



1 Forstmann Court  
Clifton, NJ 07011  
Phone: 973.772.6997  
Fax: 973.772.0747  
800.359.8561  
[info@commdevices.com](mailto:info@commdevices.com)  
<http://www.commdevices.com>

January 2005

## Encryption Algorithms Decrypted

### Overview

This paper is an attempt to simplify and explain the current state of today's National Institute of Standards and Technology (NIST) approved encryption algorithms. The algorithm that started it all, the Data Encryption Standard (DES), is in the process of being decommissioned by NIST. Single DES will be phased out by May 2007.

### DES

#### Data Encryption Standard

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 private (secret) 56-bit key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

DES was built so strong that it has never been successfully "algorithmically broken", however what is called a "brute force attack" or "key exhaustion" can eventually compromise a given encrypted message. A brute force attack attempts to decrypt an encrypted message by starting with key "0" and increasing to 2 to the 56<sup>th</sup>. Each key is used to decrypt the message with the results being compared to ASCII data. Eventually the attack will stumble on some known text (if in fact the plaintext data is ASCII and not binary). It was determined in the early 90's that the average computing horsepower available to the general public was increasing at an alarming rate making a brute force attack more cost effective than in the 80's. 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 by a factor of 3, to 168 bits. This is a three-step data encryption algorithm that evolved from DES. In essence there are three unique 56 bit keys used. The first key uses DES to encrypt the data. The second key uses DES to decrypt the data. The third key uses DES to encrypt the data again. This was deemed the strongest and most effect use of the 3 key system by NIST. 3DES is a minimum requirement for all Sensitive But Unclassified (SBU) United Sates Government data.

While 3DES is an acceptable form of encryption for government use, NIST realized a new algorithm would be required to protect data for the next few decades.

## **AES**

### **Advanced Encryption Standard**

The Advanced Encryption Standard (AES) is an encryption algorithm securing sensitive but unclassified (SBU) material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

In January of 1997, a process was initiated by the National Institute of Standards and Technology (NIST), to find a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. 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 October 2, 2000, NIST announced that Rijndael (pronounced "rain doll" or "Rhine Dahl") had been selected as the proposed standard. 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 as the Advanced Encryption Standard. Triple DES is still accepted.

## **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 that products can be measured against to ensure that they are indeed "secure" and that they meet all the government criteria for securing SBU data. There are 4 levels of security 1 through 4, 4 being the highest. The difference in the levels is mainly hardware levels of protections of keys etc. 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.