IIM SERVICES AGENCY

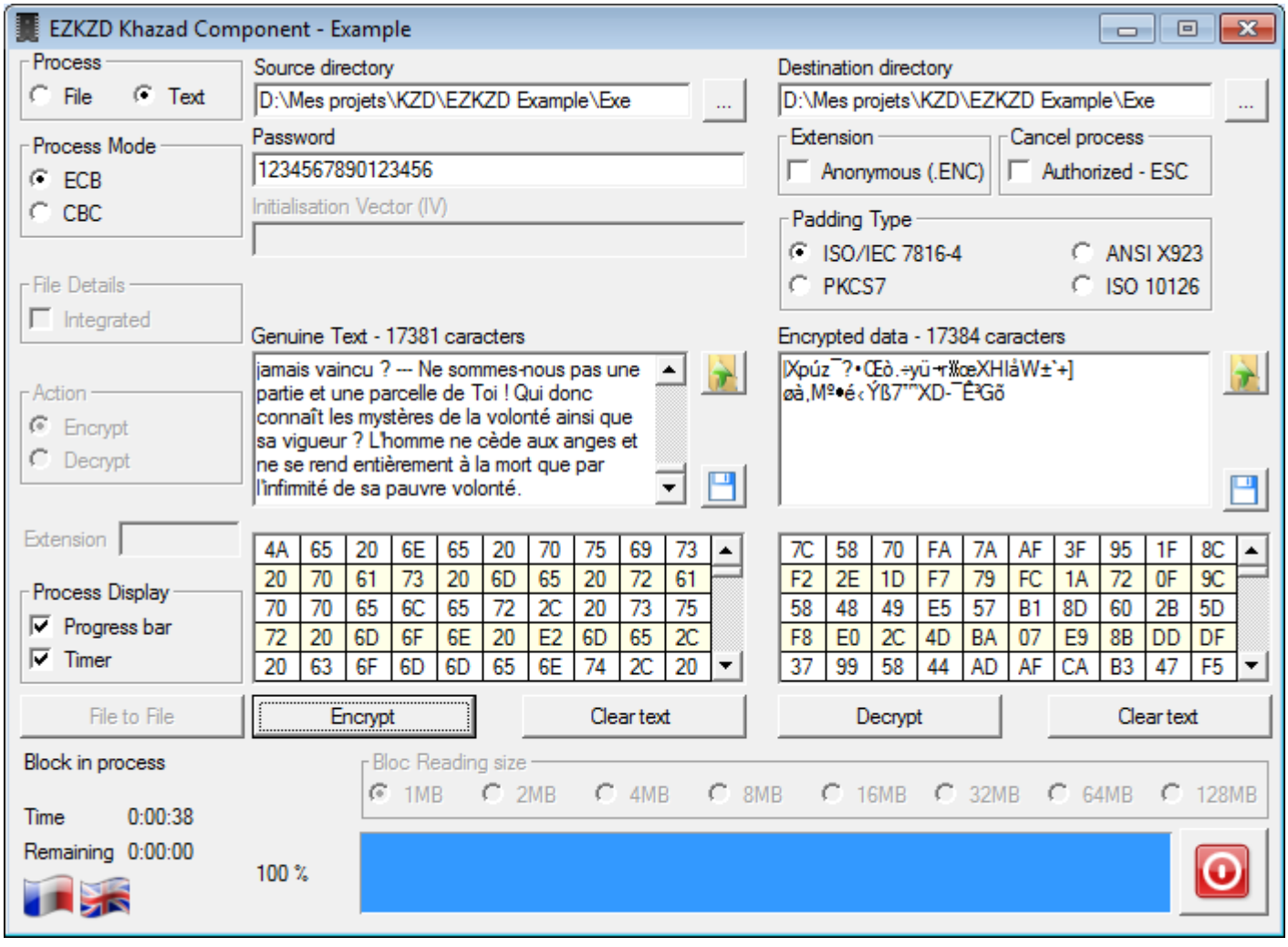
Utilitarian Component

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.



The trademarks "PCSOFT" and "WINDEV" are registered trademarks of PCSOFT France
Website : http://www.iim.ch – Email : info@iim.ch