# Advanced Encryption Standard (AES)

Return to Glossary

The **Advanced Encryption Standard (AES)** is a symmetric block cipher chosen by the U.S. government to protect classified information.

AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity, and electronic data protection.

The https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech:nist:start started the development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

NIST stated that the newer, advanced encryption algorithm would be unclassified and must be “capable of protecting sensitive government information well into the [21st] century.” It was intended to be easy to implement in hardware and software, as well as in restricted environments – such as a smart card – and offer decent defenses against various attack techniques.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, non-governmental organizations choosing to use AES are subject to limitations created by U.S. export control.

Source: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard