

CLAIMS

1. A transmission method for transmitting a plurality of data files to a plurality of recipients ($D_1, \dots, D_M$), the method being implemented by an electronic transmitting device (30) and including:

- symmetrically encrypting (100) each of the files ($F_1, \dots, F_N$) via a symmetrical encryption algorithm and with a secret session key (K_{session}), the session key (K_{session}) being unique for the plurality of files ($F_1, \dots, F_N$), wherein the symmetrical encrypting (100) is performed separately for each of the files ($F_1, \dots, F_N$);
- asymmetrically encrypting (110), for each of the recipients ($D_1, \dots, D_M$), the session key (K_{session}) via an asymmetrical encryption algorithm and with a respective public key (K_{pub_i}) for each recipient (D_i); and
- transmitting (120), to each recipient (D_i), the plurality (38) of encrypted data files and the respective encrypted session key (39).

2. The transmission method according to claim 1, wherein the method further includes, for each encrypted file, calculating a cryptographic quantity (50) via a cryptographic algorithm comprising a hash function, the cryptographic quantities (50) further being transmitted to each recipient (D_i).

3. The transmission method according to claim 2, wherein the method further includes calculating a signature (52) from the plurality of cryptographic quantities (50) and via a signature algorithm, the signature further being transmitted to each recipient (D_i), the signature preferably further depending on the session key (K_{session}).

4. The transmission method according to claim 1, wherein the method further includes calculating a signature from the plurality (38) of encrypted data files and the respective encrypted session key (39), via a signature algorithm, the signature further being transmitted to each recipient.

5. The transmission method according to any one of claims 1 to 4, wherein the transmitting (120) comprises sending the plurality (38) of encrypted data files and the respective encrypted session key (39) to a radioelectric transmitter (22), for the transmission in the form of radioelectric signals of the plurality (38) of encrypted data files and the encrypted session key (39) to each respective recipient (D_i).

6. The transmission method according to any one of claims 1 to 5, wherein the transmitting (120) comprises storing, on a computer medium, the plurality (38) of encrypted data files and the respective encrypted session key (39), said computer medium being intended for the respective recipient (D_i).

7. A computer program comprising software instructions which, when executed by a computer, carry out a method according to any one of the preceding claims.

8. An electronic transmitting device (30) for transmitting a plurality of data files to a plurality of recipients ($D_1, \dots, D_M$), the electronic transmitting device (30) including:

- a symmetrical encryption module (32) configured for symmetrically encrypting each of the files ($F_1, \dots, F_N$) via a symmetrical encryption algorithm and with a secret session key (K_{session}), the session key (K_{session}) being unique for the plurality of files ($F_1, \dots, F_N$), wherein the symmetrical encrypting is performed separately for each of the files ($F_1, \dots, F_N$);
- an asymmetrical encryption module (34) configured for, for each of the recipients ($D_1, \dots, D_M$), asymmetrically encrypting the session key (K_{session}) via an asymmetrical encryption algorithm and with a respective public key (K_{pub_i}) for each recipient (D_i); and
- a transmission module (36) configured for transmitting, to each recipient (D_i), the plurality (38) of encrypted data files and the respective encrypted session key (39).

9. A receiving method for receiving a plurality of data files from a sender, the method being carried out by an electronic receiving device (40) and including:

- receiving (150) the plurality (38) of symmetrically encrypted data files and the associated secret session key (39), asymmetrically encrypted;
- asymmetrically decrypting (160) the session key (39) via a corresponding asymmetrical decryption algorithm and with a private key (K_{priv_i}) associated with the recipient (D_i); and
- symmetrically decrypting (170) at least one encrypted file received via a corresponding symmetrical decryption algorithm and with the decrypted private session key (K_{session}), wherein the symmetrical decrypting (170) is performed separately for each of the files.

10. An electronic receiving device (40) for receiving a plurality of data files from a sender, the electronic receiving device (40) including:

- a receiving module (42) configured for receiving the plurality (38) of symmetrically encrypted data files and the associated secret session key (39), asymmetrically encrypted;

- an asymmetrical decryption module (44) configured for asymmetrically decrypting the session key (39) via a corresponding asymmetrical decryption algorithm with a private key (K_{priv_i}) associated with the recipient (D_i); and

- a symmetrical decryption module (46) configured for symmetrically decrypting at least one encrypted file received via a corresponding symmetrical decryption algorithm and with the decrypted secret session key ($K_{session}$), wherein the symmetrical decrypting is performed separately for each of the files.