Performance Analysis of DES and Triple DES

Dr. O. Srinivasa Rao
Associate Professor of CSE,
Department of Computer Science and Engineering,
University College of Engineering (Autonomous) Kakinada,
J.N.T University Kakinada, Andhra Pradesh

ABSTRACT
With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. The cryptography is most important aspect of communications security and becoming an important building block for computer security. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. This paper analyses the performance of DES & 3DES which are widely used symmetric encryption algorithms i.e. Data Encryption Standard (DES) and triple Data Encryption Standard (3DES) in terms of time computation of encryption and decryption as well as avalanche effect of the both algorithms

Keywords
Cryptography, DES, Triple DES, Avalanche effect

1. INTRODUCTION
Cryptography is about the design and analysis of mathematical techniques that enable secure communications in the presence of malicious adversaries. The security algorithms are classified into Symmetric Cipher Model and Asymmetric Cipher Model. As this paper presents the performance [9,10,11,13,14] of the DES and 3 DES, this section gives the brief overview of both the algorithms..

2. DATA ENCRYPTION STANDARD

2.1 DES Encryption
The overall scheme for DES [1,2,3,4,16] encryption is illustrated in Figure 2.1. As with any encryption scheme, there are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.

.

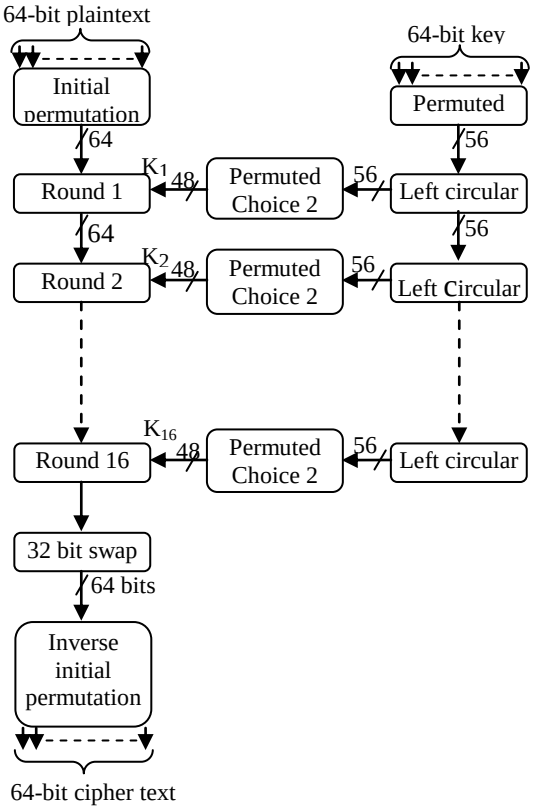


Figure 2.1 General Depiction of DES Encryption Algorithm

Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input*. This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the **pre output**. Finally, the pre output is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit cipher text. With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher.

The right-hand portion of Figure 3.1 shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the sixteen rounds, a *subkey* (K_i) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different sub key is produced because of the repeated shifts of the key bits.

2.2 DETAILS OF SINGLE ROUND:

Figure 2.2 shows the internal structure of a single round of DES. Again, begin by focusing on the left-hand side of the diagram. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right). As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \{ F(R_{i-1}, K_i)$$

The round key K_i *is* 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits (Table 3.2c).The resulting 48 bits are XORed with K_i. This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted .The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

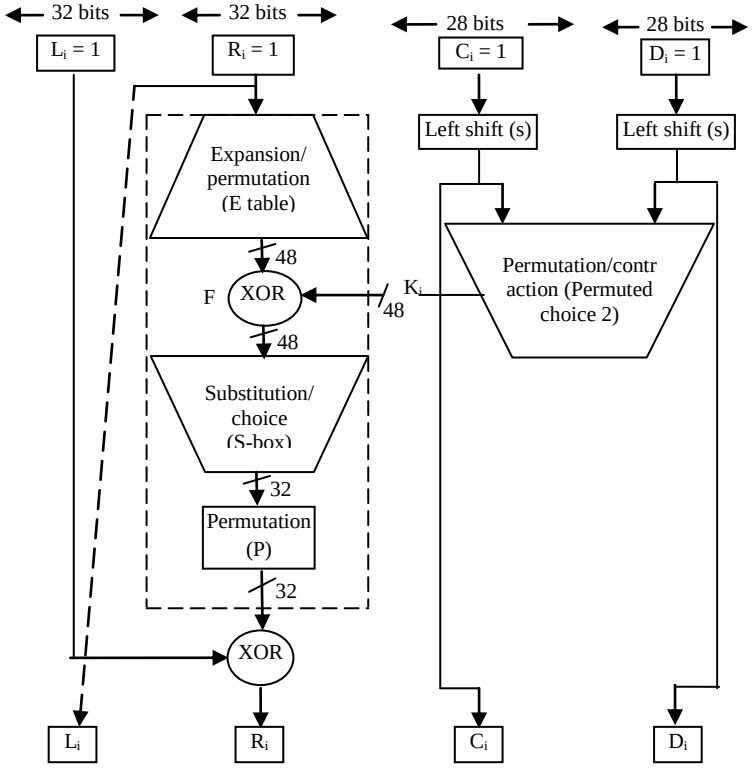


Figure 2.2: Internal Structure of Single round of DES

2.3 DES Decryption

As with any Feistel[17] cipher, decryption uses the same algorithm as encryption, except that application of the sub keys is reversed.

2.4 DES Encryption and Decryption Algorithms

DES Encryption Algorithm

function DES_ Encrypt(M,K) where M = (L, R)
M← IP(M)
for round 1 to 16
do
K_i ← SK(K,round)
L_i ← L xor F(R,K_i)
end
swap (L,R)
M← IP^{-1}(M)
return M,
end

DES Decryption Algorithm

function DES_ Decrypt(C,K) where C = (L, R)
C← IP(C)
for round 1 to 16
do
K_i ← SK(K,round)
L_i ← L xor F(R, K_i)
end
swap (L,R)
end
swap(L,R)
C← IP^{-1}(C)
return C,
end

3. TRIPLE DES

3DES or the Triple Data Encryption Algorithm (TDEA)[18,19,21,22,23] was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. Three-key 3DES has an effective key length of 168 bits and is defined as

$$C = E(K3, D(K2, E(K1, P)))$$

The encryption and decryption process is shown in the figure 2.3

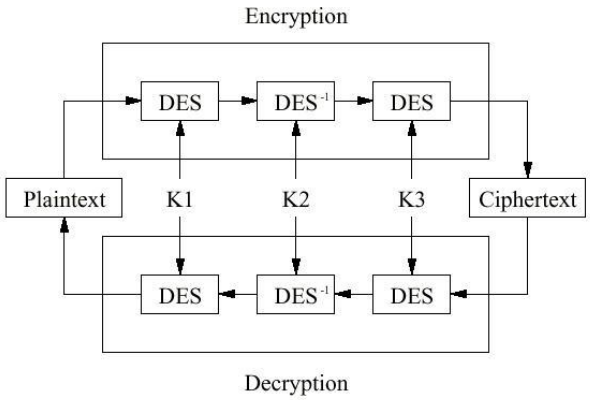


Figure 2.3 The Encryption and Decryption process of 3 DES

The standards define three keying options:

1. The preferred option employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives key space of 3 × 56 = 168 bits.
2. The second option is, it employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives key space of 2 × 56= 112 bits.

3. Third option is, by using a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm. In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods.

3.1 Triple DES Encryption and Decryption Algorithms

Triple DES Encryption Algorithm:
void DES_Encrypt(M,K1)
void DES_Decrypt(M,K2);
void DES_Encrypt(M,K3)
Triple DES Decryption Algorithm :
void DES_Decrypt(M,K1)
void DES_Encrypt(M,K2);
void DES_Decrypt(M,K3)

4. AVALANCHE EFFECT

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text. This is referred to as the **avalanche effect [12]**. This paper presents the avalanche effect and positional based avalanche effect of DES and 3 DES

5. EXPERIMENTAL RESULTS

The encryption and decryption time [6,7] of plain text for DES and 3DES is computed on Intel Core –i5 2410M, 2.3GHz , 3GB RAM , Windows-7 , 64 bit OS using Java and also observed the avalanche effect in both DES and 3 DES

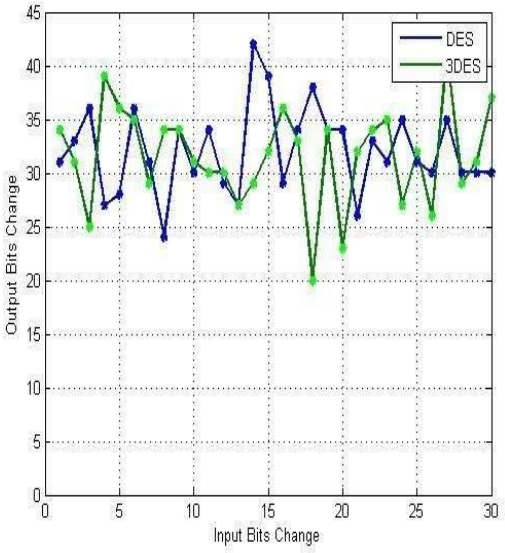
5.1 Time and Avalanche Effect Comparison between DES and 3 DES

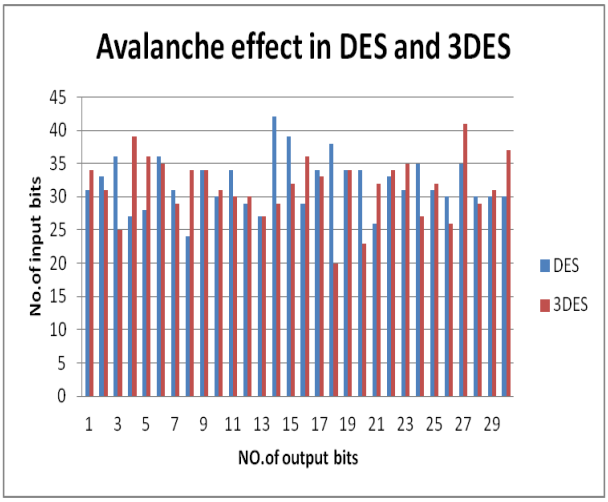
Parameter	DES	TRIPLE DES
Time taken for encryption in milliseconds	92ms	176ms
Time taken for decryption process in milliseconds	10ms	29ms
Avalanche effect (Average)	30bits	32bits
Position based avalanche effect(Average)	32bits	33bits

5.2 Avalanche Effect

No. of input bits changed in Plain Text	No. of bits changed in Cipher Text		No.of input bits changed in Plain Text	No.of bits changed in Cipher Text	
	DES	3DES		DES	3 DES
1	31	34	16	29	36
2	33	31	17	34	33
3	36	25	18	38	20
4	27	39	19	34	34
5	28	36	20	34	23
6	36	35	21	26	32
7	31	29	22	33	34
8	24	34	23	31	35
9	34	34	24	35	27
10	30	31	25	31	32
11	34	30	26	30	26
12	29	30	27	35	41
13	27	27	28	30	29
14	42	29	29	30	31
15	39	32	30	30	37

5.3 Graphical Representation of Avalanche Effect



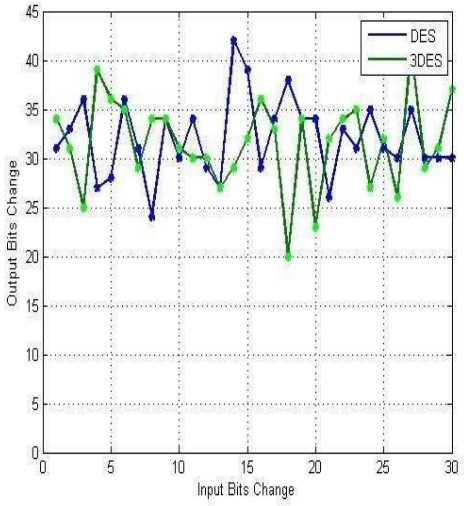


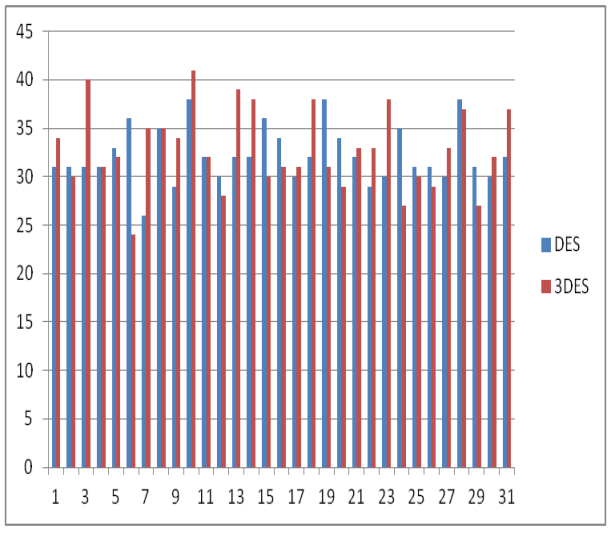
5.4 Position based Avalanche Effect

Change in Input	**No.Of Outputs bits changed**		**Change in Input**	**No.of output bits changed**	
	DES	3DES		DES	3DES
1	31	34	17	30	31
2	31	30	18	32	38
3	31	40	19	38	31
4	31	31	20	34	29

5	33	32	21	32	33
6	36	24	22	29	33
7	26	35	23	30	38
8	35	35	24	35	27
9	29	34	25	31	30
10	38	41	26	31	29
11	32	32	27	30	33
12	30	28	28	38	37
13	32	39	29	31	27
14	32	38	30	30	32
15	36	30	31	32	37
16	34	31			

5.5 Graphical Representation of Position based Avalanche Effect





6. CONCLUSION

According to research done and literature survey on DES and 3DES it can be found that 3DES algorithm is most efficient in terms of avalanche effect and also this paper presents the encryption time is more than the decryption time for both algorithms.

7. REFERENCES

[1] William Stallings, "Cryptography and network Security: Principles and Practice", Pearson Education/Prentice Hall, 5 th Edition.

[2] ISO/IEC 15946-3, Information Technology–Security Techniques–Cryptographic Techniques.

[3] Atul Kahate, "Cryptography and Network Security", McGrawHill, Second Edition.

[4] Behrouz A Forouzan, "Data Communications and Networking", Tata McGraw Hill, Fourth Edition

[5] Deepak Kumar Dakate and Pawan Dubey, "Performance comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering and Technology, Volume 3, No. 8, August 2012, pp. 163-166

[6] Biham, E. and A. Shamir, 1993 Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag Publishing.

[7] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms" IEEE International Conference on Computational Intelligence and Security 2009.

[8] National Bureau of Standards - 3-Data Encryption Standard ,FIPS Publication 46, 1977.

[9] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

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

[11] Shasi Mehlrotra seth, Rajan Mishra " Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011.

[12] Sriram Ramanujam,Marimutha Karuppiah "Designing an algorithm with high avalanche effect" International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[13] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms"

[14] Aamer Nadeem, "A Performance Comparison of Data Encryption Algorithm," IEEE 2005.

[15] Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1.

[16] Data Encryption Standard (DES), FIPS PUB 46-3 - 1999.

[17] Feistel, Cryptography and Computer Privacy, Scientific American, Volume: 28, No.5, 1973.

[18] Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.

[19] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.

[20] NIST: Advanced Encryption Standard (AES) The Federal Information Processing Standards Publication 197. NIST, November 26, 2001.

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (20.9.2006)

[21] NIST: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. NIST, May 2004. http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf (19.9.2006)

[22] NIST: Data Encryption Standard (DES) The Federal Information Processing Standards Publication 46-3. NIST, October 1999. http://www.cerberussystems. com/INFOSEC/stds/fip46-3.htm (19.9.2006)

[23] Network security (second edition) by Kaufman-PerlmanSpeciner