Common symmetric ciphers

The following table describes a few of the more common symmetric ciphers. Of course, many other ciphers exist, and more are being developed all the time.

Cipher	Description
DES	The Data Encryption Standard is a block cipher operating on 64-bit blocks of data. DES uses a 56-bit key and 16 rounds of processing to compute the ciphertext. DES was developed in the mid-1970s and standardized as an official Federal Information Processing Standard in 1978. Detractors of DES worried that the National Security Agency included "back doors" in the standard, limiting its acceptance. DES has been cracked and is generally considered insecure for most purposes.
Triple DES (sometimes called 3DES)	Triple DES, or TDES, is simply the application of the DES cipher three times with different keys for each round. This scheme enables superior encryption without requiring significant changes in software or hardware. A variant of TDES called 2TDES uses the same key for rounds one and three, reducing its effective security. The 2TDES variant remains popular in the electronics payment industry, despite the waning use of TDES everywhere else.
AES	The Advanced Encryption Standard is a block cipher operating on 128-bit blocks of data. AES can use a 128-, 192-, or 256-bit key and 10, 12, or 14 rounds of processing to compute the ciphertext. AES was developed in the late 1990s and standardized as an official Federal Information Processing Standard in 2001. It is a popular cipher, and its use is growing.
AES256	This is simply the AES cipher using 256-bit keys.
Rijndael	Essentially the same as the AES cipher. More precisely, Rijndael is AES with both key and block sizes between 128 and 256 bits, in multiples of 32 bits. Visit http://rijndael.info/audio/rijndael_pronunciation.wav for a humorous explanation of how to pronounce this cipher's name.
Blowfish	This is a public-domain block cipher developed by Bruce Schneier in 1993. He designed it to be a replacement for DES, without the encumbrances of patents and (he hoped) without the technical flaws of DES. Blowfish uses 64-bit blocks and variable-length keys with zero- to 448-bit keys. As of this writing, there are no known attacks against the Blowfish cipher.
TwoFish	Related to Blowfish, the TwoFish cipher is a symmetric block cipher. It uses 128-bit blocks and key sizes up to 256 bits. It was developed by Bruce Schneier and collaborators. Like Blowfish, it is a non-patented, public-domain cipher.

IDEA	The International Data Encryption Algorithm is a block cipher developed in 1991 as a replacement for DES and TDES. IDEA operates on 64-bit blocks using a 128-bit key. It performs a series of eight identical transformations, each called a “round.” It finishes with an output transformation called a “half-round.” Thus, IDEA is said to perform 8.5 rounds (compared to the 16 for DES). IDEA is patented, though generally free to use. It is not as popular as AES, Blowfish, or other algorithms.
RC4	This very popular stream cipher is the basis for Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP). It was developed by Ron Rivest of RSA Security. As with IDEA and other ciphers, RC4 uses key sizes between 40 and 2048 bits, with 256 rounds of processing. RC4 contains known vulnerabilities and is generally not recommended for new products.
RC5	RC5 is a block cipher with a variable block size (32, 64, or 128 bits). It also supports variable key sizes, from 0 to 2040 bits, and a variable number of rounds (0 to 255). In general, 64-bit blocks, 128-bit keys, and 12 rounds of processing are recommended as a minimum. RC5 is patented by RSA Security, which for a while offered a $10,000 prize for cracking the cipher.
RC6	This is a derivation of RC5 created to meet the entry requirements of the Advanced Encryption Standard contest. (The contest was held to select the successor to DES and was won by Rijndael.) RC6 is also patented by RSA Security.
One-time pad	The one-time pad (OTP) cipher combines the plaintext message with a key of equal length. The key is never reused and is kept secret. As with the simple ROT13 algorithm, the plaintext characters are rotated forward some number of characters. Unlike that scheme, each character is rotated by a different value. In OTP, the key is a stream of numbers indicating by how much each character should be rotated. For example, for a plaintext message containing only U.S. alphabetic characters, each value in the key would be a random number between 0 and 26. The OTP cipher is theoretically unbreakable if the digits of the key are truly random, the key is never reused, and the key is kept secret.