

## ENCRYPT ANY DOCUMENT

You can see online forums and discussions like: how can I encrypt an entire folder? (transfer the content to a ZIP file!), a PDF file? how do i encrypt a DOC file etc ..? It is a false problem, any document is nothing more than a sequence n of bytes, so the only thing that matters is to obtain an encrypted file where

byte (n) + algorithm = encrypted byte (n)

and that you can get the original document back with

encrypted byte (n) - algorithm = byte (n)

Whatever the type of document was, it returns to being available to the applications that use it, with its content and its original name.

## DOCUMENT ENCRYPTING

You can give the encrypted documents any name you want.

The name of the source file is stored in the encrypted file, so when the document is decrypted it is automatically assigned the original name without being forced to remember which document that particular file refers to.

## TEXT ENCRYPTING

What you type from the keyboard is directly encrypted,

## AUTHENTICATION

Each encrypted document contains an unrepeatable identification code (**NIDE**) that excludes any possibility of manipulation and securely certifies the identity of the sender.

The encryption system is in fact such that the same document, encrypted with the same key n times, generates n always different encrypted files and therefore n different **NIDE** (see note above)

**NIDE** is shown at the end of the encryption, checked by the system before decrypting each document and is in any case verifiable at any time with a specific function and therefore the sender and recipient can ensure the authentic origin of the encrypted document and its integrity.

In addition to the NIDE code, the following are displayed:

- creation date
- name of the key used
- who encrypted the document
- name of the original document

## THE KEY FILE

The key file contains all the user keys in the form:

KEYNAME (clear, anyone can see it) + KEY (which only you can see, because it is encrypted with the KEY. ).

Therefore, once the name of the key to be used is known, it is extracted from the archive and it is only the system that can decrypt it (with the **KEY.OF.THE.KEYFILE**) and allow its use.

The name / reference relating to the key is stored in the encrypted files and therefore the key to be decrypted will be taken without giving any indication.

This **KEY.OF.THE.KEYFILE** is the only one you need to remember but you **MUST** remember it otherwise you will never be able to recover the files already encrypted because

only those who know that **KEY.OF.THE.KEYFILE** can operate in the system

## THE KEYS

They can be generated using the program's specific function and then assigning them the desired name.

You can create a shared key with your correspondent with the key exchange process.

The process takes place in 2 stages:

A ----- data ---- »B which generates a key K

B ----- data ---- »A which generates a key = K

The name is the correspondent's user name, it is assigned automatically and allows both to correctly decrypt the messages as on each encrypted file that will be exchanged there will be the name with which the shared key was inserted in the key file.

The program shows which phase is in progress.

You just have to agree on who starts phase 1.

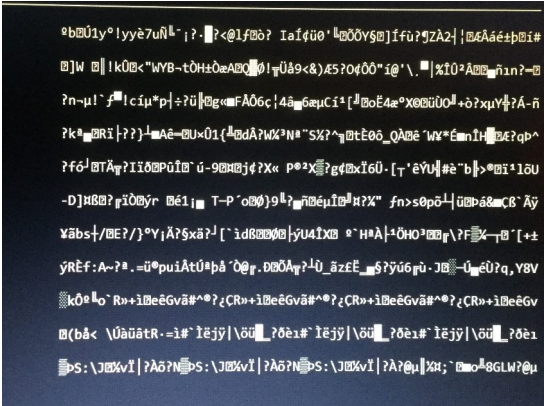
A description can be associated with the keys created to facilitate the identification of a correspondent.

A key can also be imported into the system via a file with name KIMPEXP that has the following format: key name (24) + username (24) + key (64)

The function that generates the keys allows you to export the generated key to the KIMPEXP file. With the camouflage function you can put KIMPEXP inside a photo to be sent to your interlocutor and thus make a reasonably safe key exchange. The interlocutor will do the decamouflage and import the key from the KIMPEXP extracted from the photo. it is possible to make a list in which all keys are shown (some special characters which are not viewable are replaced with ?).

**IMPORTANT:** Never enter a new key that has the same name as your nickname.

How the keys are



To have a good layout:

- create a Qcrypto link icon on desktop
- right click on link icon
- properties / layout

- in window dimensions set 30 in height and 102 in width