

Utilitarian Component



IIM SERVICES AGENCY

EZTWF

Text and files encryption using the TwoFish I - II - III protocol

EZTWF has been developed in order to bring a solution for security needs, when protecting sensitive data is mandatory either on storage, either on transferring them through a physical media or through Internet. This component allows linking any application developed with Windev and brings an easy way to have a standard between your softwares. It does provide three encryption options : TwoFish I - II - III, using a 128 bits block size, a key of 128 bits, 192 bits, or 256 bits. It was a finalist for the AES competition. No attack was able to be applied to the protocol. The exhaustive search remains the only means to break it. It seems in any case more resistant than what had initially been announced during the AES competition. Two modes are available, ECB and CBC.

Using this component is very easy. All is done through simple calls to the encryption and decryption functions. You have the possibility to display a progressbar , and / or time counter showing the treatment remaining time. Our example both in French and English provides all the details needed to use the component's functions.

Twofish Component - Example

Process: File Text

Encryption algorithm: 128 192 256

Process Mode: ECB CBC

File Details: Integrated

Action: Encrypt Decrypt

Extension: []

Process Display: Progress bar Timer

Block in process: []

Time: 0:01:51
Remaining: 0:00:00

100 %

Source directory: D:\Mes projets\TWF\EZTWF Example\Exe

Destination directory: D:\Mes projets\TWF\EZTWF Example\Exe

Password: 1234567890123456

Initialisation Vector (IV): []

Extension: Anonymous (.ENC) Authorized - ESC

Cancel process: Authorized - ESC

Padding Type: ISO/IEC 7816-4 ANSI X923 PKCS7 ISO 10126

Genuine Text - 17381 caracteres

Encrypted data - 17392 caracteres

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

1F	75	18	D0	5D	9F	2D	5D	7A	B1
70	D5	C5	D1	23	10	14	00	AB	1F
48	ED	FD	48	A1	2E	68	C1	B8	BC
EA	63	3D	2B	8D	79	26	B6	05	90
1B	4B	D1	E5	67	1E	D0	22	37	B9

File to File | **Encrypt** | Clear text | Decrypt | Clear text

Bloc Reading size: 1MB 2MB 4MB 8MB 16MB 32MB 64MB 128MB