Method and electronic device for transmitting a plurality of data files to a plurality of recipients, computer program, receiving method and electronic receiving device

The present invention relates to a transmission method for transmitting a plurality of data files to a plurality of recipients, the method being implemented by an electronic transmitting device.

The invention also relates to a computer program including software instructions which, when executed by a computer, implement such a transmission method.

The invention also relates to such an electronic transmitting device for transmitting the plurality of data files to the recipients.

The invention also relates to a receiving method for receiving a plurality of data files from a sender, the method being carried out by an electronic receiving device.

The invention also relates to such an electronic receiving device for receiving the plurality of data files from the sender.

The invention also relates to a computer program including software instructions which, when executed by a computer, implement such a receiving method.

The invention relates to the field of the secure transmission of information, in the form of encrypted data files, between a sender and recipients. The transmission of the encrypted data files is for example done in the form of radioelectric signals, or via the storage of said encrypted files on a computer medium intended to be given to the corresponding recipient.

A transmission method is known for transmitting a data file to several recipients in which, in order to secure the sending of the file to each recipient, the data file is, before being transmitted, encrypted asymmetrically via an asymmetric encryption algorithm and with a respective public key for each recipient.

When a recipient receives the encrypted file, the received file is then decrypted asymmetrically via a corresponding asymmetrical decryption algorithm and with a private key associated with the recipient.

However, such a transmission method requires performing the asymmetrical encryption of the data file for each of the recipients, and then is particularly heavy in terms of consuming time and computer resources.

The aim of the invention is then to propose a method and a device for transmitting a plurality of data files to several recipients, which allow a more effective secure transmission of the data files between the sender and the various recipients.

To that end, the present invention relates to a transmission method for transmitting a plurality of data files to a plurality of recipients, the method being implemented by an electronic transmitting device and including:

- symmetrically encrypting each of the files via a symmetrical encryption algorithm and with a secret session key, the session key being unique for the plurality of files;

- asymmetrically encrypting, for each of the recipients, the session key via an asymmetrical encryption algorithm and with a respective public key for each recipient; and

- transmitting, to each recipient, the plurality of encrypted data files and the respective encrypted session key.

With the transmission method according to the invention, the encryption of the data files is done once for all of the recipients via a symmetrical encryption algorithm and with a secret session key, the session key being unique for the plurality of files. The session key is next encrypted asymmetrically, for each of the recipients, via an asymmetrical encryption algorithm and with a respective public key for each recipient.

The transmission method according to the invention then avoids having to encrypt data files for each of the recipients.

Each of the data files further being encrypted separately, the transmission method then allows the recipient to decrypt only the data files he needs. In other words, with the transmission method according to the invention, the recipient does not necessarily have to decrypt all of the received files.

According to other advantageous aspects of the invention, the transmission method includes one or more of the following features, considered alone or according to all technically possible combinations:

- the method further includes, for each encrypted file, calculating a cryptographic quantity via a cryptographic algorithm comprising a hash function, the cryptographic quantities further being transmitted to each recipient;

- the method further includes calculating a signature from the plurality of cryptographic quantities and via a signature algorithm, the signature further being transmitted to each recipient,

the signature preferably further depending on the session key;

- the method further includes calculating a signature from the plurality of encrypted data files and the respective encrypted session key, via a signature algorithm, the signature further being transmitted to each recipient;

- the transmitting comprises sending the plurality of encrypted data files and the respective encrypted session key to a radioelectric transmitter, for the transmission in the form of radioelectric signals of the plurality of encrypted data files and the encrypted session key to each respective recipient; and

- the transmitting comprises storing, on a computer medium, the plurality of encrypted data files and the respective encrypted session key, said computer medium being intended for the respective recipient.

The invention also relates to a computer program including software instructions which, when executed by a computer, implement a transmission method as defined above.

The invention also relates to an electronic transmission device for transmitting a plurality of data files to several recipients, the electronic transmission device including:

- a symmetrical encryption module configured for symmetrically encrypting each of the files via a symmetrical encryption algorithm and with a secret session key, the session key being unique for the plurality of files;

- an asymmetrical encryption module configured for, for each of the recipients, asymmetrically encrypting the session key via an asymmetrical encryption algorithm and with a respective public key for each recipient; and

- a transmission module configured for transmitting, to each recipient, the plurality of encrypted data files and the respective encrypted session key.

The invention also relates to a receiving method for receiving a plurality of data files from a sender, the method being carried out by an electronic receiving device and including:

- receiving the plurality of symmetrically encrypted data files and the associated secret session key, asymmetrically encrypted;

- asymmetrically decrypting the session key via a corresponding asymmetrical decryption algorithm and with a private key associated with the recipient; and

- symmetrically decrypting at least one encrypted file received via a corresponding symmetrical decryption algorithm and with the decrypted private session key.

The invention also relates to an electronic receiving device for receiving a plurality of data files from a sender, the electronic receiving device including:

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

- an asymmetrical decryption module configured for asymmetrically decrypting the session key via a corresponding asymmetrical decryption algorithm with a private key associated with the recipient; and

- a symmetrical decryption module configured for symmetrically decrypting at least one encrypted file received via a corresponding symmetrical decryption algorithm and with the decrypted secret session key.

The invention also relates to a computer program including software instructions which, when executed by a computer, implement a receiving method as defined above.

These features and advantages of the invention will appear more clearly upon reading the following description, provided solely as a non-limiting example, and done in reference to the appended drawings, in which:

- figure 1 is a schematic illustration of a radioelectric station of a transmission network, the radioelectric station being capable of operating as a transmitting station or a receiving station and then comprising an electronic transmission device according to the invention and an electronic receiving device according to the invention;

- figure 2 is a schematic illustration of encrypted data files and the session key encrypted by the electronic transmission device according to the invention;

- figure 3 is a flowchart of a method for transmitting a plurality of data files to a plurality of recipients, according to the invention; and

- figure 4 is a flowchart of a method for receiving the plurality of data files, according to the invention.

A transmission network comprises a plurality of radioelectric stations 10 and is for example able to operate by frequency hopping. A radioelectric station 10 is illustrated in figure 1.

The transmission network is able to transmit, from one radioelectric station 10 to several other radioelectric stations 10, a plurality 11 of data files F_1, ... F_N, visible in figure 2. N represents the number of data files F_1, … F_N, and is an integer greater than or equal to 2.

The radioelectric station 10 designed to transmit the information is hereinafter called the transmitting station, and each radioelectric station 10 designed to receive the information is hereinafter called the receiving station.

The set of frequencies usable by the transmission network comprises a frequency plane, also called FH plane, for the frequency hopping operation. The FH plane for example belongs to the high frequency (HF) domain, comprised between 1.5 MHz and 30 MHz.

The number of radioelectric stations 10 is for example greater than or equal to five, each station 10 being able to transmit data in conference to the other stations 10 of the network.

M represents the number of recipients $D_1,\ldots, D_M$ of the plurality of encrypted data files transmitted by the transmitting station 10. M is for example equal to the total number of radioelectric stations 10 minus the transmitting station 10, and the total number of radioelectric stations 10 is then equal to M+1.

In a manner known *per se* and as shown in figure 1, each station 10 includes a transmission-reception chain 12, an antenna 14, a frequency synthesizer 16 and a processing unit 18.

The transmission-reception chain 12 is connected to the transmission-reception antenna 14, the frequency synthesizer 16 and the processing unit 18, the frequency synthesizer 16 and the processing unit 18 also being connected to each other.

The transmission-reception chain 12 comprises a receiver 20 for radioelectric signals from the antenna 14 and a transmitter 22 for radioelectric signals to the antenna 14. The transmission-reception chain 12 can be controlled in a known manner by the frequency synthesizer 16.

The processing unit 18 comprises an analog-digital converter 24 connected at the output of the receiver 20 of the transmission-reception chain, a microprocessor 26 connected at the output of the analog-digital converter 24, and a memory 28 connected to the microprocessor 26.

The analog-digital converter 24 is able to convert the voltage or current level provided by the receiver 20 into digital signal samples transmitted to the microprocessor 26.

The microprocessor 26 is connected to the frequency synthesizer 16 and the transmission-reception chain 12 for the transmission of radioelectric signals intended for other radioelectric stations 10 of the transmission network.

In the described embodiment, each station 10 is configured to operate alternatively as a transmitting station and a receiving station.

For the operation of the station 10 as transmitting station, the station 10 includes an electronic transmission device 30 for transmitting the plurality of data files F_1, ... F_N to various recipients.

The electronic transmission device 30 includes a symmetrical encryption module 32 configured for symmetrically encrypting each of the files F_1, ... 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, ... F_N.

The electronic transmission device 30 includes an asymmetrical encryption module 34 configured for, for each of the recipients D_1, ... D_M, asymmetrically encrypting the session key $K_{session}$ via an asymmetrical encryption algorithm and with a respective public key K_{pub}; for each recipient D_i, where i is an integer index representing a number of the recipient, i being between 1 and M.

The electronic transmission device 30 includes 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.

As an optional addition, the electronic transmission device 30 further includes a calculation module, not shown, configured for calculating, for each encrypted file, a cryptographic quantity 50 via a cryptographic algorithm comprising a hash function, the cryptographic quantities 50 further being transmitted to each recipient D_i. In the example of figure 2, the cryptographic quantity 50 associated with the file F_j is denoted H_j, where j is the integer index representing a number of the file, j being comprised between 1 and N.

As another optional addition, the calculation module is further configured for calculating a signature 52 from the plurality of cryptographic quantities 50 and via a signature algorithm, the signature 52 further being transmitted to each recipient. The signature 52 preferably further depends on the session key $K_{session}$, as shown in figure 2.

In an alternative that is not shown, the calculation module is configured for calculating a signature from the plurality 38 of encrypted data files and the respective encrypted session key 39, via the signature algorithm, the signature further being transmitted to each recipient. In other words, according to this alternative, the calculation module does not calculate a cryptographic quantity via a cryptographic algorithm comprising a hash function and the signature is not calculated from such cryptographic quantities, the signature being calculated directly from the plurality 38 of encrypted data files and the respective encrypted session key 39.

In the example of figure 1, the symmetrical encryption module 32, the asymmetrical encryption module 34 and the transmission module 36, as well as, optionally and additionally, the calculation module, are each made in the form of software executable by the processor 26. The memory 28 is then capable of storing symmetrical encryption software configured for symmetrically encrypting each of the files F_1 ,… F_N via the symmetrical encryption algorithm and with the secret session key $K_{session}$, asymmetrical encryption software configured for, for each of the recipients D_1, …, D_M, asymmetrically encrypting the session key $K_{session}$ via an asymmetrical encryption algorithm and with a respective public key for each recipient D_i, the plurality 38 of encrypted data files and the respective encrypted session key 39. As an optional addition,

the memory 28 is then capable of storing calculation software, not shown, configured for calculating, for each encrypted file, a cryptographic quantity 50 via the cryptographic algorithm comprising the hash function, the cryptographic quantities 50 further being transmitted to each recipient D_i. As another optional addition, the calculating software is further configured for calculating a signature 52 from the plurality of cryptographic quantities 50 and via the signature algorithm, the signature 52 further being transmitted to each recipient. In an alternative that is not shown, the calculating software is configured for calculating a signature from the plurality 38 of encrypted data files and the respective encrypted session key 39, via the signature algorithm, the signature further being transmitted to each recipient. The processor 26 is then able to execute each of the software applications from among the symmetrical encryption software, the asymmetrical encryption software and the transmission software.

In an alternative that is not shown, the asymmetrical encryption module 34 and the transmission module 36 and, optionally and additionally, the calculation module, are each made in the form of a programmable logic component, such as an FPGA (Field Programmable Gate Array), or in the form of a dedicated integrated circuit, such as an ASIC (Applications Specific Integrated Circuit).

When the transmission device 30 is made in the form of one or several software programs, i.e., in the form of a computer program, it is further able to be stored on a medium, not shown, readable by computer. The computer-readable medium is for example a medium suitable for storing electronic instructions and able to be coupled with a bus of a computer system. As an example, the readable medium is a floppy disk, an optical disc, a CD-ROM, a magnetic-optical disc, a ROM memory, a RAM memory, any type of non-volatile memory (for example, EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card. A computer program including software instructions is then stored on the readable medium.

The symmetrical encryption module 32 is configured for performing a symmetrical encryption separately for each of the files F_1, ... F_N via the symmetrical encryption algorithm and with the secret session key $K_{session}$. In other words, the symmetrical encryption module 32 is configured for generating the plurality 38 of encrypted data files, this plurality 38 comprising N separate encrypted files.

The symmetrical encryption algorithm implemented by the symmetrical encryption module 32 is for example a confidentiality-only encryption algorithm. The confidentiality-only encryption algorithm is for example an AES (Advanced Encryption Standard)algorithm, such as the AES algorithm used in CTR mode, commonly referred to as AES-CTR (*Advanced Encryption Standard - CounTeR*) or the AES algorithm used in

CBC mode and commonly referred to as AES-CBC (*Advanced Encryption Standard Cipher Block Chaining*). Alternatively, the confidentiality-only encryption algorithm is a DES (*Data Encryption Standard*), or Triple DES, algorithm.

Alternatively, the symmetrical encryption algorithm implemented by the symmetrical encryption module 32 is a confidentiality and integrity encryption algorithm. The confidentiality and integrity encryption algorithm is for example an AES algorithm, such as the AES algorithm used in GCM mode and commonly referred to as AES-GCM (*Advanced Encryption Standard Galois Counter Mode*), or used in CCM mode and commonly referred to as AES-CCM (*Advanced Encryption Standard Counter with CBC-MAC*). Alternatively, the confidentiality and integrity encryption algorithm is a DES (*Data Encryption Standard*), or Triple DES, algorithm.

The session key $K_{session}$ is unique for the plurality of files F_1, ... F_N. The session key $K_{session}$ is for example a 128-bit, 192-bit or 256-bit key, and preferably a 256-bit key.

The asymmetrical encryption key 34 is configured for performing, via the asymmetrical encryption algorithm, an asymmetrical encryption of the session key $K_{session}$ separately for each of the recipients D_1, ..., D_M and with the respective public-key K_{pub_i} associated with each recipient D_i.

Each respective public key K_{pub_i} is for example generated randomly. Each respective public key K_{pub_i} is for example a 256-bit key or a 512-bit key, and preferably a 512-bit key. The randomness is for example generated using an algorithm of the AES type used in CTR-DRBG (*CounTeR Deterministic Random Byte Generator*) mode.

The asymmetrical encryption algorithm implemented by the asymmetrical encryption module 34 is for example chosen from among the group consisting of: the ECIES (*Elliptic Curve Integrated Encryption Scheme*) algorithm, the ECDH (*Elliptic Curve Diffie–Hellman*) algorithm and the RSA-OAEP (*Rivest Shamir Adleman Optimal Asymmetric Encryption Padding*) algorithm.

The cryptographic algorithm comprising the hash function implemented by the calculation module is a hash algorithm, a signature algorithm or a HMAC (*Hash Message Authentication Code*) algorithm.

The hash algorithm is for example a SHA (*Secure Hash Algorithm*), such as one of algorithms SHA-256, SHA-384, SHA-512, SHA-512/256 and SHA-512/224, or algorithm SHA-3.

The signature algorithm implemented by the calculation module, whether to Coakley the cryptographic quantity 50 according to the aforementioned alternative or the signature 52, is for example an ECDSA (*Elliptic Curve Digital Signature Algorithm*) algorithm, such as the ECDSA-512 algorithm, or an EC-KCDSA (*Elliptic Curve - Korean*

Certificate-based Digital Signature Algorithm) algorithm, or the RSA-PSS (*Rivest Shamir Adleman - Probabilistic Signature Scheme*) algorithm.

The HMAC algorithm is an algorithm calculating an authentication code of the cryptographic message imprint with a key, using a cryptographic hash function in combination with a secret key.

The transmission module 36 is configured for sending the plurality 38 of encrypted data files and the respective encrypted session key 39 to the radioelectric transmitter 22, for the transmission in the form of radioelectric signals of the plurality of encrypted data files 38 and the encrypted session key 39 to each respective recipient D_i. The only encrypted session key 39 that is sent to the respective recipient D_i from among the various encrypted session keys is the session key encrypted asymmetrically with the respective public key K_{pub_i} for this recipient D_i.

Alternatively, the transmission module 36 is configured for 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. The computer medium on which the plurality 38 of encrypted data files and the respective encrypted session key 39 are stored is for example the computer-readable medium as defined above.

The cryptographic quantity 50 for example has a length of 224, 256, 384, 512 or 1024 bits, depending on the algorithm used. In algorithms SHA-256, SHA-384, SHA-512, the suffix refers to the size of the cryptographic quantity 50, also called hash. Algorithms SHA-512/256 and SHA-512/224 respectively generate 256-bit and 224-bit hashes.

The signature 52 for example has a length of 512 bits or 1024 bits.

For the operation of the station 10 as receiving station, the station 10 includes an electronic device 40 for receiving a plurality 38 of encrypted data files.

The electronic receiving device 40 includes a receiving module 42 configured for receiving the plurality 38 of symmetrically encrypted data files and the associated secret session key 39, asymmetrically encrypted.

The electronic receiving device 40 includes 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.

The electronic receiving device 40 includes 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 $K_{session}$.

As an optional addition, the electronic receiving device 40 further includes a verification module, not shown, configured to verify the signature 52 received via the signature algorithm.

Also as an optional addition, when the electronic transmission device 30 has transmitted the cryptographic quantities 50, the verification module is further configured to verify the cryptographic quantities 50 received via the cryptographic algorithm comprising the hash function. The verification module is preferably configured to verify only the cryptographic quantity or quantities H_j corresponding to the file(s) that the recipient D_i wishes to decrypt from among the received plurality 38 of encrypted data files.

In the example of figure 1, the receiving module 42, the symmetrical decryption module 44 and the asymmetrical decryption module 46, as well as, optionally and additionally, the verification module, are each made in the form of software executable by the processor 26. The memory 28 is then capable of storing receiving software configured for receiving the plurality 38 of symmetrically encrypted data files and the associated secret session key 39, asymmetrical decryption software configured for asymmetrically decrypting the encrypted session key 39 via the corresponding asymmetrical decryption algorithm and the private key K_{priv_i} associated with the recipient D_i, and symmetrical decryption software configured for symmetrically decrypting at least one encrypted file received via the corresponding symmetrical decryption algorithm and with the decrypted secret session key $K_{session}$. As an optional addition, the memory 28 is then capable of storing verification software, not shown, configured to verify the received signature 52 via the signature algorithm. As another optional addition, the verification software is further configured to verify the cryptographic quantities 50 optionally received via the cryptographic algorithm comprising the hash function. The processor 26 is then able to execute each of the software applications from among the symmetrical decryption software, the asymmetrical decryption software and the receiving software.

In an alternative that is not shown, the receiving module 42, the symmetrical decryption module 44 and the asymmetrical decryption module 46, as well as, optionally and additionally, the verification module, are each made in the form of a programmable logic component, such as an FPGA (Field Programmable Gate Array), or in the form of a dedicated integrated circuit, such as an ASIC (Applications Specific Integrated Circuit).

When the receiving device 40 is made in the form of one or several software programs, i.e., in the form of a computer program, it is further able to be stored on a medium, not shown, readable by computer. The computer-readable medium is for example a medium suitable for storing electronic instructions and able to be coupled with a bus of a computer system. As an example, the readable medium is a floppy disk, an

optical disc, a CD-ROM, a magnetic-optical disc, a ROM memory, a RAM memory, any type of non-volatile memory (for example, EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card. A computer program including software instructions is then stored on the readable medium.

The receiving module 42 is configured for receiving the plurality 38 of encrypted data files and the respective encrypted session key 39 from the radioelectric receiver 20 via the analog-digital converter 24, after reception by the antenna 14 and in the form of radioelectric signals from the plurality 38 of encrypted data files and the encrypted session key 39.

Alternatively, the receiving module 42 is configured for reading, on the computer medium, the plurality 38 of encrypted data files and the respective encrypted session key 39.

The asymmetrical decryption algorithm implemented by the asymmetrical decryption module 44 is the inverse algorithm of the asymmetrical encryption algorithm implemented by the asymmetrical encryption module 34.

Each private key K_{priv_i} associated with the recipient D_i is for example a 256-bit key or a 512-bit key, and preferably a 512-bit key.

The symmetrical decryption algorithm implemented by the symmetrical decryption module 46 is the inverse algorithm of the symmetrical encryption algorithm implemented by the symmetrical encryption module 32.

According to the optional addition, the verification module is configured to implement the same signature algorithm as that implemented by the calculation module.

According to the other optional addition, the verification module is configured to implement the same cryptographic algorithm comprising the hash function as that implemented by the calculation module.

Alternatively, each station 10 is configured to operate only as a transmitting station or only as a receiving station. Each transmitting station 10 then comprises only the electronic transmitting device 30. Each receiving station 10 then comprises only the electronic receiving device 40.

The transmission method according to the invention will now be described in light of figure 3 illustrating a flowchart of the transmission method.

During an initial step 100, the electronic transmission device 30 performs, via its symmetrical encryption module 32, a symmetrical encryption of each of the files F_1, ... F_N via the symmetrical encryption algorithm and with the secret session key $K_{session}$.

During a following step 110, the electronic transmission device 30 next performs, via its asymmetrical encryption module 34 and for each of the recipients D_1, ..., D_M, an

asymmetrical encryption of the session key $K_{session}$ via the asymmetrical encryption algorithm and with the respective public key K_{pub_i} for each recipient D_i.

The electronic transmission device 30 lastly transmits, during step 120 and via its transmission module 36, the plurality 38 of encrypted data files and the respective encrypted session key 39 to each recipient D_i.

As an optional addition, during an optional step that is not shown, inserted between steps 110 and 120, the electronic transmission device 30 further calculates, via its calculation module and for each encrypted file, the cryptographic quantity 50 using the cryptographic algorithm comprising a hash function. The cryptographic quantities 50 are then further transmitted to each recipient D_i during the transmission step 120.

As another optional addition, after the step for calculating the cryptographic quantities 50 and before the transmission step 120, the electronic transmission device 30 further calculates, via its calculation module, the signature 52 from the plurality of cryptographic quantities 50 and via the signature algorithm. The signature 52 preferably further depends on the session key $K_{session}$. The signature 52 is then further transmitted to each recipient D_i during the transmission step 120.

Alternatively, during an optional step inserted between the steps 110 and 120, the electronic transmission device 30 calculates, via its calculation module, the signature from the plurality 38 of encrypted data files and the respective encrypted session key 39, via the signature algorithm, the signature further being transmitted to each recipient. In other words, according to this alternative, the calculation module does not calculate a cryptographic quantity and the signature is not calculated from such cryptographic quantities, the signature being calculated directly from the plurality 38 of encrypted data files and the respective encrypted session key 39.

The receiving method according to the invention will now be described in light of figure 4 illustrating a flowchart of the receiving method.

During an initial step 150, the electronic receiving device 40 receives, via its receiving module 42, the plurality 38 of symmetrically encrypted data files and the associated secret session key 39, asymmetrically encrypted.

As previously stated, this reception is for example a reception by the radioelectric receiver 20 via the analog-digital converter 24, after reception by the antenna 14 and in the form of radioelectric signals from the plurality 38 of encrypted data files and the encrypted session key 39; or reading on the computer medium of the plurality 38 of encrypted date files and the respective encrypted session key 39.

During a following step 160, the electronic receiving device 40 performs, via its asymmetrical decryption module 44, an asymmetrical decryption of the session key 39 via

the corresponding asymmetrical decryption algorithm with the private key K_{priv_i} associated with the recipient D_i.

The electronic receiving device 40 lastly performs, during the step 170 and via its symmetrical decryption module 46, a symmetrical decryption of at least received one encrypted file, via the corresponding symmetrical decryption algorithm and with the decrypted secret session key $K_{session}$.

As an optional addition, during an optional step that is not shown, inserted between steps 160 and 170, the electronic receiving device 40 verifies, via its verification module, the received signature 52 by implementing the same signature algorithm as that implemented by the calculation module, included in the electronic transmission device 30 according to this optional addition.

As another optional addition, when the electronic transmission device 30 has transmitted the cryptographic quantities 50, the electronic receiving device 40 verifies, via its verification module, the received cryptographic quantities 50 by implementing the same cryptographic algorithm comprising the hash function as that implemented by the calculation module, included in the electronic transmission device 30 according to this optional addition.

During this optional step, the electronic receiving device 40 preferably verifies only the cryptographic quantity or quantities H_j corresponding to the file(s) that the recipient D_i wishes to decrypt from among the received plurality 38 of encrypted data files.

Thus, with the transmission method according to the invention, the encryption of the data files F1, ... F_N is done once for all of the recipients D_1, ... D_M via the symmetrical encryption algorithm and with a secret session key $K_{session}$, the session key $K_{session}$ being unique for the plurality of files. The session key $K_{session}$ is next encrypted asymmetrically, for each of the recipients D_1, ... D_M, via an asymmetrical encryption algorithm and with a respective public key K_{pub_i} for each recipient D_i. The encryption of the data files is then not done for each of the recipients D_1, ... D_M, but only once.

Each of the data files F_1, ... F_N further being encrypted separately, the transmission method then allows the recipient D_i to decrypt only the data files he needs. The recipient D_i does not necessarily have to decrypt all of the received files.

As an optional addition, the calculation, then transmission of the cryptographic quantities 50 to each recipient D_i allows the recipient D_i to verify separately that each of the data files F_1, ... F_N has not been corrupted.

As another optional addition, the calculation of the signature from the plurality of cryptographic quantities 50 and preferably further from the session key $K_{session}$ or directly from the plurality 38 of encrypted data files and the respective session key 39, then the

transmission of the calculated signature to each recipient D_i allows the recipient D_i, in case of corruption of the data by an attacker, to detect such corruption during the verification of the signature.

One can then see that the transmission method and device 30 according to the invention allow a more effective secure transmission of the data files between the sender and the various recipients D_1, ... D_M.

CLAIMS

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

- symmetrically encrypting (100) each of the files (F_1, ... 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, ... F_N);

- asymmetrically encrypting (110), for each of the recipients (D_1, ..., 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, ... D_M), the electronic transmitting device (30) including:

- a symmetrical encryption module (32) configured for symmetrically encrypting each of the files (F_1, ..., 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, ... F_N);
- an asymmetrical encryption module (34) configured for, for each of the recipients (D_1, ... 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 ($K_{session}$).

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 ($K_{session}$).