Grenze International Journal of Engineering and Technology, June Issue

A Survey on Cryptography

Sarika Nyaramneni[1], S.Yashwanth Sai[2], Talluri Nikhitha Devi[3], Tejeswara Murthy Palwadi[4] and Vibudi Durga Vara Prasad[5]
[1]Assistant Professor, Department of CSE, VNR Vignana Jyothi Institute of Engineering and Technology
Email: - sarika_n@vnrvjiet.in
[2-5]Undergraduate Student, Department of CSE, VNR Vignana Jyothi Institute of Engineering and Technology
Email: {www.sai1929, nikhitha3122, tejeswarmurthypalwadi, durgavaraprasad51}@gmail.com

***Abstract*— This survey presents a comprehensive examination of diverse encryption and decryption techniques, encompassing historical methods like DES to modern approaches such as elliptic curve cryptography and genetic algorithms applied to 3-DES encryption. The paper explores the operational principles, security features, and practical considerations of each cryptographic method, shedding light on strengths, potential vulnerabilities, and real-world applicability. Key aspects such as encryption and decryption efficiency, security mechanisms, and the interplay between symmetric and asymmetric cryptography are addressed. The survey aims to guide researchers, practitioners, and policymakers in making informed decisions for robust and secure data communication and storage. Additionally, the paper identifies potential areas for future research, emphasizing advanced encryption techniques, secure key management, and the integration of cryptographic methods to address emerging challenges in data security.**

***Index Terms*— AES, DES, RSA, 3-DES, Elliptical Curve Cryptography, Substitution Ciphers.**

I. INTRODUCTION

Encryption and decryption stand as the bedrock of modern information security, forming the bulwark that shields sensitive data from prying eyes and malicious actors in an interconnected digital landscape. Encryption, the process of converting plaintext into ciphertext using complex algorithms, renders information unreadable to unauthorized entities. Decryption, its counterpart, reverses this process, converting ciphertext back into its original plaintext form, allowing authorized parties access to the information.

This symbiotic duo operates through sophisticated mathematical algorithms and keys, where encryption transforms data into an unintelligible form, while decryption retrieves the original content using designated keys. Over time, encryption methodologies have evolved from ancient ciphers to intricate cryptographic protocols, constantly adapting to meet the escalating challenges posed by advancing technologies and evolving threats. Their significance spans across numerous domains, safeguarding financial transactions, protecting sensitive communications, fortifying healthcare records, and ensuring the integrity of government and military data. Understanding the principles, evolution, and applications of encryption and decryption is fundamental in comprehending the cornerstone they lay in maintaining confidentiality, integrity, and authenticity in the digital age.

In the digital age where information is omnipresent and data security paramount, the fields of encryption and decryption stand as pillars in fortifying the integrity, confidentiality, and authenticity of sensitive information. The

Grenze ID: 01.GIJET.10.2.139

purpose of this survey is to give an exhaustive exploration of the multifaceted landscape of encryption and decryption techniques. From their historical origins rooted in ancient cryptographic methods to the cutting-edge algorithms and protocols of today, this paper offers a comprehensive overview of their evolution. By delving into the principles, methodologies, and advancements in cryptographic techniques, this survey illuminates the intricate mechanisms behind the transformation of plaintext into ciphertext and its subsequent restoration. Beyond their technical intricacies, the paper evaluates the pervasive role of encryption and decryption across diverse sectors, including cybersecurity, finance, healthcare, and communication networks.

Moreover, this survey identifies and analyses emerging trends, challenges, and future directions in encryption and decryption technologies. This paper provides insights into the evolving landscape of information security. As a comprehensive guide for researchers, practitioners, and policymakers, this survey aims to encapsulate the historical, technical, and practical aspects of encryption and decryption, offering a roadmap to navigate the complexities and advancements in securing data in an increasingly interconnected world.

II. Literature Survey

[1] is a comprehensive review of DES, AES, and RSA encryption standards is presented, highlighting their roles in ensuring data security. The paper discusses the historical context, core operational principles, and the relationship between symmetric and asymmetric cryptography in achieving data confidentiality and integrity. It also suggests potential areas for future research in cryptography, advocating for advanced encryption techniques, key management, and security mechanisms. The authors emphasize the importance of combining asymmetric and symmetric encryption standards to establish a robust foundation for secure data communication and storage in diverse applications. [2] focused on a comparative analysis of modern cryptographic techniques. They evaluated the effectiveness of various symmetric (AES, 3DES, DES) and asymmetric (RSA, ECC) algorithms by considering different parameters like encryption/decryption time, file size and key generation time. Simulations are conducted to compare multiple cryptography algorithms in a given context, aiming to determine which algorithm suits particular quality attributes best. [3] introduced a methodology wherein both users generate key pairs (public and private) based on Elliptical Curve Cryptography (ECC) and exchange their public keys. The encryption process by User A involves the generation of random values and the computation of points, subsequently transmitting cipher characters to User B, who employs an algorithm to compute and decrypt the message character by character. ECC's formidable security is attributed to its reliance on the Discrete Logarithm Problem (DLP), making it highly resistant to computational attacks, and it can be applied for diverse cryptographic purposes, including digital signatures and authentication. Nevertheless, it's essential to note that ECC implementation can be intricate, particularly for those not well-versed in elliptic curve mathematics, presenting a notable challenge compared to simpler encryption methods. This research contributes significantly to understanding ECC's strengths and complexities in the realm of public key cryptosystems, offering valuable insights into its secure applications and potential implementation difficulties.

[4] presented a novel cryptosystem designed to optimize encryption efficiency and security. Their focus lies on encryption speed, security, entropy level and encrypted text size. The paper introduces a symmetric encryption model using substitution cipher methods and provides an in-depth explanation of its encryption process. Key elements include the utilization of Unicode encoding, ensuring compatibility with various languages and special characters, and the automatic generation of unique encryption keys for distinct plaintext blocks.

[5] introduced the encryption process encompasses both message and random value encryption, accompanied by MAC authentication, while decryption is contingent upon the possession of authorized users' private keys, but also permits verification conditions for unauthorized attempts. This approach seamlessly integrates transformation and retrieval phases to facilitate advanced data processing and retrieval. Notably, the introduction of fully verifiable outsourcing decryption ensures that users can independently verify the accuracy of decryption, reducing reliance on the cloud server. [6] discussed about homomorphic encryption. Homomorphic Encryption allows various types of operations that can be performed on ciphertext without accessing key. There is a direct correlation between the quantity of operations on the list and the efficiency and adaptability of HE. Although they are less efficient, HE schemes with more operations are thought to be more adaptable. Schemes with fewer operations, on the other hand, are more effective but less versatile.[7] discusses optimizations for encryption, decryption, and decryption processes on the GTX 690 platform. The encryption process benefits significantly from pre-computation, resulting in impressive speedups. The time consumption for the decrypt primitive is also evaluated, with the GPU multiplications and additions taking about 0.54 seconds.

[8] presented a novel approach where the focus lies on the development of dynamic encryption and decryption methods utilizing the Binary Random Hash. Their approach involves the generation of a secure working key set specifically designed for binary Hash bit mapping encryption. This is achieved through the utilization of circular queues and Hash functions to effectively process plaintext, keys, and cipher bits, with a crucial emphasis on preventing collisions for different key words. Furthermore, the researchers implement the inverse decryption operation, employing the same circular queue and Hash functions to recover plaintext from the cipher. The binary Hash bit mapping encryption method presents a promising avenue for data security, relying on Hash functions, and has the potential to offer robust protection when implemented correctly. However, it's worth noting that, although the core encryption and decryption procedures are conceptually clear, the practical implementation involving circular queue traversal and bit manipulation may introduce complexities and possible challenges that require careful consideration.[9] presented a thorough exploration of cryptographic techniques. The paper delves into the historical cryptographic algorithms, such as the Caesar Cipher, Simple Substitution Ciphers, and Transposition Ciphers, offering a detailed understanding of their encryption and decryption processes. Furthermore, the authors scrutinize modern cryptographic algorithms, including Stream Ciphers, Hash Functions, Block Ciphers, and Public Key Systems, elucidating their fundamental principles and practical use cases. This analysis underscores the crucial role of cryptography in maintaining data confidentiality, securing information during transmission, and enabling safe communication. While modern cryptographic systems can provide robust security when correctly implemented, the paper highlights the vulnerabilities of historical algorithms like the Caesar Cipher and the potential security risks associated with inadequate key management or implementation errors. Moreover, it sheds light on the computational resource requirements of Public Key Systems, which, while highly secure, may exhibit slower performance compared to symmetric cryptography. This review paper offers an in-depth and comprehensive examination of the historical foundations and contemporary challenges in the field of cryptography.

[10] introduces a document encryption method employing a mechanism inspired by the Enigma Machine. The program allows users to choose between encryption and decryption, utilizing three alternation tables that randomly shuffle the 26 English letters to substitute each letter in the alphabet. This results in a ciphertext that conceals the original text. To decrypt, the program reverses the order of the alternation tables, revealing the original document. This multi-table approach enhances security, making it difficult for unauthorized users to decipher the content. However, during encryption, punctuation and spaces are removed, potentially impacting the readability and meaning of the decrypted text, which is an important consideration in practical use cases.

[11] provides an extensive examination of various encryption algorithms, encompassing AES, DES, BlowFish, SEED, IDEA, RC2, RC4, RC6, and XTEA, all assessed under Cipher Block Chaining (CBC) mode. The study rigorously assesses their performance through metrics such as throughput, execution time, and CPU utilization, employing a Java-based simulation across different file sizes. This comprehensive analysis offers valuable insights for tailored algorithm selection based on specific application requirements. [12] introduced a significant enhancement to the Advanced Encryption Standard (AES) through the substitution of MixColumns with an innovative bit permutation technique. Their comprehensive evaluation encompasses the encryption of both text files and images, focusing on crucial performance metrics such as encryption time, CPU utilization, and the critical avalanche effect. Impressively, the modified AES exhibits expedited encryption processes and notably reduced CPU resource consumption, resulting in an overall boost in operational efficiency. Nevertheless, practical implementation may encounter challenges pertaining to compatibility and seamless integration, which warrant further exploration in real-world scenarios. [13] assessed AES, 3DES, RSA, DES and Blowfish cryptographic algorithms, evaluating their performance using parameters like encryption time, memory usage, entropy, and avalanche effect. They highlighted Blowfish's efficiency in time and memory, AES's strong avalanche effect, and RSA's higher security but slower speed. Through experiments and analysis, it aims to aid algorithm selection for various applications based on specific requirements, considering factors like speed, security, and memory efficiency.[14] discusses the effectiveness and security of the Blowfish encryption algorithm. It mentions that the cipher is effective provided that the alphabet in plaintext is dispersed uniformly and the key is selected at random. The document also mentions attempts to attack Blowfish but states that substantial flaws have not yet been demonstrated when using the full 448-bit key and 16 rounds.

[15] presented an enhancement of Data Encryption Standards Algorithm (DES)," an in-depth analysis of the Data Encryption Standard (DES) algorithm's key generation process. The research systematically compares key generation functions, specifically PC-1, shifting, and PC-2, in order to evaluate their respective effectiveness in enhancing security. The proposed algorithm introduces modifications to the key generation process, which potentially bolsters security and renders the algorithm more resilient to certain types of attacks. [16] proposed an

innovative approach to improve security of the 3-DES encryption system. Their method involves the division of the 64-bit cipher key into two segments of 32 bits each, followed by a right shift operation and mutation process to derive a novel encryption key. Significantly, the researchers employ Genetic Algorithms to generate these new encryption keys, effectively mitigating the vulnerability associated with weak keys. Although the adoption of Genetic Algorithms introduces complexity and cost, it presents a promising avenue for bolstering encryption security.[17] discussed DES and 3DES encryption methods' implementation in an NFC-based communication system, emphasizing their role in securing smart card data. It details their encryption and decryption processes, programmed in C++ for testing performance on smart cards. The research finds DES to be faster than 3DES in both writing and reading encrypted data. It highlights their differences and application in ensuring secure data communication within NFC.

[18] discussed the reverse encryption technique, a symmetric stream cypher that works well for data encryption. The additional amount of time needed for encryption and decryption is reduced using the reverse encryption algorithm.. It is mainly used because of its simplicity and efficiency. It takes variable length key. The encryption and decryption consists of same operations except two where keys are added to the text in encryption, while keys are eliminated during the decryption process.

[19] examined vulnerabilities of traditional RSA systems. This is because these systems rely on the factorization of 'n,' which is produced by multiplying two prime numbers. Once 'n' is obtained, it becomes relatively easy for attackers to derive the keys and compromise the system's security. The proposed ESRKGS (Efficient Secure RSA Key Generation Scheme) aims to address these vulnerabilities by eliminating the need to transfer 'n', so that hackers would find it challenging to determine the prime numbers that are employed in the system. This modification in the algorithm prevents attackers from easily breaking the system by obtaining 'n' through factoring methods and subsequently deriving the keys [20] explored asymmetric key cryptography, highlighting the RSA algorithm's reliance on factoring large numbers for security. It introduces the Modified RSA Encryption Algorithm (MREA) as a more secure alternative, based on factoring problems and decisional composite residuality assumptions. This modified algorithm aims to enhance security in public key systems by addressing weaknesses found in traditional RSA cryptography.

TABLE I. SUMMARY OF RELATED RESEARCH PAPERS ON ENCRYPTION AND DECRYPTION TECHNIQUES

No.	Title	Year	Methodology
1.	A Review Paper on DES, AES, RSA Encryption Standards	2020	DES, AES, RSA
2.	Implementation and Comparative Analysis of Symmetric Encryption Model Based on Substitution Cipher Techniques	2021	Transposition Ciphers, Substitution Ciphers
3.	Encryption and decryption using elliptic curves for public key cryptosystems	2017	Elliptical Curve Cryptography
4.	Full Verifiability for Outsourced Decryption in Attribute Based Encryption	2020	Attribute Based Encryption
5.	The Research of Dynamic Encryption & Decryption Methods Based on the Binary Random Hash	2019	Dynamic Encryption and Decryption, Binary Random Hash
6.	A Review Paper on Cryptography	2019	Stream Ciphers, Block Ciphers, Public Key Encryptions, Digital Signatures
7.	Document Encryption Method with Mechanism of Enigma Machine	2021	Enigma Machine
8.	Symmetric Encryption Algorithms: Review and Evaluation study	2020	Caesar, AES, DES, 3DES, Blowfish, Two Fish, Threefish, RSA
9.	Modified AES for Text and Image Encryption	2018	AES
10.	An Enhancement of Data Encryption Standards Algorithm (DES)	2018	DES
11.	The Design of 3-DES Encryption System Using Optimizing Keys.	2019	3-DES

12.	Reverse Encryption Algorithm: A Technique for Encryption & Decryption	2013	REA
13.	An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)	2014	RSA
14.	Modified RSA Encryption Algorithm (MREA)	2012	RSA
15.	Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)	2016	DES,3-DES
16.	Cryptography: A Comparative Analysis for Modern Techniques	2017	AES,DES,RSA, Elliptical Curve Cryptography
17.	A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish	2015	DES, 3DES, AES, RSA, Blowfish
18.	A Review of Homomorphic Encryption for Privacy-Preserving Biometrics	2023	Homomorphic Encryption
19.	An Implementation of the Blowfish Cryptosystem	2008	Blowfish
20.	Exploring the Feasibility of Fully Homomorphic Encryption	2015	Homomorphic Encryption

The above Table 1 provides a concise summary of various research papers and methodologies used in encryption and decryption methods research from 2008 to 2021.

III. METHODOLOGY

TABLE II. SUMMARY OF CRYPTOGRAPHIC TECHNIQUES.

No.	Cryptographic Techniques	Key Length	Input Size	Rounds of Operations
1.	AES	128,192,256 bits	128 bits	10,12,14 rounds
2.	RSA	Variable	Limited by key size	Depends on Key size
3.	Transposition ciphers	Variable	Variable	Variable
4.	Substitution ciphers	Variable	Variable	Variable
5.	Elliptical curve cryptography	Variable	Variable	Variable
6.	Attribute based encryption	Variable	Variable	Variable
7.	Dynamic Encryption	Variable	Variable	Variable
8.	Binary Random Hash	Variable	Variable	Variable
9.	Stream ciphers	Variable	Variable	Variable
10.	Block Ciphers	Variable	Variable	Variable
11.	Digital Signatures	Variable	Variable	Variable
12.	Enigma Machine	3 rotors,26 positions	Variable	Variable
13.	Caesar	Variable	Variable	Variable
14.	3DES	56,112,168 bits	64 bits	48 rounds
15.	Blowfish	32-448 bits	64 bits	16 rounds
16.	Twofish	128,192,256 bits	128 bits	16 rounds
17.	Threefish	256,512,1024 bits	256, 512, 1024 bits	72 rounds
18.	Rivest Cipher	Variable	Variable	Variable
19.	REA	Variable	Variable	Variable

The above table gives the key size, input size, numbers of rounds for all cryptographic techniques.

A. DES

DES, or Data Encryption Standard, is a symmetric-key commonly used algorithm for encrypting and decrypting data. It operates on fixed-size blocks of data using a key length of 56 bits. There are several rounds of permutation and substitution in this procedure to scramble the data, preventing it from being viewable without the matching key. Its strength lies in its simplicity and efficiency, providing reasonably strong security for its time. However, DES has faced criticism due to its key length being susceptible to brute force attacks as computational power has advanced, making it vulnerable to being cracked within a reasonable timeframe. This limitation led to the development of more robust encryption standards like AES (Advanced Encryption Standard). Despite its vulnerabilities, DES paved the way for modern encryption techniques and remains historically significant in the field of cryptography.

B. AES

AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used to secure sensitive data. It operates by transforming plaintext into ciphertext through a series of substitution and permutation steps using a symmetric key. AES has three key sizes: 128, 192, and 256 bits, determining the strength of encryption. Its advantages include robust security due to its complex mathematical structure, speed and efficiency in both hardware and software implementations, and its widespread adoption as a global encryption standard, ensuring compatibility across various systems. However, AES is not without its drawbacks. One potential disadvantage lies in its vulnerability to side-channel attacks, where attackers exploit implementation flaws rather than breaking the algorithm itself. Additionally, the reliance on symmetric keys necessitates secure key management practices, which can pose challenges, especially when distributing keys across multiple parties securely. Despite these limitations, AES remains a cornerstone in ensuring data confidentiality and security across digital platforms.

C. RSA

RSA (Rivest-Shamir-Adleman) is a widely used asymmetric encryption algorithm that operates on the principle of public and private keys. It leverages the computational complexity of factoring large prime numbers to ensure secure communication. The process begins by generating a pair of keys: a public key for encryption and a private key for decryption. The communication is encrypted by the sender using the recipient's public key, and it can only be unlocked with the recipient's matching private key. This approach guarantees authenticity and secrecy of the communication. One advantage of RSA lies in its robust security based on the difficulty of factoring large numbers, providing a strong level of protection for sensitive data. However, RSA can require a lot of processing power for both encryption and decryption, especially with longer key lengths, making it slower compared to symmetric encryption methods. Additionally, the keys used in RSA are larger in size compared to symmetric keys, which can pose challenges in key management and storage. As computing power continues to advance, RSA's vulnerability to attacks may increase, necessitating larger key sizes for continued security.

D. Transposition Ciphers

Rearranging the characters in a message is the process of transposition cyphers without altering the characters themselves. This process is based on a predetermined key or rule. The encrypted text appears scrambled, and decryption involves rearranging the characters back into their original order using the same key or method. Columnar transposition and rail fence ciphers are common examples, employing different techniques for reordering the text. These ciphers offer a range of complexities and cryptographic strengths.

E. Substitution Ciphers

A substitution cipher is a method of encryption where a fixed system replaces every letter in the plaintext with a different letter. For instance, in a simple Caesar cipher, every letter in the alphabet is moved down a specific number of positions. This method obscures the original message, making it unintelligible without the key. The advantage of substitution ciphers lies in their simplicity and ease of implementation, requiring only a basic understanding of the algorithm used. However, they are vulnerable to frequency analysis, where the frequency of letters in the ciphertext can be compared to typical letter frequencies in the language to deduce the key or plaintext. Additionally, as there are a limited number of characters in any language, substitution ciphers are susceptible to brute force attacks, where all possible keys are systematically tested until the correct one is found. This makes them relatively insecure compared to more complex encryption methods.

E. Elliptical Curve Cryptography

Elliptic Curve Cryptography (ECC) is a cryptographic system that leverages the algebraic structure of elliptic curves over finite fields for secure communication. In ECC, encryption and decryption are determined by how challenging it is to solve the discrete logarithm problem for an elliptic curve. Essentially, ECC uses a pair of keys: a public key, known to everyone, and a private key, kept secret by the owner. Messages encrypted with the public key can only be decrypted using the corresponding private key. ECC offers robust security with smaller key sizes compared to other encryption methods like RSA, making it efficient for constrained environments like mobile devices. Its advantages include strong security, faster computations, and smaller key sizes, reducing computational overhead. However, its main disadvantage lies in its complexity, making implementation and validation more intricate than traditional cryptographic systems, which could potentially lead to vulnerabilities if not implemented correctly. Additionally, concerns about the trustworthiness of the elliptic curve parameters and potential vulnerabilities to quantum attacks are also considered challenges in ECC.

F. Attribute Based Encryption

Attribute-Based Encryption (ABE) is a type of encryption where access to data is based on attributes assigned to users. In ABE, ciphertext and keys are associated with attributes rather than specific identities. This method allows data to be encrypted so that only users possessing a specific set of attributes can decrypt it, rather than being tied to individual keys. It's utilized in scenarios where access control to data is based on specific criteria or attributes, enabling flexible and fine-grained access policies.

G. Dynamic Encryption

Dynamic encryption involves altering encryption keys frequently, enhancing security by reducing the window of vulnerability. It's a strategy that changes cryptographic keys dynamically, either periodically or in response to specific triggers or events. This method mitigates risks associated with key exposure and compromises, making it challenging for attackers to decrypt information even if they gain access to encrypted data and keys. Dynamic encryption can be applied in various contexts, such as securing communications, databases, or any sensitive information, and it often complements other security measures to bolster overall data protection.

H. Stream Ciphers

Stream ciphers function by encrypting data one bit or byte at a time, working on continuous streams of data. They employ a pseudorandom or random key stream to combine it with the plaintext bit by bit, generating the ciphertext. These ciphers are fast and appropriate for real-time applications because of their capacity to process data in smaller segments continuously. They commonly use XOR operations between the plaintext and a keystream generated by the encryption algorithm, making them efficient for secure communication over a continuous data stream, like internet traffic or voice communication.

I. Block Ciphers

Block ciphers are cryptographic algorithms that encrypt fixed-size blocks of data, dividing them into blocks and encrypting each block separately. They work by transforming plaintext blocks into ciphertext blocks using a fixed key, typically operating on blocks of 64 or 128 bits. The encryption process involves multiple rounds of substitution and permutation (substitution-permutation network), where each round applies a series of complex mathematical functions to the data block.

J. Public Key Encryption

A pair of keys is needed for public key encryption, commonly referred to as asymmetric encryption. These keys are the private key and the public key. The private key, which is needed for decoding, is only known by the recipient. The Public key is available and used for encryption. Messages that have been public key encrypted cannot be decrypted without the matching private key, providing a secure way to send encrypted messages without needing to exchange secret keys beforehand.

J. Digital Signatures

Digital signatures involve using cryptographic techniques to authenticate the sender of a message and ensure the integrity of its content. This process utilizes a private key to sign the message, generating a unique digital fingerprint, which can be verified utilizing the relevant public key. It guarantees that the message hasn't been altered and that it indeed originated from the claimed sender, providing non-repudiation and security in digital communications. Upon receiving the digitally signed message, the integrity and validity of the signature can be confirmed by the recipient using the sender's public key.

K. Enigma Machine

The Enigma machine was a complex electro-mechanical device used by Germany during World War II for encryption and decryption of secret messages. It consisted of rotating disks wired with intricate settings that encoded messages through substitution and transposition. Each key press initiated a series of changes in the machine's internal wiring, creating a unique ciphertext for every letter entered. Decryption required the recipient to possess an Enigma machine set to the same settings used by the sender, ensuring secure communication for military operations. The machine's strength lay in its ability to rapidly create a vast array of potential ciphertexts, making it extremely difficult to crack without knowledge of the daily changing settings.

L.Caesar

The Caesar cypher is a substitution cypher method in which the plaintext's letters are all moved up or down the alphabet by a predetermined amount. For example, with a shift of 4, 'C' becomes 'G', 'N' becomes 'R', and so on. It's a simple and historical encryption method used by shifting characters by a fixed number, known as the key or shift value. This cipher operates under modular arithmetic, wrapping around the alphabet when reaching the end. The decryption process involves shifting the letters in reverse to reveal the original message.

M. 3-DES

Triple Data Encryption Standard (3DES) is a cryptographic algorithm that applies DES cipher three times to each data block. It operates in three phases: encryption, decryption, and encryption again, using three separate 56-bit keys. Initially, the data block undergoes an encryption process with the first key, then a decryption with the second key, and finally another encryption with the third key. The advantage of 3DES lies in its backward compatibility with the original DES while offering significantly enhanced security due to its triple encryption process. However, its main drawbacks are its relatively slow speed compared to modern encryption standards and its susceptibility to brute force attacks due to the 56-bit key size, which is considered less secure in today's computing environment. As newer, more efficient encryption algorithms have emerged, the industry has been transitioning away from 3DES to more secure and faster alternatives.

N. Blowfish

Blowfish is a symmetric-key block cipher designed for fast and secure encryption of data. It uses variable-length keys, ranging from 32 bits to 448 bits, making it adaptable for different security needs. The algorithm operates on fixed-size blocks of data and consists of a Feistel network, performing a series of substitutions and permutations. Blowfish encryption involves a key expansion phase, followed by multiple rounds of encryption, providing high security and efficiency, making it suitable for various applications where encryption speed and strength are essential.

O. Twofish

Twofish is a symmetric-key block cipher designed for fast and secure encryption and decryption of data. It operates on fixed-size blocks and uses a key length of up to 256 bits. Twofish employs a Feistel network structure with a variable number of rounds (between 16 and 32) based on the key size. Its operations involve substitutions, permutations, and key-dependent S-boxes to create complex encryption, ensuring resistance against various cryptographic attacks. Developed as a candidate for the Advanced Encryption Standard (AES), Twofish is known for its strong security and efficient performance in both software and hardware implementations.

P. Threefish

Threefish is a symmetric key block cipher designed to operate on large blocks of data (up to 2^128 bits) and uses a tweakable block cipher, which means it can encrypt data in customizable block sizes. Threefish doesn't include key scheduling, relying on an external component like Skein for that purpose. Its design emphasizes simplicity, transparency, and performance, making it suitable for various encryption applications.

Q. Reverse Encryption Algorithm

The Reverse Encryption Algorithm (REA) employs a symmetric stream cipher for encryption and decryption. For encryption, it involves adding the key to the plaintext, converting it to ASCII code, then to binary data, and performing operations to create encrypted text. Decryption, on the other hand, involves processing the ciphertext, obtaining ASCII codes, reversing the encryption steps, and removing the key to retrieve the original plaintext. The methodology prioritizes simplicity, utilizing ASCII and binary conversions alongside key manipulation for secure data transformation.

R. Homomorphic Encryption

Homomorphic encryption enables calculations using encrypted data without decryption. Partially Homomorphic Encryption (PHE) permits limited operations (addition/multiplication). Somewhat Homomorphic Encryption (SHE) expands PHE's capabilities slightly. Fully Homomorphic Encryption (FHE) enables arbitrary operations on encrypted data. Efficiency varies: FHE's flexibility comes with higher complexity. It relies on mathematical structures to preserve encrypted data properties during computation.

IV. Research Gap

Research in cryptography presents an opportunity to bridge the gap between innovative encryption techniques and their practical implementation in real-world scenarios. While numerous studies introduce novel encryption methods, their usability and seamless integration within existing systems remain underexplored. Further exploration into the usability aspects of these systems, focusing on factors like compatibility, ease of integration, and user-friendliness, could significantly bolster their adoption and effectiveness in practical settings. Additionally, delving deeper into the security assessments of these innovative methods beyond basic algorithmic descriptions would instil confidence in their robustness against diverse cyber threats, addressing concerns about their reliability and resilience.

Another vital research area lies in the realm of hybrid encryption techniques that intelligently combine symmetric and asymmetric cryptography to maximize their strengths while mitigating their weaknesses. Developing advanced methodologies that seamlessly merge these encryption paradigms could elevate overall security and efficiency in data protection. Moreover, investigating scalable, efficient, and secure methods for key management and distribution, particularly in large-scale systems, stands as a critical need. Addressing these gaps could pave the way for encryption systems that not only boast enhanced security but also exhibit practical usability and seamless integration within diverse applications, meeting the demands of modern data security landscapes.

V. Conclusion

In conclusion, this survey paper offers a comprehensive exploration of the multifaceted landscape of encryption and decryption techniques. By scrutinizing historical algorithms like the Caesar Cipher to modern, sophisticated systems such as AES, DES, and novel encryption models, it provides a panoramic view of the evolution and diversity within the field of cryptography. The survey delves into the operational principles, strengths, weaknesses, and practical considerations associated with various encryption paradigms, shedding light on their pivotal roles in safeguarding data confidentiality, integrity, and secure communication.

Furthermore, this survey identifies critical research gaps, emphasizing the need for hybrid encryption methodologies that harmonize symmetric and asymmetric cryptography for heightened security and efficiency. It also underscores the significance of addressing usability concerns, robust security assessments of novel encryption methods, and innovations in key management for practical deployment. Ultimately, this survey not only serves as a compendium of encryption techniques but also highlights avenues for future research, guiding the trajectory of advancements in encryption and decryption towards more secure, efficient, and accessible solutions in the ever-evolving landscape of cybersecurity.

References

[1] Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 333-338, doi: 10.1109/SMART50582.2020.9336800.

[2] Maqsood, Faiqa & Ahmed, Muhammad & Mumtaz, Muhammad & Shah, Munam. (2017). Cryptography: A Comparative Analysis for Modern Techniques. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080659.

[3] M. Srinivas and S. Porika, "Encryption and decryption using elliptic curves for public key cryptosystems," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2017, pp. 1300-1303, doi: 10.1109/ICCONS.2017.8250678.

[4] E. Jintcharadze, T. Sarajishvili, A. Surmanidze and D. Khojava, "Implementation and Comparative Analysis of Symmetric Encryption Model Based on Substitution Cipher Techniques," 2021 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 2021, pp. 1-6, doi: 10.1109/EWDTS52692.2021.9580978.

[5] J. Li, Y. Wang, Y. Zhang and J. Han, "Full Verifiability for Outsourced Decryption in Attribute Based Encryption," in IEEE Transactions on Services Computing, vol. 13, no. 3, pp. 478-487, 1 May-June 2020, doi: 10.1109/TSC.2017.2710190.

[6] Yang W, Wang S, Cui H, Tang Z, Li Y. A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. Sensors (Basel). 2023 Mar 29;23(7):3566. doi: 10.3390/s23073566. PMID: 37050626; PMCID: PMC10098691.
[7] Wang, Wei & Hu, Yin & Chen, Lianmu & Huang, Xinming & Sunar, Berk. (2015). Exploring the Feasibility of Fully Homomorphic Encryption. IEEE Transactions on Computers. 64. 698-706. 10.1109/TC.2013.154.
[8] G. Feng, L. Lang, Y. Si and K. Wang, "The Research of Dynamic Encryption & Decryption Methods Based on the Binary Random Hash," 2019 International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China, 2019, pp. 180-183, doi: 10.1109/ITCA49981.2019.00046.
[9] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757514.
[10] Y. Lin, X. Xia and J. Yang, "Document Encryption Method with Mechanism of Enigma Machine," 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), Xi'an, China, 2021, pp. 259-262, doi: 10.1109/CAIBDA53561.2021.00061.
[11] Alenezi, Mohammed & Alabdulrazzaq, Haneen & Mohammad, Nada. (2020). Symmetric Encryption Algorithms: Review and Evaluation study. International Journal of Communication Networks and Information Security. 12. 256.
[12] Gamido, Heidilyn & Sison, Ariel & Medina, Ruji. (2018). Modified AES for Text and Image Encryption. 11. 942-948. 10.11591/ijeecs.v11.i3.pp942-948.
[13] Patil, Priyadarshini & Narayankar, Prashant & Narayan, DG & S M, Meena. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 78. 617-624. 10.1016/j.procs.2016.02.108.
[14] R. K. Meyers and A. H. Desoky, "An Implementation of the Blowfish Cryptosystem," 2008 IEEE International Symposium on Signal Processing and Information Technology, Sarajevo, Bosnia and Herzegovina, 2008, pp. 346-351, doi: 10.1109/ISSPIT.2008.4775664.
[15] N. M. M. Alhag and Y. A. Mohamed, "An Enhancement of Data Encryption Standards Algorithm (DES)," 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2018, pp. 1-6, doi: 10.1109/ICCCEEE.2018.8515843.
[16] Wang, Li & Jiang, Guangling. (2019). The Design of 3-DES Encryption System Using Optimizing Keys. 56-58. 10.1109/AIAIM.2019.8632786.
[17] Ratnadewi, Ratnadewi & Adhie, Roy & Hutama, Yonatan & Ahmar, Ansari & Setiawan, Muhammad. (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). Journal of Physics: Conference Series. 954. 012009. 10.1088/1742-6596/954/1/012009.
[18] Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, "Reverse encryption algorithm: a technique for encryption & decryption", Volume 2 Issue 1 - January 2013
[19] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, An Enhanced and Secured RSA Key Generation Scheme (ESRKGS), Journal of Information Security and Applications, Volume 20, 2015
[20] R. S. Dhakar, A. K. Gupta and P. Sharma, "Modified RSA Encryption Algorithm (MREA)," 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 2012, pp. 426-429, doi: 10.1109/ACCT.2012.74.