JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-2, Issue-5 E-ISSN: 2347-2693

Data Encryption Approach For Security

Richa Arya

Department of Computer Science, Maharishi Dayanand University,India

www.ijcaonline.org

Received: 14/04/2014 Revised: 01/05/ 2014 Accepted: 16/05/May 2014 Published: 31/05/2014

ABSTRACT- Whenever any new algorithm for data encryption is designed the main concern is upon the security of data. As encryption is done for encrypt data or change data in a secure form, so such encryption techniques should be used which provide the best security to the network. The main goal of any algorithm should be to secure data from any outside attack. In the recent days there are so many security issues regarding exchanging of data through a network. So data has to be encrypted in such a way that there is no threaten to secutiry. A new approach for data encryption is provided in this paper which will be helpful for security of data.

Keywords- DES, Encryption, Decryption, Asymmetric Cryptography, Symmetric Cryptography

I. INTRODUCTION

Cryptography

In cryptography,encryption at sender's side and decryption at receiver's side is done for security purpose.

Encryption

When user defined data is changed into some coded data.

Decryption

Whan coded data is converted back as user defined data.

Hashing Encryption

The first encryption method, called hashing is basically used for developing signature. With hashing an algorithm is developed to work upon the given data. For different hash messages different data is there.Since a hash is unique to a specific message, eve So if any change is in the given data that also alters hash data.

So if anybody want to make a diference between hash and cryptography the fact that can be used is that if anybody make a change in the hash data by anyhow even the data is secure because whenever any data is encrypted, that data is secured by any other code and a particular receiver only can decode that data.so there is less chance for unseure data transmission.as hash data can be altered but encrypted data is not changed so easily.Algorithms for hashing are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA)[1].

Cryptographic techniques are used to decode the data in such a way that not anybody else excapt the receiver is able to decode the data.As nobody can change the data so cryptography techniques provide great security mechanism to the user's data.Because ssecurity breaks only when unauthorized person or any outsider tries to intercept data.but as in the case of cryptography only rreeceiver has this autority ao it is not changed.

Suppose now that Keshav wants to send a message to Mohan. Keshav's message which is written by keshav and contains the information which keshav want to share with mohan which is at starting not encrypted is known as plaintext. But to provide security to the data so that nobody is able to alter the data Mohan encrypts(codes) his original(plaintext) message using an encryption algorithm so that the ccodded message, known as ciphertext is coded into a secure formand it , looks unintelligible(different) to any intruder(outsider)

Keshav provides a key, KA, - which is a string of numbers or characters, taken as input to the encryption algorithm.Because key provide security mechanism to the sender. The encryption algorithm takes the key(security mechanism) and the plaintext (original data) as input and produces ciphertext as output [2].Similarly, Mohan will also use a key KB, to the decryption algorithm, that takes the ciphertext(coded data) and Mohan's key as input and produces the original(message) plaintext as output. As a single key is being shared by both mohqn and keshav it is known as symmetric key systems, Keshav and Mohan's keys are identical(same) and are secret. But there is a different case also which is known as public key systems,in which the key that Keshav uses is known to everybody , while Mohan's key is secret.

II. RELATED WORK

.

Symmetric Key Cryptography

All cryptographic algorithms(which provide security to the sender's data) involve substituting one thing for another,.Means for a given information it is changed into another information so that it is free from outsider's attacks. e.g., if we are having a piece of plaintext and by applying encryption on it then we compute the appropriate ciphertext that forms the encrypted(coded) message. In Caesar cipher (a "cipher" is a technique for encrypting data for security purpose).

For English text, the Caesar cipher generally work on a single letter of the originl message of the senderand then substitute that text (letter) with the ending letter of English alphabet. (allowing wraparound, i.e., having the letter "a" follow the letter "z") in the alphabet. For example if k=2, then the letter "c" in plaintext(original message) becomes "e" in coded message(ciphertext); "h" in plaintext becomes "j" in ciphertext, and in this way all other English alphabets can be changed by their substitutes which follows a particular pattern in this type of cryptography.. and k is known as the key in this cryptography.

Corresponding Author: *Reecha Arya*

As in this type of crytptography there is a particular pattern for chaging the data An improvement(modification) to the Caesar cipher is the so-called monoalphabetic(single alphabet) cipher that also substitutes one letter in the alphabet with another letter in the alphabet[3]. However, rather than changing according to a regular sequence (e.g., substitution with an offset of key l for all letters), any letter can be substituted(changed) for any other letter, if each letter has a unique substitute letter and this rule is applied to all the English alphabets.suppose original input contains the following characters.

plaintext letter: a b c d e f g h i f k l m n o p q r s t u v w x y z

ciphertext letter: m n b v c x z a s d f g h j k l p o i u y t r e w q

Data Encryption Standard (DES)

Data Encryption Standard (DES) , a symmetric key encryption standard which was come into the knowledge of people published in 1977 and after that it was updated most recently in 1993 by the US National Bureau of Standards for commercial and non-classified US government use. DES encodes (changes) the original text in 64 bit parts using a 64-bit key. In reality , 8 of these 64 bits are odd parity bits (one bit in every 8 bytes is an odd partity bit for that particular byte), thus the DES key defined by the sender is effectively 56 bits long.

The DES comprise two permutation steps (the initial and ending steps of the algorithm) in which all 64 bits are permuted, and 16 identical "rounds" of operation are performed in between. The working of each round is similar .in which every next round taken as the output of previous round as input. Whenever any round is performed, the rightmost 32 bits of the input are moved to the left 32 bits of the output. The entire 64-bit input to the pth round and the 48 bit key for the pth round (which is derived from the larger DES 56-bit) are considered as input to a particular function that performes expansion of 4-bit input parts into 6-bit parts, exclusive OR-ing with the expanded 6-bit parts of the 48-bit key li, a substitution operation(calculation) and after that next part is exclusive OR-ing with the leftmost 32 bits of the input; The calculated 32-bit output of the function is considered as the rightmost 32 bits of the rounds 64-bit output.

If 56-bit DES is not giving the exact result according to the user point of view, then the solution to this is to run the 56-bit algorithmagain and again , in which the 64-bit output from one round(loop) of DES as the input to the next DES loop, but for different round different keys are used every timeFor example, triple-DES (3DES). Which is caused when we repeat standard DES again and again three times.

DES in combined form with a method which is known as cipher-block chaining, in which the coded data of the jth 64-bit quantity of data is XOR'ed with the (j +1)st unit of data but it is done before the (j+1)st unit of data is coded for encryption.

Data Encryption Standard which is generally known as DES is based on a cipher Feistel block cipher. It consists of many rounds where each round having bit-shuffling, non- linear substitutions (S-boxes) and exclusive OR operations. It encrypts the given message(data) in block size of 64 bits each. After encryption generally decryption is performed which uses the same algorithm which was used in the case of encryption and it also uses the same key which was used for date encryption. Key is 56 bits long. The position of 8, 16,24,32,40,48,56,64 are not taken . DES is based on two basic properties of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting of 16 rounds. For each round shifting of key and data is done, permuted, XORed and sent through, 8 s-box. Whenever the first round is begin, 64 bit plaintext is assigned to initial permutation(IP)[4].Then IP

Divides it into 2 parts- left plaintext(LPT)and right plaintext(RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are again combined. This is the way how encryption occur.and decryption is also performed as encryption but it is taken in opposite order.

Algorithm

[1] DES works on an input of 64-bit long original data and 56-bit key (8 bits of parity) and produces encrypted data of 64 bit block.

[2] The given data which is known as plaintext block is given to an shift the bits around.

[3] The 8 parity bits are taken out from the key by allow the key to its Key Permutation.

[4] The plaintext and key are manipulated(worked) in 16 rounds consisting of:

a. The key is broken into two parts having 28 bit each.

b. Each part of the key is shifted (rotated) by one or two bits, decided by the round

. c. The parts s are again joined and subject to a compression permutation to lessen the size of the key from 56 bits to 48 bits. This reduced size key is used to encrypt this round's plaintext block

. d. The rotated key parts from step 2 are used in next round

. e. The data block is divided into two 32-bit parts. f. One part is subject to an Expansion Permutation to grow its size to 48 bits.

g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from

step 3. h. Output of step 7 is given to an S-box, which changes key bits and lessen the 48-bit block back down to 32-bits.

i. Output of step 8 is given to a P-box to permute the bits.

j. The result from the P-box is exclusive- OR'ed with other part of the data block.

k. The two data parts are interchanged and considered as the next round's input.

Triple DES As an advanced version of DES, the3DES (Triple DES) encryption standard was designed. In this standard the same procedure is applied as was used in original DES but ait was used 3 times to enhance the output of the encryption level[5]. It was used to get rid from the meet-in-the- middle attack occurred in 2-DES and the brute force attacks in DES. It also has some features of proven reliability and a longer key length that removes many of the direct attacks that can be used to lessen the amount of time it takes to break DES.

Asymmetric Cryptography

Asymmetric, or public key, cryptography is, considered as more safe than symmetric methods of encryption for securing data. When this method of cryptography is used two keys, a "private" key and a "public key," are taken to perform encryption and decryption. The use of two keys removes a major limitation in symmetric key cryptography, since only one key does not need to be securely handled among multiple users.

In asymmetric cryptography, a public key is easily available to every person involved in it and used to coded the messages before sending them. A different, private key remains with the receiver of coded messages, who uses this key to decode the data. Algorithms that use the concept of public key encryption methods include RSA .

III. PROPOSED SOLUTION

Whenever data is send from one place to the other place security of data is the biggest issue.Because if data is not secure it is of no use to the sender as well as receiver.So production of an effective key is very necessary.

Management of key is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed. At the receiver side , the information in the form of data packet will be transmitted from source to destination over transmission media using a very efficient cryptographic algorithm to encrypt the entire message which a user(sender) want to send any other person . Cryptography is the process used to appear a given message into completely changed form which is different from original message. An algorithm is a set of rules or procedures used to change, or encrypt the plaintext to produce Ciphertext. The algorithm applies a key to text . Encryption is proceed generally to provide security to the message.So it is considered as the security mechanism.. Any encryption algorithm depends on some key, and keys .So it is said that encryption is the combination of the two parts are normally generated during authentication phase,. And these two part are strongly dependent on one another .as without existing of these two parts together encryption can't be performed.

In the proposed architecture, Whenever any user want to send the data from one part to the another part of the network, then data is encrypted by using a particular key so that data is not altered by any outsider and data is safe during transmission .So a new technique is used for key generation and then a particular pattern is followed to encrypt the data.and at the receiver end the data is decrypted by applying the same procedure in different way.

Encryption Algorithm

```
    1.  Activate data P.
    2.  Generate key K by analyzing no. of 0's in the data
    (a) Develop a routine to count bits in the data
    (b) Set i=count(0)
    (c) Set K=i.
3. Apply or operation on the data
    (a) Set Ed=P OR K
    (b) Encrpted data is generated using OR operation
    (c) Set Ed=encrypted data
4.Data is encrypted and ready for transmission.
```

Example of Encryption Routine

Suppose we have a Data Packet with following Bit Stream –

10100111 10010001 11001010 10101010

The packet is represented as a 4 Byte or 32 Bits Data Packet.

Numbers of 0‟s in each byte are: 4, 2, 2, 5 Binary Equivalent of 5,3,4,4 are 0011,0101, 0100, 0100 Bitwise OR Operation for Encryption of Packet Actual Packet 10100111 10010001 11001010 10101010

Key 00000011 00000101 00000100 00000100

Then Or operation is performed.

Encrypted Packet 10100110 10010110 11001110 10101110

Decryption a Algorithm

A decryption algorithm at the destination site will check the entire encrypted packet.

. Algorithm

```
    •   For Decryption
    1.  Get Encrypted data Ed
    2.  Get the key K
    3.  Apply reverse of or operation(subtraction) on the
        data
    (a) Set Dd=Ed- K
    (b) Decrpted data is generated using reverse of OR
        operation
    (c) Set Dd=decrypted data
4.Data is decypted
5.Actual data is obtained
```

Example of Decryption Routine

Suppose we have Encrypted Data Packet with following Bit Stream –

10100110 10010110 11001110 10101110

The packet is represented as a 4 Byte or 32 Bits Data Packet

Key 00000011 00000101 00000100 00000100

Then reverse of OR operation is performed.

Decrypted(original) Packet 10100111 10010001 11001010 10101010

IV CONCLUSION

As we live in such an environment where automated information resources are highly available everywhere and cryptography will continue to increase value as a security mechanism. DES is now taken as insecure mechanism for some applications like banking system. There are also some analytical results which explains the theoretical limitations in the cipher. So it becomes very important to modify this algorithm by adding new levels of security to make it applicable. By adding new method for key generation give more smoothness and easiness to encryption algorithm and make it stronger against any kind of attack caused by any outsider.

The advantage of proven reliability and a longer key length that removes many of the attacks that can be used to reduce the amount of time it takes . Confidentiality and scalability provided by this algorithm is at the increased level and

uses less power memory and time to encrypt and decrypt the data for security purpose.
There is need to secure the data packets transferring around the network from multiple attacks using efficient cryptographic algorithms. The encryption algorithm explained in the paper is an efficient algorithm based on OR operation by counting number of zeroes which is a unique method. By applying this method, encryption and decryption can be performed effectively with different and new cryptographic technique without any complexity.

REFERENCES

[1] R. Hauser, A. Przygienda and G. Tsudik, "Reducing the cost of security in link state routing", In Symposium on Network and Distributed Systems Security (NDSS ‟97), San Diego, California, Internet Society, pp 93–99, February 1997.

[2] A. Kush, "Security Aspects in AD hoc Routing" , Computer Society of India Communications, Vol. 3 No 2 Issue 11, pp 29-33, March 2009.

[3] A. Kush, "Security And Reputation Schemes In Ad-Hoc Networks Routing" International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp 185-189, June 2009. [4] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, pp 800-848, November 2002

. [5] Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking (MOBICOM‟00), pp 275– 283, August 2000.

[6] A. Kush, C. Hwang and P. Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE), Volume 3, pp 1793-1799, May 2009.

[7] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[8] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure message transmission in mobile ad hoc networks", Elsevier Journal of Adhoc network, Ad Hoc Networks 1, pp 193–209, 2003.

[9] Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks" Elsevier Journal of Ad hoc Networks, Ad Hoc Networks 3, pp 69–89, 2005.

[10] B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, August 2001.