International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 4, No. 1, Mar. - May, 2019
Pages 51-55 | Cosmos Impact Factor (Germany): 5.195
Received: 06.03.2019 Published : 29.03.2019

SECURE COMMUNICATION USING HYBRID CRYPTOSYSTEM

[1]Dr.R.Latha, [2]R.Vinothini, [3]S.Vinothinis, [4]M.Aarthi, [5]A.Priyadharshini
[1]Principal, [2]Assistant Professor, [3,4,5] UG Scholars
Department of CSE, K.S.K College of Engineering and Technology
Kumbakonam-612001. Email: rajprithivi3@gmail.com

ABSTRACT- Security is the primary concern in the field of information technology. Cryptography and Steganography plays an important role to protect the confidential information from an unauthorized disclosure. To achieve a secure communication in network environment is the primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and ecommerce transactions, digital signatures using public key cryptography is extensively employed. To maintain confidentiality, Digital Envelope, in the combination of the encrypted message and signature with the encrypted symmetric key is used. It will also include Message authentication code to maintain integrity of message. Our results shows hiding a secret information into a images using a Triple Data Encryption Standard Algorithm.

Keywords: Secure communication, Triple DES algorithm, Hybrid Cryptosystem.

1. INTRODUCTION

Cryptography ensures the security by encrypting the plain text into 'Cipher text' form by using cryptographic algorithms and secret keys. Steganography ensures the security of secrets by hiding them within the cover files. The messages cannot be seen by the unauthorized user.

a) Symmetric Key Encryption

Encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

2. Related work

a) Data Security and Integrity in Cloud Computing Based On Triple DES Algorithm
As an enhancement of DES Algorithm, the Triple DES Algorithm was proposed. Triple DES applies DES algorithm three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
b) Security Enhancements of Networked Control Systems Using Triple DES Algorithm
Triple DES Algorithm effectively responds to this issue of smaller key size. Triple DES algorithm uses three times of key size originally introduced in DES algorithm. The process includes three set of keys each of 64 bit which results in 3 X 64 = 192 bits.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 4, No. 1, Mar. - May, 2019
Pages 51-55 | Cosmos Impact Factor (Germany): 5.195
Received: 06.03.2019 Published : 29.03.2019

3. Proposed System

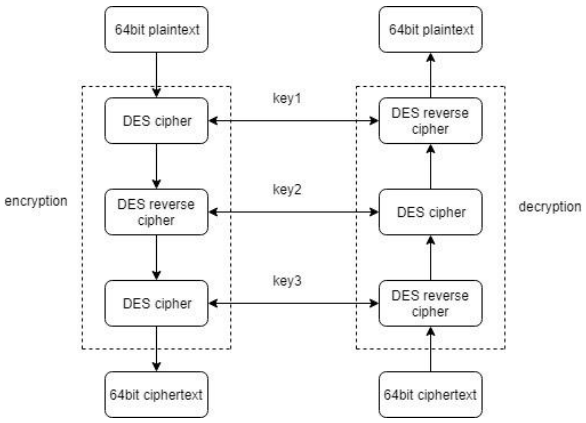
Triple DES Algorithm is same as DES Algorithm except we apply it three time. So in order to understand Triple DES, we need to understand how DES Algorithm is used to encrypt data and generating key. DES performs an initial permutation on the 64 bits block of data. Then it splits it into two parts named L and R, each 32 bit sub-blocks. Then the encryption of block of message takes place in 16 rounds. From the input key, sixteen 48 bit keys are generated, one for each round. The right half is expanded from 32 to 48 bits. The result is combined with the sub-key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half. This process is conducted for all 16 rounds. The function f in following figure makes all mapping in all rounds This completes the process of DES Algorithm. To increase the key size and the complexity of the encryption process, Triple DES encrypts any data three times and uses different keys for each step. We use three sets of 64 bits and 8 bits from each set is used as parity bits. So we are left with effective 56 bits which gives us 3 X 56 = 168 bits.

The process of encryption is as follows

1. Encrypt the data using DES Algorithm with the help of first key.
2. Now, decrypt the output generated from the first step using DES Algorithm with the help of second key.
3. Finally, encrypt the output of second step using DES Algorithm with the help of third key.

The decryption process of any cipher text that was encrypted using Triple DES Algorithm is the reverse of the encryption process i.e.,
1. Decrypt the cipher text using DES Algorithm with the help of third key.
2. Now, encrypt the output generated from the first step using the DES Algorithm with the help of second key.
3. Finally, decrypt the output of the second step using DES Algorithm with the help of first key.

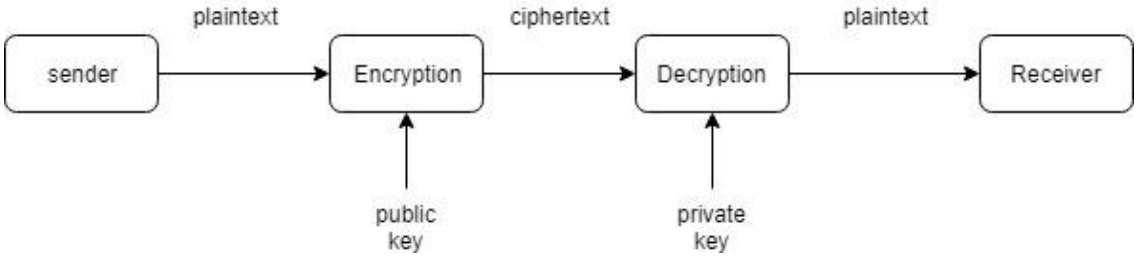
The process of encrypt – decrypt – encrypt help complexing things and securing the data. The three keys can also be same or two of them can be same. But it is recommended to use all the three keys different.



International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 4, No. 1, Mar. - May, 2019
Pages 51-55 | Cosmos Impact Factor (Germany): 5.195
Received: 06.03.2019 Published : 29.03.2019

4. ALGORITHM

a)cryptography
Cryptography means data secure, it helps to ensure data privacy, maintain data integrity, authenticate communicating parties, and prevent repudiation.



The above Figure as shown in key schedule for encryption and decryption algorithm which generates the sub keys. Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) and the remaining eight bits are either discarded or used as parity check bits. The 56 bits are divided into two 28 bit halves; each half is treated separately. In successive rounds, both halves are rotated left by one and two bits (specified for each round), and then 48 sub key bits are selected by Permuted Choice 2 (PC-2) i.e. 24 bits from the left half and 24 from the right. The rotations (denoted by "<<mean that a different set of bits is used in each sub key, each bit is used in approximately 14 out of the 16 sub keys.

c) Cryptography goals

These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

Authentication:
Authentication means before sending and receiving data using the system, the receiver and sender identity should be verified.

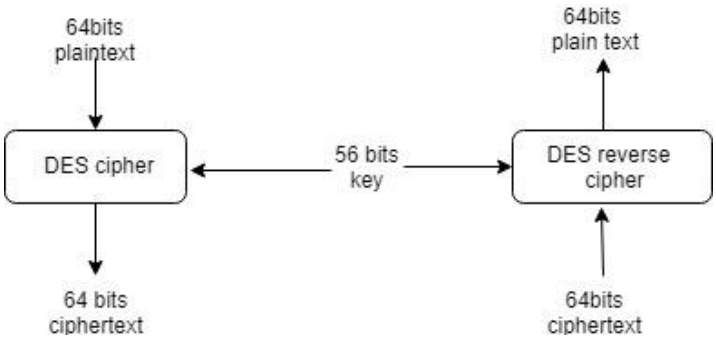
Secrecy or Confidentiality:
In this function is how most people identify a secure system. It means only the authenticated people are able to interpret the message or content and no one else.

Integrity:
Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation:
In this function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability:
Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 4, No. 1, Mar. - May, 2019
Pages 51-55 | Cosmos Impact Factor (Germany): 5.195
Received: 06.03.2019 Published : 29.03.2019



Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

- Encryption using the first secret key.
- Decryption using the second secret key.
- Encryption using the third secret key.

Encryption:
c = E3 (D2 (E1 (m)))

Decryption:
m = D1 (E2 (D3(c)))

Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In these case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)
c = E3 (D3 (E1 (m))) = E1 (m)

It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

c = E1 (D2 (E1 (m)))

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion.

5. CONCLUSION

In this paper we present a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are triple DES. In case of changing key size, it can be seen that higher key size leads

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 4, No. 1, Mar. - May, 2019
Pages 51-55 | Cosmos Impact Factor (Germany): 5.195
Received: 06.03.2019 Published : 29.03.2019

to clear change in the battery and time consumption. In future the work may be extensive by including the schemes and techniques over different types of data such as image, sound and video and rising a stronger encryption algorithm with high speed and minimum energy consumption.

REFERENCES

[1] Pooja Rani,Mrs.Preeti Sharma Cryptography and Steganography. International Journal of Computer Application , No.12, 2010,pp 63-68.
[2] Ahmed Al-shaaby,Talal Alkharobi , A New Approach of Data Hiding in Images using Cryptography and Steganography, International Journal of Computer Applications, Vol.58,No.18,2012,pp1-5.
[3] Umamaheshwari.M,Sivasubramanian.S,Analysis of different stegnographic algorithms for secured data hiding,vol.10,no.8,2010,pp 154-160.
[4] Rajyaguru,M.H.,combination of cryptogrphy and steganography with rapidly changing keys,international journal of emerging technology and advanced engineering ,vol.2,no.10.2012,pp 329-332.
[5] Kandar.S,and Maiti.A.,Variable length key based Visual cryptography scheme for color Image using Random Number,International journal of computer applications(0975-8887) vol.19,no.4,2011,pp35-40.
[6] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, 0Computer Science and Network Technology (ICCSNT), International Conference, Vol.2, No.2.11, 2011 ,pp. 1017-1020.