CA FileCipher

CA FileCipher is an application that allows to encrypt/decrypt generic files (text, image, video).

Its main characteristics are:
- No installation needed
- Windows O.S. compatibility
- Extremely user friendly
- Efficiency and speed
- High security level
- Session keys allowed
- Key management
- Modularity: key length can be chosen between 256 and 300.000 bits with no need of large numbers libraries.

The figure below describes the encryption -decryption (E/D) protocol

Encryption.

CA FileCipher allows to encrypt files for personal use or for transmission.

- The sender: selects the file to be encrypted (E1a); selects the receiver, identified by his/her public key (E1b); generates a Session Public Key (SPK) (E1c).
- The SPK (E2a), the receiver's public key (E2b) and the file (E2c) are sent to the (E/D) engine.
- The (E/D) engine uses them to produce a file dependent public key (FDPK) and to encrypt the file (E3).
- The encrypted file and the FDPK are sent to the receiver.

Decryption.

- The user selects the file to be decrypted (D1a) and generates his/her secret key through a passphrase (D1b).
- The encrypted file (D2a) and the secret key (D2b) are sent to the (E/D) engine.
- The (E/D) engine uses them to produce the decrypted file (D3).