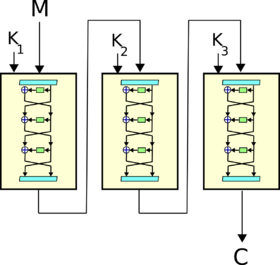
# Triple DES

En [criptografía](http://es.wikipedia.org/wiki/Criptograf%C3%ADa) el Triple DES se llama al [algoritmo](http://es.wikipedia.org/wiki/Algoritmo) que hace triple cifrado del [DES](http://es.wikipedia.org/wiki/Data_Encryption_Standard). También es conocido como TDES o 3DES, fue desarrollado por [IBM](http://es.wikipedia.org/wiki/IBM) en 1998.

**ALGORITMO**

No llega a ser un cifrado múltiple, porque no son independientes todas las subclases. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos claves diferentes se aumenta el tamaño efectivo de la clave.

La variante más simple del Triple DES funciona de la siguiente manera:

C = E_{DES}^{k_3}\Bigg(D_{DES}^{k_2}\bigg(E_{DES}^{k_1}(M)\bigg)\Bigg)

Donde M es el mensaje a cifrar y k_1, k_2 y k_3 las respectivas claves DES. En la variante 3TDES las tres claves son diferentes; en la variante 2TDES, la primera y tercera clave son iguales.

**SEGURIDAD**

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, TDES fue elegido como forma de agrandar el largo de la clave sin necesidad de cambiar de algoritmo de [cifrado](http://es.wikipedia.org/wiki/Criptograf%C3%ADa). Este método de cifrado es inmune al [ataque por encuentro a medio camino](http://es.wikipedia.org/wiki/Ataque_por_encuentro_a_medio_camino), doblando la longitud efectiva de la clave (112 bits), pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES. Por tanto, la longitud de la clave usada será de 192 bits, aunque como se ha dicho su eficacia solo sea de 112 bits.

**USOS**

El Triple DES está desapareciendo lentamente, siendo reemplazado por el algoritmo [AES](http://es.wikipedia.org/wiki/Advanced_Encryption_Standard). Sin embargo, la mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo Triple DES (anteriormente usaban el DES). Por su diseño, el DES y por lo tanto el TDES son algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad.

# Triple DES

In [cryptography](http://en.wikipedia.org/wiki/Cryptography), Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) [block cipher](http://en.wikipedia.org/wiki/Block_cipher), which applies the [Data Encryption Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES) cipher algorithm three times to each data block.

The original DES cipher's [key size](http://en.wikipedia.org/wiki/Key_size) of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made [brute-force attacks](http://en.wikipedia.org/wiki/Brute-force_attack) feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Name of the algorithm

The earliest standard that defines the algorithm (ANS X9.52, published in 1998) describes it as the "Triple Data Encryption Algorithm (TDEA)" — i.e. three operations of the Data Encryption Algorithm specified in ANSI X3.92 — and does not use the terms "Triple DES" or "DES" at all. FIPS PUB 46-3 (1999) defines the "Triple Data Encryption Algorithm (TDEA)", but also uses the terms "DES" and "Triple DES". It uses the terms "Data Encryption Algorithm" and "DES" interchangeably, including starting the specification with:

***The Data Encryption Standard (DES) shall consist of the following Data Encryption Algorithm (DES) [***[***sic***](http://en.wikipedia.org/wiki/Sic)***] and Triple Data Encryption Algorithm (TDEA, as described in ANSI X9.52).***

NIST SP 800-67 (2004, 2008[[4]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-3)) primarily uses the term TDEA, but also refers to "Triple DES (TDEA)". ISO/IEC 18033-3 (2005) uses "TDEA", but mentions that:

***The TDEA is commonly known as Triple DES (Data Encryption Standard).***

None of the standards that define the algorithm use the term "3DES".

Algorithm

Triple DES uses a "key bundle" which comprises three DES [keys](http://en.wikipedia.org/wiki/Key_(cryptography)), K1, K2 and K3, each of 56 bits (excluding [parity bits](http://en.wikipedia.org/wiki/Parity_bit)). The encryption algorithm is:

**ciphertext = EK3(DK2(EK1(plaintext)))**

I.e., DES encrypt with K1, DES *decrypt* with K2, then DES encrypt with K3.

Decryption is the reverse:

***plaintext = DK1(EK2(DK3(ciphertext)))***

I.e., decrypt with K3, *encrypt* with K2, then decrypt with K1.

Each triple encryption encrypts [one block](http://en.wikipedia.org/wiki/Block_size_(cryptography)) of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using [keying option](http://en.wikipedia.org/wiki/Triple_DES#Keying_options) 2, and provides [backward compatibility](http://en.wikipedia.org/wiki/Backward_compatibility) with DES with keying option 3.

Keying options

The standards define three keying options:

* Keying option 1: All three keys are independent.
* Keying option 2: K1 and K2 are independent, and K3 = K1.
* Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against[meet-in-the-middle attacks](http://en.wikipedia.org/wiki/Meet-in-the-middle_attack).

Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the [National Institute of Standards and Technology](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST),[[5]](http://en.wikipedia.org/wiki/Triple_DES" \l "cite_note-4) and is not supported by ISO/IEC 18033-3.

### Other terms used to refer to the keying options

"Keying option *n*" is the term used by the standards (X9.52, FIPS PUB 46-3, SP 800-67, ISO/IEC 18033-3) that define the TDEA. However, other terms are used in other standards and related recommendations, and general usage.

* For keying option 1:
  + 3TDEA, in NIST SP 800-57[[6]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-57-5) and SP 800-78-2[[7]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-78-6)
  + Triple-length keys, in general usage[[8]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-cryptography_world-7)[[9]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-IBM-8)
* For keying option 2:
  + 2TDEA, in NIST SP 800-57[[6]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-57-5) and SP 800-78-1[[7]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-78-6)
  + Double-length keys, in general usage[[8]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-cryptography_world-7)[[9]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-IBM-8)

Encryption of more than one block

As with all block ciphers, encryption and decryption of multiple blocks of data may be performed using a variety of [modes of operation](http://en.wikipedia.org/wiki/Modes_of_operation), which can generally be defined independently of the block cipher algorithm. However, ANS X9.52 specifies directly, and NIST SP 800-67 specifies via SP 800-38A[[10]](http://en.wikipedia.org/wiki/Triple_DES" \l "cite_note-9) that some modes shall only be used with certain constraints on them that do not necessarily apply to general specifications of those modes. For example, ANS X9.52 specifies that for [cipher block chaining](http://en.wikipedia.org/wiki/Cipher_block_chaining), the[initialization vector](http://en.wikipedia.org/wiki/Initialization_vector) shall be different each time, whereas ISO/IEC 10116[[11]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-10) does not. FIPS PUB 46-3 and ISO/IEC 18033-3 define only the single block algorithm, and do not place any restrictions on the modes of operation for multiple blocks.

Security

In general, Triple DES with three independent keys ([keying option](http://en.wikipedia.org/wiki/Triple_DES#Keying_options) 1) has a key length of 168 bits (three 56-bit DES keys), but due to the [meet-in-the-middle attack](http://en.wikipedia.org/wiki/Meet-in-the-middle_attack), the effective security it provides is only 112 bits. Keying option 2 reduces the key size to 112 bits. However, this option is susceptible to certain [chosen-plaintext](http://en.wikipedia.org/wiki/Chosen-plaintext_attack) or [known-plaintext](http://en.wikipedia.org/wiki/Known-plaintext_attack) attacks,[[12]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-11)[[13]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-12) and thus, it is designated by NIST to have only 80 bits of security.[[6]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-57-5)

The best attack known on keying option 1 requires around 232 known plaintexts, 2113 steps, 290 single DES encryptions, and 288 memory[[14]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-13) (the paper presents other tradeoffs between time and memory). This is not currently practical and NIST considers keying option 1 to be appropriate through 2030.[[6]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-NIST_SP_800-57-5) If the attacker seeks to discover any one of many cryptographic keys, there is a memory-efficient attack which will discover one of 228 keys, given a handful of chosen plaintexts per key and around 284 encryption operations.[[15]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-14)

Usage

The [electronic payment](http://en.wikipedia.org/wiki/Electronic_payment) industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. [EMV](http://en.wikipedia.org/wiki/EMV)).[[16]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-15)[[17]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-16)

[Microsoft OneNote](http://en.wikipedia.org/wiki/Microsoft_OneNote) and [Microsoft Outlook](http://en.wikipedia.org/wiki/Microsoft_Outlook) 2007 use Triple DES to password protect user content.[[18]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-17)[[19]](http://en.wikipedia.org/wiki/Triple_DES#cite_note-18)