ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18395-18398

Enhancing the Security of Data Using DES Algorithm along with Substitution Technique

Yashwant kumar[1], Rajat joshi[2], Tameshwar mandavi[3], Simran bharti[4], Miss Roshni Rathour[5]

[1]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492 001
yashwantd1994@gmail.com

[1]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492 001
rajatjogi1994@gmail.com

[1]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492 001
tameshwarmandavi93@gmail.com

[1]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492 001
simranbharti53@gmail.com

[5]Miss Roshni Rathour, Assistant professor, Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
roshnimtech1991@gmail.com

Abstract:

The security is important issue of the field of networking. Security is the initial stage of authentication and the authentication is highly influencing of modern cryptography. The Data encryption standard (DES) algorithm is a symmetric key algorithm for the using of encryption of electronic data and secure of information. The DES algorithm is provided security of brute force attack. To improve the security of DES algorithm using substitution technique is added before the DES algorithm to perform its process. The substitution cipher is the method of encoding by which unit of plaintext are replaced with cipher text. If the substitution technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then substitution technique.

Keywords: Cipher text, DES algorithm, triple DES algorithm, substitution technique, Caesar cipher.

1. INTRODUCTION

In recent years, a lot of applications are internet security and Authentication based like online shopping and internet banking transaction or bill payment etc. Such a transaction or Authentication over wire or wireless networks demand end to end secure connections, that confidential, to ensure data authentication, availability , integrity, and confidentiality [1].

Encryption is one of the principle means to guarantee security of our information. Cryptography is a part of secret information and it is science and art of secure the information over the medium. The cryptography is mainly using the encryption decryption method, the process of encoding the plaintext into the cipher text is called encryption and the reverse process of decoding cipher text to plaintext is decryption [1]. The substitution technique of single letters separately simple substitution can be demonstrated writing the alphabet in some order to present the substitution. This is a term of substitution alphabets.

Simplified data encryption standard- DES is a block cipher system which transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. It is use of 16 round Feistel structure the block size of 64-bit

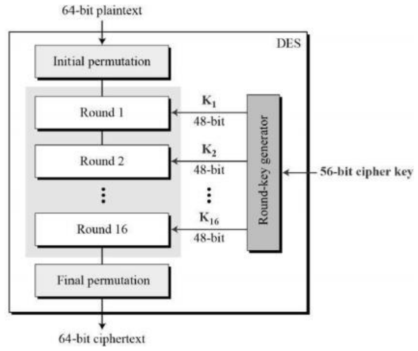


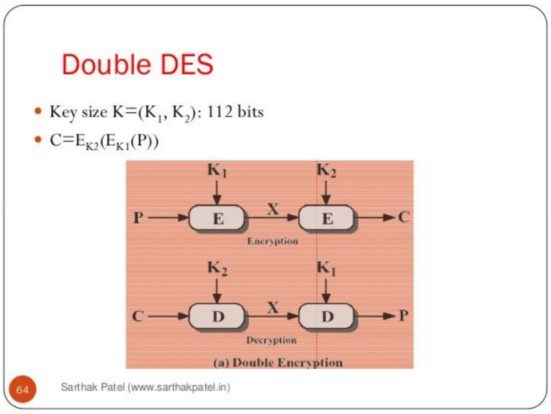
Figure 1. The conceptual working of DES algorithm.

DES is based on the two basic attributes of cryptography: Transposition (Diffusion) and Substitution (Confusion). DES algorithms consist of 16 steps each of which is called as a Round algorithm [3-4].

- The first step of initial 64-bit plain text block is handed over to the initial permutation function.

- The initial permutation is performed on the 64-bit plain text.
- The initial permutation produce to halves of permuted block: Left plain text and Right plain text.
- Now each of Left plain text (LPT) and Right plain text (RPT) goes through 16 rounds of encryption process. Each with its own keys.
    - From the 56-bit key, a different 48-bit sub-key is generated using key transformation.
    - Using the expansion permutation, the right plain text is expanded from 32-bit to 48-bit.
    - Using the S-box substitution produce the 32-bit from 48-bit input.
    - There are 32-bits are permuted using P-box permutation.
    - The result of the XORed 32-bit it becomes the Right plain text (RPT) and old RPT becomes the LPT. This process is called as swapping.
    - Now the RPT again given to the next round and performed 15 more rounds.
    - After the completion of 16 rounds the final permutation is performed.

Double DES algorithm- The Double DES algorithm is a similar to the DES algorithm but in this some process are repeated two times using to key K1 and K2. First key K1 is applied on the plain text and it is converted into the cipher text and the key K2 is applied to produce the resultant cipher text [4].



Double DES

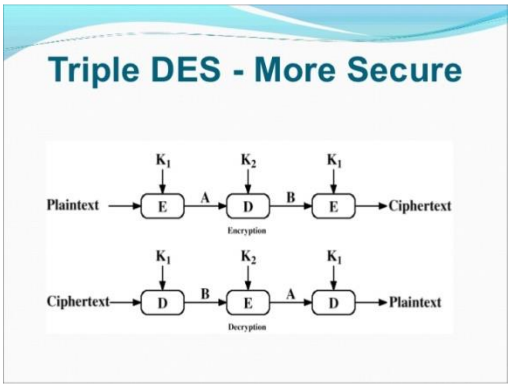
- Key size K=(K_1, K_2): 112 bits
- C=$E_{K2}(E_{K1}(P))$

64 Sarthak Patel (www.sarthakpatel.in)

Figure 2. Double DES algorithm

- DES used a 56-bit key, this raised concerns about brute force attacks.
- Ones proposed solution: Double DES
- Apply DES twice using two keys K1 and K2. This leads to a 2*56=112 bit key so it is more secure then DES algorithm [4].

Triple DES algorithm- The triple DES algorithm is using three key of DES algorithm. Which contain three different keys K1, K2 and K3. This means that the actual key has length 3*56=168 bit [4]-[5].



Triple DES - More Secure

Figure 3. Triple DES algorithm

Substitution Technique- Study of substitution technique enables us to illustrate the basic approaches of symmetric encryption used today and the type of crypt-analytic attacks must be anticipated. A substitution technique is one which the latter of plain text are replaced by other latter or by numbers or symbols [6]. If the plain text is viewed as a sequence of bits, then substitution technique involves. Substitution cipher encrypts plain text by changing the plain text one piece at a time. The Caesar cipher is an early substitution cipher. In the cipher each characters is shifted three place up. Therefore A becomes D and B becomes E and C becomes F etc. [7].

This figure 4 shows “HELLO” being encrypted with the Caesar substitution cipher [8].

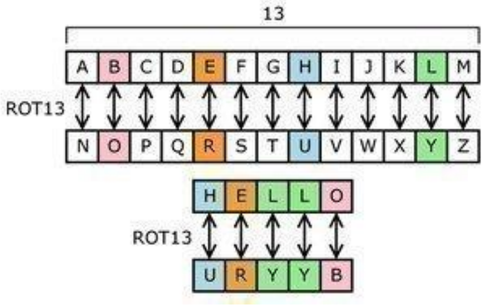


Figure 4. Caesar substitution technique

Caesar Cipher- Caesar cipher is a shift cipher, Caesar’s code or Caesar shift is one of the most widely known encryption technique.

This is the type of substitution cipher in which each latter in the plain text is replaced by a latter some fixed number of position down the alphabets [9]. To pass an encrypted message from one person to another, it is necessary that both parties have the 'key' for the cipher text, so that the sender may encrypt it and the receiver may decrypt it. For the Caesar cipher, the key is the number of characters to shift the cipher alphabet.

Example of the encryption and decryption steps involved with the Caesar cipher. The text we will encrypt is defending the east wall of the castle, with a shift (key) of 1.

Plain text: defend the east wall of the castle

Cipher text: efgfoe uif fbtu xbmm pg uif dbtumf

It is easy to see how each character in the plain text is shifted up of the alphabet. Decryption is just as easy, by using an offset of -1.

Plain text: abcdefghijklmnopqrstuvwxyz

Cipher text: bcdefghijklmnopqrstuvwxyza

Obviously, if a different key is used, the cipher text alphabet will be shifted a different amount [10].

2. LITERATURE SURVEY

Implementation of DES Using S-box – DES algorithm uses 8 different S-box, each of which Contain 64-bit values. Essentially an S-box can be thought of as a function that take 6-bit as input and produce 4-bit as output [11].

Gunjan gupta et.al: Proposed on the computer network security is a new and fast moving technology in the field of computer science. As such the technique of security it still a moving target security courses originally focused on mathematical and algorithmic aspect such as encryption and Caesar Technique [12].

Mr. Satish Dhull et.al: Work on the order of encryption decryption and authentication scheme for protection of communication. They composed a symmetric encryption decryption and authentication scheme for building secure channels for the protection of communication over insecure network. They also provide that the other method of composing encryption and authentication which include the authentication encryption method was not so much secured against Random Attackers [13].

Encryption is a process of generating secret key text from the input text using a secret key and an encryption algorithm [14].

Rajesh R Mane Proposed Hash Function –also called message digest (MD) and one way encryption , are algorithm that in some reason, use no key instead , a key fixed length has value is calculated based upon the plain text that make it not possible for both the contents and extents of the plain text to be recovered. Hash method are frequently used to present a digital fingerprint of a file inside often used to make certain that the file has not been changed by an intruder or virus. Hash functions are also frequently engaged by many operating systems to encrypt password [15].

Piya Techateerawat: work on the brute force attacks, this method defeat cryptography by trying every possible key. It expects to find the correct key approximately at half of key domain (e.g. if there is 2^n possible key, BFA will average be found correct key at 2^{n-1}). However this theory has a limitation in real world that array processor require a large amount of energy and continue operation for long period [16].

Sub-Key Set Generation: One set of eight sub key Kts_0, Kts_1…..Kts_7 are generated using the secret key K such that: Kts_n = character in column 0 through column 15 in row n of matrix M concatenated. These key are used in translation rounds. Another set of sub key s Ktp_n0, Kps_n1,Ktp_n2and Ktp_3are generated such that Ktp_n0=character of matrix M with row number n and column number 0.here each key is a character represented by the corresponding element in the matrix M. These key are used in transposition rounds [17].

Maryam Ahmed et.al Presented the Diffie-Hellman Algorithm can be described in relatively simple mathematics. The algorithm is does not encrypt data but if generated a secret key common to both the sender and the receiver [18].

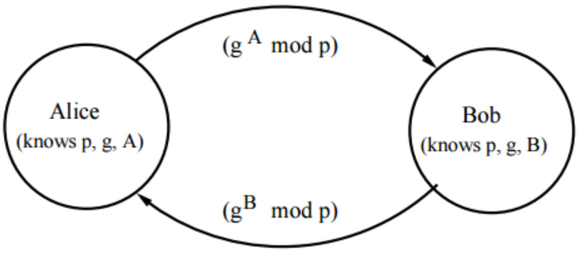


Figure 5. Diffie-Hellman algorithm

3. CONCLUSION

This paper presents a details study of the popular encryption decryption algorithm such as DES, 2DES, 3DES and substitution technique. The use of internet and network is maturation rapidly. So there are more requirements to secure data transmission over different network using different service. To provide the security to the network and data different encryption method are used. In this paper a survey on the existing work on the encryption decryption technique has been done. To sum up all the technique are useful for real time encryption. Each technique is a unique its own way. According to research done and literature survey it can found that the DES algorithm is most efficient in term of speed out through put and avalanche effect. The security provided by this algorithm can be enhanced further, if more than one algorithm is applied to data. Our future work will be explored this concept and a combination of algorithm either sequentially or parallel to setup to work secure environment for data storage and retrieval.

4. REFERENCE

[1] Gurpreet Singh, Supriya, “A Study of Encryption Algorithm (RSA, DES, 3DES and ASE) for information security”, International Journal of Computer Application, Volume 67, No-19, April 2013, Pages 33-38.

[2] Shombir Singh, Sunil K. Maaker ,Dr. Sudesh Kumar , “ Enhancing the Security of DES Algorithm Using transposition Encryption Technique ”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6,June 2013, Pages69-73.

[3] Rupali Mehta, Prof. Jitendra Agrawal, “ Enhancing the Performance of Symmetric Key Cryptography Schema”, International Journal of Engineering Innovation & research, Volume 1, Issue 3, 2012 ,Pages 296-299.

[4] Atish Jain, Ronak dedia, Abhijit patil, “ Enhancing the security of Caesar Cipher Substitution Method Using a Randomized Approach for More Secure Communication “, International Journal of Computer Application, Volume 129, No-13, Page 6-11.

[5]Bhanupriye Vyas, Amit Vajpayee, “Local Data Security Thought Encryption”, IJSART, Volume 2, Issue 8, August 2016, Pages 10-15.

[6] Cryptography and Network security [online], Available: https://meherchilakalapudi.wordpress.com/2011/09/07/cryptography-and-network-security

[7] Shobha Vasta,Tanmeya Mohan, A.k Vasta, “ Novel Cipher Technique Using Substitution Method”, International Journal of Information & Network Security, Volume 1,Issue 4 ,October 2012, Pages 313-320.

[8] Substitution and Transposition cipher [online], Available: www.tech.feq.com/substitution-and-transposition cipher.html.

[9] Mr. Vinod Saroha, Suman Mor, Anurag Dagar, “ Enhancing Security by Caesar Cipher by Double Columnar Transposition Method”, volume 2, issue 10, October 2012, Pages 86-88.

[10] Programmer Enas Ismael Imran, Programmer Farah abdulameerrabdulkareem, “ Enhancement Caesar Cipher for Battery Security”, IOSR Journal of Computer Engineering ,Volume 16,Issue 3,May-Jun 2014,Pages 01-05.

[11] Swati Kashyap, Er. Neeraj Madan, ” A Review On : Network Security and Cryptographic Algorithm”, International Journal of Advance Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015, Pages 1414-1418.

[12]Gunjan Gupta, Rama Chawla, “ Review on Encryption Cipher on Cryptography in Network Security”, International Journal of Advance Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012, Pages 211-213.

[13] Reetu, Ms. Mamta, Mr. Satish Dhull, “A Review Paper on Data Encryption and Decryption”, Imperial Journal of Interdisciplinary Research, Volume 2, Issue 8, 2016, Pages 1381-1386.

[14] Lovedeep Singh, Er. Mandeep Kaur, “Review paper on: Novel technique of Cryptography Algorithm for Improving Data Security”, Global Journal of Advanced Engineering Technologies, Volume 3, Issue 4, Pages 481-484.

[15] Rajesh R. Mane, “ A Review on Cryptography Algorithm, Attacks and Encryption tools ”, International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 9,September 2015, Pages 8509-8514.

[16] Piya Techateerawat, “ A review on Quantum Cryptography Technology”, International Transection Journal of Engineering Management & Applied science & Technologies, Volume 1, Issue 01, 2010 , Pages 035-041.

[17] Shaik Rasool, G.Sridhar, Hemnath Kumar, P. Ravi Kumar, “Enhanced Secure Algorithm for Message Communication ” , International Journal of Network Security and its Application , Volume 3,Issue 5,September 2011, Pages 33-42.

[18] Maryam Ahmed , Baharam Sanjabi, Difo Aldiaz Amirhossein Rezaei, Habeeb Omotunde, “ Diffie-Hellman and it’s Application in Security Protocol”, International Journal of Engineering Science and Innovative Technology, Volume 1, Issue 2,November 2012, Pages 69-73.