IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 14, Issue 4, Ser. I (Jul.-Aug. 2019), PP 17-20
www.iosrjournals.org

Double Encrypted Secure Data Communication Using DES and Ceaser Cipher Technique

Chithra. V [1], Anusree K.P[2], Anjana V Chandran[3], Akhila C P[4] ,Hyfah M [5]

[1] *(Assistant Professor, Department of ECE, Institute of Engineering and Technology University of Calicut, India)*
[2,3,4,5]*(B.Tech student, Department of ECE, Institute of Engineering and Technology University of Calicut, India)*

Abstract: *We are living in the new era of information. We need to keep information about every aspect of life and that information need to be secured from attacks. To be secured, information needs to be hidden from unauthorized access i.e. confidentiality and protected from unauthorized change i.e. integrity and also available to an authorized entity when it is needed i.e. availability. Information is now distributed but these three requirements have not changed. Cryptography is the technique which is can ensure for secure transmission of the data. Cryptography's main advantage is that the information is somehow distorted, scrambled by the sender, an encryption key is known only by the intended receiver who decrypts the message. Here Data Encryption Standard (DES) Algorithm and Caesar Cipher algorithm are used to enhance data security.64 bit message and 64 bit key is given to DES, after encryption the encrypted message is given to Caesar block. Here the encrypted data is again encrypted and in the receiver section the data is first decrypted using Caesar Cipher method and then decrypted using DES decryption algorithm which gives the original data. Same set of key is used for both DES and Caesar.*

Date of Submission: 03-07-2019 Date of acceptance: 18-07-2019

I. Introduction

Data communication is an important aspect of our living. So, protection of data from the unauthorized access and misuse is essential. The need of security is to ensure that our information remains confidential and only authorized users can access it, and ensuring that no unauthorized user has changed our information, so that it provides full accuracy and efficiency.

Cryptography defines a pair of data transformations called encryption and decryption. Encryption is the process of converting the message or plain text into meaningless word with the help of algorithm and keys. Based on the number of keys used encryption is classified into two i.e. symmetric and asymmetric encryption. In symmetric key cryptography same key is used for both encryption and decryption and in the case of asymmetric key encryption different keys are used for encryption and decryption. This conversion of data into a non-readable form at transmission section and convert that data in readable form again at the reception end helps to provide security to the data. This method of providing the ability to read data only to authorized person by creating non readable data or cipher text is called Cryptography. It is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. In Cryptography, Caesar cipher and DES are the most widely known encryption decryption algorithms. Another classical encryption method is Caesar cipher which is a type of substitution cipher in which each letter in the plaintext is replaced by a letter that is fixed number of positions down the alphabet. The Data Encryption Standard (DES) is a symmetric-key block cipher method which contains 16 rounds of operations in both encryption and decryption.

As data is transmitted through the internet or other media type every second, it's important to search for the best solution to offer the protection to data against the along with it providing the services up to date is one of the most active subjects in the security related communities. The data cannot be modified by any external user or intruder .So here double encryption and decryption is doing that is the data encrypted by using DES algorithm is again encrypted and decrypted by using Caesar cipher algorithm and the original data will get by using DES decryption algorithm. By combining both DES and Caesar cipher algorithms, it provide more and more secured data transmission.

II. Related Works

A. *Advance Encryption and Decryption Technique using Multiple Symmetric Algorithm*

Here a new algorithm is proposed for encrypting the plain text message into cipher text. This algorithm combine different symmetric algorithm into one algorithm with little change in those algorithm. The entire traditional algorithm is very week and cryptanalysis easily cracked the cipher text and converts that cipher text into the plain text. In this algorithm, a new substitution technique i.e. Hill Cipher & Caesar Cipher are combine with the transposition technique i.e. Rail fence technique. This is used to make more secure and stronger algorithm. The proposed algorithm is divided into three Phases. First the plain text is Encrypted using Substitution technique i.e. Caesar Cipher after that substitution technique i.e. Hill cipher is used. Next the Transposition Technique i.e. Rail Fence technique is applied in the Second encrypted text and the cipher text is generated, At the Receiver side if the receiver uses appropriate key they will convert the cipher text into the plain text.

The proposed system is depending on the multiple substitution cipher and the Transposition technique whose substitution transposition key depends on the string length, which makes the key dynamic and variable for each string. Hill cipher makes the message more secure and unbreakable. Using hill cipher makes the information unstructured. It's difficult to decrypt the encrypted message using traditional crypto-analysis tools. The brute force attack also fails in this technique.

B. *Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security*

Security of data or documents is a very important thing. Given that nowadays many exchange data electronically. It will result in a lot of processes that can compromise the security of data. Therefore, we need a way to be able to secure the important data that are not easily obtained by others who are not interested. One of the main that we can secure is the data in the form of text. The knowledge that can keep a message or data Cryptography is the science. This proposed method combining WAKE and binary Caesar cipher cryptographic method for the better data security. Mechanisms to improve security are to use encryption technology. Encryption is the conversion of an original text or plain text into the hidden text (cipher text) that usually berbetuk codes. And vice versa if the data is hidden the wish to be returned must decrypt it first. The step is to encrypt text data with the method and the result is encrypted WAKE back to Caesar Cipher method, so that the data to be kept secret remains safe.

WAKE method uses a 128 bit key and a table 256 x 32 bits. In the algorithm, this method uses the XOR, AND, OR, and Shift Right operation. In the process, this method has a simple and quick process to produce cipher text keys that have played as many rounds in XOR with the plaintext and the key to produce the plaintext of n rounds played in XOR with the cipher text that was generated at the time of encryption. And the simplest possible substitution cipher is the Caesar cipher, reportedly used by Julius Caesar during the Gallic Wars. Each letter in the plaintext is replaced by a letter shifted a fixed number of places to the right (Automatic Key Generation of Caesar Cipher). WAKE algorithm can be combined with the Caesar Cipher to increase the level of data security.

C. *An Enhancement of Data Encryption Standards Algorithm (DES)*

The Data Encryption Standard (DES) algorithm has been considered as the most popular symmetric key, blocks ciphering cryptographic. Even though the DES algorithm had still been used in some applications, it was considered unsafe because of the short key length (64 Bits), besides, the Brute force attack has shown that the DES practically can be attacked. In January 1999, the DES key was cracked in only (22 hours) and (15 minutes). The aim of this research is to improve the DES algorithm by increasing the key length (1024 bits) that is to be divided into 16 keys (64 bits each), each key is independently generated for the different algorithm cycles. The results of the proposed algorithm were much better than the old algorithm for detecting the encryption key or the total number of keys that could be generated by following Blind search method (try all possible keys), Increasing the key length (degree of complexity) makes it difficult to search in a vast space of numbers and attempts. The Java Virtual Machine (JVM) environment: (TextPad), and the results are much better than the old algorithm for detecting the encryption key or the total number of keys that can be generated by blind search (all possible keys) as increasing the key length (complexity). The basic idea of the proposed improvement is the disconnection between the sub keys and to find sixteen keys independent of each other.

III. Materials and Methods

This proposed system uses double encryption algorithm for enhancing data security. Cryptographic techniques are done by using DES (Data Encryption Standard) and Caesar Cipher algorithm. The DES is a block cipher i.e. a cryptographic key and algorithm are applied to a block of data simultaneously instead of one bit at a time. To encrypt a message, first DES is grouped into 64-bit blocks. With the help of permutation and substitution each block is then enciphered using the secret key into a 64-bit cipher text. It has 16 rounds and which runs in four different modes, which encrypt blocks individually or makes each cipher block dependent on all the previous blocks. In decryption the inverse of encryption is done, following the same steps but the order in which the keys applied is reversed. Most basic attack is brute force, where each key is tried until you find the right one. The length of the key will determines the number of possible keys and the feasibility of this type of attack. DES uses a 64-bit key; out of it eight bits are used for parity checks, which will limit the key to 56-bits. Hence, it will take a maximum of 2^56 i.e. 72,057,594,037,927,936, attempts to find the right key.

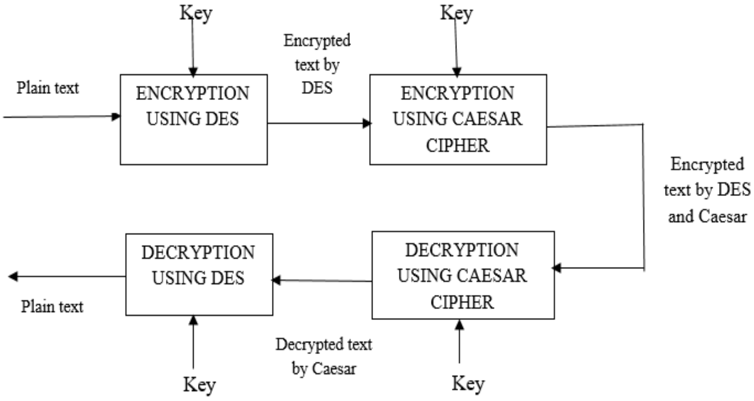


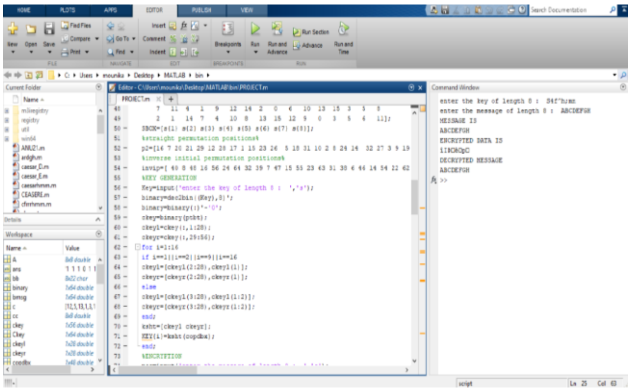
Figure 1: Block diagram of Double encryption

DES encryption is followed by Caesar cipher cryptographic technique. The Caesar cipher is based on transposition and involves shifting each letter of the plain text message by a certain number of letters, historically three. The cipher text can be decrypted by applying the same number of shifts in the opposite direction. This type of encryption is known as a substitution cipher, due to the substitution of one letter for another in a consistent fashion.This proposed system increases data security by combining both DES and Caesar cipher algorithms along with the input plain text message. By using this double encryption technique it is more difficult to crypt-analyse and brute force attack is not possible.

IV. Results

Data security is enhanced here with the help of double encryption. First encryption method used here is DES which can encrypt 64 bit binary data at a time. It is a powerful Cryptographic algorithm. Even though the output of DES itself provides data security the second method i.e. Caesar Cipher will provide more confusion, which helps to enhance security. For proper working of DES Algorithm inputs message and key should be of 64 bit length. Here input is given as string, it can be alphanumeric or symbols. 8 letters can be given whose binary will be 64 in bit length

.

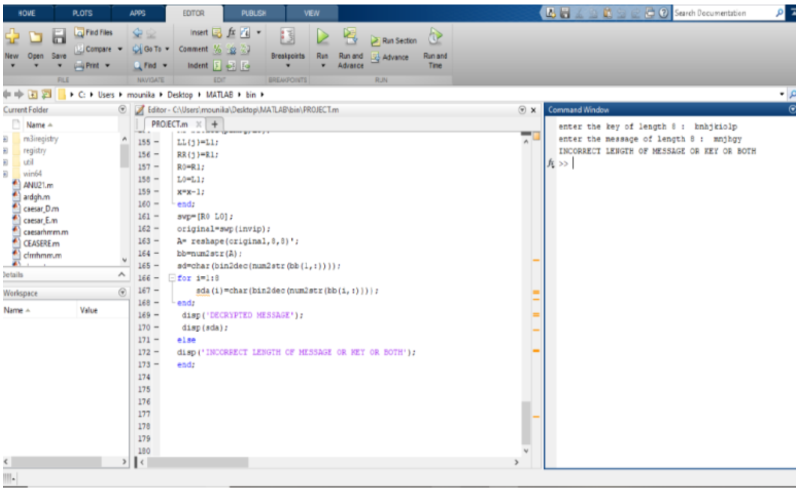


```
        7   11   4   1   9   12  14  2   0   6   10  13  15  3   5   8
        2   1   14   7   4   10  8   13  15  12  9   0   3   5   6   11];
    SBOX=[s(1) s(2) s(3) s(4) s(5) s(6) s(7) s(8)];
    %straight permutation positions%
    p2=[16 7 20 21 29 12 28 17 1 15 23 26  5 18 31 10 2 8 24 14  32 27 3 9 19
    %inverse initial permutation positions%
    invip=[ 40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62
    %KEY GENERATION
    Key=input('enter the key of length 8 :  ','s');
    binary=dec2bin((Key),8)';
    binary=binary(:)'-'0';
    ckey=binary(pcbt);
    ckeyl=ckey(:,1:28);
    ckeyr=ckey(:,29:56);
  for i=1:16
    if i==1||i==2||i==9||i==16
    ckeyl=[ckeyl(2:28),ckeyl(1)];
    ckeyr=[ckeyr(2:28),ckeyr(1)];
    else
    ckeyl=[ckeyl(3:28),ckeyl(1:2)];
    ckeyr=[ckeyr(3:28),ckeyr(1:2)];
    end;
    ksht=[ckeyl ckeyr];
    KEY(i)=ksht(copdbx);
    end;
    %ENCRIPTION
```

```
enter the key of length 8 :  S4f^h;mn
enter the message of length 8 :  ABCDEFGH
MESSAGE IS
ABCDEFGH
ENCRYPTED DATA IS
iIBCèCpC
DECRYPTED MESSAGE
ABCDEFGH
>>
```

Figure 2: Encrypted output with correct number of bits

There are two different cases i.e. with 8 letter as input (both message and key) and input letters (message or key or both) with any length other than 8. Case 1: In figure 2 shows the first case Message is “ABCDEFGH” and the key given here is “S4f^h;mn” and the output obtained here is the decrypted message i.e. “ABCDEFGH”. Case 2: In Figure 3shows the second case. Here the message is “mnjhgy” and the key is “bnhjkiolp” both are not 8 in length so the output obtained is “INCORRECT LENGTH OF MESSAGE OR KEY



```
    LL(j)=L1;
    RR(j)=R1;
    R0=R1;
    L0=L1;
    x=x-1;
  end;
  swp=[R0 L0];
  original=swp(invip);
  A= reshape(original,8,8)';
  bb=num2str(A);
  sd=char(bin2dec(num2str(bb(1,:))));
  for i=1:8
      sda(i)=char(bin2dec(num2str(bb(i,:))));
  end;
   disp('DECRYPTED MESSAGE');
   disp(sda);
  else
  disp('INCORRECT LENGTH OF MESSAGE OR KEY OR BOTH');
  end;
```

```
enter the key of length 8 :  bnhjkiolp
enter the message of length 8 :  mnjhgy
INCORRECT LENGTH OF MESSAGE OR KEY OR BOTH
>>
```

Figure 3: Encrypted output with incorrect number of bits

V. Conclusion

In this automated world the information resources are automated which increases cryptography and will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security is achieved by using Cryptography technique. Both DES and Caesar cipher are cryptographic algorithms used here for enhancing data security in the communication system.

DES algorithm is used for the cryptographic process. So in order to make it applicable it is important to augment this algorithm by adding new levels of security. By adding keys, S-Box design, function implementation and executing XOR operation as proposed by this to give more robustness to data security and it will make it stronger against all kind of intruding. DES Encryption with keys already will increase the efficiency of cryptography. And Caesar cipher being one of the simplest and widely used encryption techniques can be fortified beyond what common Caesar cipher algorithm can achieve. Different methods are used for Security purpose based on the Caesar cipher algorithms. By combining both the cryptographic algorithms will prevent brute force attacks and improve efficiency of data communication.

The data must me secured more and more during the transmission in any fields including banking .So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. In the future work we can use various types of keys in one method also we can add more algorithms to enhance the security. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against all type of intruding. In the future work we can use various types of keys in one method also we can add more algorithms to enhance the security. Along with the modification in DES, we can also use improved Caesar cipher algorithm for providing maximum security during the data transmission.

References

[1] ShariquaIzhar, AnchalKaushal, Ramsha Fatima, Mohammed A Qadeer-"Enhancement in Data Security using Cryptography and Compression"- 2017 7th International Conference on Communication Systems and Network Technologies

[2] Taranpreet Singh Ruprah-"Advance Encryption and Decryption Technique using Multiple Symmetric Algorithm",Computer Science & Engineering Department Anna SahebDange College of Engineering & Technology ,Ashta-Sangli, India,ruprahtaran@gmail.com

[3] Mikha Dayan Sinaga, Nita Sari Br Sembiring, FrintoTambunan, Charles JhonyManthoSianturi -"Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security",Faculty of Engineering and Computer Science,UniversitasPotensiUtama ,Jl. K.L. YosSudarso Km. 6,5 No. 3A – Medan, 20241, Indonesia

[4] Jawahar Thakur1, NageshKumar2-"DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459, Volume 1, Issue 2, December 2011

[5] Vishwa Gupta, Gajendra Singh and Ravindra Gupta-"Advanced Cryptography Algorithm for Improving Data Security",International Journal of Advanced Research in ComputerScience and Software Engineering, vol. 2, January 2012.

[6] Davida, George I., and YvoDesmedt,-"Cryptography based data security",Advances in Computers 30 (1990): 171-222.

[7] Huang, Scott C H., David Mac Callum, and Ding-Zhu -"Network security",Springer Science & Business Media,2010.

[8] Saleh Saraireh -"A Secure Data Communication System using Cryptography and Steganography", International Journal of Computer Networks and Communications, vol. 5, May 2013.

[9] Robling Denning, Dorothy Elizabeth-"Cryptography and datasecurity", Addison-Wesley Longman Publishing Co., Inc., 1982.Carle E. Landwehr, "Security Issues in Networks with InternetAccess", Member, IEEE.