Cryptographic Algorithms: Current Status and Future Directions

[1]Roopesh Kumar
[1]Assistant Professor
Department of Computer Science
Banasthali Vidyapith
Banasthali, Newai, Rajasthan, India -304022

Email: roopeshkumar@banasthali.in
ORCID ID:- https://orcid.org/ 0000-0001-7293-744X

[2]Dr.Ajay Kumar Yadav
[2]Assistant Professor
Department of Computer Science
Banasthali Vidyapith
Banasthali, Newai, Rajasthan, India -304022

Email: ajay.iitdhn@gmail.com
ORCID ID:- https://orcid.org/0000-0002-3032-3105

Abstract—
Cryptography is significant in every area of IT applications, as security is essential in every small area that aids in thwarting the deciphering of the encrypted data. Since it is necessary to protect the privacy of data that is spreading across a network and to assure the security of information transmission, academics, professionals, and researchers have used a variety of cryptographic algorithms. The goal of the current work is to give readers suggestions for their future research areas by providing a review of popular cryptographic algorithms at the moment.
Keywords: Cryptography; Privacy; Security; Information.

I. INTRODUCTION

In contemporary communication networks, network security and data encryption have become critically significant. Ensuring the confidentiality of information when transmitting sensitive content between two parties (e.g. client –server) is of paramount importance, preventing unauthorized access by hackers or intruders. This necessitates encrypting messages in a manner that renders decryption impossible without the corresponding decryption key. The realm of cryptography is currently experiencing rapid growth as researchers strive to create robust encryption algorithms that thwart any attempts by intruders to intercept encrypted communications. Cryptography traces its origins to the Greek terms kryptos, signifying "concealed," and grafein, denoting "to inscribe." Throughout history, its primary objective has been safeguarding messages by obscuring their substance from potential eavesdroppers, frequently using conventional methods of communication.[1].The primary goal is to ensure secure communication by rendering information incomprehensible to those without authorization. Encryption stands as a fundamental method in contemporary cryptography, encompassing the conversion of plain text into cipher text. This process allows solely authorized entities to reverse the encryption and regain the original information. Cryptography also encompasses the creation and assessment of protocols and

algorithms dedicated to enhancing the security of information and communication pathways. Examining mathematical techniques related to aspects of information security, such as maintaining confidentiality, assuring data integrity, authenticating the identification of entities, and establishing the source of data, is what cryptography entails. One subset of the approaches used to ensure information security is cryptography. In general, cryptography provides privacy and helps to authenticate entities [1].Simply we can understand working of cryptography by the following diagram:

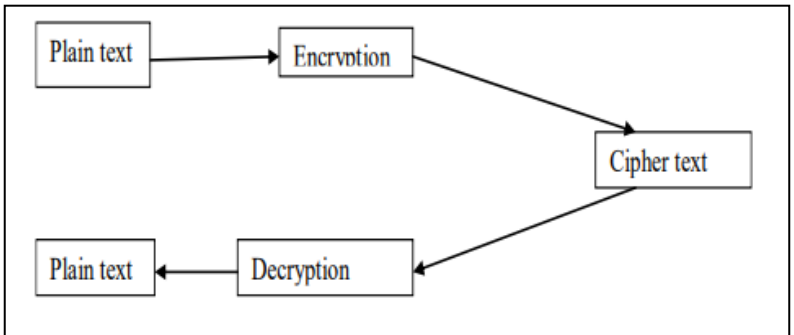


Figure1: Concept fo cryptography

In cryptography we simply take original text and modified it using encryption technique which produces cipher text to send the other party. After receiving the cipher text, the recipient decrypts the message using the identical algorithm, resulting in the plain text or original text. Classification of cryptography can be given as fig.2

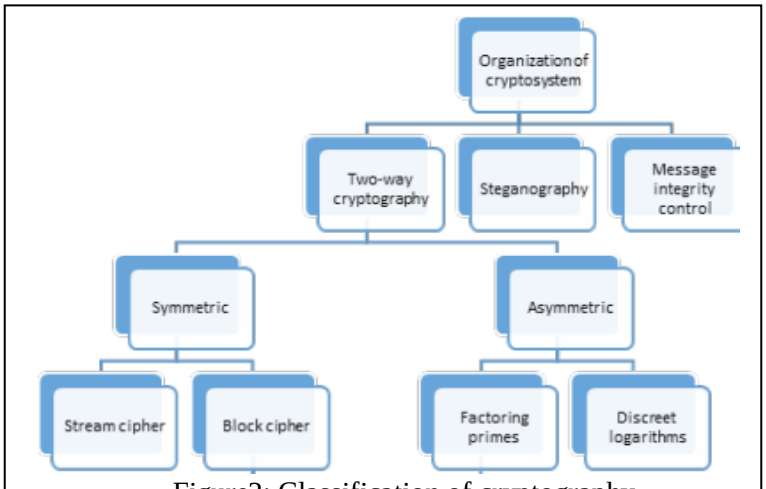


Figure2: Classification of cryptography

Since W.Diffie and M.Hellman have proposed the public key cryptography for the first time in 1976. It attracts more attention of the computer security department [2]. Open networks like the Internet frequently use data encryption to ensure security. The capabilities of cryptosystems like RSA and Diffie-Hellman have become insufficient due to the rapid improvements in computer technology and cryptography research, primarily because they require large numbers of bits [3].

The paper's organization can be outlined as follows:

The subsequent section offers a descriptive exploration or related data study. In Section III, we have conducted a summarized analysis of the data. Finally, Section IV presents the conclusion..

II. RELATED WORK

Here authors have improved the public key cryptography using chaotic neural network. "They used the amplified Logistic mapping to select the attraction domain and regarding low phenomenon of avalanche effect test result, hybrid encoding is used to make every bit of code influenced by the pervious code"[2]. An affine point transforms the plaintext ASCII value. It is necessary because the character's single-digit ASCII integer is translated into a set of coordinates to fit the EC and add non-linearity, completely masking the character's identity. This character is used for encryption and decryption by elliptic curve cryptography [3, 5]. The author introduces a revolutionary visual cryptography technique that involves creating shares using a visual cryptography model. It works with binary inputs, converting real-world images into halftone images having white and black pixels [4]. "In the present work the authors have introduced an integrated symmetric key cryptographic method DJMNA which combine two independent methods (i) Modified Generalized Vernam Cipher (MGVC) method and (ii) DJSA method which is an extension of MSA method. The Generalized Vernam Cipher algorithm extends text encryption to any type of data encryption [6]". This paper concentrated on various security concerns related to establishing a secure and efficient cryptographic technique within the framework of a block cipher. Many of these concerns arise when users neglect their keys, opt for easily memorable keys, or persist with the same keys for extended periods. Here solution tool is also provided [7]. The study offers a DNA-based cryptography method and discusses its potential extension using cutting-edge ideas in steganography, authentication, signature, and encryption. The approach makes use of DNA computing's potential and can tackle practical problems in industrial and management engineering [8]. With the help of a key-dependent transposition scheme and traditional substitution, this work introduces a new block cipher. The cipher is constrained by a poor key schedule, despite successfully combating frequency analysis and utilizing dependency. One-way functions or hash-based keys creations are proposed as improvements [9] This paper introduces a novel text encryption algorithm leveraging natural language processing. It outlines the prerequisites and details the procedures for both text encryption and text distillation [10]. The abstract compares 160-bit field elliptic curve cryptography (ECC) to 1024-bit RSA, showing similar attack resistance with shorter ECC keys for better storage and performance. ECC offers computational benefits over ElGamal and MVECC, requiring fewer operations and avoiding certain complexities like inverse calculations and point embedding for plaintext [11]. The paper provides an improved RSA method that strengthens security against factorization attacks by removing the weakness of 'n' and replacing it with a newly generated value. The algorithm's overall security is improved by this change, albeit at the cost of a slight increase in time complexity [12]. The authors suggested an attribute-encryption method based on identity-based broadcast encryption with constant cipher texts that supports zero inner product inclusion. Decryption requires only two pairs of computations [13]. In this paper wrapping cipher text is used by the system to conceal its location and thwart hacking attempts. It uses highly random webpage content to encrypt using TRNS, making it resistant to decryption [14]. The paper presents an algorithm with rapid execution using simplified arithmetic and logic operations, with a 128-bit key size for high security. Security is enhanced through iterative repetition of steps, achieving a balance between high throughput and robust protection [15]. This paper introduces the UPMM algorithm, a novel encryption technique that operates on the ASCII values of data. The encryption process involves utilizing Palindrome numbers and a distinctive alphanumeric ID as part of the encryption key. The alphanumeric ID is transformed into an ASCII

value, enhancing network authentication [16].This paper introduces Chaive Unica (CU), a unique one-time key generation method, and Advanced Substitution Technique (AST), a more secure encryption approach. It employs double encryption of plaintext before inputting it into the algorithm also a new architecture is proposed for enhanced text encryption security [17].With a magic rectangle that prevents cipher text repetition and gives letters separate values, the MRGA work improves security. This complexity prevents unauthorized decryption attempts from succeeding. Despite having efficiency and security requirements, magic rectangle construction takes more time [18]. The discussed novel symmetric algorithm utilizes a straightforward mapping technique that enhances security. Its adaptability across diverse language domains also supports the localization of Cryptographic Software tools[19]. This paper proposes a method for hiding numerous plaintexts within a single cipher text and shows how we can use it for secure communication via TCP/IP multicast. The suggested approach, AMSC, resists security assaults in different applications [20]. The Horse Step Algorithm, a cutting-edge 2D matrix-based encryption technique, is introduced in this paper. The Horse Step Algorithm, a cutting-edge 2D matrix-based encryption technique, is introduced in this paper. Although it is more efficient than RSA, AES is slow rough, it is more efficient than RSA, AES [21]'here authors presented new algorithm using last decimal digit of number. It provides high security [22]. The authors present a novel encryption/decryption approach in this paper that uses randomized algorithms. It generates significant data sub keys based on a secret key. Here technique employs different random numbers for each encryption. Notable results include the secure transmission of the random numbers and the algorithm's robust defense against attacks [23].In this paper study of different cryptographic techniques have presented[24]. Among asymmetric algorithms, RSA stands out as widely renowned. For security purposes, adjustments have done. In this work, the authors further enhance the modified RSA by incorporating the Binary conversion principle. It involves the conversion of cipher text into binary format, thereby augmenting the level of security [25].Researchers presented a new method of encryption using a genetic algorithm that is immune to brute force attacks [26]. In this study, authors objective was to secure data for a basic messaging application using a letter-shifting technique between the upper and lower layers. However, this approach is not feasible for numeric data or cases involving special symbols [27]. Here a new symmetric approach to text encryption and decryption is presented. The process entails turning the text into a graph and creating the cipher text using a pre-shared matrix key and the matrix graph representation [28]. DNA has transformed the landscape of cryptography. By incorporating DNA into cryptography, higher levels of security can be attained. Authors have leveraged DNA in conjunction with AES cryptography to modify the key size [29]. With the help of digits, the Vigenère table's capabilities are to be improved by the authors. The new table has been created, this update makes it possible to encrypt numerical data [30]. The encryption and decryption process involves utilizing a modified Blowfish algorithm. This modification entails incorporating an MD5-generated hash code, which is employed to identify the hash, and subsequently appending this hash code to the plaintext before encryption [31].The modified shift encryption technique, which produces a 0% character error rate and demonstrates good execution time, utilizes two shift operations to scramble the text [32]. This research introduces an approach to enhance data security using a technique known as dual-layer encryption. The method put forward comprises of two sequential encryption phases: the initial stage involves applying the Beaufort cipher method, followed by the second stage which employs the hill cipher method. It gives better Avalanche Effect (AE) value [33]. To enhance security, a hybrid cryptosystem has been created by combining AES and RSA together. On the other hand, Twofish and RSA are also combined. The results demonstrate the advantages of both systems [34]. The goal of the study is to methodically list and assess the cryptography algorithms in order, as well as to clarify the relationships that exist between them. Investigating the connections between symmetric and asymmetric algorithms, as well as exploring those that utilize secret keys versus those that involve key pairs, is a part of this [35]. This study presents a novel symmetric cryptography method based on the Caesar cipher. This method creates an encrypted message of the original text or message. In this technique, the sender provides a hash code rather than a symmetric key, which gives the recipient the symmetric key they

need to decode the sender's message.[36]. The innovative encryption approach involves splitting and mixing a 256-bit plaintext into two blocks of 128 bits. After that, only the standard 128-bit AES encryption is employed. This strategy ensures elevated security standards [37].In this study, an improved iteration of the DES algorithm has developed, named KE-DES. Within this framework, a novel KD function was formulated for both the key and data, aimed at enhancing security and improving the efficiency of textual data encryption [38].The study presents a new "chaos 2D encryption" to secure text in digital images. It involves bit-plane slicing to divide text into seven bit-planes, followed by chaos encryption with varied parameters for each plane, enhancing security[39].The paper proposes a user-friendly method for message cryptography involving block division of the message (size 2 to 60). A secret color image generates an array matching block count as a private key, determining left rotation digits for block encryption [40]. Here the authors integrated three distinct cryptography fields: symmetric, asymmetric, and biological DNA cryptography. The aim is to achieve a harmonious equilibrium between heightened complexity and the duration required for encryption processes. This algorithm is faster than previous algorithms [41]. Here researchers developed the Padding Key Encryption (PKE) algorithm. This algorithm provides secure communication between the sender and receiver by generating keys for plaintext [42]. By incorporating two private keys and using different encryption constants for each round, the study presented an enhanced Elliptic Curve Cryptography (ECC) encryption/decryption procedure. The strength of ECC is improved by this invention, which changes the linear equation's single unknown into a more reliable equation with two unknowns, improving overall security and cryptographic effectiveness [43].

III. ANALYSIS AND DISCUSSION

By the study of previous research, we can analyze the different features of cryptographic methods as mentioned in table I.

Table 1: Comparison of Cryptography Methods

Sr. No	Reference	Cryptography	Avalanche effect	Efficiency	Security	speed	Remarks
1	[2]	Chaotic Neural Networks	38.455	High	High	---	It provide new trend of cryptography .Result shown chipperbalance text test and independent test are good.
2	[3]	Elliptic Curve	----	High on small data	High	Higher	It shows lower power consumption and can be used for large image encryption.
3	[6]	DJMNA symmetric key algorithm	-----	High on small data	High	-----	Suitable for use on the short message, password, ATM, mobile, and defense

							networks.
4	[8]	DNA based	-------	High	High	Higher	It is widely useful in industrial engineering.
5	[12]	Modified RSA	--------	High	High	Slowest, Slightly High	Eliminate mathematical factorization attack.
6	[18]	MRGA	------	High	High	----	Extra Time needed
7	[21]	Horse Step	-------	High	High	slow	It provides more flexibility and capacity.
8	[23]	Randomize Encryption	64.6	High	High	----	Tracking Algorithm NP complete. Computational time is low
9	[25]	Binary RS A	-----	High	High	Slow	It uses binary code conversion for more security.
10	[26]	Bit level using Genetic Algorithm	-------	High	High	----	Each time key is modified .
11	[27]	Character Jumble	-----	Average	Average	----	Simple character order has changed.
12	[29]	DNA computing	--	High	High	Low	It provide new roadmap for cryptography
13	[30]	Vigenere and Modified Caesar	----	High	High	-----	It very robust and secure for cryptography
14	[32]	Bit circular shift	50.0	High	High	High	It took less time CER is 0.
15	[33]	Beaufort and Hill Cipher	40.80	High	High	High	Two encryption method is used.
16	[34]	Hybrid Twofish, AES, ElGamal and RSA Cryptosystems	---	High	High	High	It shows Twofish +RSA is faster
17	[38]	Key-Based Enhancement	---	High	High	High	New key is generated
18	[39]	Bit Plane Slicing,	51.16	High	High	High	More secure

		and Chaos System					against statistical attack.
19	[41]	Symmetric, Asymmetric and DNA Based	-----	High	High	High	It add the complexity of Biocomputing
20	[42]	Padding Key Encryption	-----	High	High	High	Security performance is 92%

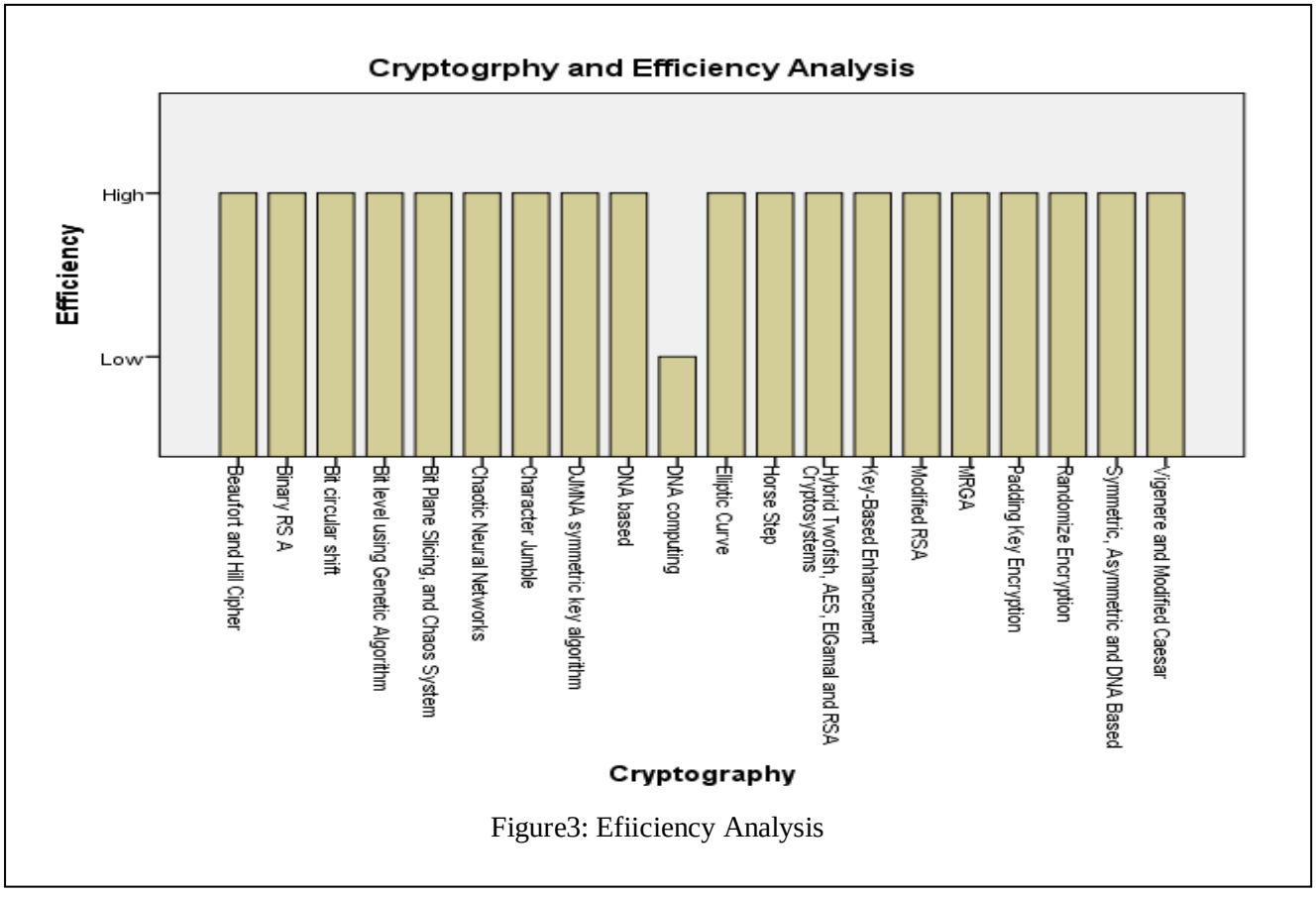


Figure3: Efiiciency Analysis

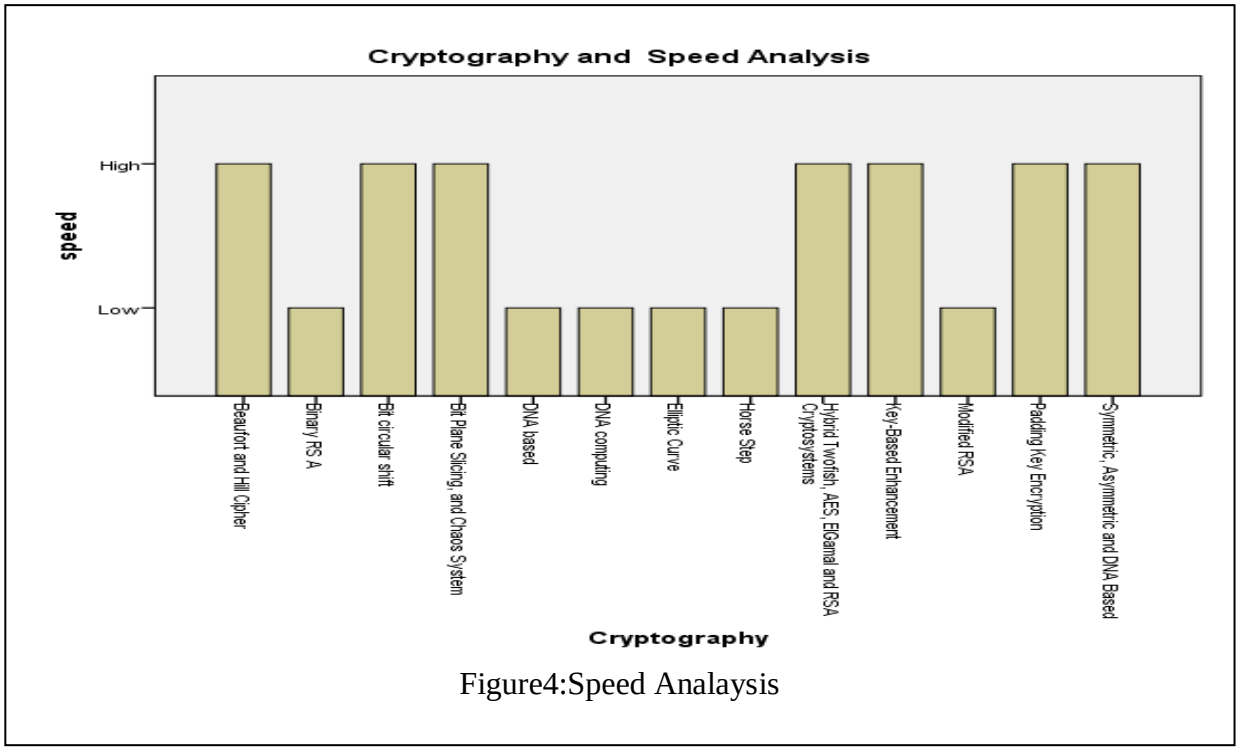
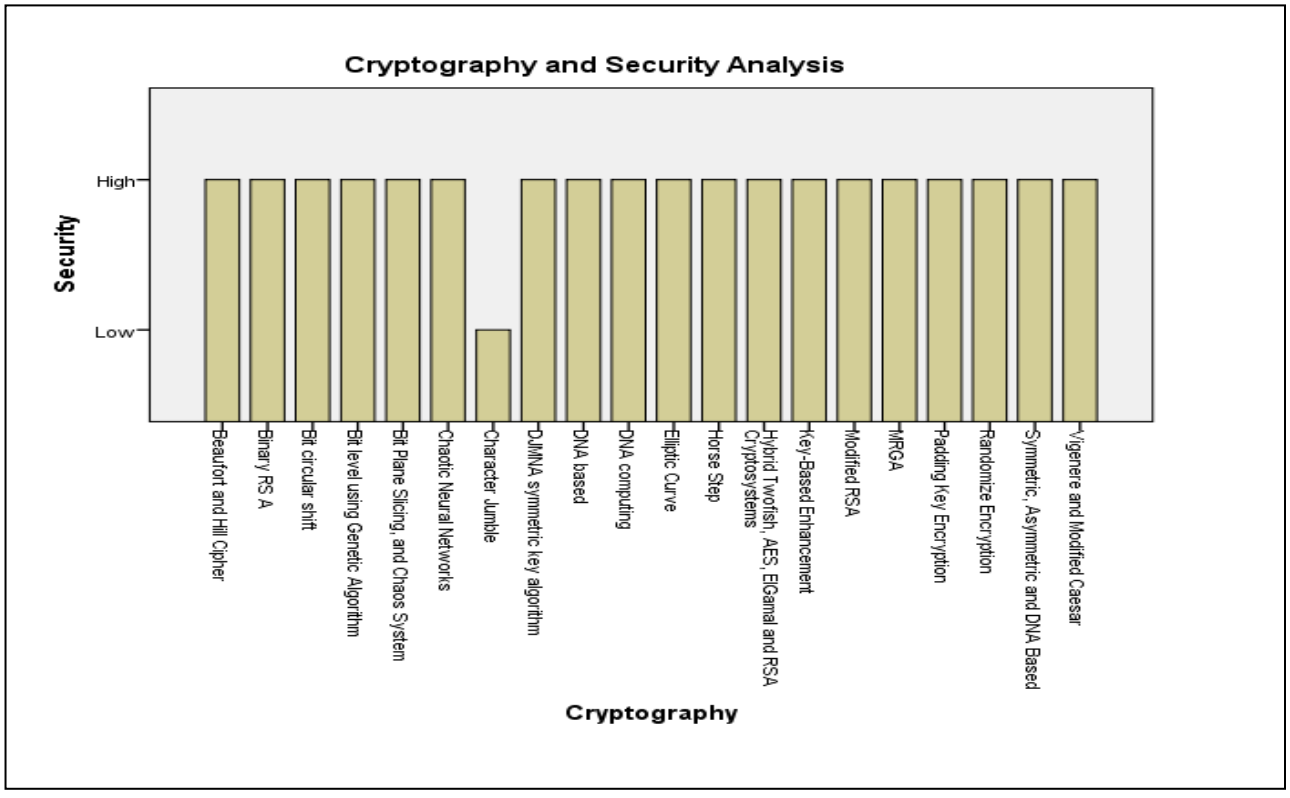


Figure4:Speed Analaysis

As Figure 3 demonstrates, all the cryptographic algorithms exhibit higher efficiency through their performance. Figure 4 illustrates that most of the algorithms have high speeds, while some of them have lower speeds. When discussing security, there is no doubt that all the algorithms employ specific techniques to provide security; thus, the majority of the algorithms exhibit high security.



The avalanche effect is a crucial characteristic of cryptographic algorithms since it adds to their security against attacks and unpredictable nature. To maintain the encryption level, academics and practitioners implement their algorithms to demonstrate a strong avalanche effect when reviewing and constructing them. Figure 6 Show the analysis of Avalanche effect. Higher value provide the good result.

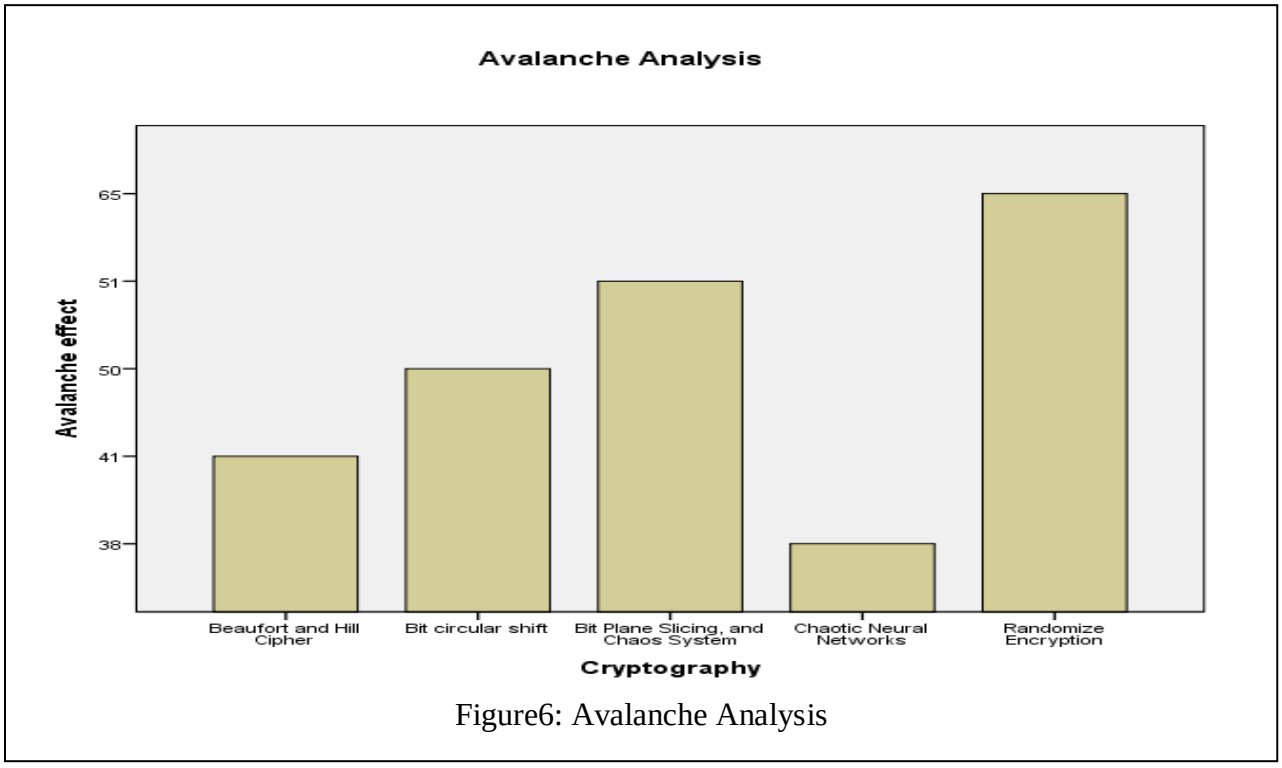


Figure6: Avalanche Analysis

IV.CONCLUSION

Here, we have delved into the study of various cryptographic methods and attempted to identify the trends that are predominantly employed to ensure information security. We have observed that each algorithm plays a significant role and yields favorable results based on its implementation. However, the latest advancement in cryptography involves DNA technology for novel biological enhancements, presenting a new path for the future. Additionally, it has noted that few researchers compare the Avalanche value for cryptographic algorithms, despite its potential as a valuable parameter for assessing block cipher algorithms. Therefore, here we have presented a comprehensive study of contemporary cryptographic techniques.

REFERENCES

1. Alfred J. Menezes, Paul C. Van Oorschot, and Scott A.Vanstonr, “Handbook of Applied Cryptography”, Boca Raton Florida, CRC Press, October 19962008

2. Y. Zhang, T. Xue, Z. Zhai, C. Ma and X. Cai, "The Improvement of Public Key Cryptography Based on Chaotic Neural Networks," 2008 Eighth International Conference on Intelligent Systems Design and Applications, Kaohsuing, Taiwan, 2008, pp. 326-330, doi: 10.1109/ISDA.2008.267.

3. S. M. C. Vigila and K. Muneeswaran, "Implementation of text based cryptosystem using Elliptic Curve Cryptography," 2009 First International Conference on Advanced Computing, Chennai, India, 2009, pp. 82-85, doi: 10.1109/ICADVC.2009.5378025.

4. D. Jena and S. K. Jena, "A Novel Visual Cryptography Scheme," 2009 International Conference on Advanced Computer Control, Singapore, 2009, pp. 207-211, doi: 10.1109/ICACC.2009.109.

5. Y. Qu and Z. Hu, "Research and design of elliptic curve cryptography," 2010 2nd International Conference on Future Computer and Communication, Wuhan, China, 2010, pp. V2-191-V2-195, doi: 10.1109/ICFCC.2010.5497370.

6. D. Das, M. Mukherjee, N. Choudhary, A. Nath and J. Nath, "An integrated symmetric key cryptography algorithm using Generalised Modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm," 2011 World Congress on Information and Communication Technologies, Mumbai, 2011, pp. 1199-1204, doi: 10.1109/WICT.2011.6141419.

7. A. M. AL-Abiachi, F. Ahmad and K. Ruhana, "A Competitive Study of Cryptography Techniques over Block Cipher," 2011 UkSim 13th International Conference on Computer Modelling and Simulation, Cambridge, UK, 2011, pp. 415-419, doi: 10.1109/UKSIM.2011.85.

8. B. Roy, G. Rakshit, P. Singha, A. Majumder and D. Datta, "An Improved Symmetric Key Cryptography with DNA Based Strong Cipher," 2011 International Conference on Devices and Communications (ICDeCom), Mesra, India, 2011, pp. 1-5, doi: 10.1109/ICDECOM.2011.5738553.

9. S. Malik, "A Novel Key-Based Transposition Scheme for Text Encryption," 2011 Frontiers of Information Technology, Islamabad, Pakistan, 2011, pp. 201-205, doi: 10.1109/FIT.2011.44.

10. X. Jing, Y. Hao, H. Fei and Z. Li, "Text Encryption Algorithm Based on Natural Language Processing," 2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2012, pp. 670-672, doi: 10.1109/MINES.2012.216.

11. A. M. Sagheer, "Elliptic curves cryptographic techniques," 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, QLD, Australia, 2012, pp. 1-7, doi: 10.1109/ICSPCS.2012.6507952.

12. R. Minni, K. Sultania, S. Mishra and D. R. Vincent, "An algorithm to enhance security in RSA," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013, pp. 1-4, doi: 10.1109/ICCCNT.2013.6726517.

13. Y. Qi, C. Tang, Y. Lou, M. Xu and B. Guo, "An Attribute-Based Encryption Scheme with Constant-Size Ciphertexts," 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 2013, pp. 1086-1088, doi: 10.1109/GreenCom-iThings-CPSCom.2013.186.

14. Y. -L. Huang, F. -Y. Leu, J. -H. Chen, C. -C. Chu and C. -T. Yang, "A True Random-Number Encryption Method," 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Taichung, Taiwan, 2013, pp. 654-659, doi: 10.1109/IMIS.2013.118.

15. D. Nilesh and M. Nagle, "The new cryptography algorithm with high throughput," 2014 International Conference on Computer Communication and Informatics, Coimbatore, India, 2014, pp. 1-5, doi: 10.1109/ICCCI.2014.6921739.

16. J. Gitanjali, N. Jeyanthi, C. Ranichandra and M. Pounambal, "ASCIi based cryptography using unique id, matrix multiplication and palindrome number," The 2014 International Symposium on Networks, Computers and Communications, Hammamet, Tunisia, 2014, pp. 1-3, doi: 10.1109/SNCC.2014.6866509.

17. S. Gomathi, "A cryptography using advanced substitution technique and symmetric key generating algorithm," 2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2014, pp. 224-228, doi: 10.1109/ISCO.2014.7103948.

18. D. I. G. Amlarethinam and J. S. Geetha, "Enhancing Security Level for Public Key Cryptosystem Using MRGA," 2014 World Congress on Computing and Communication Technologies, Trichirappalli, India, 2014, pp. 98-102, doi: 10.1109/WCCCT.2014.32.

19. K. Dasari, V. Srikanth, B. Veramallu, S. S. Kumar and K. Srinivasulu, "A novelty approach of symmetric encryption algorithm," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-4, doi: 10.1109/ICICES.2014.7033797.

20. R. Bassous, R. Bassous, H. Fu and Y. Zhu, "Ambiguous Multi-Symmetric Cryptography," 2015 IEEE International Conference on Communications (ICC), London, UK, 2015, pp. 7394-7399, doi: 10.1109/ICC.2015.7249508.

21. N. Nurwhaju, B. Hidayat and I. Iwut, "Novel cryptography using Horse Step Algorithm for more flexible key," 2015 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), Bandung, Indonesia, 2015, pp. 114-119, doi: 10.1109/APWiMob.2015.7374950.

22. A. Soloi, "An encryption algorithm," 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2015, pp. P-53-P-59, doi: 10.1109/ECAI.2015.7301252.

23. J. A. M. Azzam, "A Randomized Encryption Scheme," 2015 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2015, pp. 715-721, doi: 10.1109/CSCI.2015.171.

24. A. Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 2016, pp. 208-212, doi: 10.1109/ICICCS.2016.7542353.

25. P. M. Aiswarya, A. Raj, D. John, L. Martin and G. Sreenu, "Binary RSA encryption algorithm," 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India, 2016, pp. 178-181, doi: 10.1109/ICCICCT.2016.7987940.

26. A. Sen, A. Ghosh and A. Nath, "Bit level symmetric key cryptography using genetic algorithm," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, India, 2017, pp. 193-199, doi: 10.1109/CSNT.2017.8418536.

27. R. K. Singh, T. Begum, L. Borah and D. Samanta, "Text encryption: Character jumbling," 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2017, pp. 1-3, doi: 10.1109/ICISC.2017.8068691.

28. S. Hraiz and W. Etaiwi, "Symmetric encryption algorithm using graph representation," 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 2017, pp. 501-506, doi: 10.1109/ICITECH.2017.8080049.

29. O. G. Abood, S. Mesbah and S. K. Guirguis, "Enhancing AES Algorithm with DNA Computing," 2018 28th International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, 2018, pp. 35-41, doi: 10.1109/ICCTA45985.2018.9499202.

30. D. Gautam, C. Agrawal, P. Sharma, M. Mehta and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018, pp. 1-9, doi: 10.1109/ICOEI.2018.8553910.

31. S. Akhter and M. B. Chowdhury, "Bangla and English Text Cryptography Based on Modified Blowfish and Lempel-Ziv-Welch Algorithm to Minimize Execution Time," 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 96-101, doi: 10.1109/ICREST.2019.8644450.

32. H. N. Noor Muchsin, D. E. Sari, D. R. Ignatius Moses Setiadi and E. H. Rachmawanto, "Text Encryption using Extended Bit Circular Shift Cipher," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 2019, pp. 8138-8143, doi: 10.1109/ICIC47613.2019.8985708.

33. M. Fadlan, Suprianto, Muhammad and Y. Amaliah, "Double Layered Text Encryption using Beaufort and Hill Cipher Techniques," 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICIC50835.2020.9288538.

34. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems," 2020 IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

35. A. 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.

36. S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, "A Novel Approach of Symmetric Key Cryptography," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343.

37. P. R. Surabhi and T. V. Meenu, "Advanced 256-Bit AES Encryption With Plain Text Partitioning," 2021 International Conference on Advances in Computing and Communications (ICACC), Kochi, Kakkanad, India, 2021, pp. 1-3, doi: 10.1109/ICACC-202152719.2021.9708158.

38. O. Reyad, H. M. Mansour, M. Heshmat and E. A. Zanaty, "Key-Based Enhancement of Data Encryption Standard For Text Security," 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 2021, pp. 1-6, doi: 10.1109/NCCC49330.2021.9428818.

39. D. R. Ignatius Moses Setiadi, E. Hari Rachmawanto, R. Zulfiningrum and M. K. Sarker, "Text Encryption using Transform Dimension, Bit Plane Slicing, and Chaos System," 2022 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 2022, pp. 51-55, doi: 10.1109/iSemantic55962.2022.9920413.

40. M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi and B. Al-Ahmad, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," in IEEE Access, vol. 10, pp. 69388-69397, 2022, doi: 10.1109/ACCESS.2022.3187317.

41. V. Yadav and M. Kumar, "A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption," 2023 3rd International Conference on Intelligent Communication and Computational

Techniques (ICCT), Jaipur, India, 2023, pp. 1-5, doi: 10.1109/ICCT56969.2023.10076124.

42. A. Mittal and F. Sidney, "Secure Data Communication Using Padding Key Encryption Cryptography Algorithm," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-5, doi: 10.1109/ICICACS57338.2023.10099570.

43. David, A. O., & Sulaimon, O. (2023). Text Encryption with Improved Elliptic Curve Cryptography. Journal of Advances in Mathematics and Computer Science, 38(3), pp32-41.