International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cryptographic Algorithm to Augment Data Security

Vipin R Bharadwaj[1], Nalina V[2], Rithvik Mohan V[3]

[1]Bengaluru, India
vipinrbharadwaj[at]gmail.com

[2]BMSCE, Bengaluru, India
nalinav.ise[at]bmsce.ac.in

[3]Bengaluru, India
rithvikvm[at]gmail.com

Abstract: ***Technology has become essential in everybody's life. The advancement in technology over the years have been an indirect cause to be subjected to cyber - attacks. Any confidential data that is transferred over the internet can be hacked and can cause huge discrepancy even if the data is received by intended personnel. Due to these concerns, there is a requirement to improve and fortify data security. This paper talks about a new cryptographic algorithm, designed to secure transmitted data for enhanced data integrity. The proposed solution can be implemented with any web application that interacts with a server.***

Keywords: Cryptography, Data security, Encryption, Decryption, Cybersecurity

1. Introduction

With technologies improving all around the world, it is also providing an opportunity for attackers to steal or alter data confidential to an individual or a group of individuals. This is a huge worry in today's environment, as everything is becoming digitised. Cryptography is the answer to this problem since it gives a way to ensure data secrecy and integrity. Cryptography protects data by changing the original text into a format that is incomprehensible to unauthorised individuals while in transit and then converting it back to the original text when received by authorised persons [1].

Generally, Cryptography converts plain text to cypher text using an encryption key, and may also convert cipher text back to plain text using the same or a different encryption key depending on the encryption technique used to encrypt the data [2].

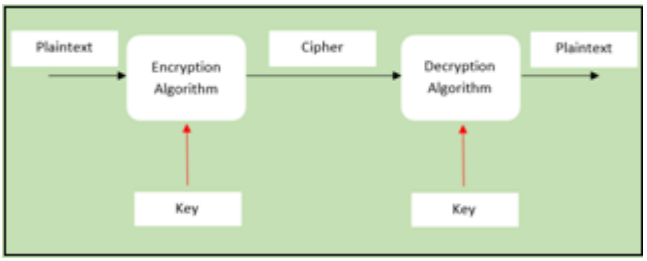

Figure 1: Concept of Cryptography

In Cryptography terms [3],

1) **Plaintext** is the original message provided to the encryption algorithm.
2) **Encryption algorithm** technique that converts plaintext to cipher text.
3) **Cipher text** is the encrypted message.
4) **Decryption Algorithm** is the technique that converts cipher text back into plaintext.
5) **Key** is a set of characters that is used in the process of encryption and decryption.

The ciphering and decoding processes of the cryptographic algorithm presented in this work differ slightly. This method eliminates the need for the user to enter a secret key to encrypt and decrypt data. Instead, the data is encrypted and decrypted by iterating over itself and replacing each plaintext character with one from a set created by the algorithm. The key to decode the cipher is embedded within the cipher.

2. Literature Survey

A. Gupta [5] discussed the history and significance of cryptography, as well as how information security has become a difficult problem in the computer and communications areas. This paper also provides various asymmetric algorithms that have given us the ability to protect and secure data, in addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by providing security and privacy. Abhishek Joshi and their co - author [6] proposed "An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryplanalytic Attacks". The article explains the cryptographic technique as well as how it protects against Brute Force assaults. The author demonstrates that this approach has a wide range of applications.

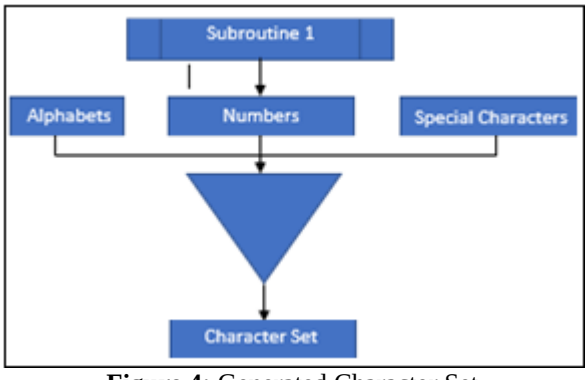

Figure 4: Generated Character Set

Proposed Algorithm

a) **SETS USED:**

- **Alphabet_Array** – consisting of 26 uppercase and 26 lowercase English alphabets.
- **Number_Array** – consisting of 10 numbers, 0 to 9.
- **Special_Character_Array** – consisting of 32 special characters.
- **Character_Set** – set belonging to union of all the above - mentioned arrays with size 2 times the sum of length of all 3 arrays.

b) **Principle:**

Dividend = **Quotient** * **Divisor** + **Remainder**

c) **Encryption Algorithm:**

Step 1: Generate character set.
Step 2: Extract each character from plaintext into an array.
Step 3: For each character, choose an encryption character from the generated character set.
Step 4: Find the ASCII value of each character and its respective character chosen from character set.
Step 5: Add the ASCII values of both characters found in Step 4.
Step 6: Find the value of the sum modulo length of generated character set.
Step 7: Replace the character with character from character set at the index of modulo value calculated in Step 6.
Step 8: Include the key of length same as length of plaintext and generated character set along with Cipher excluding any 2 [number of different arrays used – 1] values from the set.
Step 9: Return the generated Cipher Text calculated in Step 8 with length calculated below,

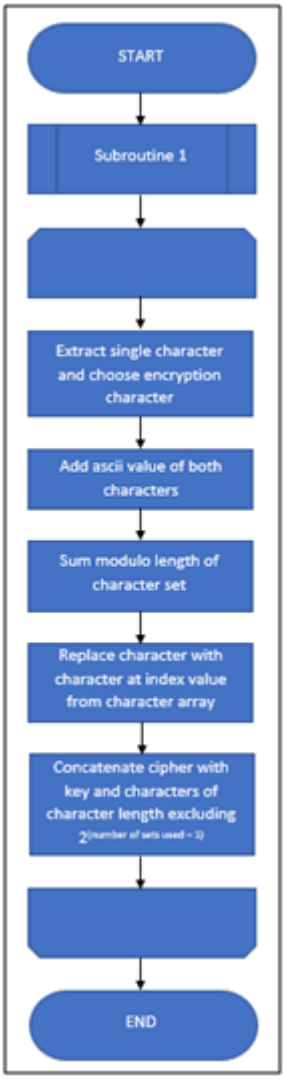

Figure 3: Encryption Algorithm

Length of Cipher Text = (2 * length of plaintext) + (Length of generated Character set - $2^{[\text{number of different arrays used} - 1]}$)

Example:

a) Plaintext is of type string: Let us consider a single character 'T'

Step 1: Generate character array having length – 94.
Step 2: Extract a character from generated character set.
Step 3: Add the ASCII value of chosen character to 84 (ASCII value of T).
Step 4: Find the value of the sum modulo 94.
Step 5: Replace T with the value present at the calculated index, here the encrypted key is 'S4'.
Step 6: Generate a string including the encrypted character along with the key of length 124 (128 – 4).
Step 7: Return the generated Cipher Text of total length 124 + 2 = 126 – "**E8VzBNcTgTO%8qUzd: wyq%r!7EY2IlDxmUpFTRMLF]v_SjfGhfj?y=k7xXZ8 o2NS45LQH ^u%C63rzMR9lzb#nwQ907Wze6GIPR9yAEsc11JE6a 5fXXa6K`tJ2) i!SB**"

Figure 2: Encryption of Single Character

b) Plaintext is of type JSON object: Let us consider a simple JSON Object {name: 'Dan', age: '24'}

Step 1: Generate character array having length – 94.
Step 2: Extract a character for each character in plaintext from generated character set.
Step 3: Add the ASCII value of chosen character to ASCII value of each character in plaintext.
Step 4: Find the value of the sum modulo 94 for each character.
Step 5: Replace the character with the value present at the calculated index.
Step 6: Generate a string including the encrypted character along with the key of length 124 (128 – 4).
Step 7: Return the generated Cipher Text –
"**8{4^6`iWUgdGo5NZD?Mdm2Zmy]hR2.5/C0LrX, J: e. n8xub'q%tJsoHsO) KkP, rYYL31F! kmElRZA?udc [IopizKV+S0Q: 7aaFvDGzw) T|jKW[at]B!g!lK1^0Mff9) 9BvBRBGBzB4BSAh BzBlBvABA7BWBjBZBBAdBDB1AnC**"

Figure 6: JSON Object Encryption Example

c) Decryption Algorithm:
Step 1: Extract cipher and the key from cipher text.
Step 2: Decode each character by using the principle of dividend.
Step 3: Using the dividend found in Step 2, get the corresponding character from generated character array.
Step 4: Find the ASCII value of each character and its respective character chosen from character set.
Step 5: Return the obtained plaintext calculated in Step 4.

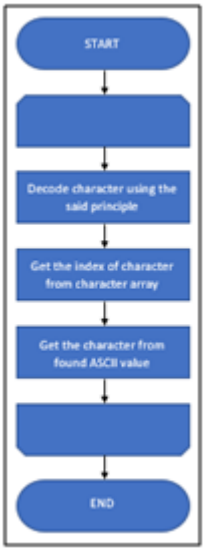

Figure 5: Decryption Algorithm

Example:
a) Cipher is of type string: Let us consider a cipher text – "E8VzBNcTgTO%8qUzd: wyq%r!7EY2IlDxmUpFTRMLF]v_SjfGhfj?y=k7xXZ 8o2NS45LQH^ u%C63rzMR9lzb#nwQ907Wze6GIPR9yAEsc11JE6a 5fXXa6K`tJ2) i!SB"
Step 1: Extract cipher 'S4' from cipher text.
Step 2: Complete the character set extracted from the cipher text.
Step 3: Decode 'S4' using the principle of dividend, using the index of Character present in character set.
Step 4: Using the index, decode 'S4' to get the ASCII value of original text, value calculated is 84.
Step 5: Return the character, T.

Figure 7: Decryption of Single Character

b) Cipher Text is of type JSON object: Let us consider "8{4^6`iWUgdGo5NZD?Mdm2Zmy]hR2.5/C0LrX, J: e. n8xub'q%tJsoHsO) KkP, rYYL31F!kmElRZA?udc [IopizKV+S0Q: 7aaFvDGzw) T|jKW[at]B!g!lK1^0Mff9) 9BvBRBGBzB4BSAhBzBlBvABA7BWBjBZBBAdB DB1AnC"
Step 1: Extract cipher from cipher text.
Step 2: Complete the character set extracted from the cipher text.
Step 3: Decode each character using the principle of dividend, using the index of each character present in character set.
Step 4: Using the index, decode each character to get the ASCII value of original text.

Step 5: Return the object – {name: 'Dan', age: '24'}

Figure 8: JSON Object Decryption Example

3. Experimental Analysis

For Experimental analysis, the proposed cryptographic algorithm is developed with ReactJS as frontend and Nodejs as backend, hosted on firebase as cloud function, with React version being 17.0.2 and node version 14.

The following figures show example of encryption and decryption of a single character, a string and a JSON Object.

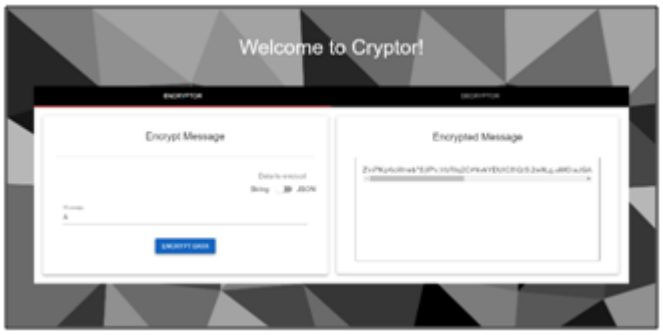

Figure 9: Encryption of Single Character

Figure 10: Decryption of Single Character

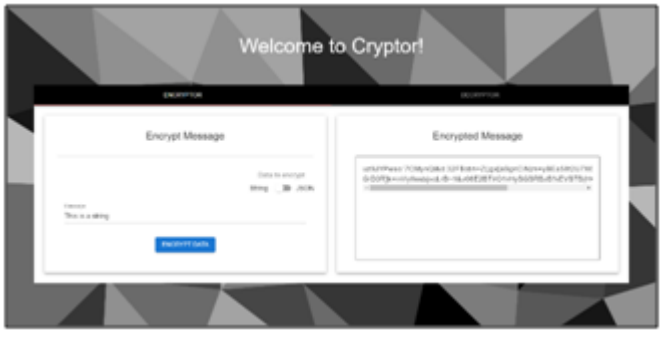

Figure 11: Encryption of String

Figure 12: Decryption of String

Figure 13: Encryption of JSON Object

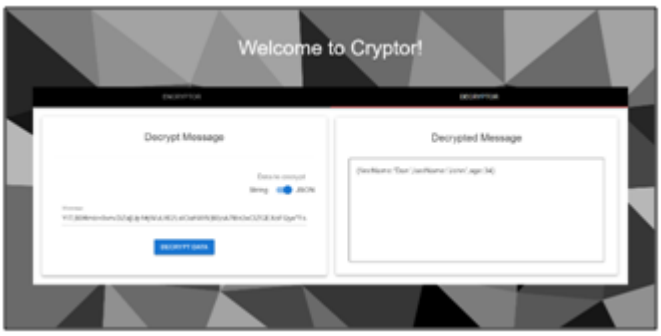

Figure 14: Decryption of JSON Object

4. Conclusion

Authentication, integrity, secrecy, and no - repudiation are all major security goals that cryptography helps to achieve. To accomplish these objectives, cryptographic algorithms are created. The objective of cryptography is to provide dependable, strong, and robust network and data security. To secure confidential data from one party to another, cryptography plays its part by converting plain text into incomprehensible reading language. There is a necessity to share a variety of private data via the internet. The original message, i. e., plain text, is protected from unwanted access via cryptography by changing it to an unreadable format using a simple, yet difficult to decipher, mathematical principle. This study introduces a secure Cryptography technique that is very basic in nature with maximum integrity. Furthermore, the suggested technique for the Encryption and Decryption Process is simple to implement in a real - world project.

References

[1] Batool, Sabiha. (2020). Information Security using Cryptographic Techniques.

[2] 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)
[3] Tushar, Aniket Sharma, Ankit Mishra, 2021, Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 03 (March 2021)
[4] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography.1 - 6.10.1109/ISDFS.2019.8757514.
[5] Gupta and N. K. Walia, "Cryptography Algorithms: A Review, " NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol.2, no.2, pp.1667 - 1672, 2014.
[6] 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