

Private key cryptography is on the order or 1,000 to 10,000 times faster than public key cryptography.

Common Cipher Algorithms

Each additional "bit" of data added to the key size means the key takes twice as long to break. This means a 40-bit key is 2^{16} times, or 65,536 as strong as a 56-bit key.

Symmetric Key Algorithms

| | | | | |
|---|-------------------------------|---|--------------------------------|--|
| Data Encryption Standard (DES) (IBM "Lucifer" project) Used with SET (Secure Electronic Transaction) | 1972 | Block cipher 64-bit blocks 16-rounds | 56-bit key (64-8 parity) | Four modes CBC - Cipher Block Chaining - each block XOR ed with previous ciphertext ECB - Electronic Code Book (native mode) - DES applied to each block CFB - Cipher Feedback - encrypts then does an XOR . OFB - Output Feedback (similar to CFB) |
| Triple DES (3DES) (Double DES in no more secure than single) | 1998 (approx.) | Block cipher 64-bit blocks 48-rounds | 168-bit key | DES-EE3 (three different keys) (encrypt-encrypt-encrypt or EDE3 encrypt-decrypt-encrypt) |
| Rijndael Advanced Encryption Standard (AES) | 2000 (replaced Triple DES) | Block cipher variable block length | 128, 192, or 256-bit key | Substitution-linear transformation using four (4) layers of substitutions, and |
| Twofish <i>Bruce Schneier and others</i> | 1998 (June) | Block cipher 128-bit blocks 16-rounds | 128, 192, or 256-bit key | Unpatented (Twofish test) |
| IDEA Cipher (International Data Encryption Algorithm) | 1992 | Block cipher 64-bit blocks 8-rounds (16-bit sub-blocks) | 128-bit key | |
| RC4 Cipher (Ronald Rivest) | 1994 | Stream cipher | Variable length 0-2048 bits | |
| RC5 Cipher (Ronald Rivest) | 1994 | Block cipher variable block length 32, 64, and 128 bits (number of rounds) | | |
| Skipjack Clipper Chip system | 1987 | Block cipher | | |
| Blowfish <i>Bruce Schneier</i> | 1993 | Block cipher | | |

Asymmetric Public Key Algorithms

| | | | | |
|--|--|--|--|--|
| Diffie-Hellman Key Exchange | | | | |
| RSA (SSL) (Rivest, Shamir, Adleman) Used with SET for Key exchange | | | | |
| El Gamal | | | | |
| Merkle-Hellman | | | | |
| ECDSA | | | | |