# The Data Encryption Standard (DES)

**Vivek[1] Dr. Hemlata[2]**
[1]Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Central University of Haryana, India

*Abstract*— The Data Encryption Standard (DES) was developed by an IBM team around 1974 and adopted as a national standard in 1877. Since that time, many cryptanalysts have attempted to find shortcuts for breaking the system. We show some of the safeguards against differential cryptanalysis that were built into the system from the beginning, with the result that more than 10 5 bytes of chosen plaintext are required for this attack to succeed.

***Keywords:*** Data Encryption Standard (DES), Cryptography

## I. INTRODUCTION

Cryptography has long been in use by governments, particularly in the realms of military and diplomatic communication. It is hard to imagine military communication without cryptography; cryptanalysis, or secretly deciphering the opponent's messages, is perhaps of even greater value. Much has been written about cryptography by in the military; During the early 1970s, it became apparent that the commercial sector also has a legitimate need for cryptography. Corporate secrets must be transmitted between distant sites, without the possibility of eavesdropping by industrial spies. Personal data on databases need to be protected against espionage and alteration.

A familiar example is the communication between an automatic teller machine (ATM) and a central computer. The user inserts a magnetic card and types a few numbers. The ATM sends messages to the computer. The computer checks the account balance and returns a message authorizing the ATM to dispense funds. Obviously, if these messages are unprotected, a thief can tap the wires, find the message authorizing the dispensing of funds, and send multiple copies of that message to the ATM, thereby "cleaning out" the supply of cash from the ATM.

In the entry 1970s, a banking customer asked IBM to develop a system for encrypting ATM data. With this problem as a starting point, a team was formed from

In this research work, the secret data or document is encrypted before embedding in a cover file. We have compared DES, AES and RSA encryption technique to encrypt a data or document. Let us describe the algorithms one by one. 1) DES: Data Encryption standard (DES) mainly adopted by industry for security products. Algorithm design for encryption and decryption process has been done with same key. This algorithm processes the following steps. DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64 bit block. The plaintext block has to shift the bits around. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation. The plaintext and key will processed by following

a) The key is split into two 28 halves
b) b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
c) c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
d) d. The rotated key halves from step 2 are used in next round.
e) The data block is split into two 32-bit halves.
f) One half is subject to an expansion permutation to increase its size to 48 bits.
g) Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
h) Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
i) Output of step 8 is subject to a P-box to permute the bits.
j) The output from the P-box is exclusive-OR'ed with other half of the data block.
k) The two data halves are swapped and become the next round's input. Algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used.

## II. DIFFERENTIAL CRYPTANALYSIS

1) We present here an overview of the cryptanalytic attack known as "di8erential cryptanalysis." (Within IBM, the attack was formerly known as the
2) ("T attack"). Our purpose in presenting this is to show how the criteria for the S-boxes and the permutation were developed to thwart such attacks.
3) A cryptanalyst trying to break the system may be in possession of large amounts of plaintext and corresponding
4) Now suppose that there is a relation between input di8erences and output di8erences for some S-box. That is, the 64 possible 6-bit inputs to *S,* can be divided into 32 pairs, so that the XOR of the two inputs in each pair is the given nonzero value km [32, 1, 2, 3, 4, 5]. We call this di8erence ñ/„1 , because this is the change of inputs on the
5) ith round for *S I* . For each such pair of inputs, consider the
6) pair of 4-bit outputs, and consider their XOR, called hO„ . Diderential cryptanalysis depends on the fact that many input pairs with a given input diderence h/, give rise to the same output diderence *b 0* . For example, if *II* , is 110100, only eight of the 16 possible values of TO, , can occur, and one value of AO, , (0010) occurs for eight of the 32 input pairs sharing the diderence fi/ , = 110100

## III. DESIGN CRITERIA

We list here the criteria is the S-boxes and the permutation *P*, which were used in the original specifications, and which are satisfied by the design of DES.

 

The relevant criteria for the S-boxes are as follows:

1) (S-1) Each S-box has six bits of input and four bits of output. (This was the largest size that we could accommodate and still fit all of DES onto a single chip in 1974 technology.)
2) (S-2) No output bit of an S-box should be too close to a linear function of the input bits. (That is, if we select any output bit position and any subset of the six input bit positions, the fraction of inputs for which this output bit equals the XOR of these input bits should not be close to 0 or 1, but rather should be near 1/2.)
3) (S3) If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained exactly once as the middle four input bits range over their 16 possibilities.
4) (S-4) If two inputs to an S-box dider in exactly one bit, the outputs must dider in at least two bits. (That is, if |Af „| = 1, then | AO | * 2, where |x| is the number of 1-bits in the quantity x.)
5) (S-5) If two inputs to an S-box differ in the two middle bits exactly, the outputs must dider in at least two bits. (If fi/= 001100**,** then |AO, | * 2.)
6) (S-6) If two inputs to an S-box dider in their first two bits and are identical in their last two bits, the two outputs must not be the same. (If fif,, = **11xy00,** where x and y are arbitrary bits, then *TO . r* 0.)
7) (S-7) For any nonzero 6-bit difference between inputs, *Al; q,* no more than eight of the 32 pairs of inputs exhibiting Af. may result in the same output diderence $\Delta O$
8) (S-8) Similar to (S-7), but with stronger restrictions in the case fiO, = 0, for the case of three active S-boxes on round *i.* See the discussion below.

Other criteria dealt with ease of implementation; those presented above are the only cryptographically relevant criteria.

– The analysis is similar to the case of two active S-boxes previously discussed. The three S-boxes have a total of 14 input bits, which we label as in. The labeled bits such as a and b are understood to be XORs of input
– bits, i.e., part of *km.* Since finn, , = Am,, $_1$ = 0, we must have AO,,, = 0 for all *k.* Since y — 1 is inactive, the leftmost two bits of Af,, are 0. That fact, together with
– *lsO* . — 0 and criterion (S-3), enable us to conclude (as we did in the case of two active S-boxes) that the rightmost
– bit of d/ is 1. Similarly, the $\Delta I_{i,i+1}$ rightmost two bits of
– are 0, and the leftmost bit is 1. So far, our knowledge of the input bits is as summarized in Figure 1(b).
– Applying (S-6) to $S+_2$, we find that j = 0. Then, applying (S-3) to $S+_{,,}$ we find that e = 1, so our information is as in Figure 1(c). That is,
– *6I* = 0 0 c d 1 1,
– *b I* +, = 1 1 g h 1 0,
– *b I* + = 1 0 k m 0 0.

## IV. AES:

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10,12 and 14 round depending on key size as shown in Figure-3. .it can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. The following steps processed in AES algorithm

### *A. Twa active S-boxes*

Suppose first that round *i* has exactly two active S-boxes and that they are adjacent, *S* and S ". (The nonadjacent case is similar to the case of one active S-box, which is treated below.) Because *S* , is inactive on this round, we know that the two left-hand bits of Af, are zero; because *S* , $_2$ is inactive on this round, the two right-hand bits of Af" „ are zero. We claim that either *ñQ* 0 or AO; , $_1$ 0 (or both); the proof is by contradiction. If $\frac{\Delta O_{i,j}}{\Delta I_{i,j}}$ = 0, then (S-3) and the fact that the left-hand two bits O are 0 together imply that the rightmost bit *ot* df, is 1. [We know that the leftmost bit is 0. If the rightmost bit were also 0, this would imply that for the two inputs to *St* on round *i* in the two decipherments, m and m', the leftmost and rightmost input bits of S would be fixed. Some of the other four bits are varied, however. (S-3) implies that the two outputs must be diderent, so $TO_{\langle V} \neq$ This 0. contradicts our assumption, so we conclude the rightmost bit is 1.] Because of the sharing of message bits, the rightmost bit of Af,g is also the second bit from the left of Af,,,,. Similarly, if fiOq,, = 0, then (S-3) and the fact that the two right-hand bits of dfq,, are 0 imply that the leftmost bit of ñf,q+ is 1. Combining these facts: if $\Delta O_{i,j}$ -- *ISO* , --- 0, then Afq,, is of the fomi llxytEi. In this case, (S-6) implies that *bO;j,* 0. The conclusion is that we cannot have *60 --- i!sO* ,, --- 0.

Remembering that the bits of ñO;,,, *dO,,,,,* are part of *f(k , m,) @ f{k,,, m,')* --- *bm,,, @ bm,,*

This contributes to our conclusion that there will be a large number of active S-boxes over the course of the 12-round or 16-round pattern

## V. CONCLUSION

In Data communication, encryption algorithm plays an important role. Our research work surveyed the existing encryption techniques like AES, DES algorithms along with LSB substitution technique. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm.

## REFERENCES

[1] A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique B. Padmavathi1 , S. Ranjitha Kumari2
[2] Data Encryption Standard," *Federal Information Processing Standards Publication* 7Vo*. 46,* National Bureau of Standards, January 15, 1977.
[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," J. *Cryptol.* 4, 3—72 (1991).

 