NIST: SP 800-34E Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices

return to the NIST Standards

Table 1: Data sheet for Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices

Title	Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices
Acronym	XTS-AES
Version	2010
Series	SP
Document Number	SP 800-38E
Release Date	January 2010
Download	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

> **Note**: The following is an excerpt from the official NIST catalog. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Introduction

The XTS-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES) [1)] algorithm. The Security in Storage Working Group (SISWG) of the P1619 Task Group of the Institute of Electrical and Electronics Engineers, Inc (IEEE) developed and specified XTS-AES in IEEE Std. 1619-2007 [2)] . This Recommendation approves the XTS-AES mode as specified in that standard, subject to one additional requirement on the lengths of the data units, which is discussed in Section 4 below.

The XTS-AES mode was designed for the cryptographic protection of data on storage devices that use of fixed length “data units,” as defined in Ref. [3)] . Note that other approved cryptographic algorithms continue to be approved for such devices. The XTS-AES mode was not designed for other purposes, such as the encryption of data in transit.

The XTS-AES mode is an instantiation of Rogaway’s XEX (XOR Encrypt XOR) tweakable block cipher [4)], supplemented with a method called “ciphertext stealing” to extend the domain of possible input data strings. In particular, XEX can only encrypt sequences of complete blocks, i.e., any data string that is an integer multiple of 128 bits; whereas for XTS-AES, the data string may also consist of one or more complete blocks followed by a single, non-empty partial block. (The acronym XTS stands for the XEX Tweakable Block Cipher with Ciphertext Stealing).

The specification of the ciphertext stealing method in Ref.[5)] includes an ordering convention for the final complete block and partial block of the encrypted data string. A different convention, in which the order

is swapped, may be desirable in some cases. The specification in Ref.[6] provides flexibility in the physical location of these elements, as long as interoperability is not compromised, as discussed in Section 5.

The XTS-AES mode provides confidentiality for the protected data. Authentication is not provided, because the P1619 Task Group designed XTS-AES to provide encryption without data

expansion, so alternative cryptographic methods that incorporate an authentication tag are precluded. In the absence of authentication or access control, XTS-AES provides more protection than the other approved confidentiality-only modes against unauthorized manipulation of the encrypted data.

Annex D of Ref.[7] discusses in detail the design choices for XTS, including the resistance to manipulation of the encrypted data, and their ramifications for the incorporation of XTS-AES into an information system. Prospective implementers of XTS-AES should consider this information carefully to ensure that XTS-AES is an appropriate solution for a given threat model.

1)
Federal Information Processing Standards (FIPS) Publication 197, Announcing the Advanced Encryption Standard (AES), U.S. DoC/NIST, Nov. 26, 2001.
2) 3) 5) 6) 7)
IEEE Std 1619-2007, The XTS-AES Tweakable Block Cipher, Institute of Electrical and Electronics Engineers, Inc., Apr. 18, 2008.
4)
P. Rogaway, Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Computer Science, vol. 3329, pp. 16-31, Springer-Verlag, 2004