

## Utilitarian Component



IIM SERVICES AGENCY

# EZKZD

### Text and files encryption using the KHAZAD protocol

**EZKZD** 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. KHAZAD was presented at the first NESSIE workshop in 2000, and selected as a finalist in the project. It has an eight-round substitution-permutation network structure with a 64-bit block size and a 128-bit key. It makes heavy use of involutions as subcomponents minimizing the difference between the algorithms for encryption and decryption. 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.

**EZKZD Khazad Component - Example**

Process:  File  Text

Process Mode:  ECB  CBC

File Details:  Integrated

Action:  Encrypt  Decrypt

Extension: [ ]

Process Display:  Progress bar  Timer

Block in process: [ ]

Time: 0:00:38  
Remaining: 0:00:00

100 %

Source directory: D:\Mes projets\KZD\EZKZD Example\Exe

Destination directory: D:\Mes projets\KZD\EZKZD 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 characters

Encrypted data - 17384 characters

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

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

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