Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **S-6 Year 2023** Page **978:983***

A New Hybrid Diffie-Hellman and Caesar Cipher Algorithm for Cryptography

Manoj Sharma V[1], Manthan N R[2], Lalith Kumar Nitesh Kumar Mehtha[3] , Krishnapuram Kalyan Kumar Reddy[4], Shaik Hussain Shaik Ibrahim[5]

[1,2,3,4,5]*Computer Science and Engineering, REVA University Bangalore.*
Email: R18CS218@cit.reva.edu.in[1] , R18CS219@cit.reva.edu.in[2] , R18CS200cit.reva.edu.in[3] , R18CS191@cit.reva.edu.in[4] , shaikhussain2207@gmail.com[5]

**Corresponding author's E-mail: R18CS218@cit.reva.edu.in*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 30 Nov 2023

Abstract

Caesar cipher algorithm is one of the ancient algorithms. However, due to advances in technology the algorithm is now much simple to breach. This is because; each letter in the message is replaced by the same letter as specified. To raise the safety, some changes can be made. So, here we are going to use another arithmetic algorithm Diffie - Hellman's mode of changing the key to find the secret key and use simple calculations to verify data encryption. After obtaining a private shared key using the Diffie-Hellman method, depending on the operating mode with 26 keys to get the value of 26 or less, then the current character is taken with the key when the additional value of the new character. In any letter in the position of an 'x', the key first increases with an 'x' and is adjusted to get the encrypted letter. Therefore, 2 messages are repeated 2 times and the third letter has 3. This increases safety. This technology can be used to securely transfer sensitive information from one person to another.

Keywords: *Diffie-Hellman, cryptography, encryption, Caesar Cipher, secret key*

1. Introduction

Data safety is important aspects of human life. No one can communicate safely. Leak information is always possible. This helps make data safer. There are two types of cryptographic methods: symmetric and public. Symmetric is a method of applying the same key. Public key cryptography is a method in which only one key is used in the encryption process and another special key is used in the encryption process. As with both encryptions only one key is used for the decryption purpose. However, since such cryptography is the most important feature of science, it is not important to the outside world at any cost. For example, a shift of 2 means A, which is then replaced by C, B and B. The sender can encrypt the data using this key and the recipient can decrypt it by using the same key. The below is made using 5 keys.

Table 1: Encryption

Plain text	Cipher text
I love my life.	N qtaj rd qnkj

As you can see from above example, the plain text is simply shifted by 5 alphabets. In order to decrypt the above cipher text we simply should shift 5 alphabets backward.

Table 2: Decryption

Cipher text	Plain text
Thjfs nx gqzj	Ocean is blue.

Diffie-Hellman is a method of creating shared privacy between the two persons , thus the secret cannot be seen . This is very useful because you can use this method to create an encryption key with someone else, and then start encrypting your traffic with the same key. Even if the traffic is recorded and analyzed later, there is no way to know what the key is, even if the exchanges that do it appear. It is not asymmetric cryptography.

Literature Survey

This paper expands the domestic table with numerical knowledge, so this number system can be used. It combines Vigenere's coding and modified Caesar cipher technique to retrieve cipher text from a given plain text and key [1].

Encryption is the conversion of plain text or plain text into hidden text (cipher text), usually the Beributuk code [2]. Encryption of text data Step and result with this method WAKE encrypts back in Caesar cipher technology, thus protecting encrypted data [4].

This encryption technology adopts a combination of Caesar cipher and XOR encryption and is programmed using C ++ [6].

Subsequently, some possible scenarios were tested to verify the strength of the security program, suggesting an improvement in the security of the data transmission over the wireless medium without affecting the processing time [7].

III. Problem Definition

Now-a-days there is issues in cyber security where there are number of data breaches taking place, this can be overcome by our process in which we use hybrid of Caesar Cipher and Diffie-Hellman algorithm.

To streamline this process, we aim to develop an algorithm that can simulate this workflow by allowing the motivation that systems use mathematical operations that are hard to reverse

This algorithm allows the process to be completed in less time compared to AES and DES algorithms and more secure than existing Caesar Cipher.

IV. Proposed Algorithm

In the first part of the proposed algorithm a public key exchange takes place between the two users. This exchange is slightly different Diffie-Hellman method. The algorithm is shown below.

A. Algorithm 1: Diffie-Hellman

Step1: Start

Step2: Select two different independent keys A and B

Step3: Now select the shared private key A and B

Step4: Now send a duplicate secret key shared from A to B and vice versa from B to A

Step5: Multiply the value obtained by the secret key to get the key called the shared crypto key, let this number be called 'x'

Step6: Stop

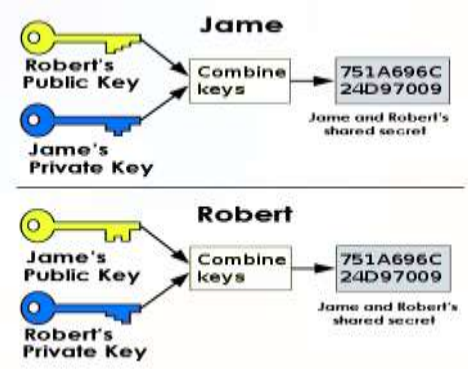

Fig 1: Encryption and Decryption of Diffie-Hellman technique

To make a Diffie-Hellman, the last two users are Jame and Robert, they communicate in the same channel, knowing that they are private, receiving whole numbers corresponding to P and Q, i.e. P is the first number and Q is producers of p. Generator q is a multiplied number of whole numbers less than p, which does not give the same result of two whole numbers. The value of P can be but the value of q is small

B. Algorithm 2: Caesar Cipher

Step1: Start

Step2: The Exchange key takes place and a shared crypto key 'x' is available

Step3: For the first letter change in z mod 26, save k = x mod 26

Step4: Now with the second letter onwards repeat the next to the end if the character is a space replaced by kth letter alphabet one store z = x / k then get m = x + z and save k = m mod 26 and convert the character by k

Step5: Stop

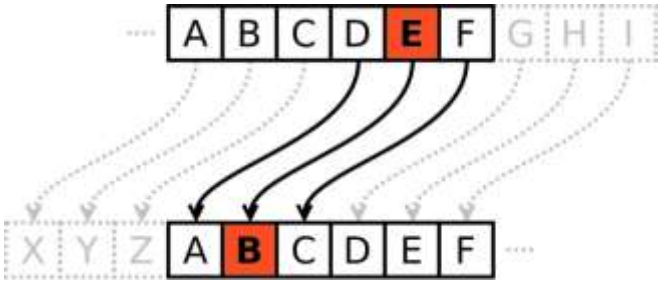

Fig 2: Encryption and Decryption of Caesar Cipher technique

In order to encrypt a given text, we must provide the full value as input, which shifts those multiple numbers of positions. So this encryption can now be represented by a modular arithmetic by first converting the letters into numbers in order.

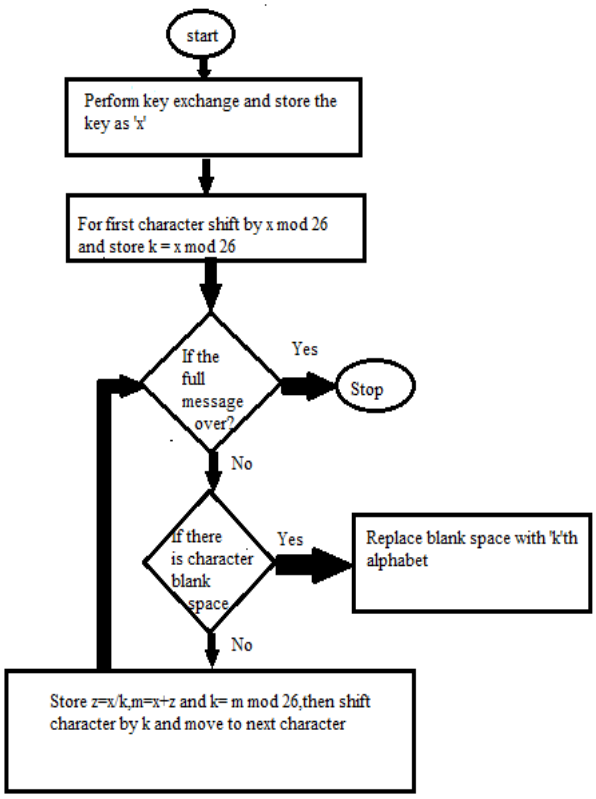

Fig 3: Proposed system flowchart

3. Results and Discussion

In order to find out how efficient the proposed algorithm is? Let us take the example of two of the most secure cryptographic algorithms in use which are AES and DES algorithms.

Table 3: For Encryption

File size	AES	DES	Proposed
10kb	1.794 seconds	2.165 seconds	0.501 seconds

Table 4: For Decryption

File size	AES	DES	Proposed
10kb	1.998 seconds	2.215 seconds	0.564 seconds

From the table III, the time taken for the execution of file by encryption technique for AES, DES, and Proposed algorithm is 1.794seconds, 2.165 seconds, 0.501 seconds respectively

From the table IV, the time taken for the execution of file by decryption technique for AES, DES, and Proposed algorithm is 1.998 seconds, 2.215 seconds, 0.564 seconds respectively

As you can see our proposed algorithms takes far less time compared to those secure algorithms. As security is not the only criteria an algorithm can be assessed, the proposed algorithm might not be more secure than AES and DES algorithms, but it certainly is faster than those two algorithms.

We are generating a private key using two public keys from two users, then that generated private key is used for encryption or decryption technique, It is shown in below figure.4

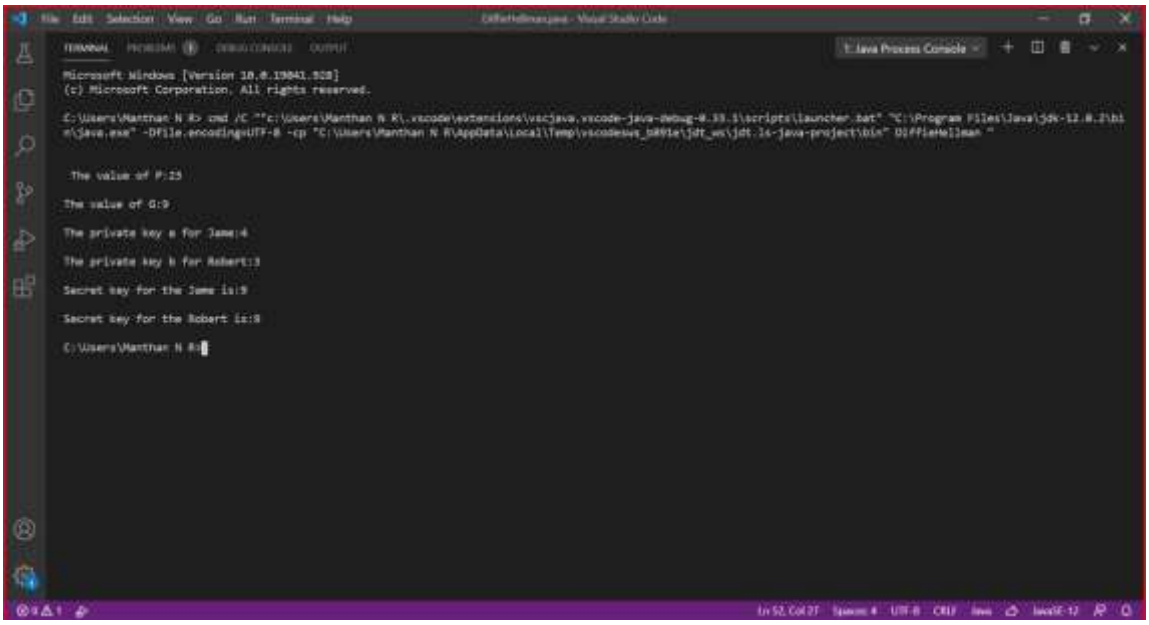

Fig 4: Execution of Diffie-Hellman algorithm

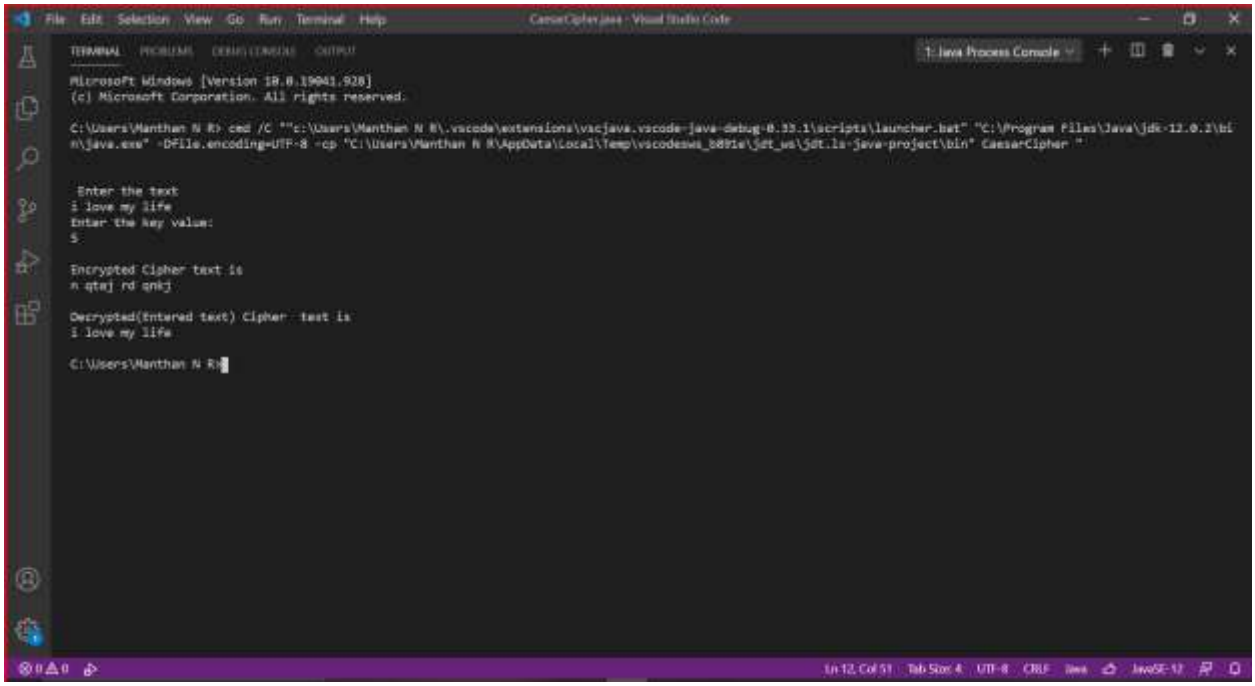

Fig 5: Execution of Caesar Cipher algorithm as mentioned in table 1

From Fig.5, the entered text “I love my life” is converted in to encrypted cipher text as “n qtaj rd qnkj” with a key value of 5, we can get back our original text by decryption

From Fig.6, the entered text “Ocean is blue” is converted in to encrypted cipher text as “thjfs nx gqzj” with a key value of 5, we can get back our original text by decryption

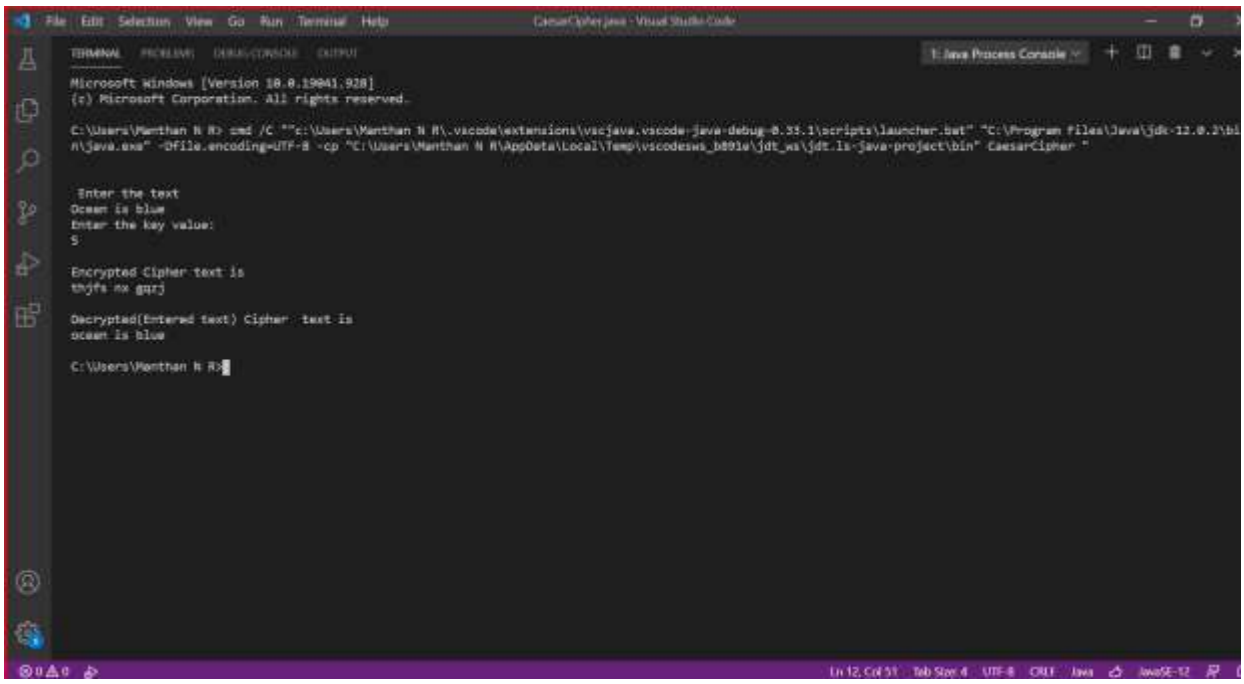

Fig 6: Execution of Caesar Cipher algorithm as mentioned in table 2

4. Conclusion

This algorithm is considered effective if there are sufficient guarantees to protect certain data. When there is no difference in security, execution time is important because it should not take much time to execute a particular algorithm. The given algorithm delivers results much faster than modern cryptographic methods such as AES, DES and DFS algorithms, which are widely used in NASA, FBI and ISRO. Characters such as spaces are also hidden. It abbreviates Caesar cipher algorithm, which ensures quick encryption and provides additional security.

Acknowledgement

The authors are very much grateful to the reviewers’ highly valuable comments and suggestions that improved the manuscript

References:

[1] Y. He, G. Wang, W. Li and Y. Ren, "Improved Cube Attacks on Some Authenticated Encryption Ciphers and Stream Ciphers in the Internet of Things," in IEEE Access, vol. 8, pp. 20920-20930, 2020, doi: 10.1109/ACCESS.2020.2967070.

[2] K. Singh, R. Johari, K. Singh and H. Tyagi, "Mercurial Cipher: A New Cipher Technique and Comparative Analysis with Classical Cipher Techniques," 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2019, pp. 223-228, doi: 10.1109/ICCCIS48478.2019.8974473.

[3] 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, 2018, pp. 1-9, doi: 10.1109/ICOEI.2018.8553910.

[4] M. D. Sinaga, N. S. B. Sembiring, F. Tambunan and C. J. M. Sianturi, "Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, pp. 1-5, doi: 10.1109/CITSM.2018.8674346.

[5] F. Farahmand, W. Diehl, A. Abdulgadir, J. Kaps and K. Gaj, "Improved Lightweight Implementations of CAESAR Authenticated Ciphers," 2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), Boulder, CO, 2018, pp. 29-36, doi: 10.1109/FCCM.2018.00014.

[6] M. D. Sinaga, N. S. B. Sembiring, F. Tambunan and C. J. M. Sianturi, "Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security," 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018, pp. 1-5, doi: 10.1109/CITSM.2018.8674346.

[7] Abbas, H. Mostafa and A. N. Mohieldin, "Low Area and Low Power Implementation for CAESAR Authenticated Ciphers," 2018 New Generation of CAS (NGCAS), 2018, pp. 49-52, doi: 10.1109/NGCAS.2018.8572255.