What is DES?
These days, security is the primary concern for everyone in IT. Given that $155 billion in expenditure on information security and risk management is expected to increase to $172 billion in 2022, according to Gartner, it must be. While there are many tools you can purchase to protect your data, encryption is one security tool that every computer user should be familiar with.
Initial Permutation (IP)
The basic text is broken up into smaller, 64-bit-sized pieces. Before the first round, the IP is conducted. The transposition process' implementation is described in this step. For instance, the first bit is replaced by the 58th bit, the second bit by the 50th bit, and so on. Left Plain Text (LPT) and Right Plain Text (RPT) are the two equal 32-bit halves of the final 64-bit text.

Step 1: Key Transformation

We already know that the DES algorithm employs a 56-bit key, which is created by removing every bit from a 64-bit key's eighth place. A 48-bit key is produced in this stage. The 56-bit key is divided into two equal halves, with the number of rounds determining how many times the bits are circularly moved to the left.

As a result, the bits in the key are all rearranged. It is clear that some bits are lost during the shifting procedure, resulting in a 48-bit key. Compression permutation is the procedure in question.

Step 2: Expansion Permutation

Let's have a look at a 32-bit RPT that is produced at the IP step. It is increased from 32 to 48 bits in this stage. The RPT of 32-bit size is divided into 8 chunks of 4 bits each, with an additional 2 bits added to each chunk. The bits are then permuted among one another to produce 48-bit data. The 48-bit key acquired in step 1 and the 48-bit enlarged RPT are combined using an XOR function.

Triple DES Algorithm
Triple DES uses the DES cipher in triple and is a symmetric key-block cipher. It encrypts with key number one (k1), decrypts with key number two (k2), and then encrypts with key number three (k3).

Main Points

The DES algorithm had to be replaced by the NIST because, in light of the more powerful processing of modern computers, its 56-bit key lengths were insufficient. Because key size affects encryption strength, DES became obsolete due to continual advancements in computing technology. When the new encryption issues arose, 56-bit encryption was no longer sufficient.
The fact that DES is no longer the NIST federal standard should not be taken to imply that it is no longer in use. Even though Triple DES is still in use today, it is regarded as an old encryption algorithm. Keep in mind that starting in 2024, NIST intends to outlaw all variations of Triple-DES.
DES Algorithm Procedure
In plain English, DES transforms 64-bit plain text into a 64-bit cipher text. The same key is also utilized to decode the text because asymmetric methods are being employed.

The following steps comprise the algorithmic process:

The 64-bit plain text block is first sent to an initial permutation (IP) function to start the process.
The plain text is subsequently subjected to the initial permutation (IP).
The Left Plain Text (LPT) and Right Plain Text (RPT) portions of the permuted block are then created by the initial permutation (IP).
There are 16 rounds of encryption for each LPT and RPT.

Finally, the LPT and RPT are reunited, and the newly combined block is subjected to a Final Permutation (FP).
This procedure provides the necessary 64-bit ciphertext as a result.
The phase of the encryption process (step 4, above) is further divided into the following five stages:

Key transition
Expansion permutation
XOR and swap
S-Box
P-Box permutations
We employ the same procedure for decryption and arrange the 16 round keys in the other direction.

Let’s study about the several ways that DES might operate next so that we can better comprehend what it is.

Modes of Operation for DES
There are five main modes of operation available to experts utilizing DES.

(ECB) Electronic Codebook. Each 64-bit block is separately encrypted and decrypted.
CBC, or cypher block chaining. Each 64-bit block employs an Initialization Vector (IV) and is dependent on the previous one.
CFB, or Cypher Feedback. The previous unit of cipher text serves as the input for the encryption algorithm, which generates pseudorandom output that is then XORed with the plaintext to create the following unit of cipher text.
OFB (Output Feedback). similar to CFB, but where the input for the encryption technique is the result of the previous DES
CTR, or counter. An encrypted counter is XORed with each plaintext piece. Following that, the counter gets increased for each additional block.
We’ll then deepen our understanding of DES by examining its implementation and testing.

Testing and Implementation of DES
A security provider is required for DES deployment. Even if there are several suppliers to choose from, choose one is the crucial first step in deployment. Your choice could be influenced by the language you’re working in, such as MATLAB, Java, Python, or C.

Once you’ve selected a provider, you must pick whether to use a plaintext or byte array to construct a key that will be randomly created by the Key Generator.

To make sure the encryption is used correctly, it is also crucial to test it