Available ONLINE www.visualsoftindia.com/journal.html

VSRD International Journal of
Computer Science & Information Technology

ISSN No. 2231-2471

VSRD-IJCSIT, Vol. 1 (7), 2011, 465-470

RESEARCH ARTICLE

Analysis Improved Cryptosystem Using DES with RSA

[1]Gaurav Shrivastava*

ABSTRACT

The Data Encryption Standard (DES) is the most common Secret Key Cryptography scheme. DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS). This paper proposes a new scheme to enhance the security of cryptosystem. DES is widely used throughout the world for information security. DES so far has been stronger than other cryptosystems in the security. But, due to the advancement in the hardware technique, DES may be attacked by parallel processing. Thus a new scheme to strengthen the DES is needed to protect the cryptosystem. This new scheme will use Triple DES Three Times with RSA Algorithm. This will provide 504 bit key length. This results in enhancing the security level along with an increase in File size which is the major drawback in this scheme. In future we are trying that security level is increased but file size remain constant.

Keywords : Cryptography, Cryptanalysis, Data Encryption Standard, DES, RSA, Triple DES, Key Length.

1. INTRODUCTION

Information security is an important issue in our information society, when we transmit valuable information, it is frequently protected physically through the use of shielded cable and the like, such measures do not securely protect information, and they are very expensive and uneconomical. More efficient techniques should be employed. Under the existing circumstances cryptography is evolving as the natural solution to such problems. The DES, one of the most commonly used encryption algorithms, has encountered many problems since its publication in NBSL21. A differential cryptanalysis attack against the DES requires 1015 chosen plaintext messages, an enormous amount. But as the process time of cryptanalysis gets shorter because hardware technique has developed rapidly, in the future the DES may be attacked by various kinds of cryptanalysis using parallel process. We can consider carefully that the DES algorithm should be improved against the differential cryptanalysis. [1]

[1]Assistant Professor & Head, Department of Information Technology, Mathura-Devi Institute of Technology & Management, Indore, Madhya Pradesh, INDIA. *Correspondence: gaurav2086@gmail.com

This new scheme uses features of both DES (Symmetric key Cryptography) and RSA (Asymmetric key Cryptography). It would be very effective to combine the two cryptography mechanisms, so as to achieve the better of the two and yet do not compromise any of the features.

2. LITERATURE REVIEW

The Data Encryption Standard (DES) also called as the Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO has, been a cryptographic algorithm used for over three decades. Of late, DES has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been slightly on the decline however, no book on security is complete without DES, as it has been a landmark in cryptography algorithms.

The origins of DES go back to 1972, when in the US, the National institute of Standards and Technology (NIST) embarked upon a project for protecting the data in computers and computer communications. They wanted to develop a single cryptographic algorithm. After two year, NBS realized that IBM's Lucifer could be considered as a serious candidate, rather than developing a fresh algorithm for from scratch. After a few discussions, in 1975, the NBS published the algorithm. Towards the end of 1976, the US Federal Government decided to adopt this algorithm and soon, it was renamed as Data Encryption Standard (DES). Soon, other bodies also recognized and adopted DES as a Cryptographic algorithm.

2.1. DES

DES is a block cipher. It encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bit of cipher text The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

- To encrypt plain text (P) with key (k1) then produces cipher text (C) C = Ek1 (P)
- To decrypt cipher text (C) with key (k1) then produces plain text (P) P = Dk1 (C)

2.2. Variations of DES

The DES is susceptible to possible attacks. However, because DES is already proven to be a very competent algorithm, it would be nice to reuse DES by making it stronger by some means. Rather than writing a new cryptographic algorithm. Writing a new algorithm is not easy, more so because it has to be tested sufficiently so as to be proved as a strong algorithm. Consequently the two main variation of DES have emerged, which are Double DES and Triple DES.

2.3. Double DES

Double DES is quite simple to understand. Essentially, it does twice what DES normally does only once. Double DES uses two keys, says k1and k2. It first performs DES on the original plain text using k1 to get the encrypted text. It again performs DES on the encrypted text, but this time with the other key k2. The final output is the encryption of encrypted text.

$$C = E_{k2} (E_{k1} (P))$$

$$P = D_{k2} (D_{k1} (C))$$

2.4. Triple DES

In triple DES the plain text P is encrypted with a key k1, then encrypted with a second key k2, and finally encrypted with a key k3. Where k1, k2 and k3 are all different from each other.

$$C = E_{k3} (E_{k2} (E_{k1} (P)))$$

$$P = D_{k3} (D_{k2} (D_{k1} (C)))$$

The key length of 3DES is 168 bits three times as large as with DES (56 bits), making the key complexity by a factor of $2^{112}$is increased. The effective key length is 112 bits but only due to the possibility of the so-called meet-in -the-middle attack: If the attacker in possession of a pair of plain text and cipher, so he can attack the encryption of both sides. The plain text is all possible keys for encrypted (2^{56} possibilities). The resulting texts are also with all possible keys for each level 2 encrypted (2^{112} possibilities). Their results are compared with the results of decryption of the cipher text with all keys (2^{56} possibilities). So overall have only $2^{112} + 2^{56}$ encryption and decryption are performed, instead of 2^{168} when using the brute force method.

2.5. Attempts to attack DES

It was not easy to attack on DES in the past, despite the efforts of researchers over many years. The first method was brute-force exhaustive search of the key space; this process takes 255 steps on average, the time of a specialized computer to perform exhaustive search (requiring 3.5 hours on average) as well as this estimated was recently update to give an average time of 35 minutes for the same cost machine.[3]

Exhaustive search in terms of computational requirements which announced by Balham and Shame by using a new technique known as differential cryptanalysis, this attack requires the encryption of 247 chosen plaintexts; by using this method the plaintexts are chosen by the attacker, despite it is a theoretical breakthrough, actually this attack is not practical because of both the large data requirements and the difficulty of mounting a chosen plaintext attack. The third method to attack DES is Known as liner cryptanalysis, using this attack the DES key can be recovered by the analysis of 243 steps known as plaintext, the first experimental cryptanalysis of DES, was successfully achieved in an attack as well as this method of attack is still impractical[2].

A DES cracking machines used to recover a DES key in 22 hours, the agreement of the cryptographic community is that DES is not secure, basically because 56 bit keys are vulnerable to exhaustive search. DES is no longer commonly used for encryption, the 56-bit key can be found in matter of hours with a relatively inexpensive cracker machine; most of the following alternatives have a good cryptanalytic strength and remain invulnerable to brute-force attack.

3. METHODOLOGY

The DES is the most widely known symmetric cryptosystem. The DES has the same algorithm for the

encryption and the decryption. The DES enciphers a block 64 bit of data with a 56 bit key. And Triple DES is use triple time DES use a 64 bit of data with a 168 bit key. The New Scheme is based on overall structure of DES. We implement a new scheme to enhance the security of DES. We will use a Triple DES use in a Three Time with RSA Algorithm. We use a 504 bit key (k1, k2, k3). Each key length 168 bits and k1, k2, k3, Keys are using independently. In RSA Algorithm use generate randomly public and private keys pair.

3.1. Encryption Process

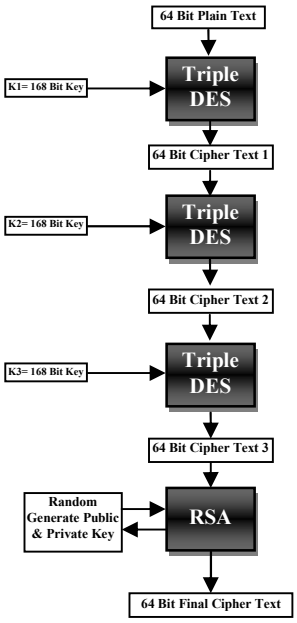

Fig 1: Encryption Process

$$\text{Triple DES} = 3D^{E} = E_{k3}\,(E_{k2}\,(E_{k1}\,(P))); \; C = (3D^{E}{}_{K3}\,(3D^{E}{}_{K2}\,(3D^{E}{}_{K1}\,(P)))$$

3.2. Decryption Process

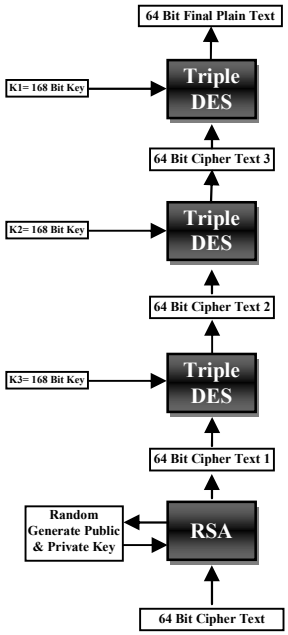

Fig 2: Decryption Process

$$P = (3D^{D}{}_{K3}\,(3D^{D}{}_{K2}\,(3D^{D}{}_{K1}(C)))$$

4. RESULTS

There are several analysis methods for cryptosystems. We have implemented new scheme in microcomputer and observed that the file size after the encryption of the plain text increases (for example 1MB file size after encryption becomes 2.33 MB). Now after decryption, the file size comes to its original size (1MB). This means that RSA algorithm used in new scheme enhances the security level but is also responsible for increase in the file size. This works very well where security is a major concern as the cryptosystem cannot be bypassed.

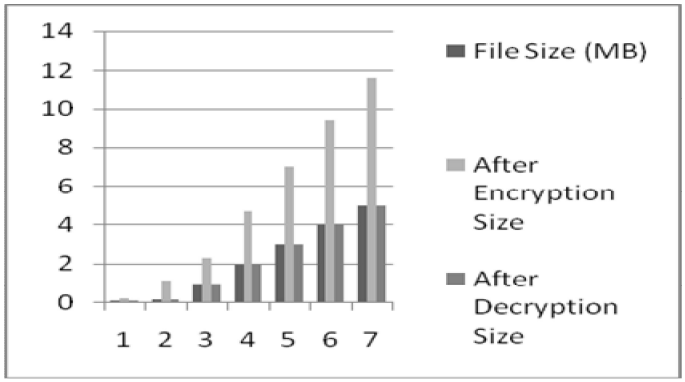

Fig 3: Analysis of File Size using New Scheme

The results of study are as follows:

- To increase time complexity and space complexity against the exhaustive attack and the time-memory trade off attack, the key length is increased to 504 bits (k1, k2, and k3).
- We removes the main difficulty arises in Brute-force attack; it almost minimizes the cause of meet-in-middle attack.
- We improve the security level but File size is increased after encryption, is major drawback in this scheme. In future we are trying that security level is increased but file size remain constant.

Table 1. File size Using New Scheme

File Size (MB)	After Encryption Size	After Decryption Size
0.1	0.234	0.1
0.2	1.14	0.2
1	2.33	1
2	4.7	2
3	7.0	3
4	9.4	4
5	11.6	5

5. CONCLUSION

The volume of information exchanged by electronic means such as internet, wireless phones, Fax, etc. is increasing very rapidly. It is very serious that information through internet, an enormous computer network, is vulnerable to hackers and that privacy of wireless phones without security can be invaded. We should develop

improved cryptosystems to provide greater security. This paper has designed the DES like cryptosystem called a new scheme. In this scheme increase a time complexity and space complexity against the exhaustive attack and the time complexity trade off attack, the key length is increased to 504 bits (k1, k2. k3).

6. REFERENCES

[1] Sung-Jo Han, Heang-Soo Oh, Jongan Park, The improved Data Encryption Standard (DES) Algorithm,Department of Electronic Engineering, Chosun University. South Korea.1996 IEEE

[2] Charels Connell, An Analysis of New DES: A Modified Version of DES, Locust Street Burlington, USA, Boston MA 02215 USA

[3] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg, An Innovative Approach to Enhance the Security of Data Encryption Scheme. International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010)

[4] Subbarao V. Wunnava, Data Encryption Performance and Evaluation Schemes, Florida International University, Miami, FL Ernest0 Rassi; Florida Intemational University, Miami, FL 0-7803-7252-2/02/$10.00 0 2002 IEEE Proceedings IEEE Southeastcon 2002)

[5] D. Coppersmith, The Data Encryption Standard (DES) and Its strength Against attacks, IBM J. RES. Develop. VOL.38 NO.3 MAY 1994.

❑❑