IIM SERVICES AGENCY

# Encryption Components for Windev
# DES / 3DES
# AES I – II – III
# TwoFish I – II - III
# Serpent I – II - III
# KHAZAD
# ANUBIS I to VII

**Presentation of available components since version 14 of Windev**

**DES / 3DES :** The Data Encryption Standard (DES) is a symmetrical encryption algorithm (block cipher) using keys of 56 bits. The Triple DES (also known as 3DES) is also a symmetrical encryption algorithm (block cipher) , has a key length of 168 bit chaining 3 different DES keys of 56 bits on the same block of data. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV)

**AES I – II – III :** Advanced Encryption Standard or AES also known under the name of Rijndael, is a symmetrical encryption algorithm. The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. AES has been adopted by the U.S. government and is now used worldwide.

**Presentation of available components since version 16 of Windev**

**TwoFish I – II – III :** TwoFish is a symmetrical encryption algorithm (block cipher). It encrypts blocs of 128 bits with a key of 128, 192 or 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Due to its complexity, the cryptanalysis of this algorithm remains delicate. In spite of its assets, it remains relatively little used and was supplanted by the winner in AES, Rijndael. It is an attractive alternative to the current AES if this one became vulnerable.

**Serpent I – II – III :** Serpent is a symmetrical encryption algorithm (block cipher). Quite as the other candidates for AES, Serpent has a size of block of 128 bits and supports keys of 128, 192 or 256 bits. It was considered more careful than Rijndael, the winner of AES, in terms of security. The designers left the principle that 16 rounds were enough to push away conventional attacks, but to counter the cryptanalysis to come, they opted for 32 rounds.

**KHAZAD :** KHAZAD is a symmetrical encryption algorithm (block cipher). It has a size of block of 64 bits and a key of 128 bits. It uses in an intensive way the involutions as the sub-components in its structure, this technique allows to minimize the differences between the encryption and the decoding.

**ANUBIS I - VII:** ANUBIS is a symmetrical encryption algorithm (block cipher). It has a size block of 128 bits and a key of 128 up to 320 bits, by steps of 32 bits. It uses in an intensive way the involutions as the sub-components in its structure, this technique allows to minimize the differences between the encryption and the decoding. Anubis is named after the Egyptian god of entombing and embalming, which the designers interpreted to include encryption. They claim that violators of the cipher will be cursed.

**The components are downloadable for testing purposes, with a full example of use and programmation, in English and French. They are activated on production by buying a user's licence.**


Website : http://www.iim.ch – Email : info@iim.ch