# Table 2: Symmetric Key Algorithms – Features and Uses

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Algorithm | Key Length (commonly used) | Block/Stream | Features & Properties | Common Uses |
| AES | 128, 192, 256 bits | Block | Fast and efficient Secure with current key sizes  Adopted as a federal standard by the US government | Encrypting data in transit and at rest  Used in many secure communication protocols |
| DES | 56 bits | Block | Considered broken due to short key length and vulnerabilities  Succeeded by 3DES and AES | Historical use in older systems and protocols |
| 3DES | 168 bits | Block | More secure than DES but slower  Considered secure but being phased out in favor of AES | Banking and financial transactions  Legacy systems |
| RC4 | 402048 bits | Stream | Fast but has vulnerabilities  No longer recommended for use | Previously used in SSL/TLS  Wireless encryption (WEP) |
| Blowfish | 32448 bits | Block | Designed as a replacement for DES  Fast and compact | Disk encryption  VPNs |
| Twofish | 128, 192, 256 bits | Block | Successor to Blowfish  Considered secure and efficient | Disk encryption  Secure communications |
| CAST128 | 40128 bits | Block | Derived from Carlisle Adams and Stafford Tavares's research  Secure for its time | S/MIME email encryption  Some VPNs |
| IDEA | 128 bits | Block | Previously used in PGP  Considered secure but less common than AES | Email encryption (PGP) |
| Camellia | 128, 192, 256 bits | Block | Developed in Japan  Similar security and performance to AES | Secure communications  Used in some Asian countries' standards |