



Appendix E: US Government Role in Current Encryption Standards

NSA provided the Review Group the following information, outlining the reliability of certain encryption systems. Our recommendation 31 would give the force of law to prohibitions on undercutting these and other standards.

Most of the standards described below are approved by NIST for protecting unclassified US Government information and by NSA for protecting classified US Government information. AES, SHA-2, EC-DSA, and EC-DH make up the core of “Suite B,” NSA’s mandated set of public standard algorithms, approved in 2006, for protecting classified information.¹⁸² Each algorithm discussed below is currently in use in National Security Systems, although NSA is pursuing the transition from SHA-1 to SHA-2. For further information on all but SHA-1 see <https://www.cnss.gov/policies.html> and references contained there.

In general, NSA applies the deep cryptanalytic tradecraft and mathematical expertise developed over decades of making and breaking codes, to ensure that cryptography standardized by the US Government is strong enough to protect its own sensitive communications.

¹⁸² This paper addresses the strength of standard cryptographic algorithms. Any cryptographic algorithm can become exploitable if implemented incorrectly or used improperly. NSA works with NIST to ensure that NIST standards incorporate guidance on correct implementation and usage. NSA will exploit vulnerable implementations and uses to support the lawful conduct of signals intelligence.

AES - The Advanced Encryption Standard - FIPS 197

NSA did not contribute to nor modify the design of the Advanced Encryption Standard (AES). It was designed by two European cryptographers: Joan Daemen and Vincent Rijmen. It was published and submitted in 1998 for NIST's AES competition and selected in 2001 as the Advanced Encryption Standard. NSA extensively examined the algorithms in the competition and provided technical guidance to NIST during the competition to make sure that NIST's final selection was a secure algorithm. NIST made the final algorithm choice under its own authority, independent of NSA. Both NSA and the academic cryptography community have thoroughly analyzed the AES.

RSA - The Rivest, Shamir, Adelman Public Key Algorithm - FIPS 186, NIST SP 800-56B

NSA did not contribute to, nor modify, the design of RSA, but it did provide input on RSA usage in standards. It was designed in 1977 by three cryptographers working at MIT: Americans Ron Rivest, and Leonard Adelman, and Israeli Adi Shamir. The algorithm was independently designed earlier by Cliff Cocks of UK GCHQ in 1973 but was not published, and was only declassified in 1997. Both NSA and the academic cryptography community have thoroughly analyzed the RSA algorithm both as a digital signature (FIPS-186) and as an encryption algorithm for keys (SP 800-56B).

Diffie-Hellman/Elliptic Curve Diffie-Hellman - The Diffie-Hellman Key Exchange Algorithm - NIST SP 800-56A

NSA did not contribute to, nor modify, the design of Diffie-Hellman. The Diffie-Hellman Key Exchange Algorithm was designed by American cryptographer Whitfield Diffie and Martin Hellman at Stanford University in 1976. It was invented by Malcolm Williamson of GCHQ a few years earlier, but never published. The elliptic curve variant of the Diffie-Hellman key exchange was invented independently by American cryptographers Victor Miller and Neal Koblitz in 1985. NSA ensured that a class of potentially weak elliptic curve parameters was not included in the NIST standard. Both NSA and the academic cryptography community have thoroughly analyzed both the Diffie-Hellman Key Exchange algorithm and its elliptic curve variant (both found in NIST SP 800-56A).

DSA/ECDSA – The Digital Signature Algorithm/Elliptic Curve DSA – FIPS 186

NSA designed the algorithm known as DSA as the original signature algorithm in FIPS 186 initially in 1991-1993, then contributed advice on later versions of the standard. NSA also designed a variant of DSA that uses the mathematics of elliptic curves and is known as the “Elliptic Curve DSA” or ECDSA. Both NSA and the academic cryptography community have thoroughly analyzed the DSA (FIPS 186).

SHA-1 - The Secure Hash Algorithm Variant 1 - FIPS 180-1

NSA designed the SHA-1 algorithm as a correction to the SHA-0 algorithm, a longer (160-bit) variant of the MD5 algorithm designed by Ron Rivest.

SHA-0 was an NSA design standardized in 1993. In 1994, NSA acted quickly to replace SHA-0 with SHA-1 as a NIST standard when NSA cryptanalysts discovered a problem with the SHA-0 design that reduced its security. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-1 (FIPS 180). For many years NIST and NSA have recommended that people stop using SHA-1 and start using the SHA-2 hash algorithms.

SHA-2 - The Secure Hash Algorithm Variant 2 - FIPS 180-2

NSA designed the four different-length hash algorithms contained in FIPS-180-2 and collectively known as SHA-2. Because of their longer hash lengths (224, 256, 384, and 512 bits), the SHA-2 hash lengths provide greater security than SHA-1. SHA-2 also blocks some algorithm weaknesses in the SHA-1 design. These algorithms were standardized in 2002. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-2 hash algorithms (FIPS 180).