

NOAO Acceptable Encryption Use Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

The NOAO CIS Departments will be glad to provide guidance on these very technical issues if you have questions.

2.0 Scope

This policy applies to all NOAO employees and affiliates.

3.0 Policy

Proven, standard algorithms such as DES, 3DES, AES, Blowfish, RSA (or Diffie-Hellman), RC5 and IDEA should be used as the basis for encryption technologies. Symmetric crypto-system (such as AES, DES, 3DES, Blowfish and IDEA) key lengths must be at least 128 bits. Asymmetric crypto-system (such as RSA and RC5) keys must be at least 1024 bits. NOAO's key length requirements will be reviewed annually and upgraded as technology allows.

These algorithms represent the actual cipher used for an approved application. For example, PGP Corporation's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA, while Secure Socket Layer (SSL) uses RSA encryption. The ssh protocol combines an asymmetric cipher such as RSA-1028 for key exchange and a symmetric cipher such as AES-128 for bulk data transfer. Apple's encrypted disk images in MacOS X use AES-128; TrueCrypt uses AES-256.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the CIS Departments. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Terms & Definitions

Proprietary Encryption

An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem

A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem

A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

5.0 Revision History

First Edition: March 15, 2007