An Innovative Approach to Enhance the Security of Data Encryption Scheme

D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg

Abstract— **In this paper, we proposed a new scheme to enhance the security of data Encryption scheme. With cascading of data encryption standard in three times, we become able to counter the famous meet in middle attack in double and triple data encryption standard. We show how the random key stream can be used to create lifetime supply of keys for one time pads. Here we provided the practical approach that we can use to set up our own one-time pad encryption. For simplicity let's study how randomized key can be achieved. Random key generation can simply be obtained via use of permutation. Permutation technique can be used in conjunction with other technique includes substitution, encryption function etc. for effective performance. The goal of this article to show how the one-time pad encryption technique can be achieved by the suitable combination of these techniques.**

Index Terms— **DES, Privacy & authentication, Symmetric Key, Security, Cryptography**

I. Introduction

DES is most widely used symmetric cipher and although numerous symmetric cipher have been developed since the introduction of DES like Double DES, Triple DES. In DES 64-bit block, 56-bit key and Fiestel structure approach is used.

Critics believe that the most serious weakness of DES is in key size. Differential crypto analysis is the first published attack that is capable of breaking DES is less than 255 complexities. If we can make a computer with one million chips (Parallel Processing) than we can test the whole key domain in approximately 20 hours. When DES was introduced the cost of such computer was over several million dollars but now it may be reduced to few hundred dollars and less in future.

One solution to improve the security of DES is to abandon DES and design a new scheme and the second solution is to use multiple (Cascaded) instances of DES with multiple keys which does not require and investment in new software and hardware. Here we study the second solution use of multiple key as one time pad with some new approach [1].

II. Preliminaries

DES relies upon the encryption techniques of confusion and diffusion. Confusion is accomplished through substitution. Specially chosen sections of data are substituted for corresponding sections from the original data. The choice of the substituted data is based upon the key and the original plaintext. Diffusion is accomplished through permutation. The data is permuted by rearranging the order of the various sections. These permutations, like the substitutions, are based upon the key and the original plaintext.

The substitutions and permutations are specified by the DES algorithm. Chosen sections of the key and the data are manipulated mathematically and then used as the input to a look-up table. In DES these tables are called the S-boxes and the P-boxes, for the substitution tables and the permutation tables, respectively. Usually the S- and P-boxes are combined so that the substitution and following permutation for each round can be done with a single look-up. In order to calculate the inputs to the S- and P-box arrays, portions of the data are XORed with portions of the key. One of the 32-bit halves of the 64-bit data and the 56-bit key are used. Because the key is longer than the data half, the 32-bit data half is sent through an expansion permutation which rearranges its bits, repeating certain bits, to form a 48-bit product. Similarly the 56-bit key undergoes a compression permutation which rearranges its bits, discarding certain bits, to form a 48-bit product. The S- and P-box look-ups and the calculations upon the key and data which generate the inputs to these table look-ups constitute a single round of DES.

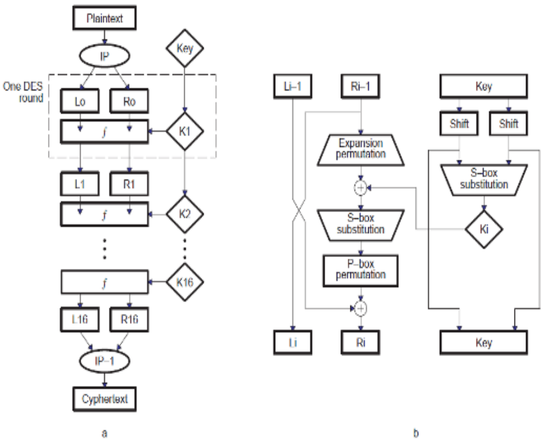


Fig. 1(a) DES Core Algorithm (b) Single Round Expanded

This same process of S- and P-box substitution and permutation is repeated sixteen times, forming the sixteen rounds of the DES algorithm (see Fig. 1(a)). There are also

Dr. D.B.Ojha, R.K.G. Institute of Technology,Gzb.U.P.(India) (corresponding author, phone: 09868580827,e-mail: deobratojha@rediffmail.com)

Mr.Ramveer Singh,R.K.G.Institute of Technology,Gzb.U.P.(India),e-mail: ramveersingh_rana@yahoo.co.in

Mr.Ajay Sharma, R.K.G.Institute of Technology,Gzb.U.P.(India),e-mail: ajaypulast@rediffmail.com

Mr. Awaksh Mishra,R.K.G Engineering College Gzb.U.P.(India),e-mail: awakashmishra@gmail.com

Ms. Swati Garg, R.K.G.Institute of Technology,Gzb.U.P.(India),e-mail: enggswatigarg@yahoo.com

initial and final permutations which occur before and after the sixteen rounds. These initial and final permutations exist for historical reasons dealing with implementation on hardware and do not improve the security of the algorithm. For this reason they are sometimes left out of implementations of DES. They are, however, included in this analysis as they are part of the technical definition of DES.

A. *Triple Data Encryption Algorithm*

Let EK(P.T.) and DK(P.T.) represent the DES encryption and decryption of P.T. using DES key K respectively. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations are used:

1) TDEA encryption operation: the transformation of a 64-bit
block P.T. into a 64-bit block C.T. that is defined as follows: C.T = EK3(DK2(EK1(P.T.))).

2) TDEA decryption operation: the transformation of a 64-bit
block P.T into a 64-bit block C.T. that is defined as follows: C.T. = DK1(EK2(DK3(P.T.))).

The standard specifies the following keying options for bundle (K1, K2, K3)

1) Keying Option 1: K1, K2 and K3 are independent keys.
2) Keying Option 2: K1 and K2 are independent keys and K3 = K1.
3) Keying Option 3: K1 = K2 = K3.

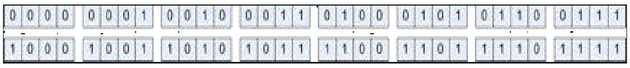
A TDEA mode of operation is backward compatible with its single DES counterpart if, with compatible keying options for TDEA operation,

1) An encrypted plaintext computed using a single DES mode of operation can be decrypted correctly by a corresponding TDEA mode of operation; and
2) An encrypted plaintext computed using a TDEA mode of
operation can be decrypted correctly by a corresponding single DES mode of operation[1,5,6].

III. ATTACK ON DES

A. *Brute Force Attacks*

A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or ciphertext-only attack. Here is an example of a brute force attack on a 4-bit key:



0000	0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110	1111

Given a finite key length and sufficient time, a brute force attack is always successful. Encryption algorithms can become susceptible to brute force attacks over time as CPU speeds increase. Single DES encryption has an effective key length of 56-bits, and any key can be cracked within days using specialized hardware, If a machine could crack one DES key per second, it would take 149 thousand-billion (149 trillion) years to crack a 128-bit AES key.

One challenge associated with a ciphertext-only brute force attack is determining when it is successful. If a 15-byte plaintext of "This is secure" is encrypted with a one-time pad, a brute force attack reveals the plaintext, but it also reveals many additional possible plaintexts, such as "This is purple."

B. *Meet-in-Middle Attack*

Meet-in-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. An example of a successful meet-in-middle attack is the attack versus Double DES.

To improve the strength of 56-bit DES, Double DES (two rounds of DES encryption using two different keys, for a total key length of 112 bits) was suggested.

The meet-in-middle attack is a known plaintext attack; the cryptanalyst has access to both the plaintext and resulting ciphertext. In this example, assume the plaintext is "Cat," and the resulting double DES ciphertext is "BzX." The cryptanalyst wants to recover the two keys (called Key1 and Key2) used for encryption.

The cryptanalyst first conducts a brute force attack on Key1 using all 256 different Single-DES keys to encrypt the plaintext of "Cat" and saves each key and the resulting intermediate ciphertext in a table. The analyst then brute forces Key2, decrypting "BzX" up to 256 times.

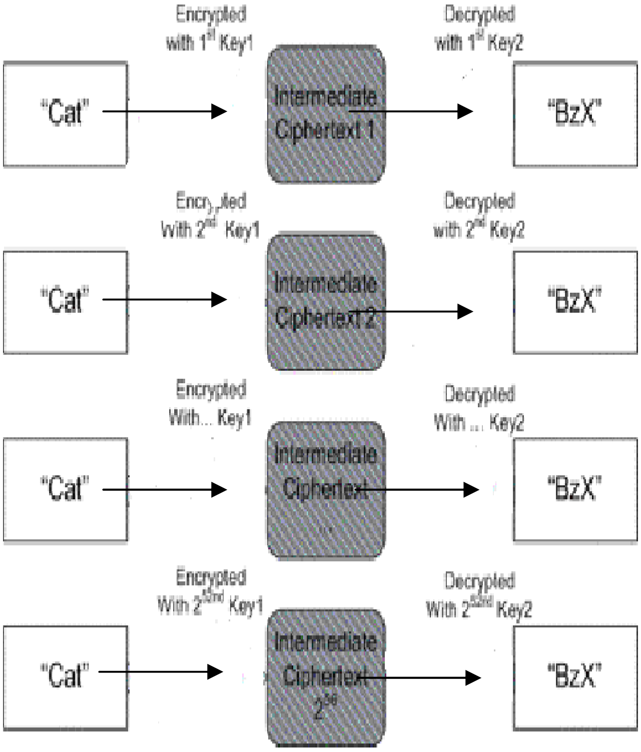


Fig. 2 Meet in middle attack

When the 2nd brute force attack decrypts an intermediate ciphertext that is in the table, the attack is complete and both keys are known to the cryptanalyst. The attack takes 256 plus at most 256 attempts, or a maximum of 257 total attempts. This is far easier than 2112 attempts. As a result of the meet-in-middle attack, Double DES has not been widely used [4].

C. *Linear Cryptanalysis and Differential Cryptanalysis*

Differential cryptanalysis and linear cryptanalysis are related attacks used primarily against iterative symmetric key block ciphers. An iterative cipher (also called a product cipher) conducts multiple rounds of encryption using a subkey for each round. Examples include the Feistel Network used in DES and the State rounds used in AES. In both attacks, a cryptanalyst studies changes to the intermediate ciphertext between rounds of encryption. The attacks can be combined, which is called differential linear cryptanalysis.

A goal of strong encryption is to produce ciphertexts that appear random where a small change in a plaintext results in a random change in the resulting ciphertext. This quality is called diffusion, and any changed ciphertext bit should have a 50% chance of being a 1 or a 0. Both attacks seek to discover non-randomness (cases where the 50% rule is broken) in an effort to discover potential subkeys.

1) Linear Cryptanalysis-

Linear cryptanalysis is a known plaintext attack that requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key. It focuses on statistical analysis against one round of decryption on large amounts of ciphertext.

The cryptanalyst decrypts each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext to seek the least random result. A subkey that produces the least random intermediate cipher6 for all ciphertexts becomes a candidate key (the most likely subkey).

2) Differential Cryptanalysis-

Differential cryptanalysis is a chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm.

A plaintext pair is created by applying a Boolean exclusive or (XOR) operation to a plaintext. For example, XOR the repeating binary string 10000000 to the plaintext. This creates a small difference (hence the term differential cryptanalysis) between the two. The cryptanalyst then encrypts the plaintext and its XORed pair using all possible subkeys, and it seeks signs of non-randomness in each intermediate ciphertext pair. The subkey that creates the least random pattern becomes the candidate key [2, 3].

IV. Our Approach

As we know the security of Data Encryption Standard (DES) is depend on the key, which is use for encryption and decryption. If the attacker get the key, he can be break our code or reveal our plaintext.

In our approach we use a single 64-bit key (K), as we use previously for encryption and decryption in DES. As we know that DES is based on block cipher scheme, suppose our full message (Plaintext) M break in N blocks of plaintext.

Message M = {M1, M2, M3, ………………….., MN}

Here we generate N different key for each block from our previous used key K.

Key K = {K1, K2, K3, …………….............., KN}

Now,
K1 is used for encrypt and decrypt M1.
K2 is used for encrypt and decrypt M2
K3 is used for encrypt and decrypt M3

.
.
.
.
KN is used for encrypt and decrypt MN

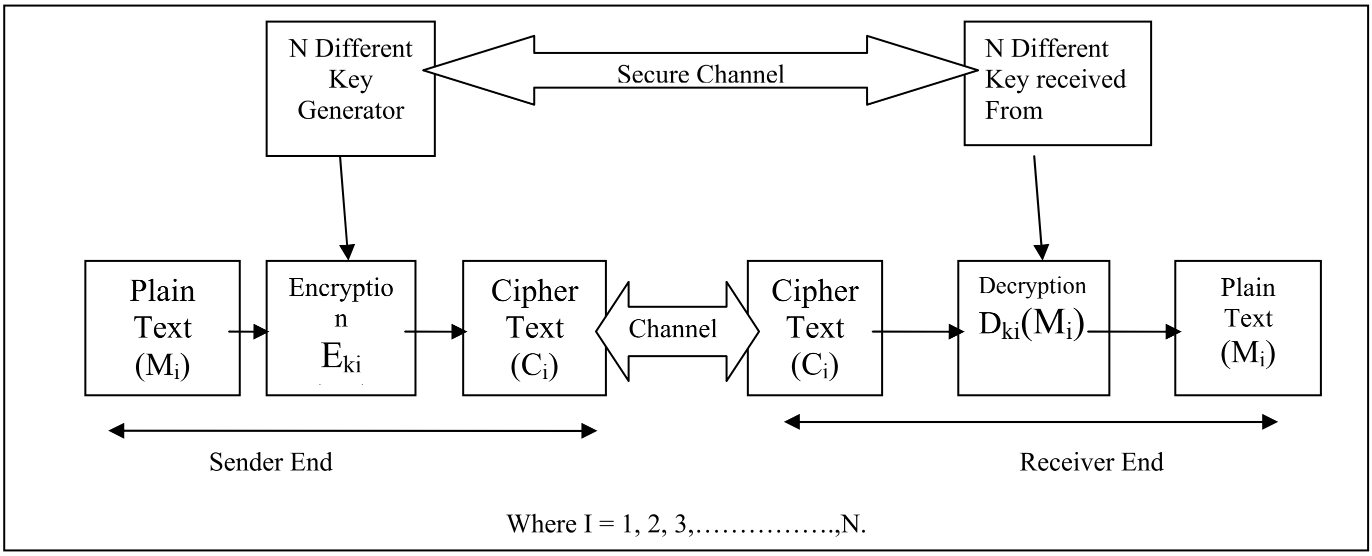


Fig. 3 Proposed Approach for Efficient DES.

The proposed model use multiple symmetric keys instead of one key during the complete session of the data transfer.

$C_i = E_{ki} (M_i)$

Where I = 1,2,3,……..…………..N.

Now the received cipher text Ci is then decrypt with the symmetric key Ki received to the receiver from the sender end through secure channel.

Mi = Dki (Ci)
Where I = 1, 2, 3,…………….. N.

Next, To find complete message we combine all message blocks.
M = M1, M2, M3…………………… MN

This technique behaves like a onetime pad for each block, which enhance the security of DES. Using the variation of key in our approach, we improve the efficiency and security of DES against various attacks like Meet - In - Middle attack.

V. CONCLUSION

Hence, our technique certainly solves the difficulties and ambiguities of above shown attacks in a very simple and efficient manner with optimized security and consumed processing time. As discussed above it removes the main difficulty arises in Brute-force attack, it almost minimizes the cause of meet-in-middle attack. Simultaneously, it nullifies the sure chances of breaking keys with complete permutation of sub key, which is a major disadvantage in linear cryptanalysis and differential cryptanalysis. Hence our approach provides n-times more security due to its way of choosing one key out of N sub-keys randomly.

REFRENCES

[1] M.Matsui: "The First Experimental Cryptanalysis of the Data Encryption Standard", Crypto'94, LNCS 839, Springer, pp. 1-11, 1994.

[2] Eli Biham and Adi Shamir: "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology, vol. 4, pp. 3-72, IACR, 1991.

[3] M. Matsui: "Linear Cryptanalysis Method for DES Cipher", Eurocrypt'93, LNCS 765,Springer, pp. 386-397, 1993.

[4] Orr Dunkelman, Gautham Sekar, and Bart Preneel: "Improved Meet-in-the-Middle Attacks on Reduced-Round DES", To appear in Indocrypt 2007.

[5] DATA ENCRYPTION STANDARD (DES), Federal Information processing standards, Publication 46-3, 1999 October 25.

[6] Alejandro Hevia, Marcos Kiwi, Strength of two data encryption standard implementation under timing attacks, ACM Transactions on Information and System Security (TISSEC), Volume 2, Issue 4 (November 1999) Pages: 416 – 437.

Dr. Deo Brat Ojha, Birth Place & date –Bokaro Steel City, (Jhatkhand), INDIA on 05/07/1975. Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. The degree field is Optimization Techniques In Mathematical Programming. The major field of study is Functional Analysis.

He has more than five year teaching experience as ASSISTANT PROFESSOR & more than eight year research experience. . He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/co-author of more than 30 publications in technical journals and conferences.

Ramveer Singh, Birth Place & Date - Meerut (U.P.), INDIA on 03/09/1983. Bachelor of Engineering from Dr. B.R. Ambedkar university, Agra (U.P.), INDIA in 2003. Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), INDIA in 2007. The major field of study is Cryptography and network security.

He has more than six year experience in teaching and research as ASSIETANT PROFESSOR. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security.

Mr. Singh is the life-time member of Computer Society of India and Computer Science Teacher Association.

Ajay Sharma, Birth Place & Date - Meerut (U.P.), INDIA on 08/08/1978. Master of Technology from Guru Jambheswar University, Hisar (Haryana), INDIA in 2004. The major field of study is Cryptography and network security.

He has more than five year experience in teaching and research as ASSIETANT PROFESSOR. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network Security.

Awakash Mishra, Birth Place & Date - Varanasi (U.P.), INDIA on 10/04/1985. Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2007.

He has more than three year experience in teaching and research as LECTURER. He is working at Raj Kumar Goel Engineering College, Ghaziabad (U.P.), INDIA. The current research area is Symmetric Key Cryptography.

Swati Garg, Birth Place & Date - Muzaffernagar (U.P.), INDIA on 15/08/1983. Bachelor of Engineering from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2005. The major field of study is Cryptography and network security.

She has more than four year experience in teaching and research as LECTURER. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security.

Ms. Garg is the life-time member of Computer Society of India and computer science teacher association.