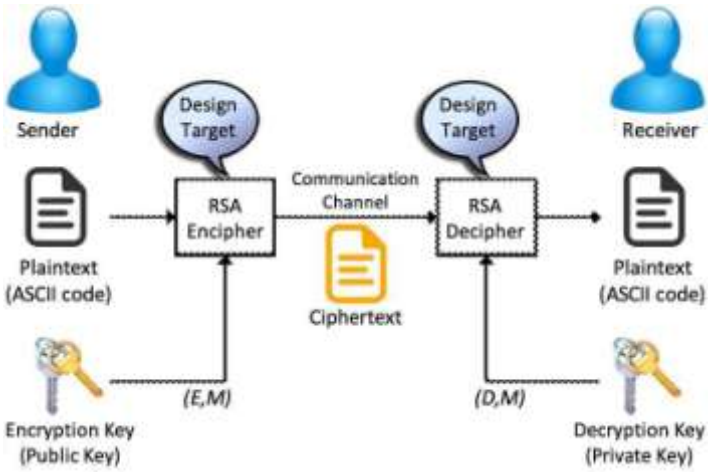
Basically in this paper ECC is widely described and its comparison with RSA.

VI. Rsa:

MIT mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman created the first and most widely used implementation of public key cryptography [13]. These days, RSA is found in hundreds of software programs and can be used for digital signatures, key exchange, and encryption of tiny data blocks. RSA employs a variable size key and a variable size encryption block. The source of the key-pair is a very big integer, n, which is the product of two prime numbers selected based on specific criteria. These primes can each have 100 or more digits, so the resulting n has around twice as many digits as the prime factors. The three stages of RSA are encryption, decryption, and key generation.

Mathematical Concept:

Euler's totient function, modular arithmetic, and Euler's theorem are among the basic mathematical ideas that the RSA algorithm uses to create keys, encrypt communications, and decrypt them. After determining the product of two large prime integers and Euler's totient, it chooses a public key (e) and computes a private key (d) based on these values, making sure that the product is equal to 1 modulo Euler's totient.



VII. Ecc:

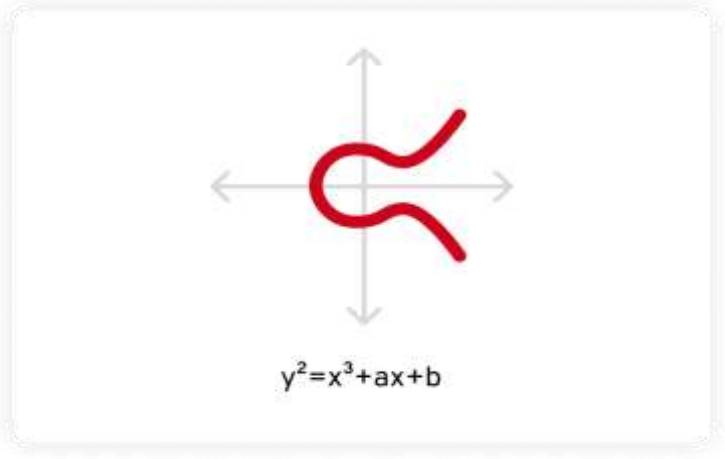
Diffie-Hellman Key Exchange is analogous to it. The elliptic curve-based public key cryptography algorithm is called ECC [14,15]. Numerous elliptic curve cryptography (ECC) techniques, such as key exchange, encryption, and digital signatures, can be created using elliptic curve arithmetic. An elliptic curve equation defined over a finite field is used in elliptic curve arithmetic for ECC purposes. The equation's variables and coefficients are components of a finite field. The intractability of ECDLP, or the Elliptic Curve Discrete Logarithm Problem, is the foundation for ECC security.

Mathematical Concept:

The cubic equation for the elliptic curve over a finite field Fp, with p is a large prime number is given the same to the equation used for calculating the circumference of the elliptic curve. The cubic equation is in the form of

$$\mathbf{y^2 = x^3 + ax + b \ldots(1)}$$

where a , b are the real numbers constant and x,y are the variables.



VIII. Hash Functions :

Diffie-Hellman Key Exchange is similar to it. The elliptic wind-grounded public key cryptography algorithm is called ECC [14,15]. multitudinous elliptic wind cryptography (ECC) ways, similar as crucial exchange, encryption, and digital autographs, can be created using elliptic wind computation. An elliptic wind equation defined over a finite field is used in elliptic wind computation for ECC purposes. The equation's variables and portions are factors of a finite field. The insubordination of ECDLP, or the Elliptic wind Discrete Logarithm Problem, is the foundation for ECC security. Examples of these two styles are Whirlpool and SHA, independently. A contraction function, f, is constantly used in the hash algorithm to induce a- bit affair from two inputs a- bit block and a- bit input from the former phase, known as the chaining variable. The algorithm specifies an original value for the chaining variable at the morning of mincing. The hash value is the last value of the chaining variable. We can observe that b > n. A pseudorandom function (PRF) or pseudorandom number creator (PRNG) can be created using a cryptographic hash function.

IX. Public-Key Cryptography And Secret-Key Cryptography Benefits:

- Since the private keys are no way need to be transferred or bared to third parties, public- crucial cryptography's main benefit is enhanced security. An adversary might, still, always find out the secret key while it's being communicated in a secret- crucial system.
- The capability of public- crucial systems to offer a digital hand fashion is another significant benefit. participating some secrets and sometimes gaining the trust of a third party are prerequisites for authentication through secret- crucial systems. Once a communication has been inked, the sender might drop it by stating that one of the actors traduced the participated secret in some way.
- Also, a judge or other third party can corroborate the authenticity of digitally inked dispatches, making them fairly binding. rather of authenticating papers, which is better fulfilled using digital autographs, secret-crucial authentication systems like Kerberos were created to authenticate access to network coffers [9].

X. Public-Key Cryptography Drawbacks:

zSpeed is a significant drawback of employing public-key cryptography for encryption; that is, documents encrypted with public key cryptography have substantially slower transmission times than those encrypted with symmetric cryptography. Since there are well-liked secret-key encryption techniques that are far faster than any public-key encryption technique now in use, it is actually prohibitive to transmit very huge documents.

XI. The Encryptionte Chniques:

- Because any modification to a message's contents will cause the recipient to calculate a different hash value than the one the sender put in the transmission, the three encryption algorithms are well-suited for guaranteeing data integrity. Data integrity is guaranteed to a high degree of confidence because it is extremely improbable that two distinct messages will produce the same hash value [10].
- Secret key cryptography is best suited for encrypting messages, which ensures confidentiality and privacy. To encrypt a communication, the sender can create a session key for each message; naturally, the recipient must also have the same session key to decrypt the message.
- To use a pun, key exchange is a crucial use of public-key cryptography. Asymmetric techniques can also be used for user authentication and non-repudiation; only this sender could have sent the message if the

recipient could get the session key encrypted with the sender's private key. Although it is rarely done since secret-key cryptography works around 1000 times faster than public-key cryptography, public-key cryptography could theoretically also be used to encrypt messages.

XII. Conclusion:

This paper show an overview about cryptography and its types. With chance in environment the security of our personal data is an essential requirement for the humans. There are both benefits and damage of everything including this security system. Cryptography plays a vital role in the modern world by securing the vast amount of sensitive data exchanged across digital platforms. In an age dominated by online communication, e-commerce, cloud computing, and mobile applications, protecting personal information, financial transactions, and corporate data has become crucial. Cryptography ensures confidentiality, integrity, and authenticity by encrypting data, preventing unauthorized access, tampering, or identity theft. It is the foundation of technologies such as secure messaging, digital signatures, block chain, and secure communications in government and military operations. As cyber threats continue to evolve, the importance of cryptography in safeguarding privacy, enabling trust, and maintaining the stability of digital infrastructure is more significant than ever.

References:

[1]. Mohamed Barakat; Christian Eder; and TimoHanke,2018,"AnIntroductionto Cryptography"www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdfAccessed on 15th June 2021

[2]. Christ of Paar; and Jan Pelzl, 2010, "Understanding Cryptography; A Textbook for Students and Practitioners". Springer- Verlag Berlin Heidelberg.

[3]. Cheswick, W.R; and Bellovin, S.M., 2003, "Firewalls and Internet security". Addison-Wesley, USA

[4]. Davies, D.W; and Price, W.L., 1989,"Security for Computer Networks". John Willey & Sons, Inc., Second Edition

[5]. Savu, L., 2013, "Cryptography Role in Information Security". University of Bucharest, Romania

[6]. Davis, D; and Swick, R., 1990, "Network Security via Private-Key Certificates. ACM SIGOPS Operating Systems ReviewVolume 24,Issue 4,pp 64–67 https://doi.org/10.1145/94574.94579

[7]. Waleffe D. de; and Quisquater, J.J.,1993,"Computer Security and Industrial Cryptography". Springer, VIII.

[8]. Diffie, W; and Hellman, M.E., 1976, "New DirectionsinCryptographyTheory".IEEETransactiononInformationTheory, VOLIT-22, No6, pp644-654

[9]. Fiat,A;andShamir,A.,1987,"How to prove yourself, Advances in Cryptology"- Proc.OfCrypto86, pp.641-654

[10]. Krawczyk, H; Bellare, M; and Canetti, R.,1997,"HMAC:Keyed-hashing for Message Authentication".https://www.rfceditor.org/rfc/pdfrfc/rfc2104.txt.pdf' Accessed on 21st May,2021

[11]. Menezes, A.J ; Van Oorschot, P.C; and Vanstone, S.A., 1997,"Handbookof Applied Cryptography". https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838&rep=rep1&type=pdf Accessed on 24th May, 2021

[12]. Vangelis Karatsiolis; Lucie Langer; Axel Schmidt; Erik Tews; and Alexander Wiesmaier, 2020, "Cryptographic Application Scenarios". https://www.researchgate.net/publication/2285598 03_Cryptographic_Application_Scenarios? Accessed on 5th May 2020

[13]. R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978

[14]. Koblitz, N., 1987. "Elliptic curve cryptosystems. Mathematics of Computation" 48, 203-209.

[15]. Miller, V., 1985. "Use of elliptic curves in cryptography". CRYPTO 85.