Data Encryption Standard (DES)

The Data Encryption Standard (DES) is an outdated symmetric-key method of data [encryption](http://searchsecurity.techtarget.com/definition/encryption).

DES works by using the same [key](http://searchsecurity.techtarget.com/definition/key) to encrypt and decrypt a message, so both the sender and the receiver must know and use the same [private key](http://searchsecurity.techtarget.com/definition/private-key).

The Data Encryption Standard is a [block cipher](http://searchsecurity.techtarget.com/definition/block-cipher), meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one [bit](http://whatis.techtarget.com/definition/bit-binary-digit) at a time. To encrypt a [plaintext](http://searchsecurity.techtarget.com/definition/plaintext) message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit [ciphertext](http://whatis.techtarget.com/definition/ciphertext) by means of permutation and substitution.

The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.

DES uses a 64-bit key, but eight of those bits are used for parity checks, effectively limiting the key to 56-bits. Hence, it would take a maximum of 2^56, or 72,057,594,037,927,936, attempts to find the correct key.