# Triple Data Encryption Standard (Triple-DES)

http://www.vocal.com

VOCAL Technologies, Ltd. encryption software libraries include DTCP, DES, AES, CCMP, RC4, and SHA algorithms in ANSI C and optimized assembly language for ADI, AMD-Alchemy, ARM, DSP Group, LSI Logic ZSP, MIPS and TI. This software is modular and can be executed as a single task under a variety of operating systems or it can execute standalone with its own kernel

Triple DES is based on the DES algorithm; it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end the National Institute of Standards and Technology (NIST). the Advanced Encryption Standard (AES) as a replacement for DES. Triple DES has been endorsed by NIST as a temporary standard to be used until the AES was finished. The AES is at least as strong as Triple DES and much faster. Many security systems use both Triple DES and AES. AES is the default algorithm on most systems. Triple DES will be kept around for compatibility reasons for many years after that.

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

**Modes of Operation:**

- **Triple ECB (Electronic Code Book)**. This variant of Triple DES works exactly the same way as the ECB mode of DES. This is the most commonly used mode of operation.

- **Triple CBC (Cipher Block Chaining)**. This method is very similar to the standard DES CBC mode. As with Triple ECB, the effective key length is 168 bits and keys are used in the same manner, as described above, but the chaining features of CBC mode are also employed. The first 64-bit key acts as the Initialization Vector to DES. Triple ECB is then executed for a single 64-bit block of plaintext. The resulting ciphertext is then XORed with the next plaintext block to be encrypted, and the procedure is repeated. This method adds an extra layer of security to Triple DES and is therefore more secure than Triple ECB, although it is not used as widely as Triple ECB.

VOCAL Technologies, Ltd.

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675

http://www.vocal.com