Secure Communication Using Hybrid Cryptosystem

Dr.R.Latha* , Mrs.R.Vinothini# , @Ms.S.Vinothinis , @Ms.M.Aarthi , @Ms.A.priyadharshini
Principal , Assistant Professor# , @UG Scholar*
@Department of CSE, KSKCET
KSK College of Engineering and Technology,Kumbakonam
Tamilnadu,India

ABSTRACT*- Security is the most important concern in the field of information knowledge. 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 most important requirement to access remote income in a outlawed and efficient way. For validation and authentication in e- banking and ecommerce transactions, digital signatures using public key cryptography is extensively in work. To continue confidentiality, Digital Envelope, in the combination of the encrypted message and cross with the encrypted symmetric key is used. It willpower what's accompanying include Message authentication code to maintain honor of announcement. Our results shows hiding a secret information into a metaphors using a Triple Data Encryption Standard Algorithm.*

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

I. 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.

II. Related work

a) Data Security and Integrity in Cloud Computing Based On Triple DES Algorithm

As an augmentation of DES Algorithm, the Triple DES Algorithm was future. Triple DES relate DES algorithm three period to each dahunk. Triple DES provide a relatively uncomplicated technique of mounting the key bulk of DES to protect poignant such attack, missing the call for to plan a totally new block nonentity algorithm.

b) Security Enhancements of Networked Control Systems Using Triple DES Algorithm

Triple DES Algorithm successfully respond to this subject of lesser key size. Triple DES algorithm uses three times of key in size first introduce in DES algorithm. The course include three set of keys each of 64 bit which results in 3 X 64 = 192 bits.

III. Proposed System

Triple DES Algorithm is identical as DES Algorithm not including we relate it three instance. So in systematize to be well-known with Triple DES, we call for to be appreciative for how DES Algorithm is tatty to encrypt data and manufacture key. DES act upon an innovative amend on the 64 bits chunk of data. Then it crack it hooked on two ingredient given name L and R, apiece one 32 bit sub-blocks. Then the encryption of block of memo take place in 16 round. From the input solution, sixteen 48 morsel keys are produce, one for apiece around. The right half is long-drawn-out from 32 to 48 bits. The cause is joint with the sub-key for that encircling via the XOR operation. Using the S-boxes the 48 consequential bits are then transformed again to 32 bits, which are subsequently permutated up till now another time with yet an supplementary deposit chart. This by currently warily shuffle right half is at the present united with the left half using the XOR operation. In the next surrounding, this mix together be used at the same time as the new-fangled gone moderately This progression is demeanor for all 16 rounds. The essence in succeeding figure craft all part of map in all part of rounds

This completes the progression of DES Algorithm. To magnify the key size and the obscurity of the encryption process, Triple DES encrypts whichever data three times and uses analogous keys for each step. We use three sets of 64 bits and 8 bits from apiece situate is worn as stability bits. So we are left with efficient 56 bits which give us 3 X 56 = 168 bits.

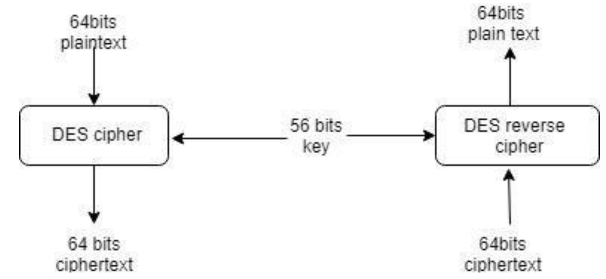
The progression of encryption is as follows

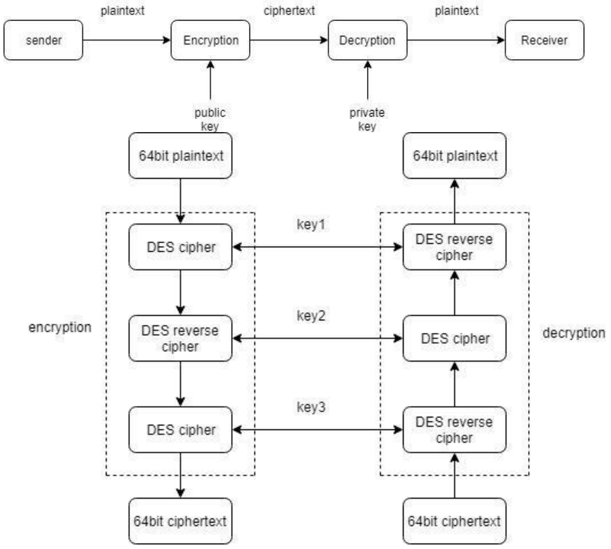
1. Encrypt the data by DES Algorithm in the midst of the rally round of foremost key.
2. Now, decrypt the amount produced generate from the first stride with DES Algorithm with the help of jiffy key.
3. Finally, encrypt the harvest of jiffy step using DES Algorithm in the midst of the rally round of third key.

The decryption process of in the least cipher text that be encrypted using Triple DES Algorithm is the annul of the encryption route i.e.,

1. Decrypt the nobody text using DES Algorithm amid the lend a hand of third key.
2. At this instant encrypt the harvest generate commencing the foremost step with the DES Algorithm in the middle of the rally round of second key.
3. Finally, decrypt the output of the second step using DES Algorithm with the facilitate of first key.

The process of encrypt – decrypt – encrypt help concluding things and secure the data. The three key tin can also be alike or two of them can be identical. But it is suggested to use all the three keys different.





IV. 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 elected from the initial 64 by Permuted Choice

Encryption:

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

Decryption:

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

Using decryption in the subsequent stair during encryption provides backward compatibility with common DES algorithm. In these case first and second underground keys or instant and third covert key are the same any key.

c = E3 (D1 (E1 (m))) = E3 (m)
c = E3 (D3 (E1 (m))) = E1 (m)
It is possible to use 3DES cipher with a top secret 112-bit key. In this case earliest and third underground keys are the equal.

1 (PC-1) and the remaining eight bits are either unnecessary or used as parity check bits. The 56 bits are divided into two 28 bit halves; each half is treated singly. In successive rounds, in somebody's company halves are rotated left by one and two bits (individual for each in circles), and then 48 sub key bits are select by Permuted Choice 2 (PC-2) i.e. 24 bits from the left fairly and 24 from the right. The rotations (denoted by "<<connote that a different set of bits is used in each minor key, each bit is used in just about 14 out of the 16 sub keys.

b) Cryptography goals

These functions are usually referred to as the goals of the refuge system. These goal can be involuntary under the subsequent five main category:

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:

In this utility is how a large amount people make out a secure system. It property only the legitimate public are able to take to mean the letter or unhappy and no one in addition.

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:

In this value is how a large quantity people make out a make safe classification. It chattels only the valid public are able to take to imply the letter or gloomy and no one in calculation.

Triple DES algorithm use three iterations of widespread DES cipher. It receive a covert 168- bit key, which is not dialogue hooked on three 56- bit keys.

- Encryption with the first covert key.
- Decryption using the second surreptitious key.
- Encryption using the third surreptitious key

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

Triple DES is useful because it has a notably sized key length, which is longer than most key lengths joined with other encryption modes. DES algorithm was replace by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives beginning single DES but the system is used in triplicate and involve three sub keys and key padding when necessary. Keys must be increased to 64 bits in duration Known for its compatibility and litheness can without difficulty be renewed for Triple DES enclosure.

V. 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 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] PoojaRani,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,An alysis 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.