iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Performance Comparison of Cryptanalysis Techniques over DES

Anupam Kumar[1], Aman Kumar[2], Sahil Jain[3], P Kiranmai[4]
[1,2,3,4]Dept. of Computer Science, MAIT, GGSIP University, Delhi, INDIA

Abstract--The primary requirement of a good encryption technique is that it is either impossible or difficult to deduce the plaintext out of a ciphertext without the knowledge of key. Cryptanalysis is the technique that violates this requirement. It focuses on either determining the plaintext out of a ciphertext or guessing the key without trying all the possible combinations of key. Since the development of DES (Data Encryption Standard) in 1977 many cryptanalysis methods have been developed and improved to test security provided by it. Two of the widely used techniques are Linear and Differential cryptanalysis. This paper is aimed at comparing the efficiency of these cryptanalysis methods over Brute Force approach based on experimental results carried out on S-DES. The performances of these methods are compared based on time required for guessing the actual key.
Keywords---S-DES, Plaintext, Ciphertext, Linear cryptanalysis, Differential cryptanalysis, Brute Force attack.

I. INTRODUCTION

Cryptology is an art and science of hidden or secret writing. It has two main components: Cryptography and Cryptanalysis[1]. Cryptography is concerned with writing secret messages and making them immune to any type of cryptanalysis attack whereas cryptanalysis is mainly concerned with breaking the codes or extracting the hidden message without the knowledge of key.
Types of attacks:
Cipher Text only: In this type of attack, attacker has access only to the encrypted messages. It can only be applied to simple ciphers.
Known plaintext: In this, attacker has access to plaintexts and corresponding ciphertexts and uses the relation between these two to find out the key, example Linear Cryptanalysis.
Chosen plain text: Attacker obtains the various ciphertext corresponding to the plaintexts.
Chosen cipher text: Attacker obtains various plaintexts corresponding to cipher texts.
Related key Attack: Like the chosen plaintexts, attacks in which the attacker can obtain the ciphertexts encrypted with two keys. These are unknown, but the relationship between them is known such as, they differ in one bit[12].

Computational Resources: Cryptanalysis Techniques are also differentiated based on these factors:
Time: amount of time required to perform various computational tasks such as encryption or finding out relations.
Memory and processing speed: As the number of key bits increases, number of computations required also increases exponentially. Hence, more the computational speed available, less is the time required.
Data: The amount of plaintexts or cipher texts required[12].

Brief Introduction of S-DES and Cryptanalysis Techniques used
DES is a symmetric encryption algorithm. It is a block cipher; meaning a cryptographic key and algorithm are applied to a block of data (64-bit) simultaneously rather than one bit at a time.[5] S-DES (Simplified DES) is the condensed version of DES that was designed to test various cryptanalytic methods. It has similar properties as that of DES but works on smaller block of input (8-bit) and key size of 10 bits[7].
Its components are:

A. Keys

A 10 bit key (K) is used to generate two subkeys (K_1 & K_2) of 8 bits each using two permuted choices (let's say PC_1 & PC_2) and left shift operation on bits[9].

B. Cipher

This is the procedure used for encryption.
$C = E(P, K) = IP^{-1}(r_2(r_1(IP(P))))$
where

©IJRASET: All Rights are Reserved

C = Ciphertext
P = Plaintext
IP = Initial Permutation
r_1 & r_2 = Two rounds of S-DES
The whole process of encryption in diagrammatic form is given below:

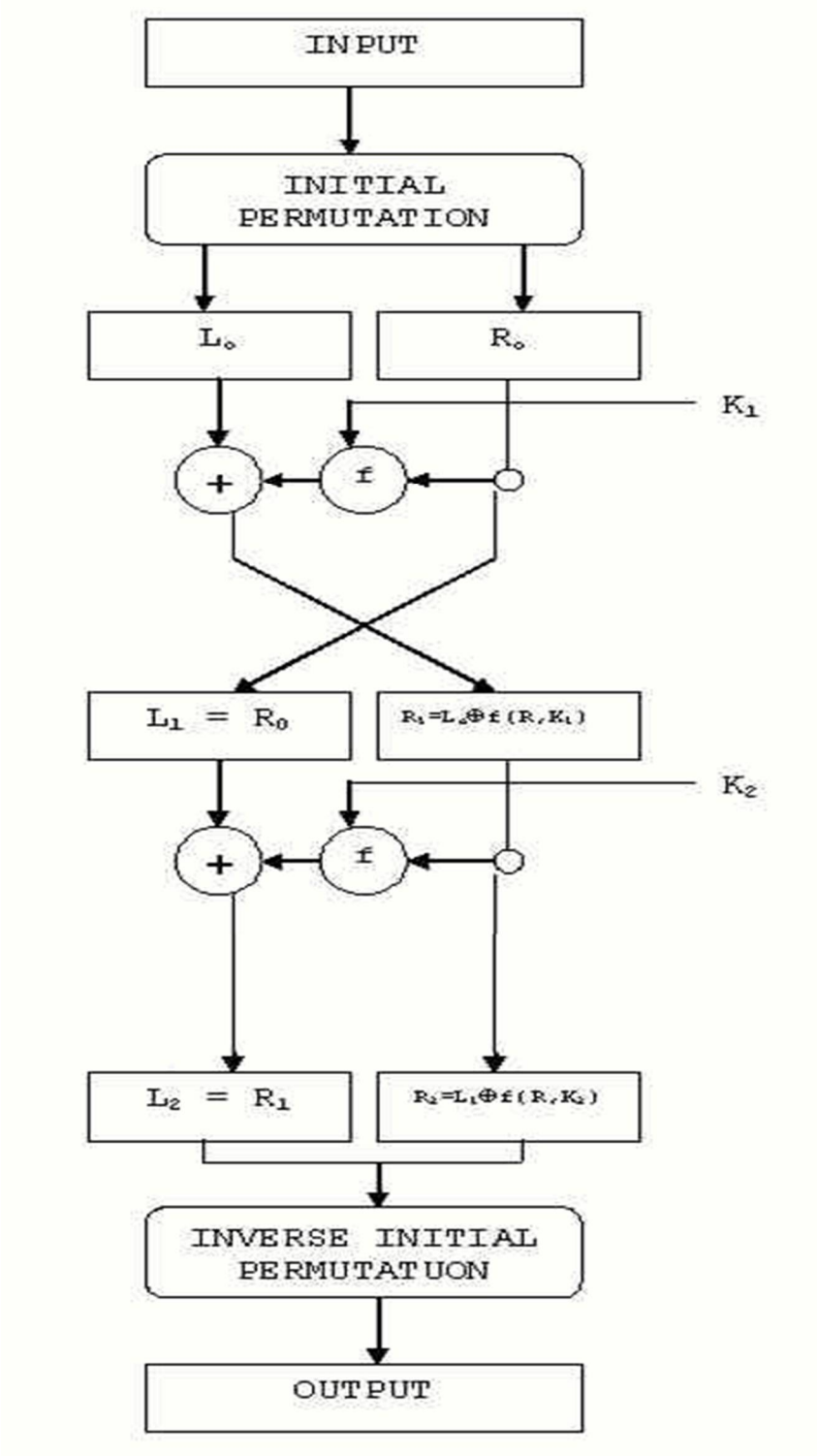


Figure 1. Encryption of S-DES

©IJRASET: All Rights are Reserved

C. Cipher Function f

The function f defined in this algorithm expands the input bits which further passes through S-boxes (S_0 & S_1). The S-boxes take 4 bit as input and produces two bits as output. These s-boxes are the heart of the encryption algorithm. Any cryptanalysis technique tries to guess the S- boxes based on different ciphertext-plaintext pairs[4].

D. Brute Force Approach

As its name suggests the deduction of plaintext is based on trying all the possible combinations of keys. This approach is gaining popularity nowadays due to continuously increasing computational power which makes it easy to try all combinations in less time. Still, it is an inefficient technique for key size more than 56 bits[8].

Hence it is possible to use Brute Force attack on S-DES with a key size of 10 bits trying all combination of keys on ciphertext until the appropriate plaintext is generated[6].

E. Differential Cryptanalysis

It is a chosen plaintext attack in which we try to find out a relationship between the ciphertext produced by two plaintexts. It focuses on statiscal analysis of two inputs and two outputs of the cryptanalytic algorithm that are encrypted under the same key. By careful analysis of the data, probabilities are assigned to different possible keys and the most probable key is identified as the actual key[10].

Based on the relationship between ciphertexts-plaintext pairs a difference distribution table is constructed. The difference distribution table is the core of Differential cryptanalysis. We can gather interesting information from distribution tables. Two of the possibilities are:

We can obtain possible input and output values if their differences are given.

We can obtain the key bits involved in the S-Box using known input pairs and output differences of the S-Box.

Using the two given possibilities we can now obtain the partial subkeys K_1 and K_2. After obtaining the partial subkeys whole key could be obtained easily using 22 possibilities[11].

F. Linear Cryptanalysis

This is a known plaintext attack that requires access to large amount of plaintext and ciphertext pairs that are encrypted using unknown keys. It focuses on statistical analysis against one round of decryption on large number of ciphertexts[11]. The attacker decrypts each cipher text using all possible subkeys for one round of encryption and studies the resulting intermediate cipher text to seek the least random result. A subkey which generate the least random intermediate cipher for all cipher texts is the possible candidate key[3].

It was invented by Mitsuru Matsui. Based on his experimental results it requires 247 known plaintexts.

Two steps involved in Linear cryptanalysis are:

1) *Constructing Linear Equations:* First we construct linear equations involving plaintext, ciphertext, and key bits that have high bias i.e. whose probability of holding is close to either 0 or 1. Mostly, these equations hold a probability of ½. In DES, the analysis is concentrated to the non-linear part of the algorithm i.e. S-Boxes. These linear approximations are combined with other approximations to derive a linear relationship for entire cipher.
2) *Deriving Key Bits:* After obtaining linear equations we can use Matsui's algorithm and known plaintext-ciphertext pairs to guess the key bits involved. Then, we calculate a number of the plaintext-ciphertext pairs out of all taken that satisfy the approximation. Let's call this number T. The partial key whose T has the greatest absolute difference from half the number of plaintext-ciphertext pairs is designated as the most likely set of values for those key bits. This is because it is assumed that the correct partial key will cause the approximation to hold with a high bias[2].

II. WORK DONE

A literature survey of S-DES and cryptanalysis techniques was conducted. To perform cryptanalysis on DES high computation power is needed, also the space and time complexity is higher. Since the performance ratio of DES and S-DES is same, we have chosen the reduced version of DES i.e. S-DES and performed encryption and decryption on it and finally different cryptanalysis techniques on it are implemented and their performance is compared to Brute Force approach. In every cryptanalysis attack performed, the program asks for a predetermined key by the user, if not provided it uses the default key of the program. On the basis of key provided it performs encryption with the help of given I/O table and at last performs cryptanalysis and generates a key and it

©IJRASET: All Rights are Reserved

is possible that it is different from the predetermined key. At last it will calculate the execution time taken to crack the key.

III. TESTING PROCEDURE

We have used Intel processor (i3-core) and 4 GB of memory. The code of S-DES and all cryptanalysis techniques is written in C and compiled on GCC compiler. We made a file containing different bit combinations as key and served this file as input to all the three codes. Then the time is measured to perform cryptanalysis on each combination for every type of attack. The data collected is processed to find out the average time required by each technique and compared with the time required to guess the key using Brute Force approach. The results are provided below.

IV. RESULT

The results show that the Linear cryptanalysis is the fastest of all three techniques and it takes the least time to deduce the plaintext.

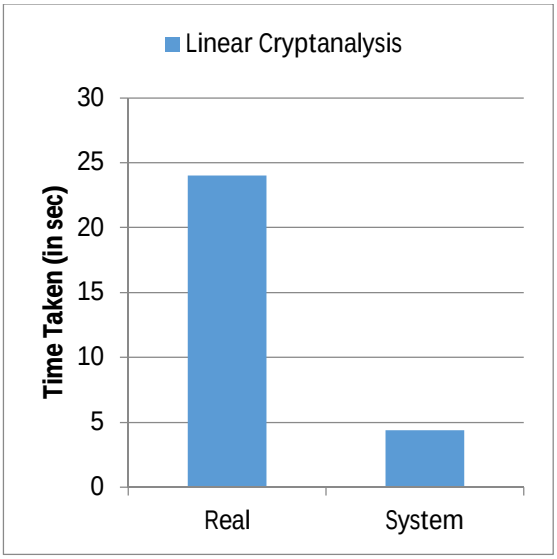


Figure 2. Time analysis of Linear Cryptanalysis

Brute Force attack is the worst of all three as it takes the maximum time.

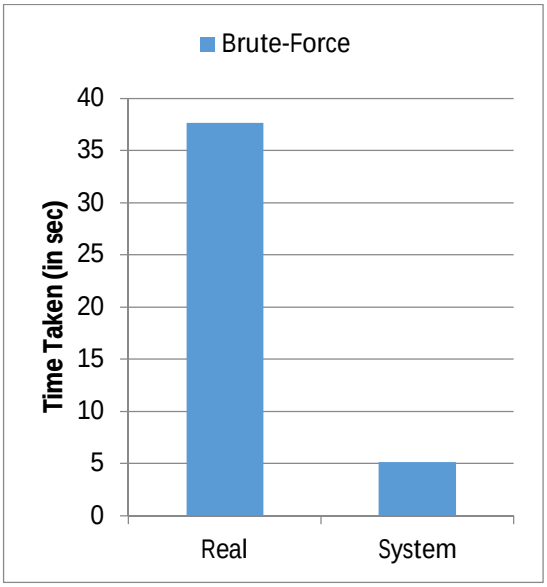


Figure 3. Time analysis of Brute-Force Attack

Differential cryptanalysis lies in between the Linear and Brute Force techniques.

©IJRASET: All Rights are Reserved

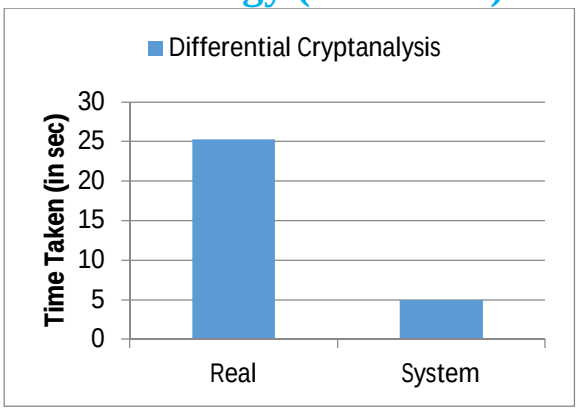


Figure 4. Time analysis of Differential Cryptanalysis

Following data were obtained for all the three attacks over S-DES:-
Linear Cryptanalysis took a total of 24.017 seconds on an average in order to bypass S-DES where as Differential cryptanalysis took 25.268 seconds for the same process.
Brute Force attack took the maximum time for the same work to be done which was 37.64 seconds on an average.
Although the success rate of attacks is high, the probability of success depends greatly on the amount of plaintexts used.

V. CONCLUSION

Linear Cryptanalysis is 35.14% faster as compared to Brute Force attack where as Differential Cryptanalysis is 32.43% faster than Linear Cryptanalysis. Linear and Differential techniques showed almost similar results. Hence, if S-DES is extended to DES the results would be same as the cryptanalysis of DES is mainly centered on S-boxes. Therefore, Linear cryptanalysis would be the best technique for attacking DES. The results show the behavior of the techniques conveying that Linear cryptanalysis is the most efficient of all the three, Differential cryptanalysis is similar to Linear where as the Brute-Force attack is the least efficient of the three. The following graph shows the comparison between all the three techniques on the basis of total time taken by the system by various cryptanalysis techniques over DES.

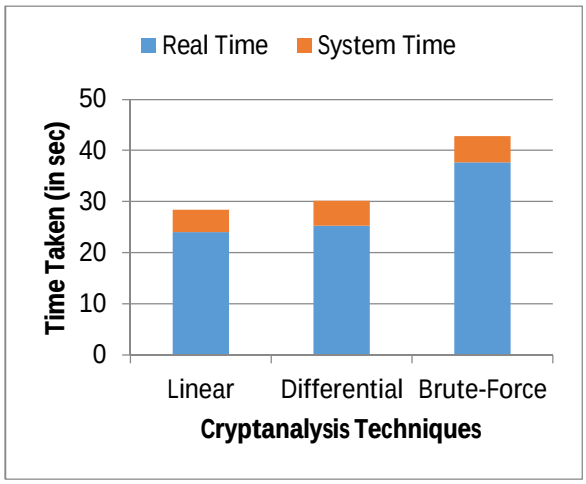


Figure 5. Comparison between various cryptanalysis techniques over S-DES

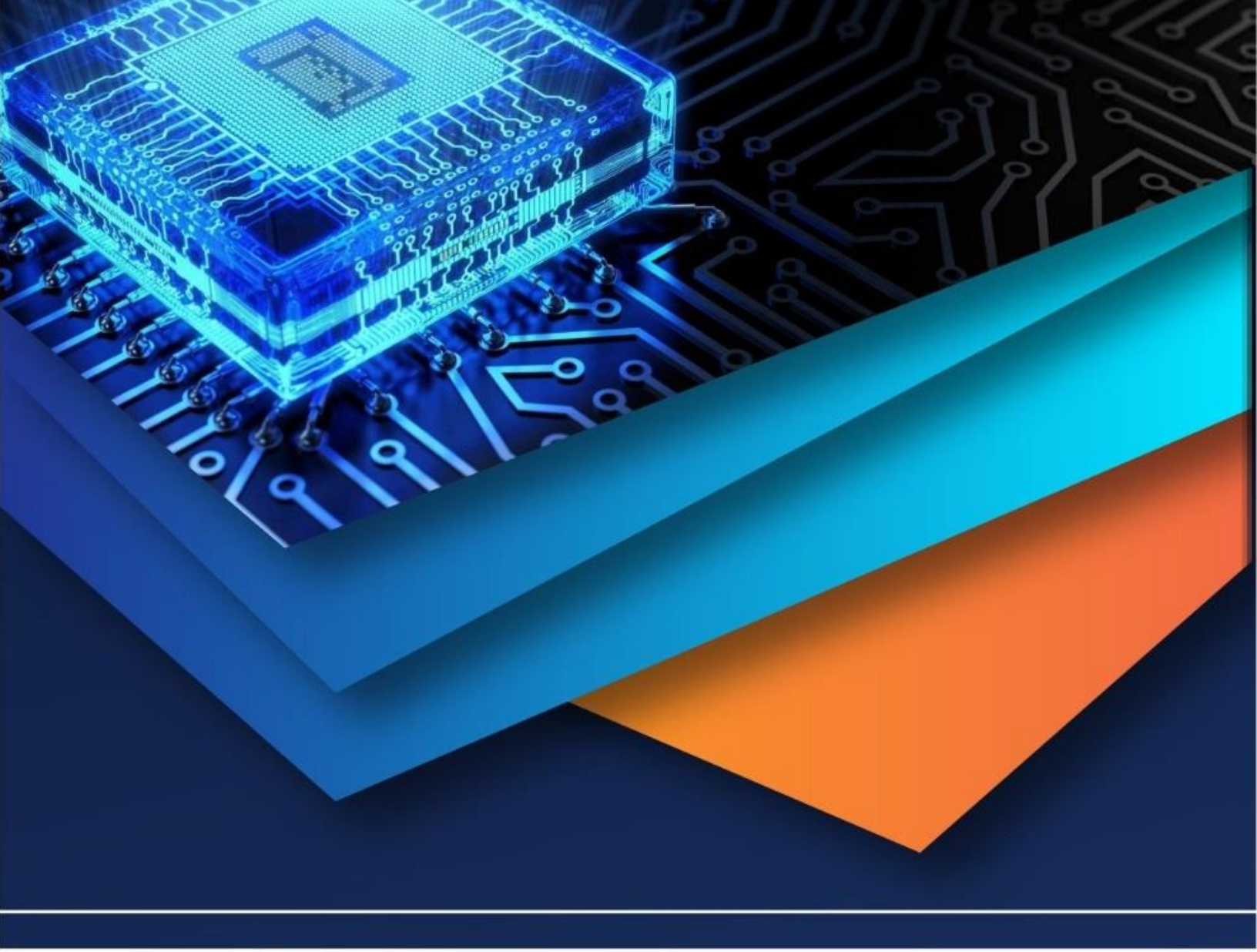
REFERENCES

[1] E. Biham, A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” Journal of Cryptology, Vol. 4, No.1, page 3-72, 1991.
[2] Celine Blondeau and Kaisa Nyberg, ”New Links between Differential and Linear Cryptanalysis”, In T. Johansson and P. Q. Nguyen, editors, EUROCRYPT, Vol. 7881, page 388-404, Springer, 2013.
[3] Mitsuru Matsui, “Linear Cryptanalysis Method for DES Cipher”, In T. Helleseth, editor, EUROCRYPT, Vol. 765, page 386-397, 1993.
[4] M. Matsui, “On correlation between the order of S-boxes and the strength of DES”, In Advances in Cryptology, EUROCRYPT’94, Vol. 950, page 366–375, Springer-Verlag, 1995.
[5] ANSI X3.92, “American National Standard for Data Encryption Algorithm (DEA),” American National Standards Institute, 1981.

©IJRASET: All Rights are Reserved

[6] Nimmi Gupta, ”Implementation of Optimized DES Encryption Algorithm”, International Journal of Computer Technology and Electronics Engineering, Vol.2, no.1, page 82-86, 2010.
[7] Ruth M. Davis, “The Data Encryption Standard” Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, NBS Special Publication 500-27, page 5-9, Feb. 1977.
[8] Vimalathithan. R, Dr.M.L.Valarmathi, ” Cryptanalysis of S-DES using Genetic Algorithm”, International Journal of Recent Trends in Engineering, Vol. 2, No. 4, page 76-79, November 2009.
[9] National Bureau of Standards, “Data Encryption Standard”, Federal Information Processing Standard 46, 1977.
[10] H.M. Heys and S.E. Tavares, "Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis", Journal of Cryptology, Vol. 9, No.1, page 1-19, 1996.
[11] William Stallings, Cryptography and Network Security: Principles and Practices, 2nd ed., Prentice Hall, 1999.
[12] James L. Massey, “An Introduction to Contemporary Cryptology”, IEEE, VOL. 76, NO. 5, page 533-549, MAY 1988.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)