



IIM SERVICES AGENCY

Composant utilitaire

EZKZD

Chiffrement de textes et fichiers en utilisant le protocole KHAZAD

EZKZD 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 une option de chiffrement. KHAZAD fut présenté au concours NESSIE en 2000 et sélectionné comme finaliste. L'algorithme possède huit tours d'un réseau de substitution permutation et une taille de bloc de 64 bits et une clé de 128 bits, utilisant de manière intensive les involutions comme sous-composants dans sa structure, permettant de réduire les différences entre le chiffrement et le déchiffrement. 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.

EZKZD Khazad Composant - Exemple

Traitement: Fichier Texte

Mode de traitement: ECB CBC

Détails du fichier: Intégrés

Action: Cryptage Décryptage

Extension: []

Affichage du traitement: Barre progression Chronomètre

Répertoire source: D:\Mes projets\KZD\EZKZD Exemple\Exe

Mot de passe: 1234567890123456

Vecteur d'Initialisation (IV): []

Répertoire destination: D:\Mes projets\KZD\EZKZD Exemple\Exe

Extension: Anonyme (.ENC) Autorisé - ESC

Arrêt traitement: Autorisé - ESC

Terminaison: ISO/IEC 7816-4 ANSI X923 PKCS7 ISO 10126

Texte Original - 17381 caractères

Texte Crypté - 17384 caractères

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

7C	58	70	FA	7A	AF	3F	95	1F	8C
F2	2E	1D	F7	79	FC	1A	72	0F	9C
58	48	49	E5	57	B1	8D	60	2B	5D
F8	E0	2C	4D	BA	07	E9	8B	DD	DF
37	99	58	44	AD	AF	CA	B3	47	F5

Fichier à Fichier

Crypter le texte Effacer le texte Décrypter le texte Effacer le texte

Bloc traité

Durée: 0:00:38

Reste: 0:00:00

Taille Bloc lu: 1MB 2MB 4MB 8MB 16MB 32MB 64MB 128MB

100 %