



digi gone



there when you need it... *gone in a flash!*



AES Encryption Algorithm

The Advanced Encryption Standard (AES) specifies a Federal Information Processing Standards (FIPS)-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

The algorithm specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. The algorithm shall be used in conjunction with a FIPS approved or National Institute of Standards and Technology (NIST) recommended mode of operation. Object Identifiers (OIDs) and any associated parameters for AES used in these modes are available at the Computer Security Objects Register (CSOR), located at <http://csrc.nist.gov/csor/>

Implementations of the algorithm that are tested by an accredited laboratory and validated will be considered as complying with this standard. Since cryptographic security depends on many factors besides the correct implementation of an encryption algorithm, Federal Government employees, and others, should also refer to NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, for additional information and guidance (NIST SP 800-21 is available at <http://csrc.nist.gov/publications/>).

DigiGone™ uses the NIST approved Rijndael 256-bit AES algorithm on File and Folder Encryption as well as Packet Encryption for data sent to and from the Secured Proxy Servers.



For more information, call (727) 393-3037 or email us at info@diginonymous.com

*This product is the subject of one or more pending patent applications filed with the United States Patent & Trademark Office. copyright 2007, Diginonymous LLC, all rights reserved.

