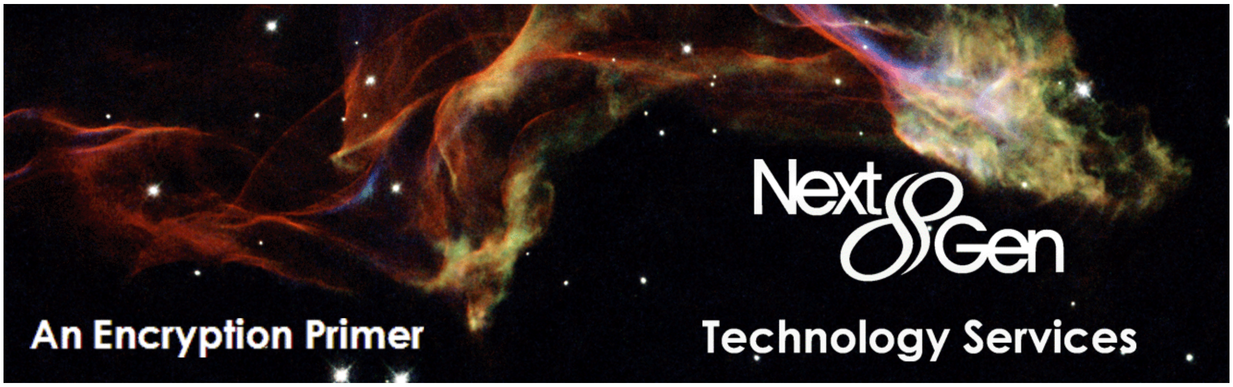


Encryption Algorithms Decrypted

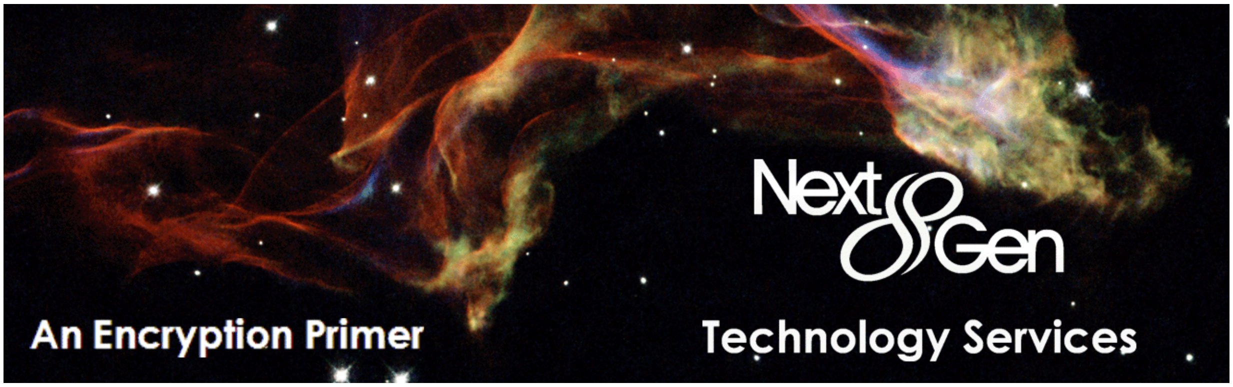
Overview

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency whose mission is to advance measurement science, and create technology standards. They, among other things, have been chartered by the federal government to define standards and measures for the federal government's use of encryption. They continually evaluate encryption algorithms and select an algorithm that will serve the government for an extended period of time. We will attempt to simplify and explain the current state of (NIST) approved encryption algorithms.

DES - Data Encryption Standard

The algorithm that started it all, the Data Encryption Standard (DES), was phased out by May 2007. DES originated at IBM in 1977 and was adopted by the National Bureau of Standards (now NIST) and the U.S. Department of Defense. It was a widely-used method of data encryption using a secret 56-bit key.

DES was so secure that no one has found a way to break its encryption short of trying all the possible keys. This "brute force attack" or "key exhaustion attack" will eventually compromise a given encrypted message. A brute force attack attempts to decrypt an encrypted message by starting with key 0 and trying all 70 quadrillion possible keys. Each key is used to decrypt the message with the results being compared to ASCII data. In theory, the attack will eventually stumble on some known text (if in fact the plaintext data is ASCII or EBCDIC and not binary). In 1998, a computer was built (EFF DES cracker) for $250,000 that could decrypt a DES encrypted message in only 2 days. This brought about the creation of Triple DES which can be termed 3DES, TDES, or TDEA.



3DES - Triple DES

3DES increases the key size of the DES algorithm from 56 bits to 168 bits. In essence, the message is encrypted 3 times with 3 unique 56 bit keys. The first key uses DES to encrypt the data. The second key is used to decrypt the data from the first encryption. The third key is used to encrypt the data again. This was deemed the strongest and most effect use of the 3 key method. 3DES is a minimum requirement for all Sensitive But Unclassified (SBU) United Sates Government data.

While 3DES was an acceptable form of encryption for government use, there were several issues associated with its usage; but primarily, it was the time and overhead necessary to perform this triple encryption process on large amounts of data. NIST concluded that a new algorithm would be required to protect data for the next few decades.

AES - Advanced Encryption Standard

In November of 2001 NIST announced that it would adopt the Advanced Encryption Standard (AES) as the encryption algorithm for securing Sensitive But Unclassified (SBU) material. Several algorithms were evaluated by NIST over a five year period. The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. On December 6, 2001, the Secretary of Commerce officially approved Federal Information Processing Standard (FIPS) 197, which specifies that all sensitive, unclassified documents will use Rijndael (named after the developers, Vincent Rijmen and Joan Daeman) as the Advanced Encryption Standard.

FIPS 140-2 - Federal Information Processing Standards 140-2

Just because a given product set uses any one of the above algorithms (or any algorithm for that matter) does not make it secure. FIPS 140-2 is a NIST standard against which products can be measured to ensure that they are indeed "secure" and that they meet all the government criteria for securing sensitive data. There are 4 levels of security 1 through 4, 4 being the highest. The difference is mainly the hardware levels of protections of keys, detection against tampering and how the systems respond to attempts at tampering. Products need to be CERTIFIED for FIPS 140-2 (or FIPS 140-1 and soon to be FIPS 140-3) to be eligible for installation in government SBU networks. There are currently only 10 certified labs in the world to perform this certification. Do not be fooled by products that are "built to the standard" or "compliant." Ask for the NIST certification.