The following are the most commonly used symmetric algorithms:

- **Data Encryption Standard (DES):** Originally developed by IBM as the Lucifer algorithm, DES was modified by the National Security Agency (NSA) and issued as a national standard in 1977. Its definition was updated in FIPS PUB 46-3. It uses a 56-bit key and operates on 64-bit blocks of data. The algorithm is optimized for hardware—rather than software—use, and it can rapidly encrypt large amounts of data. It is public domain. DES was once a state-of-the-art algorithm. With rapid advances in hardware capabilities and attack methods, it now can be cracked in as little as a few days. It is no longer a secure algorithm.
- **Triple DES:** This consists of three passes of DES—encrypt, decrypt, and encrypt—using multiple keys. It increases the keyspace from 56 to 112 or 168 bits, depending on whether two or three keys are used. Triple DES is computationally secure because of the underlying security of the DES algorithm and the vastly increased keyspace. Note that using the same key three times produces the same result as single DES. It, too, is contained in FIPS PUB 46-3 and is public domain.
- **International Data Encryption Algorithm (IDEA):** Like DES, this block cipher operates on 64-bit blocks. It uses a 128-bit key and runs faster than DES in hardware and software. It is patented by Ascom-Tech AG—U.S. patent 5,214,703—but is free for noncommercial use.
- **Carlisle Adams and Stafford Tavares (CAST):** CAST is a substitution-permutation algorithm similar to DES. Unlike DES, its authors made its design criteria public. This 64-bit symmetric block cipher can use keys from 40 to 256 bits. CAST-128 is described in RFC 2144; CAST-256 is described in RFC-2612. Although patented—U.S. patent 5,511,123—its inventors, C. M. Adams and S. E. Tavares, made it available for free use.
- **Blowfish:** Blowfish is a 64-bit block cipher that has a variable key length from 32 to 448 bits. It is much faster than DES or IDEA. It is a strong algorithm that has been included in more than 150 products as well as v2.5.47 of the Linux kernel. It has been placed in the public domain by its author, Bruce Schneier. Schneier's Twofish was a candidate for the Advanced Encryption Standard (AES).
- **AES:** AES was designed by Vincent Rijmen and Joan Daemen and issued as FIPS PUB 197. The AES algorithm can use cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The cipher can also operate on variable block lengths. It is both strong and fast.
- **RC2:** RC2 is a variable key-size block cipher designed by Ronald Rivest—RC stands for Ron's Code. It was designed as a drop-in replacement for DES and operates on 64-bit blocks. It uses a salt as part of its encryption routine to make cryptanalysis more difficult. RSA Security owns it.

- **RC4:** RC4 is a variable key-size stream cipher with byte-oriented operations produced by RSA Security. RC4 is often used in Internet browsers to provide a Secure Sockets Layer (SSL) connection.