ISSN:0975-9646



# AN INSTINCTIVE APPROACH FOR SECURE COMMUNICATION - ENHANCED DATA ENCRYPTION STANDARD (EHDES)

Ramveer Singh[1] , Awakash Mishra [2] and D.B.Ojha [3]

[1] *Department of Information Technology, Raj Kumar Goel Institute of Technology, 5th K.M. Stone Delhi – Meerut Road Ghaziabad, U.P., INDIA, 201003,*
**e-mail:** ramveersingh_rana@yahoo.co.in,

[2] *Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P.,INDIA*
**e-mail:** awakashmishra@gmail.com

[3]*Department of Mathematics, Raj Kumar Goel Institute of Technology, 5th K.M. Stone Delhi – Meerut Road Ghaziabad, U.P., INDIA, 201003*
**e-mail:** ojhdb@yahoo.co.in

***Abstract*— In this article, we establish a new architecture of information security for secure or more secure communication in network. Data encryption process is the main precious and important for secure transaction of information. The identity of key is a essential part of data encryption and decryption process. The base of this proposed scheme is by generating more complex keys during the encryption and decryption. Day by day security of data and safe communication is become comprehensively vital. Due to this current era problem of security, we are trying to enhanced security majors and strength of process fussily possible. We emphasis on the security of data as well as key. We generate various secret keys to moderate key bit value of secret key so that key play the imperative role and make our data as much secure for communication. 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.***

***Keywords*— Data encryption Standard, Encryption, Decryption, Secret key, Random Number Generator, Cryptography.***

**Introduction**

Data encryption is the vital role of cryptography process. On the prima facie status, we found two types of cryptography. In this way of its classification:

1. Classical Cryptography
2. Modern Cryptography.

The classical cryptography is based on the substitution and permutation and the modern cryptography is used various way to encrypt the message. In both classifications, unanimously key have pivotal role. So, we always emphasis on security of key as well as data or message. Example: As we do in real life, we store our important things in a briefcase and have the key of briefcase in our pocket. In this manner, the briefcase and key both are very much crucial to secure. If we lose any one either briefcase or key, our system is fail.

To remember the importance of key and data or message, we enhance the security level or strength of Data Encryption Standard (DES) using variation of single key (Symmetric Key). The variation of symmetric key in Data Encryption Standard (DES) provide the high level security of data, just like in asymmetric key. For the security of key, we use another secure channel so that our scheme provide the security strength as higher as possible in Data Encryption Standard.

## I. PREMILINARIES

An Cryptography (or cryptology; from Greek κρυπτός, kryptos, "hidden, secret"; and γράφω, gráphō, "I write", or -λογία, -logia, respectively) is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

Until modern times cryptography was referred almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms which create the encryption and the reversing decryption.

DEFINITION:

A cryptosystem is a five -tuple (M, C, K, E, D), where the following conditions are satisfied:

1. M is a finite set of possible plain texts.
2. C is a finite set of possible ciphertexts.
3. K, the keyspace, is a finite set of possible keys.
4. For each K ε k, there is an encryption rule eK ε E. and a corresponding decryption rule dK ε D. Each eK : M →C and dK : C → M are functions such that dK(eK(x)) = x for every plaintext x ε M.

The main property is property 4. It says that if a plaintext x is encrypted using eK, and the resulting ciphertext is subsequently decrypted using dK, then the original plaintext x results.

*A. Classical Cryptosystem*

Classical ciphers are often divided into transposition ciphers and substitution ciphers.

*I. Substitution ciphers*

In a substitution cipher, letters (or groups of letters) are systematically replaced throughout the message for other letters (or groups of letters). For instance a simple (and therefore easy to crack) encryption would be to substitute each letter for the next letter in the alphabet (a to b, b to c, and so on with z being substituted by a). Using this encryption the sentence "Hello my name is Alice." would be encrypted as "Ifmmp nz obnf jt Bmjdf."

*II. Transposition ciphers*

In a transposition cipher, the letters themselves are kept unchanged, but their order within the message is scrambled according to some well-defined scheme. A lot of transposition ciphers are done according to a geometric design. A simple (and once again easy to crack) encryption would be to write every word backwards. For example "Hello my name is Alice." would now be "olleH ym eman si ecilA." A scytale is a machine that aids in the transposition of methods.

*B. Data Encryption Standard*

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.

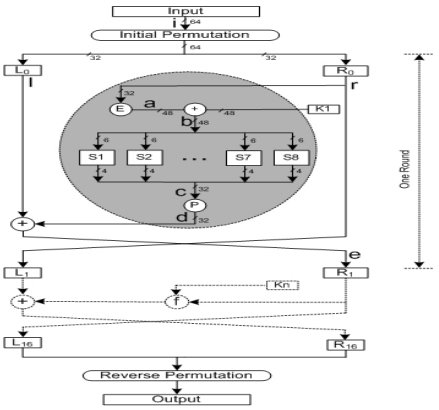


Figure 1: Functionality of one round in DES.

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 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.

## II. OUR APPROACH

In Enhanced Data Encryption Standard (EHDES), we use the block ciphering of data and a symmetric key. As traditional Data Encryption Standard (DES), we also break our data into 64-Bit blocks and use a symmetric key of 56-Bit.

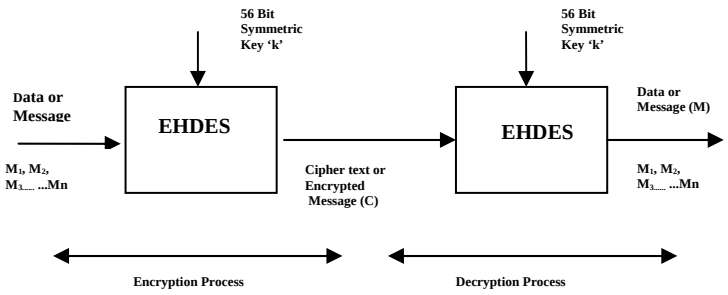


Figure 2: Encryption and Decryption process of EHDES.

### 3.1 Enhanced Data Encryption Standard (EHDES)

Enhanced Data Encryption Standard (EHDES) having three phases.

1. Key Generation. 2. Encryption on Input Data. 3. Decryption on Input Cipher.

#### 3.1.1 Key Generation

In this phase of EHDES, We moderate the initial 56 Bit key using Random Number Generator (RNG) for every block of

message ($M_1$, $M_2$, $M_{3\ ...Mn}$). The new generated 56 Bit keys ($K_{new1,}$ $K_{new2,}$ $K_{new3.....}$ $K_{new\ n}$) from initial key K is used for encryption and decryption for each block of data. For new keys, we generate a random number and implement a function F on generated random number ($N_{RNG}$) and the initial key K.

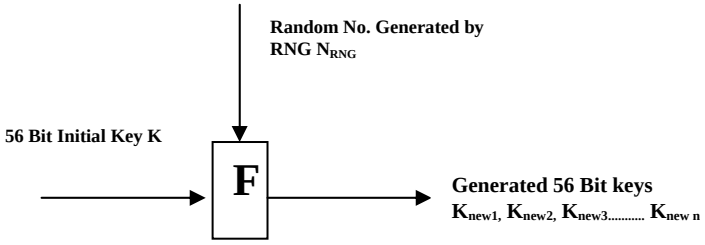


Figure 3: Process of new generated key ($K_{new\ i}$) of EHDES.

### 3.1.2. Encryption on Input Data.

As we know Data Encryption Standard (DES) is based on block cipher scheme. Message breaks in 64 Bit n blocks of plain text.

$$\mathbf{M = \{M_1, M_2, M_{3,.....}, M_n\}}$$

Now, we encrypt our message {$M_1$, $M_2$, $M_{3,.....}$, $M_n$} blocks by each new generated key $K_{new1,}$ $K_{new2,}$ $K_{new3.....}$ $K_{new\ n}$.

### 3.1.3. Decryption on Input Cipher

Decryption is the reverse process of encryption. For decryption, we also used the same key which is used in encryption. On the receiver side, the user also generate the same new key $K_{new\ i}$ for each block of cipher and generate plain text through decryption process of data encryption standard.

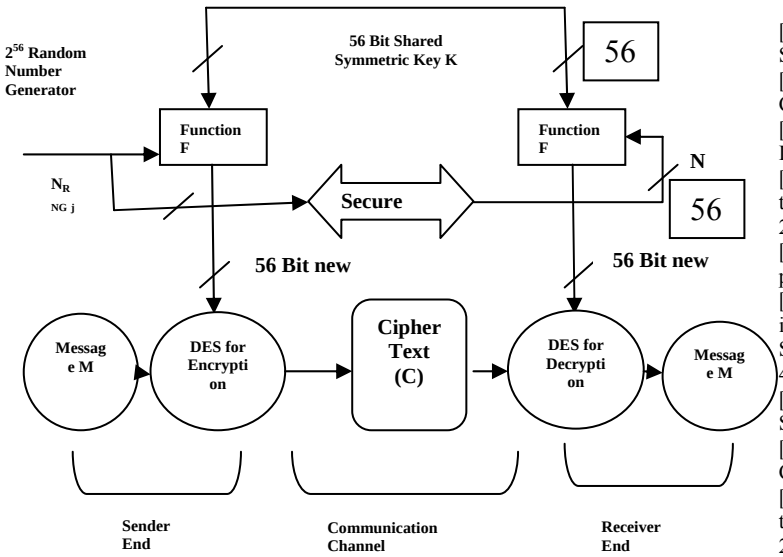


FIGURE 4: FUNCTIONALITY OF EHDES.

## III. SECURITY ANALYSIS

Data Encryption Standard (DES) is the broadly used cryptosystem. Due to its small key in size and simple feistel structure, many cryptanalysts generates various methods, like parallel and exhaustive attack, to break DES. We show analytically that the modified DES (EHDES) is stronger against cryptographic attacks. The variation in new generated key shows that strength of key n-times more than the tradition initial secret key. The base of this method is by generating more complex keys from single 56-bit initial key during the encryption/decryption. It removes the main difficulty arises in Brute-force attack, it almost minimizes the cause of meet-in-middle attack due to single key for each block. 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. Here, we generate n different key for all n different block of data. So, the security level of proposed scheme Enhanced Data Encryption (EHDES) is definitely n times more than Data Encryption Standard (DES).

## IV. CONCLUSION

A commonly accepted definition of a good symmetric key algorithm, such as the DES, is that there exists no attack better than key exhaustion to read an encrypted message. Critics argued that the 56-bit DES key was too short for long-term security, and that expected increases in computer power would soon make a 56-bit key vulnerable to attack by exhaustion. Hence our approach provides n-times more security due to its way of choosing one key out of N sub-keys randomly. This approach provides provable security against both linear and differential attacks. This algorithm is resistant against exhaustive key search.

## REFERENCES

[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.
[7] M.Matsui: "The First Experimental Cryptanalysis of the Data Encryption Standard", Crypto'94, LNCS 839, Springer, pp. 1-11, 1994.
[8] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography" IEEE transactions on Information Theory, 22, 644-654
[9] Orr Dunkelman, Gautham Sekar, and Bart Preneel: "Improved Meet-in-the-Middle Attacks on Reduced-Round DES", to appear in Indocrypt 2007.
[10] Nicolas Courtois, Gregory V. Bard: "Algebraic Cryptanalysis of the Data Encryption Standard", to appear in 11-th IMA Conference, Cirencester, UK, 18-20 December 2007,
[11] Thomas Baignères, Pascal Junod and Serge Vaudenay: "How Far Can We Go Beyond Linear Cryptanalysis", to appear in Asiacrypt 2004, 5-9 Dec. 2004, Korea, LNCS, Springer.

[12] Nicolas Courtois, "Feistel Schemes and Bi-Linear Cryptanalysis", Appears in Crypto 2004, LNCS 3152, pp. 23-40, Springer 2004.
[13] Alex Biryukov, "Christophe de Cannière and Michael Quisquater: On Multiple Linear Approximations". Will be presented at Crypto 2004, August 15-19, LNCS, Springer.
[14] 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, 2010,1793-8201

**Dr. Deo Brat Ojha,** Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. . He is working as a Professor at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/co-author of more than 50 publications in International/National journals and conferences.

**Ramveer Singh**, 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. Persuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than eight year experience in teaching and research as ASSOCIATE 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.

**Awakash Mishra**, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2007. Persuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. He has more than four 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.