**Difference Between AES and Blowfish Algorithms**

| **Aspect** | **AES (Advanced Encryption Standard)** | **Blowfish** |
| --- | --- | --- |
| **Developer** | Developed by Vincent Rijmen and Joan Daemen for the U.S. National Institute of Standards and Technology (NIST). | Developed by Bruce Schneier in 1993. |
| **Year Introduced** | 2001 | 1993 |
| **Key Length** | 128, 192, or 256 bits. | 32 to 448 bits (user-definable). |
| **Block Size** | Fixed at 128 bits. | Fixed at 64 bits. |
| **Algorithm Type** | Symmetric block cipher. | Symmetric block cipher. |
| **Number of Rounds** | 10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys. | 16 rounds, regardless of key size. |
| **Encryption Speed** | Faster for large datasets and better suited for modern hardware with hardware acceleration support. | Slightly slower due to the initialization of its subkeys but efficient for smaller data sizes. |
| **Flexibility** | Standardized and widely used; suitable for various applications such as secure communications, data storage, and encryption. | More flexible in terms of key size but less commonly used today due to its smaller block size. |
| **Security** | Considered highly secure with proper key length (192 or 256 bits). Vulnerable to side-channel attacks if improperly implemented. | Secure for most applications but considered outdated for modern systems due to its smaller block size. |
| **Vulnerability** | Vulnerable to brute-force attacks only if the key length is short (e.g., 128 bits may become insecure over time). | Vulnerable to brute-force attacks and not recommended for systems requiring long-term security. |
| **Use Cases** | Widely adopted in government, commercial applications, SSL/TLS, disk encryption, and VPNs. | Historically used in embedded systems and for legacy applications, such as password management. |
| **Adoption** | Official encryption standard adopted worldwide (FIPS 197). | Not standardized but used in specific applications like bcrypt for password hashing. |

**Summary**

* **AES** is modern, standardized, and more secure with its larger block size (128 bits) and key lengths up to 256 bits. It is suitable for most contemporary encryption needs.
* **Blowfish** is faster in software for smaller data sizes but has a smaller block size (64 bits), making it less secure against certain modern cryptographic attacks (e.g., birthday attacks). It is now less commonly used in favor of AES.