|| Volume 6 || Issue 6 || June 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

AES (ADVANCED ENCRYPTION STANDARD) AND RC4

Prof. Sarika Patil[1], Yash Garole[2], Shivam Yadav[3], Priti Jawale[4], Sumit Kaygude [5]

Department of Computer, Keystone School of Engineering, Pune, India

sarikap@keystonesoe.in, yash.garole99@gmail.com, shivamsky5555@gmail.com, pritijawale61@gmail.com

sumit95kaygude@gmail.com

---------- ***----------

Abstract: **The goal of this project is to construct a new hybrid cypher by combining the features of two existing cyphers: AES (Advanced Encryption Standard) and Rc4 (also known as ARC4). The qualities of both cyphers are explored, and a new cypher that combines the traits of both cyphers and is more secure than the original cyphers is produced. AES's major characteristics are its security and attack resistance, whereas Rc4's key feature is its speed. As a result, the newly created cypher inherits these characteristics. As a result, in terms of speed and security against most attacks, it exceeds the original AES. Three combination tactics, as well as the technique and its strengths and limitations, have been devised in order to construct a hybridised cypher. The third cypher, which is the major cypher, is the subject of this study. This encryption is also shown to be robust to the majority of attacks. This ensures the confidentiality and secrecy of the messages encrypted by it.**

Keywords: - *Encryption Henon chaotic map RC4 , S-Box , security .*

----------***----------

I INTRODUCTION

Researchers are drawn to cryptography because it is one of the most essential topics of information and data security. There are two main classes: symmetric and asymmetric. Algorithms that are asymmetric The first class is the subject of the paper. which includes block cypher algorithms and stream cypher algorithms the use of algorithms The Substitution Box (S-Box) is one of the most popular types of substitution boxes. The only nonlinear component is also one of the most important. component that ensures the most common component's confusion characteristic Data Encryption Standard, for example, is a well-known block cypher. (DES) and the Advanced Encryption Standard (AES) are two types of encryption algorithms (AES). 'The' The effectiveness of these algorithms is determined by the way they are designed. S-Box is cryptographically secure. The S-Box is created using The well-known RC4 key-scheduling technique is used, and As a result, the S-Box is named after the key. We will discuss this in this paper. Two novel approaches for generating S-Boxes are proposed: The S-Box is a device that allows you to play video games rely on the RC4 method for key and text, and The S-Box is based upon key and plaintext utilising the RC4 chaotic algorithm. a computer programme

II PROBLEM STATEMENT

Without revealing the underlying plaintext, convert a ciphertext under one access policy into ciphertexts of the same plaintext but under different access rules. A cypher or hack can be broken in a number of ways.

III MOTIVATION

Encrypted data is safely kept using keys. The key is distributed to a group and then used to decrypt the data. We can use access policies to specify which types of users are permitted to access a certain file. The ag algorithm is used to detect file content duplication.

IV OBJECTIVES

To convert cypher texts with the same plaintext but different access rules into cypher texts with the same plaintext but different access policies without revealing the underlying plaintext. To ensure that the data in the system is consistent. Unless the adversary acquires the plaintext contained in the cypher text by accident, undertake repeat faking assaults.

V LITERATURE REVIEW

Amira S. El Batouty, Hania H," New Hybrid AES Static S-Box Algorithm Using Chaotic Maps" [1] — To combat emerging data theft strategies, security methods must be upgraded. The encryption of block cyphers is based on the substitution table. The encryption algorithm's security is enhanced by S-well-designed Box's design. This work presents two algorithms for generating modified S-Boxes, which use the RC4 technique to rely on key and plaintext. The S-Box, on the other hand, is based on a key and plaintext utilising the RC4 chaotic algorithm. The purpose of this research is to evaluate and contrast the suggested SBoxes to the current AES and Dynamic S-Boxes.

Mathew K. Samimi "3-D Millimeter-Wave Statistical Channel Model for 5G Wireless System Design",[2] a 3-D statistical channel impulse response (IR) model for urban LOS and non-LOS channels derived from ultrawideband propagation measurements at 28 and 73 GHz in New York City, useful in the design of 5G wireless systems that will operate in both the ultra-high frequency/microwave and millimeter-wave (mmWave) spectrum to increase channel capacities. A 3GPP-like stochastic IR channel model is developed using measured power delay profiles, angle of departure, and angle of arrival power spectra. The data is used to build a channel model and simulator capable of generating 3-D mmWave temporal and spatial channel parameters for any mmWave carrier frequency, signal bandwidth, and antenna beamwidth. The model provided here faithfully reproduces true IRs of measured urban channels,

enabling for the design of mmWave transceivers, filters, and multi-element antenna arrays at the air interface.

Nur Atikah 'AES-RC4 Encryption Technique to Improve File Security",[3] Data security becomes crucial while connecting via public networks. Third-party data theft carries a number of concerns. Cryptography is one method of securing data. Decryption process are the two fundamental methods of cryptography. The process transforms a plaintext file to an encrypted or ciphertext file is called encryption. Plain text into cipher text of converting encrypted or ciphertext material back to its original or plaintext form. There are numerous encryption techniques available today, with more complex encryption being logically stronger and more difficult to crack. To ensure data secrecy, this paper recommends combining the AES and RC4 algorithms. This method is combined with others to enhance the algorithm's sophistication and robustness. Utilize the avalanche effect to determine the safety of an algorithm (AE). The distinction between the two conclusions is between ciphertext and AE measurements, which are performed by altering the value of a single bit in the key. The bigger the discrepancy between the two values, the more secure the encryption. The ideal AE value is roughly 50%, and the greater the AE value, the higher the encryption quality. The AES-RC4 approach when coupled produces the best AE results of 58.2 percent, which is significantly higher than the AES algorithm, RC4 alone, or RC4-AES.

Anirban Bhowmick and Nishith Sinha. "Permutation-Substitution Architecture Based Image Encryption Algorithm Using Middle Square and RC4 PRNG"[4] - In recent years, the growing importance of information security has encouraged the development of secure encryption techniques. The majority of classic algorithms, such as AES and DES, require a lot of processing power. As a result, we offer a simple but secure symmetric key encryption scheme in this study. To encrypt images, the image encryption method employs two pseudorandom number generators. The Middle Square Algorithm is used to swap the image's columns before switching the rows. The intermediary cypher image is created as a result of this permutation process. Following that, the RC4 technique is employed to generate a stream of pseudo-random numbers. These numbers are used to replace the pixel intensity of the intermediary cypher image, resulting in the final encrypted image. The quality of the encrypted image is subjected to a variety of analytic procedures. These experiments show that the suggested approach is both secure and efficient.

Nariman Farsad,." A Comprehensive Survey of Recent Advancements in Molecular Communication"[5] Nano- and nanoscale technologies are becoming a reality as a result of the previous decade's great advancements in nanotechnology, bioengineering, and synthetic biology. Even so Nonetheless, the question of building a robust communication system for small devices remains unsolved. Despite radio communication's widespread use, there are still regions where standard electromagnetic waves are either impossible or excessively expensive to reach. The majority of points of interest are buried and embedded in industry, cities, and medical applications, accessible only via ventricles at scales too small for conventional radio waves and microwaves, or are positioned in such a way that focused high frequency systems are inefficient. One solution to these challenges is molecular communication (MC), which is inspired by nature and transmits information via chemical signals. While scientists have been investigating MC for decades, it has just recently been researched from a communication engineering perspective. Numerous publications have been published to date, although many of the findings are preliminary due to the requirement for interdisciplinary study. This overview summarises the most significant recent advances in the field of MC engineering. To begin, the biological, chemical, and physical mechanisms by which an MC system operates are addressed. This category encompasses a range of MC transmitter and receiver components, as well as propagation and transport systems. Then, through the lens of communication engineering, a complete review of several recent works on MC is offered. The study concludes with a technical readiness assessment of MC and recommendations for future research.

VI SYSTEM ANALYSIS

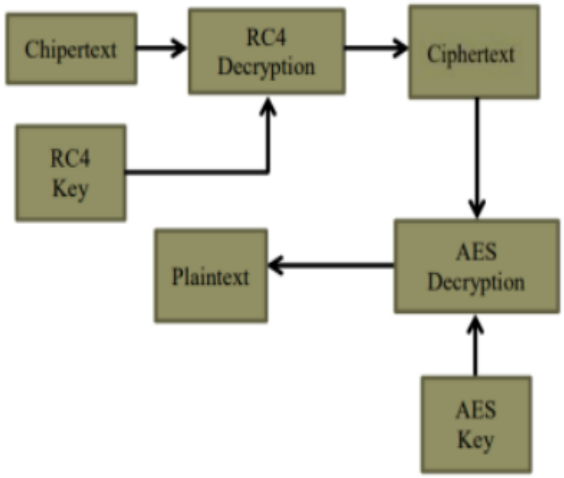

FIG. SYSTEM ARCHITECTIRE

VII CONCLUSION

In the proposed system, the owner uploads the file with its properties and access policy, as well as the access time. After uploading the file, it is checked to see if it is duplicated or not. Following this, if the file is duplicated, the owner receives proof of ownership; if the file is original, it is stored on the cloud, and when a user requests access to a file, the authority checks the user's attributes and only the user receives the key to access the file from the cloud. As a result, the proposed system is deduplication-secure.

REFERENCES

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto, and M. Do□heir, "A Comparative Study of Image Cryptographic Method," in 2018 5th International Conference on Information Technology, Computer, and Electri cal Engineering (ICITACEE), 2018, pp. 336– 341.

[2]D. R. I. M. Setiadi, "Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation," Intl J. Electron. Telecommun., vol. 65, no. 2, pp. 295–300, 2019.

[3] M. Mohurle and V. V. Panchbhai, "Review on realization of AES encryption and decryption with power and area optimization," in 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Sys tems (ICPEICES), 2016, pp. 1–3.

[4] A. Setyono, D. R. I. M. Setiadi, and Muljono, "Dual encryption techniques for secure image transmission," J. Telecommun. Electron.

[5] Balajee Maram K, J M Gnanasekar. Evaluation of Key Depend S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output. TEM J. 2016; 5:67–75.

[6] Haoran Wen, A review of the H´enon map and its physical interpretations. School of Physics Georgia Institute of Technology, Atlanta, GA 30332-0430, U.S.A (Dated: April 21, 2014).

[7]Pedro Miguel Sosa. Calculating Nonlinearity of Boolean Functions with Walsh Hadamard Transform. UCSB, Santa Barbara, CA – USA April 23, 2016.

[8] A. Vassilev and R. Staples, "Entropy as a Service: Unlocking Cryptography's Full Potential," Computer (Long. Beach. Calif)., vol. 49, no. 9, pp. 98–102, Sep. 2016.

[9] C. P. Dewangan, S. Agrawal, A. K. Mandal, and A. Tiwari, "Study of avalanche effect in AES using binary codes," in 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICAC CCT), 2012, pp. 183–187.

[10] S. K. Mandal and A. R. Deepti, "A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme," Int. J. Comput. Sci. Inf. Technol., vol. 7, no. 4, pp. 2096–2099, 2016.

[11] B. B. Mohammed, "Automatic Key Generation of Caesar Cipher," Int. J. Eng. Trends Technol., vol. 6, no. 6, 2013.

[12] Ritambhara, A. Gupta, and M. Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IoT)," in 2017 International Conference on Com puting, Communication and Automation (ICCCA), 2017, pp. 422–427.

[13] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, "A perfor□mance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," in International Seminar on Application for Technology of Infor mation and Communication, 2017.

[14] C. Irawan, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, "Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security," J. Phys. Conf. Ser., vol. 1201, no. 1, p. 012022, May 2019.