IJITKMSpecial Issue (ICFTEM-2014) May 2014 pp. 1-5 (ISSN 0973-4414)

Improvement of Performance in Cryptography

Parneet Kaur[1], Jagmohan Singh[2], Kamaljit Singh[3]
[1-3]Asst. Prof. – SSIET, DeraBassi
[1]parneetwaliya@ymail.com, [2]saini.jagmohansingh@gmail.com, [3]kamaljitsingh011987@gmail.com

Abstract— The security of any cryptography algorithm depends upon its key length and block size, by increasing the key length we actually enhance the security of the data being encrypted by a particular algorithm. Depending upon the requirements and confidentiality of the data we use the various cryptography algorithms available till now that may include DES .AES which is a successor of DES having 128-bit key length, SMS4 which also makes use of 128-bit key length, besides these there are many other encryption algorithms in practice. But with the advancement in technology has made the process of cryptanalysis much easier and faster, so in order to secure a highly confidential data of the level of national security, the use of 128-bit key cannot solve the purpose and hence there is need to increase the key length to enhance the security.
Keywords— DES, Cryptography, Key length, bits

1. Introduction

Cryptographyis the method of designing algorithms for securing the data from being accessed by the intruders (both active and passive) within a communication system as well as to ensure the authenticity of the data to receive at the other end by applying suitable mathematical operations.Cryptography is divided into two categories depending upon the era.

2. Classical Cryptography

The method of conversion of entire message from a comprehensible form into an in comprehensible form and vice-versa, making it unreadable by the adversaries without the knowledge of the secret is referred as classical cryptography. The main emphasis is on the confidentiality of the data and not the authentication or integrity of the data.
The various methods of encryption that constitute the classical cryptography are:

a. Transposition Ciphers

In this method the position of the plaintext characters are shifted according to a regular system so that the cipher text constitutes a permutation of plaintext.
it includes Rail Fence Cipher, Route Cipher, Column Transposition, Double Transposition etc.

b. Substitution Ciphers

It is the method of encryption in which the units of plaintext are replaced with the units of cipher text according to a regular system. The units may be single letter or set of multiple letters. It includes Simple Substitution (e.g. Caesar Cipher, Pigpen Cipher), Homophonic,Substitution,Polyalphabetic,Substitution, Polygram Substitution, One Time Pad etc.

3. Modern Cryptography

The cryptography techniques that are currently in practice and make use of the modern technology to perform complex mathematical operations to produce cipher text may be termed as modern cryptography. They not only ensure data confidentiality but also ensure data authentication, Non repudiation and integrity control.

Modern Cryptography is broadly classified into three categories:

a. Symmetric Key Cryptography

It is the method that makes use of a single key for both encryption and decryption of the data. E.g. DES, AES, RC1, Blowfish etc.

b. Asymmetric Cryptography

The cryptography that makes use of one key for the encryption of the data and another key for the decryption of the data is called asymmetric cryptography. E.g. RSA,Digital Signature Algorithm (DSA), PKCS, Key Exchange Algorithm (KEA) etc.

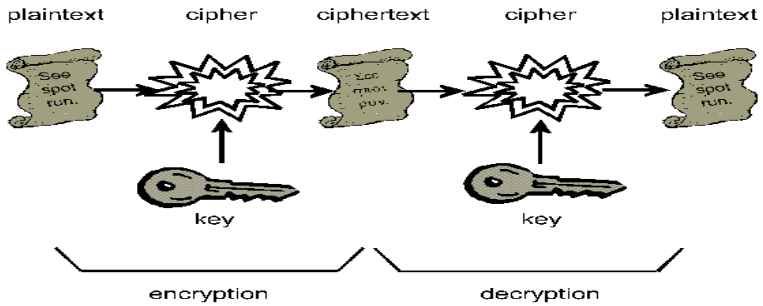

Fig.1 Symmetric Cryptography

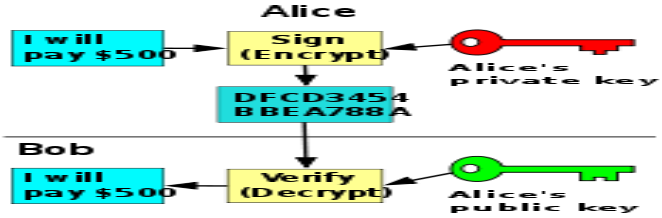

Fig.2 Asymmetric Cryptography

c. Hash Functions

These are the one way encryption algorithms also termed as message digest that in some sense doesn't make use of a key but uses a mathematical transformation to irreversibly encrypt information. E.g. Message Digest (MD, MD2, MD4, MD5), FIPS180-2, Whirlpool, Tiger etc.

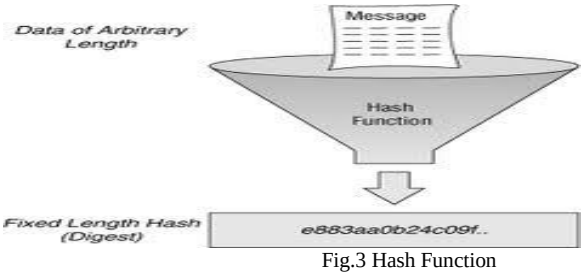

Fig.3 Hash Function

4. Literature Survey

DES is a very popular block cipher in the world and it uses 64 bit key to encrypt or decrypt the data block. DES established necessary theoretical basis for cipher theory research and development. It also provides important reference for block cipher's design and application. It is widely used in many fields, especially in commerce, financial and electronic business [1]. But because the key of DES algorithm is short and it belongs to iterative cipher, it is vulnerable to break brute-force attack and differential cryptanalysis. To research and improve on DES algorithm must have some practice values. Chaos system has good cryptography characteristics. It is wildly used in information security and secure communications fields. It is sensitive to initial values. Even the variation of initial values is very small; the out put of the system is completely different uncorrelated chaotic sequence. Because of it's characteristics such as good securitylarge key space and randomness unease prediction and so on., chaotic sequences are suitable for application in secure communication In view of DES algorithm's existing weaknesses, such as small key space16-round structure[4], the possibly 'trap door', the paper presents an improved DES algorithm. This algorithm is based on DES algorithm. Chaotic encryption is embedded into DES algorithm's iteration.

The AES algorithm [6] takes the Cipher Key, K, and performs a Key Expansion routine to generate a key schedule. The Key Expansion generates a total of Nb(Nr + 1) words: the algorithm requires an initial set of Nbwords, and each of the Nr rounds requires Nbwords of key data. The resulting key schedule consists of a linear array of 4-byte words, denoted [WI], with 'i' in the range0 £ i <Nb (Nr + 1). The expansion of the input key into the key schedule proceeds according to the pseudo code in Sub Word() is a function that takes a four-byte input word and applies the S-box to each of the four bytes to produce an output word. The function RotWord () takes aword [a0, a1,a2,a3] as input, performs a cyclic permutation, and returns the word [a1,a2,a3,a0]. The round constant word array, Rcon[i], contains

the values given by [xi-1,{00},{00},{00}], with x i-1 being powers of x (x is denoted as {02}) in the field GF(28), as discussed in Sec. 4.2 (note that i starts at 1, not 0)., it can be seen that the first Nkwords of the expanded key are filled with the Cipher Key. Every following word, w[i], is equal to the XOR of the previous word, w[i-1], and the word Nkpositions earlier, w[i-Nk]. For words in positions that are a multiple of Nk, a transformation is applied to w[i-1] prior to the XOR, followed by an XOR with a round constant, Rcon[i]. This transformation consists of a cyclic shift of the bytes in a word (RotWord()), followed by the application of a table lookup to all four bytes of the word(Sub Word()).It is important to note that the Key Expansion routine for 256-bit Cipher Keys (Nk= 8) is slightly different than for 128- and 192-bitCipherKeys. If Nk= 8 and i-4 is a multiple of Nk, then Sub Word() is applied to w[i-1] prior to the XOR.Implementation technique.

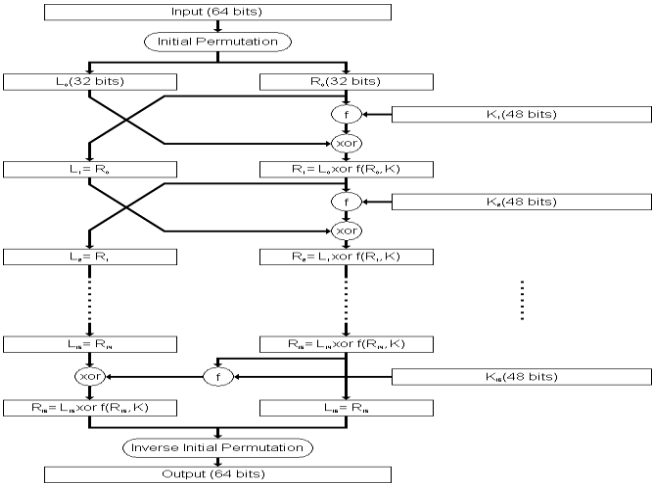

Fig.4 DES process

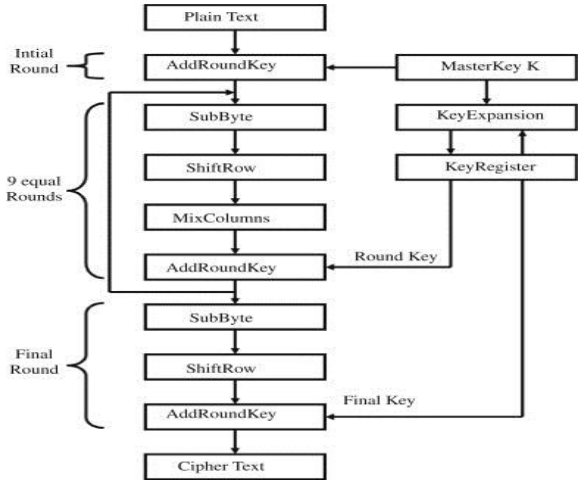

Fig.4 DES process

5. Implementation Technique

In view of enhancement of encryption method key feature is to increase the security of the encryption technique algorithm, the paper presents a new encryption scheme based on the algorithm and chaotic encryption. The chaotic Sequence is implemented in the DES algorithm to improve the initial keys and the iterating operations, so that the chaotic encryption is combined with DES algorithm. The new algorithm is illustrated by text encryption process. VB 6.0 is chosen as software, where encryption method has been implemented. encryption process is as follows:

Stage 1: In this stage we have generated numeric code by using the formula (p+k) mod256 .by using this formula we generate intermediate cipher stage1.

Stage 2: In this stage we are generating binary data of the given text on which we are performing bitwise transformation and generate intermediate cipher stage2.
Stage 3: In this stage we are generating blocks of 265 bit each and further dividing it into 4 groups of 64 bits each further we perform the operations as shown in figure 1.6

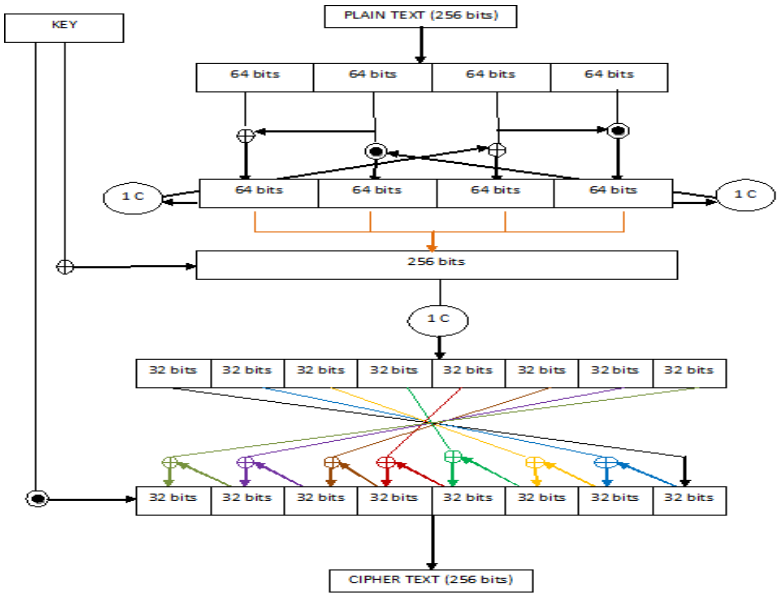

Fig.6 Stage 3 of Encryption Technique

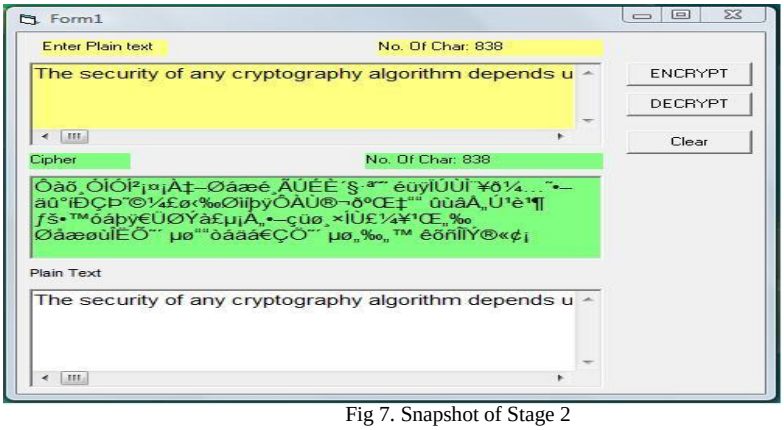

Fig 7. Snapshot of Stage 2

In the snapshot of the stage 2 implementation, we have test the working of algorithm as per the design, where encryption and decryption process generating the results. Our work on the testing parameters is in process.

6. Conclusions

As the implementation of original DES and AES has many weaknesses, there is a scope to decrypt the cipher easily. To overcome this weakness, we have designed 3 stage algorithm of "Enhanced Cryptography Technique". By using this technique, we have increased the bit length of 256 bits which will help to increase the security of the ciphers inspite of the increased the time complexity. We can enhance it more by increasing the no. of iterations in stage 2 &3.

References

[1] Dr. Mohammed M Alani , "DES96 IMPROVED DES SECURITY" in Proc.IEEE Multi-Conference on Systems, Signals and Devices , pages 1-4, 2010.

[2] B.Schneier, Applied cryptography, John Wiley & sons, new york, 1996.

[3] E. Biham, "On Matsui's Linear Cryptanalysis", in Proceedings ojEUROCRYPT'94, page 341.

[4] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", in Proc. OjCRYPTO'92, page 487.

[5] Chong Hee Kim, "Improved Differential Fault Analysis on AES Key Schedule", IEEE 2011.

[6] C. Giraud. DFA on AES. In Advanced Encryption Standard - AES, 4th International Conference, AES 2004, volume 3373 of Lecture Notes in Computer Science, pages 27–41. Springer, 2005.

[7] Raphael C.-W. Phan, "Reducing the exhaustive key search of the Data Encryption Standard (DES)", sciencedirect , Computer Standards & Interfaces, Volume 29, Issue 5, Pages 528-530, July 2007.

[8] Chang-Doo Lee, Bong-Jun Choi, Kyoo-Seok Park, "Design and evaluation of a block encryption algorithm using dynamic-key mechanism, Future Generation Computer Systems", Volume 20, Issue 2, Pages 327-338, 16 February 2004.

[9] Raphael C.-W. Phan, Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES), Information Processing Letters, Volume 91, Issue 1,Pages 33-38, 16 July 2004.

[10] Marie A. Wright, The Advanced EncryptionStandard, Network Security, Volume 2001, Issue 10, Pages 11-13, 31 October 2001.

[11] Juan C.Asenjo,Thales e-Security, The Advanced Encryption Standard — Implementation and Transition to a New Cryptographic Benchmark, Network Security, Volume 2002, Issue 7, Pages 7-9, 1 July 2002.