International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

# Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach

Tushar[1], Aniket Sharma[2], Ankit Mishra [3]
Department of Computer Science, Amity University Chhattisgarh
Department of Computer Science, Amity University Chhattisgarh
Department of Electrical and Electronics Engineering , Amity University Chhattisgarh

***Abstract*: The quick progress of this technology becomes vital in upcoming years. Any type of data present in cloud is confidential for individual and this can be hacked by attackers while sharing it with the intended recipient.The demand for veracity, privacy, fortification, solitude and procedures required for handling is increased. This paper discussed brief about cryptographic methods and a new cryptographic Algorithm method for securing the data for Enhancing Data Security that can be used to secure applications on cloud computing**

***Keywords:- Cryptography,Symmetric key , 2's Compliment encryption, Data Security, Encryption, Decryption***

## I. INTRODUCTION

The Greek meaning of Cryptography is Secret Writing. Data Security is one of the major concerns in today's world. Cryptography is a method to fulfill the confidentiality of data. Cryptography provides the privacy of data for an individual or organization by converting the original data to a readable ununderstandable format for an unauthorized person and converting back to original data for the authorized individual[1]. Cryptography Technique translates the plain text to another format, which is called cipher Text with an Encryption Key and can also Convert cipher text back to plain text with the same or different encryption key based on the technique used to encrypt the data.

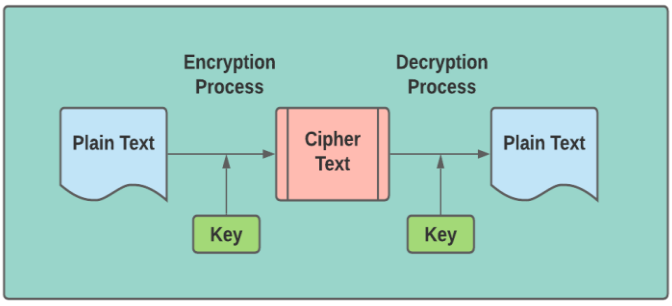


Fig. 1 Cryptography Process

### (A). CHARACTERISTICS OF CRYPTOGRAPHY

- Data Security – Secures the plain text
- Data Breaches – Protects from the release of confidential information to the environment
- Authentication and Authorization – Allow only the authentic individual to read/write the data

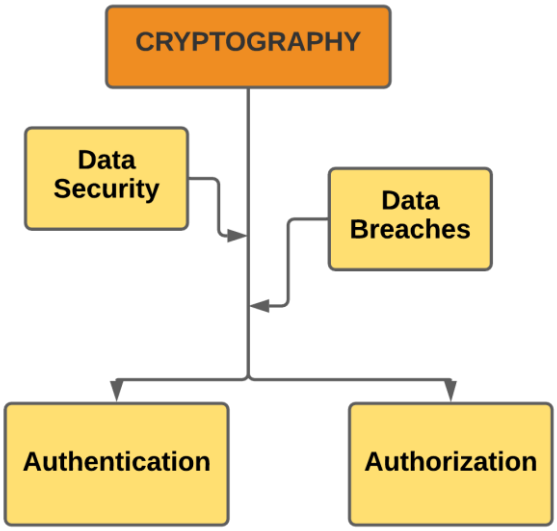


Fig. 2 Cryptography Characteristics

### (B). TYPES OF CRYPTOGRAPHY

Cryptography is a method that is linked to convert plain text into cipher text i.e called encryption and convert back to plain text i.e know as decryption. Various type of encryption and decryption are available but the most commonly used algorithms for cryptography are

### (C). SYMMETRIC KEY CRYPTOGRAPHY

In this Cryptographic approach, a single key is used to encrypt and decrypt the data. The key must be known to both the clients to read/write the data. There are different methods of Symmetric key Algorithm like DES, 3DES, AES, and more.

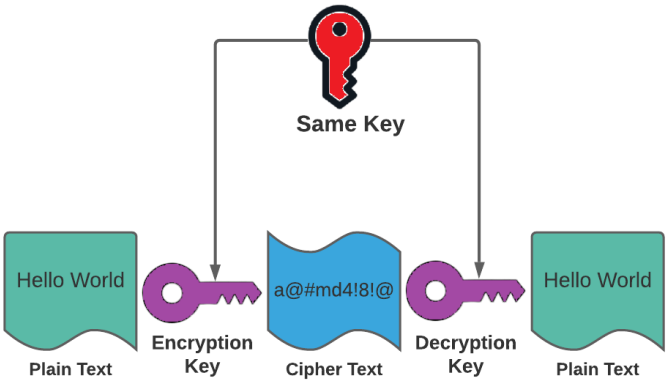


Fig. 3 Symmetric Cryptography

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

**(D). ASYMMETRIC KEY CRYPTOGRAPHY**

In this Cryptography approach, there are two different keys to encrypt and decrypt the data. The key used to encrypt the data is called Public Key and the second key is used to decrypt the data called the Private key. Both keys are different from each other. Private Key is only available to the receiver.

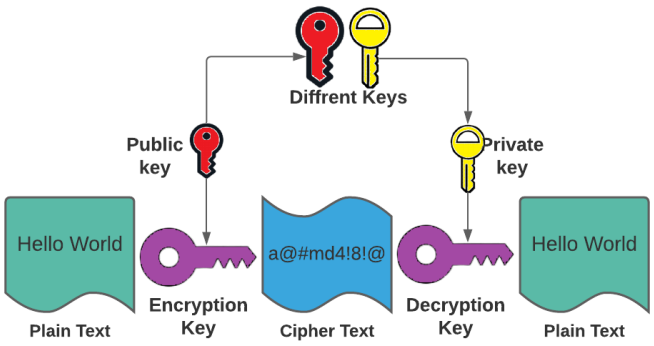


Fig. 4 Asymmetric Cryptography

## II. LITERATURE REVIEW

1. Reema Gupta proposed "Efficient Encryption Techniques in cryptography Better Security Enhancement." The paper promotes the encryption technique and reviewed their restrictions and approach. Also, talked about the transpositional approach like Simple columnar, simple row, Route Cipher transposition.[2]
2. Ayushi proposed "A Symmetric Key Cryptographic Algorithm."; She had introduced two primary types of cryptography, Symmetric Key and Asymmetric Key technique. She also proposed a fast symmetric cryptography algorithm. She used keys as greater or equal to 1000 and converted the plain text to cipher text using some binary and mathematical calculations.[3]
3. Ekta Agarwal et al. had proposed "A Secure and Fast Approach for Encryption and Decryption of Message Communication"; the Authors had discussed Cryptography architecture, performance, and more. They had compared the symmetric technique of Ayushi[3] with their proposed algorithm and found their algorithm much faster.[4]
4. Abhishek Joshi and their co-author proposed "An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryplanalytic Attacks," The paper describes the cryptographic scheme and protection from Brute Force attacks. The author shows that this technique can be used for significant applications.[5]
5. Suyash Verma et al. proposed "An efficient Developed New Symmetric Key Cryptography Algorithm for Information Security." The proposed new block cipher technique is faster than the existing mechanism. They concluded the result by calculating with different plain text in the same key(DPSK) mode.[6]
6. Dr. Prerna Mahajan et al. proposed "A Study of Encryption Algorithm AES, DES, and RSA for Security," Authors reviewed three encryption techniques like AES, DES, and RSA mentioned the comparison results of the effectiveness of each algorithm.[7]

## III. SYMMETRIC APPROACH

Symmetric Key Encryption takes less execution time and is always easy to implement in real-life applications, yet their drawback is that both clients need to move their key's security[8]. This approach highlights improving the standard method of encryption by using the Substitution technique[4]. In this proposed algorithm, the first single character is converted into its respective ASCII code value, and further encryption continues.

## IV. PROPOSED SYMMETRIC KEY ALGORITHM

- **Encryption Algorithm**

Step 1: Convert a **Single Character** to its ASCII value.
Step 2: Add a key as **100**, add it to the character's ASCII value and store it in a variable.
Step 3: Generate the Binary value from the variable got in Step 2.
Step 4: Make the Binary Number of 8 digits by adding 0 on the number's left side.
Step 5: Reverse the Binary got from Step 4.
Step 6: Split Binary numbers in two equal parts as element-1 and element-2.
Step 7: Find the 2's Compliment for both equal parts and store them in complementElement-1 and complementElement-2, respectively.
Step 8: Concatenate complementElement-2 with complementElement-1
Step 9: Find the 2's Compliment of the Binary got in Step 8
Step 10: Generate the Hexadecimal value of the Binary got in Step 9.
Step 11: Formate the Hexadecimal value got from Step 10 to have a minimum of eight-digit if already the code is not of a minimum of eight-digit and return that as a **CipherText**.

**Example:-**

Let us take a **Single Character,** "C" Now, we will get the following steps according to my proposed algorithm.

Step 1: ASCII of "C" is 67.
Step 2: Adding 100 as a key to ASCII of "C" in s1=100+67=167
Step 3: Now we got the Binary of 167 as 10100111
Step 4: Binary in Step 3 is already of 8 digits to continue with Binary we have in Step 3 as 10100111.
Step 5: Now, the reverse of the Binary we have in Step 4 will be 11100101.
Step 6: Now, we have to split the Binary from Step 5 into equal halves as *element-1: 1110 and element-2: 0101*.
Step 7: Now, 2's Compliment of each element got in step 6 respectively will be *complementElement-1: 0010 and complementElement-2: 1011*.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

Step 8: Next, we have to Concatenate complementElement-2 with complementElement-1 that will be *10110010*.
Step 9: Further, 2's Complement of Binary got in Step 8 will be *01001110*.
Step 10: Finally, the Binary received from Step 9 in hexadecimal will be *f4696*.
Step 11: Formating the Hexadecimal code got from Step 10 to a minimum of eight-digit as *000f4696*.

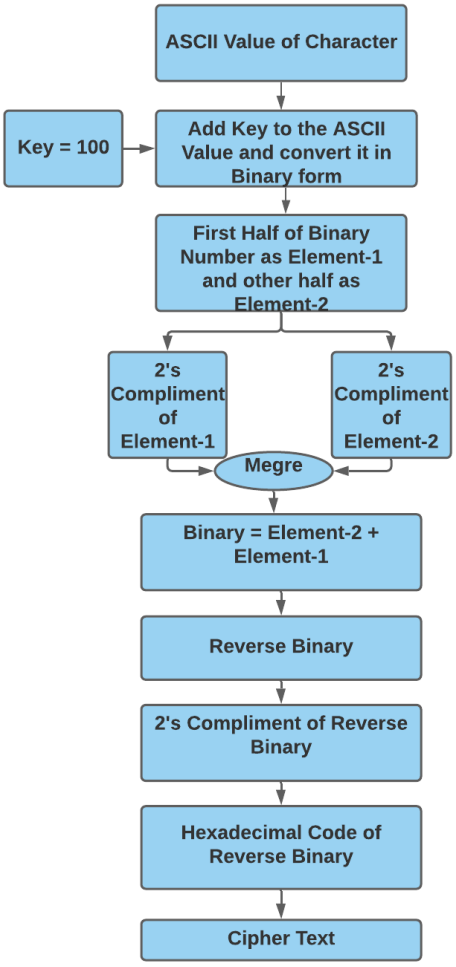


Figure 5 shows the architecture of the proposed encryption Algorithm

- **Decryption Algorithm**

Step 1: Convert **CipherText** to Binary.
Step 2: Format the Binary to 8 digits by adding 0 on the left side of the Binary is not already formatted.
Step 3: Find 2's Compliment of the Binary got in Step 1.
Step 4: Split the Binary got in Step 2 into two halves as element-1 and element-2.
Step 5: Find the 2's Compliment for both equal parts and store them in complementElement-1 and complementElement-2, respectively.
Step 6: Concatenate complementElement-2 with complementElement-1
Step 7: Reverse the Binary got from Step 5.
Step 8: Find the ASCII value of the Binary got from Step 6.
Step 9: Subtract the Key **100** from the ASCII got in Step 7.Step 10: Convert and return the ASCII value from Step 8 to its respective Character value as **Single Character**.

**Example:-**
Now, Let us take **CipherText** as "*000f4696"*. Now according to the proposed decryption algorithm, we will get the following steps.

Step 1: Converting CipherText to Binary, we would get *1001110*.
Step 2: After Formating Binary Number from Step 1 to 8 digit, we will get *01001110*.
Step 3: 2's Complement of Binary got in Step 2 will be *10110010*.
Step 4: Now, we have to split the Binary from Step 4 into equal halves as *element-1: 1011 and element-2: 0010*.
Step 5: Now, 2's Compliment of each element got in step 4 respectively will be *complementElement-1: 0101 and complementElement-2: 1110*.
Step 6: Next, we have to Concatenate complementElement-2 with complementElement-1 that will be *11100101*.
Step 7: Now, the reverse of the Binary we have in Step 6 will be 10100111.
Step 8: ASCII of the Binary got from Step 7 will be *167*.
Step 9: After Subtracting the key (100) from the value received in Step 8, we get *67 (167-100).*
Step 10: The character Value of the ASCII we get from Step 9 will be "*C*," which is the *Plain Text*

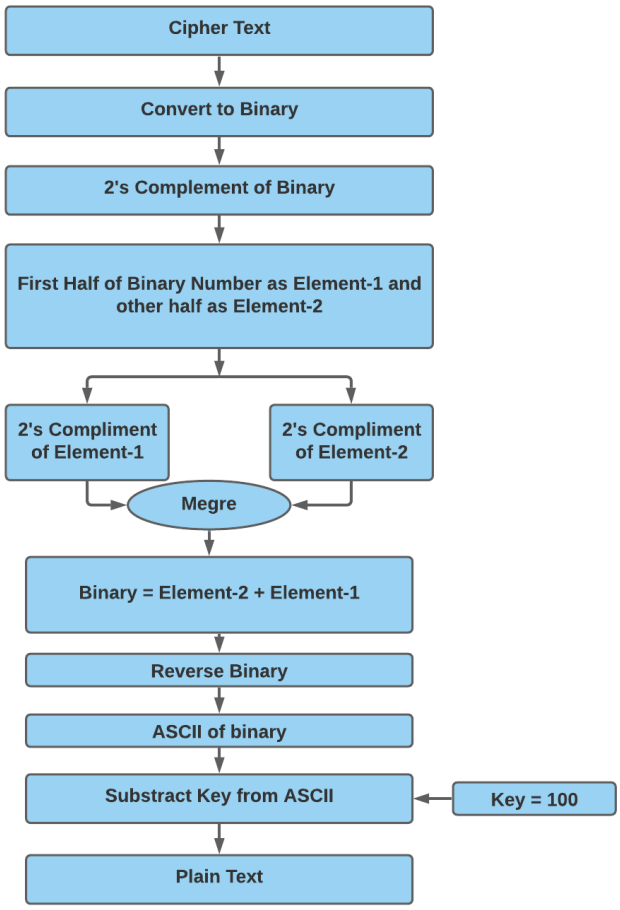


Fig 6: Shows the architecture of the proposed decryption Algorithm

## V. EXPERIMENTAL ANALYSIS

For experimental analysis, the proposed algorithm with the symmetric key is codded in Python 3.8.5. The i7

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

preprocessor(2.6GHz Intel processor with 12MB cache memory) and 8GB RAM(DDR4 2933 Mhz). A single Character show encrypted and Decrypted in shown figures.

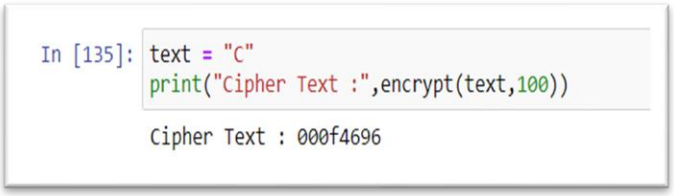


Figure 7. Encryption Output


Fig 8. Decryption Output

## VI. CONCLUSION

**Cryptography** is transforming plain text to non-understandable readable text to protect private data[9][10]. We have to exchange multiple types of data on the internet that can be confidential. Cryptography is used to hide the original data, i.e., plain text, from unauthorized access by converting it to an un-understandable format by some mathematical combination[10][8]. This paper has introduced a new Efficient algorithm of Cryptography that is very simple to nature with the least execution time for encryption and decryption. Also, the proposed algorithm is easy to apply in a real-life project for the Encryption and Decryption Process.

## VII. REFERENCES

[1] Neha Sharma, Prabhjot and Er. Harpreet Kaur, "A Review of Information Security using Cryptography Technique", International Journal of Advanced Research in Computer Science – Volume 8, No. 4, May 2017 (Special Issue)

[2] Reema Gupta " Efficient Encryption Techniques In Cryptography Better Security Enhancement" Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at www.ijarcsse.com Available:https://www.ijarcsse.com/docs/papers/Volume_4/5_May2014/V4I5-0450.pdf

[3] Ayushi. "Article: A Symmetric Key Cryptographic Algorithm." International Journal of Computer Applications 2010; 1(14):1–4, DOI: 10.5120/331-502.

[4] Ekta Agrawal, Dr. Parashu Ram Pal, "A Secure and Fast Approach for Encryption and Decryption of Message Communication," International Journal of Engineering Science and Computing. Volume 7 Issue No. 5

[5] Abhishek Joshi, Mohammad Wazid, R.H. Goudar, An Efficient Cryptographic Scheme for Text Message Protection Against Brute Force and Cryptanalytic Attacks, Procedia Computer Science, Volume 48, 2015, Pages 360-366, ISSN 1877-0509.

[6] Suyash Verma, Rajnish Choubey, Roopali soni (2012): "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security," International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012) 18.

[7] Mahajan, Prerna and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." Global journal of computer science and technology 13 (2013)

[8] Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 763-770

[9] T.Saravanan, Dr. S.Venkatesh Kumar, "A Review Paper on Cryptography-Science of Secure Communication," International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 4, Jul-Aug 2018

[10] 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.