

EZAES



IIM SERVICES AGENCY

Chiffrement de textes et fichiers en utilisant le protocole AES – I – II – III

EZAES a été développé pour répondre à un besoin de sécurité pour protéger les données sensibles, lors de leur stockage, envoi sur un support physique, ou via Internet. Ce composant permet le lien entre les applications développées avec Windev et assure ainsi un standard entre vos divers logiciels. Il offre trois options de chiffrement, soit AES I, II, et III, respectivement avec une clef de 128 bits, 192 bits, 256 bits. L' AES a remporté en octobre 2000 le concours AES, lancé en 1997 par le NIST et est devenu 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. Deux modes sont disponibles, l' ECB et le CBC.

L'utilisation du composant se fait au travers d'appels simples aux fonctions de chiffrement et déchiffrement. Vous avez la possibilité d'afficher une barre de progression, et / ou un compte à rebours du temps de traitement restant. Notre exemple en français et anglais vous fournit tous les détails pour l'utilisation des fonctions du composant.

The screenshot shows the 'AES 128-192-256 Composant - Exemple' window. It is configured for text encryption using AES I (128 bits) in ECB mode. The source and destination directories are 'C:\Program Files\IIM\EZAES Exemple'. The password is '1234567890123456'. The source text is 17381 characters long, and the resulting encrypted text is 17392 characters long. The progress bar is at 100%.

Bloc traité									
4A	65	20	6E	65	20	70	75	69	73
20	70	61	73	20	6D	65	20	72	61
70	70	65	6C	65	72	2C	20	73	75
72	20	6D	6F	6E	20	E2	6D	65	2C
20	63	6F	6D	6D	65	6E	74	2C	20

Texte Crypté - 17392 caractères									
77	60	BB	E6	62	65	23	3C	0A	43
2A	80	D4	18	8C	0F	D8	53	BA	C0
15	C1	C9	08	C1	EB	3D	5C	25	55
39	7D	E5	55	42	35	41	F7	80	2C
89	31	47	84	02	B2	D3	C5	A4	4E