Claims

1. A method for improving security of data on a mobile terminal in an off-line state, encrypted data being decrypted in the off-line state without accessing a server, the method, comprising:

generating a service key; and

encrypting/decrypting the service key including:

generating a key pair including a first public key and a first private key;

acquiring, by the mobile terminal, identification information of the mobile terminal; and

encrypting, by the mobile terminal, the key pair including the first public key and the first private key by using the identification information of the mobile terminal, to obtain a first encrypted public key and a first encrypted private key and save them;

wherein the encrypting the key pair including the first public key and the first private key by using the identification information includes:

generating a character string according to the identification information wherein the generating a character string according to the identification information includes performing a hash algorithm processing on the identification information, to obtain the character string;

and encrypting the key pair including the first public key and the first private key separately by using the character string to obtain the first encrypted public key and the first encrypted private key.

2. The method improving security of data on a mobile terminal in an off-line state of claim 1, wherein the identification information comprises one or more of the following types:

an international mobile equipment identity;

an international mobile subscriber identification number,

a media access control address; and

a universally unique identifier of the mobile terminal.

3. An apparatus for encrypting/decrypting data on a mobile terminal and for improving security of data on a mobile terminal in an off-line state, encrypted data being decrypted in the off-line state without accessing a server, the apparatus comprising:

a first generation unit configured to generate a service key;

a second generation unit configured to generate a key pair including a first public key and a first private key;

a first acquisition unit configured to acquire identification information of the mobile terminal;

a first encryption unit configured to encrypt the key pair including the first public key and the first private key by using the identification information, to obtain a first encrypted public key and a first encrypted private key and save them;

wherein the first encryption unit is further configured to generate a character string according to the identification information wherein the generating the character string according to the identification information includes performing a hash algorithm processing on the identification information, to obtain the character string.; and encrypting the first public key and the first private key separately by using the character string;

a first decryption unit configured to decrypt the first encrypted private key by using the identification information, to obtain the first private key;

wherein the first decryption unit is further configured to generate a character string according to the identification information; and decrypt the first encrypted private key by using the character string.

a second encryption unit configured to encrypt the service key by using the first private key, to obtain an encrypted service key;

a second decryption unit configured to decrypt the first encrypted public key by using the identification information, to obtain the first public key;

wherein the second decryption unit is configured to generate a character string according to the identification information; and decrypt the first encrypted public key by using the character string.

a third decryption unit configured to decrypt the encrypted service key by using the first public key, to obtain the service key;

a second acquisition unit configured to acquire data that needs to be encrypted/decrypted on the mobile terminal;

a third encryption unit configured to encrypt the data by using the service key; and

a fourth decryption unit configured to decrypt the data by using the service key.

4. The apparatus for encrypting/decrypting data on a mobile terminal and for improving security of data on a mobile terminal in an off-line state of claim 3, wherein the identification information comprises one or more of the following types:

an international mobile equipment identity;

an international mobile subscriber identification number,

a media access control address; and

a universally unique identifier of the mobile terminal.