IIM SERVICES AGENCY

Composants de chiffrement pour Windev
DES / 3DES
AES I – II – III
TwoFish I – II - III
Serpent I – II - III
KHAZAD
ANUBIS I à VII

Présentation des composants disponibles depuis la version 14 de Windev

DES / 3DES : Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Le Triple DES (aussi appelé 3DES) est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.

AES I – II – III : Advanced Encryption Standard (« standard de chiffrement avancé »), ou AES aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été également approuvé par la NSA (National Security Agency) pour les informations top secrètes. L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ». Le niveau « TOP SECRET » nécessite des clés de 192 ou 256 bits.

Présentation des composants disponibles depuis la version 16 de Windev

TwoFish I – II – III : TwoFish est un algorithme de chiffrement symétrique par bloc. Il chiffre des blocs de 128 bits avec une clé de 128, 192 ou 256 bits. Twofish était l'un des cinq finalistes du concours AES. De par sa complexité, la cryptanalyse de cet algorithme reste délicate. Malgré ses atouts, il reste relativement peu utilisé et a été supplanté par le gagnant de AES, Rijndael. Il n'en demeure pas moins une alternative séduisante à l'actuel AES si celui-ci devenait vulnérable.

Serpent I – II – III : Serpent est un algorithme de chiffrement symétrique par bloc. Tout comme les autres candidats pour AES, Serpent a une taille de bloc de 128 bits et supporte des clés de 128, 192 ou 256 bits. Serpent a été jugé plus prudent que Rijndael, le vainqueur de AES, en termes de sécurité. Les concepteurs sont partis du principe que 16 tours suffisaient à repousser les attaques conventionnelles, mais pour contrer la cryptanalyse à venir, ils ont opté pour 32 tours.

KHAZAD : KHAZAD est un algorithme de chiffrement symétrique par bloc. Il a une taille de bloc de 64 bits et une clé de 128 bits. Il utilise de manière intensive les involutions comme sous-composants dans sa structure, cette technique permet de minimiser les différences entre le chiffrement et le déchiffrement.

ANUBIS I - VII: ANUBIS est un algorithme de chiffrement symétrique par bloc. Il a une taille de bloc de 128 bits et une clé de 128 à 320 bits, par incrémentation de 32 bits. Il utilise de manière intensive les involutions comme sous-composants dans sa structure, cette technique permet de minimiser les différences entre le chiffrement et le déchiffrement. Il est appelé comme le Dieu égyptien du fait de l'enterrement et embaumement, que les créateurs ont interprété pour créer le cryptage. Ils prétendent que les violeurs du chiffrement seront maudits.

Les composants sont téléchargeables pour test, avec un exemple complet d'utilisation et programmation en français et anglais. Ils deviennent utilisables en production par l'achat d'une licence d'utilisation.

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