IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 1, May 2022

Encryption and Decryption of Text

Mr. Vishal Kumar, Mr. Vikash Kumar, Ms. Bhanu Bhardwaj
Assistant Professor, Department of Computer Science and Engineering
Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh, India

Abstract: *One of the most effective ways to protect the privacy and security of data is by implementing encryption. This method uses a key known as a decryption process to hide the original content of the data. The objective of this method is to prevent unauthorized access to the data. This method is very simple and can be easily implemented. It takes 8 bit code value of the alphabet and performs some simple calculation such as logical not and simple binary division.*

Keywords: Encryption and Decryption.

I. Introduction

Data security has become most important aspect while transmission of data and storage. The transmission and exchange of image also needs a high security. Cryptography is the art of secret writing. Cryptography is used to maintain security. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Figure 1 shows the information transmitting between sender and receiver. Figure 2 shows the creation of interrupts between sender and receiver. Figure 3 shows the changes, theft or delete information between sender and receiver.

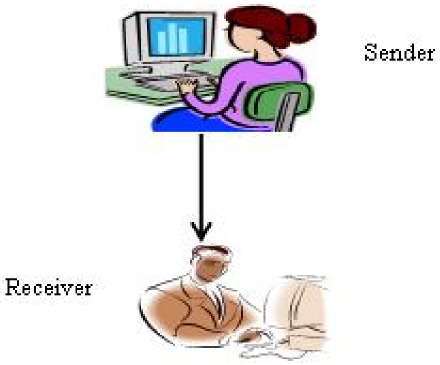

Figure 1: Information Sender and Receiver

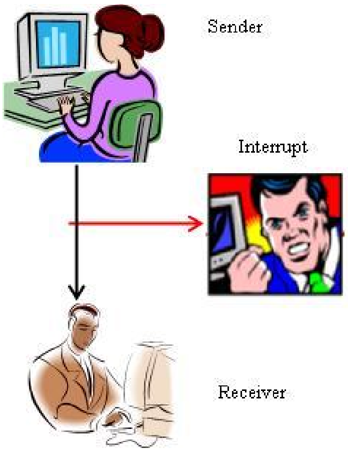

Figure 2: Creating Interrupts between Sender and Receiver

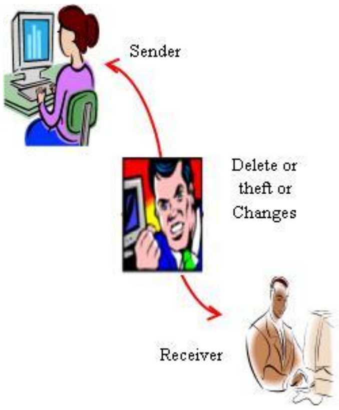

Figure 3: Changes, Theft or Delete Information between Sender and Receiver

II. Symmetric Approach

Symmetric technique has emphasized on improving conventional method of encryption by using substitution cipher. Substitution techniques have used alphabet for cipher text. In this symmetric algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. A single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. She represents various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained.

2.1 Symmetric Key Cryptographic Algorithm

A. Encryption Algorithm

Step 1: Generate the ASCII value of the letter

Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]

Step 3: Reverse the 8 digit's binary number

Step 4: Take a 4 digits divisor (>=1000) as the Key

Step 5: Divide the reversed number with the divisor

Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s(zeros) in the left hand side. So, this would be the cipher text I.e. encrypted text

B. Decryption Algorithm

Step 1: Multiply last 5 digits of the cipher text by the Key

Step 2: Add first 3 digits of the cipher text with the result produced in the previous step.

Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number

Step 4: Reverse the number to get the original text i.e. the plain text

III. Proposed Approach

A. Encryption Process

Step 1: Use ASCII 8 bit value letters.

Step 2: Inverse the odd position bits of the 8 bit element.

Step 3: Interchange bit for consecutive position

Step 4: Divide 8 bits into two part first four digits as element-1 and last four digits as element-2.

Step 5: Use 100 as key and divide and element-1 and element-2.

Step 6: Get the quotient-1, remainder-1 and quotient-2, remainder-2.

Step 7: quotient-1, remainder-2, quotient-2, and remainder-1

Step 8: Merge to get the 8 bit cipher text.

B. Decryption Process

Step 1: Take the cipher text mark (right to left) first two bit as quotient-, next two bit as remainder-2, now next two quotient-2 and last two bit remainder-1.

Step 2: Multiply the quotient-1 with the key and then add the result with remainder-1 to get element-1. Similarly multiply the quotient-2 with the key and then add the result with remainder-2 to get element-2.

Step 3: Merge element-1 and element-2

Step 4: Interchange bit for consecutive position

Step 5: Inverse the odd position bits of the 8 bit element. And this will be our plain text which was encrypted

DOI: 10.48175/IJARSCT-3546

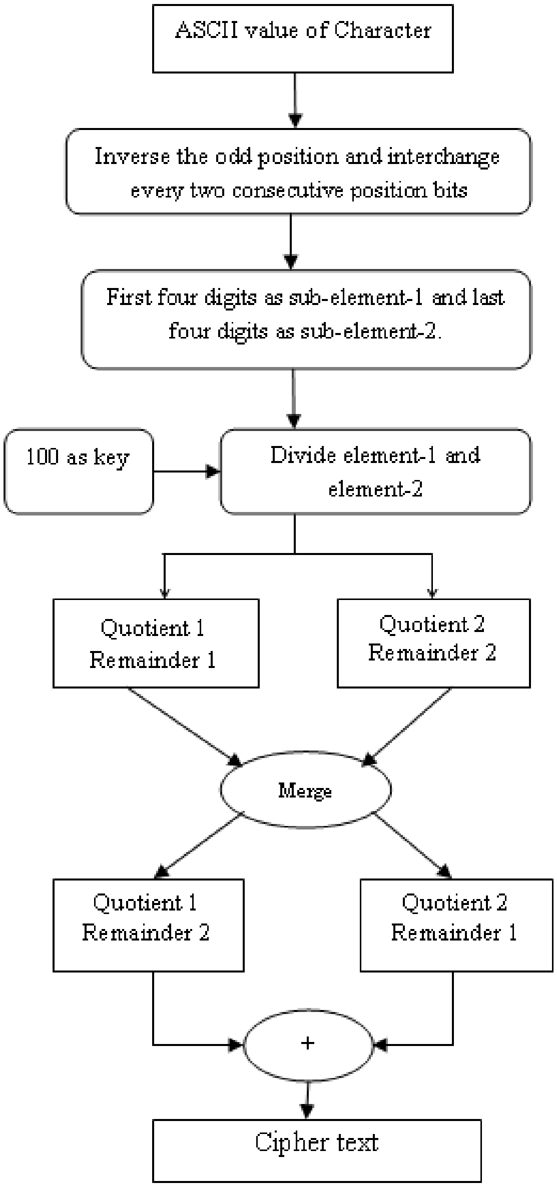
ASCII value of Character
Inverse the odd position and interchange every two consecutive position bits
First four digits as sub-element-1 and last four digits as sub-element-2.
100 as key
Divide element-1 and element-2
Quotient 1 Remainder 1
Quotient 2 Remainder 2
Merge
Quotient 1 Remainder 2
Quotient 2 Remainder 1
+
Cipher text

Figure: The architecture and flow of proposed algorithm.

IV. Experimental Analysis

For experimental analysis, proposed algorithm with symmetric key algorithm has been implemented and compare with some parameter like key size, message size encryption, decryption time. The i3 pre-processor (2.5GHz Intel Processor with 4M cache memory) and 2GB main memory with Windows7 OS have been used. The algorithms are implemented in using C# Dot net frame work version 10. The simple text message including text only is used. Figure shows the encryption algorithm of the proposed method as sender screen. Decryption algorithm of the proposed technique as receiver screen. Time required for execution on file

Approach	Key Size (in bytes)
Symmetric Approach	64
Proposed Approach	48

V. CONCLUSION

The proposed method is used for message communication. Short message can be send securely using encryption techniques. The proposed approach is based on number of characters in message and simple calculation and operations are performed to minimize the execution time. In future this work for special characters will be implemented.

REFERENCES

[1]. William "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.

[2]. Schneier B, "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

[3]. Abhishek Joshi a, Mohammad Wazid b, R. H. Goudarc"An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks" Available online at www.sciencedirect.comInternational Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India Available: http://www.sciencedirect.com/science/article/pii/S1877050915007036

[4]. Ashraf Odeh, ShadiR.Masadeh, Ahmad Azzazi "A Performance Evaluation Of Common Encryption Techniques With Secure Watermark System (SWS)"International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3,May 2015. Available: http://airccse.org /journal/nsa/7315nsa03.pdf

[5]. Sushil Kumar Tripathi "An Efficient Block Cipher Encryption Technique Based OnCubical Method and Improved Key" Imperial Journal of Interdisciplinary Research (IJIR)Vol- 2, Issue-6, 2016ISSN: 2454-1362, Available: http://www. Imp eria ljournals.com/index.php/IJIR/article/view/836

[6]. Sanidhya U, Shrikanth N.G "An Efficient Encryption And Searching Technique For Cloud Using Rijndael Algorithm" International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 3 (MayJune, 2016), PP. 262-267 Available: http://www.ijtra.com/ abstract.php?id=an-efficient-encryption-and-searching-technique for-cloud-using-rijndael-algorithm

DOI: 10.48175/IJARSCT-3546