

METHOD AND APPARATUS FOR ENCRYPTING/DECRYPTING DATA ON MOBILE TERMINAL

Technical Field

The present application relates to the field of data processing and, in particular, to a method and an apparatus for encrypting/decrypting data on a mobile terminal.

Background

With the development of mobile communications and network technologies, people have gradually developed a habit of accessing the Internet by using mobile terminals (such as mobile phones and tablet computers). Therefore, a lot of private data, including a unique identifier of a mobile phone device and some key service data, needs to be saved on a mobile terminal. Such data needs to be securely stored on the mobile terminal, and therefore, a secure data encryption method is needed to ensure that the private data will not be stolen or tampered with.

In the prior art, data on a mobile terminal is protected by means of hardware protection or public and private key protection. The hardware protection is generally a method of using an encryption card or a mobile phone shield as a carrier for protecting private data on the mobile terminal, to store the private data in plain text. For example, key seeds are integrated in a central processor by using a certificate shield of a bank, to encrypt and decrypt data. To protect data on the mobile terminal by using public and private keys, the data needs to be encrypted by using keys exchanged on a network.

The method of protecting data on a mobile terminal by using hardware is expensive, and is not suitable for promotion and popularization among the public. When data on a mobile terminal is protected by using public and private keys, data needs to be decrypted on a server, which can be implemented only in the case of a network connection, and cannot be used in an offline state.

Summary of the Invention

An objective of the present application is to provide a method and an apparatus for encrypting/decrypting data on a mobile terminal, which can protect the data in an offline state without hardware protection, so that the data will not be stolen or tampered with.

According to a first aspect, the present application provides a method for encrypting/decrypting data on a mobile terminal, including generating a service key, and

encrypting/decrypting the service key, which includes:

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

- acquiring identification information of the mobile terminal;

- encrypting 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;

- acquiring the identification information of the mobile terminal during encryption of the service key;

- decrypting the first encrypted private key by using the identification information, to obtain the first private key;

- encrypting the service key by using the first private key, to obtain an encrypted service key;

- acquiring the identification information of the mobile terminal during decryption of the service key;

- decrypting the first encrypted public key by using the identification information, to obtain the first public key;

- decrypting the encrypted service key by using the first public key, to obtain the service key;

- acquiring data that needs to be encrypted/decrypted on the mobile terminal; and

- encrypting/decrypting the data by using the service key.

According to a second aspect, the present application provides an apparatus for encrypting/decrypting data on a mobile terminal, including:

- 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;

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

- 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;

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.

The method and apparatus for encrypting/decrypting data on a mobile terminal provided in the embodiments of the present application implements protection for private data on a mobile terminal by using processes of initialization, encryption, and decryption. Moreover, there is no need for hardware, data protection costs are low, and the data can be protected in an offline state, so that the data will not be stolen or tampered with.

Brief Description of the Drawings

FIG. 1 is a flowchart of a method for encrypting/decrypting data on a mobile terminal according to Embodiment 1 of the present application; and

FIG. 2 is a schematic diagram of an apparatus for encrypting/decrypting data on a mobile terminal according to Embodiment 2 of the present application.

Detailed Description

To make the objectives, technical solutions, and advantages of the embodiments of the present application clearer, the technical solutions in the embodiments of the present application will be clearly and completely described below with reference to the accompanying drawings in the present application. Apparently, the described embodiments are merely some but not all of the embodiments of the present application. All other embodiments obtained by those of ordinary skill in the art based on the embodiments in the present application without creative efforts fall in the protection scope of the present application.

To facilitate comprehension of the embodiments of the present application, the following provides further detailed descriptions with reference to the accompanying drawings and specific embodiments, and the embodiments do not constitute a limit to the embodiments of the present application.

A method and an apparatus for encrypting/decrypting data on a mobile terminal

provided in the embodiments of the present application are applicable to mobile terminals, such as a mobile phone and a tablet computer.

FIG. 1 is a flowchart of a method for encrypting/decrypting data on a mobile terminal according to Embodiment 1 of the present application. Steps of the method are performed by a mobile terminal. As shown in FIG. 1, the method specifically includes:

S101: generating a key pair including a first public key and a first private key.

Specifically, the mobile terminal generates a key pair including a first public key and a first private key; a generation method belongs to the prior art, and is not described in detail herein. The first public key and the first private key are generated simultaneously. Information encrypted with the first public key can only be decrypted with the first private key, and information encrypted with the first private key can only be decrypted with the first public key.

S102: acquiring identification information of the mobile terminal.

Specifically, the identification information of the mobile terminal is acquired by using a code.

The identification information includes one or more of the following types:

an International Mobile Equipment Identity (IMEI), an International Mobile Subscriber Identification Number (IMSI), a Media Access Control (MAC) address, and a Universally Unique Identifier (UUID) of the mobile terminal.

S103: generating a character string by using the identification information.

Specifically, hash algorithm processing is performed on the identification information, to obtain the character string.

A hash algorithm maps a binary value of any length into a shorter binary value with a fixed length, and this shorter binary value is referred to as a hash value. The hash value is a unique and extremely compact numeral expression form of a data segment. In hashing of a plain text, if only one letter of the paragraph is changed, a different hash value will be generated subsequently. It is impossible in calculation to find two different inputs that are hashed to a same value. Therefore, a hash value of data may be used to check the integrity of the data, and is generally used in quick search and encryption algorithms.

S104: encrypting the first public key and the first private key by using the character string, to obtain a first encrypted public key and a first encrypted private key.

Specifically, the first public key and the first private key are encrypted by using the character string and a symmetric encryption algorithm, to obtain the first encrypted public key and the first encrypted private key.

The encryption algorithm may be: an Advanced Encryption Standard (AES), a Data Encryption Standard (DES), a triple data encryption algorithm, and the like.

It should be noted that, the character string is a root key, and after being generated, is used for encrypting the first public key and the first private key. The root key is not saved, and is generated by using the identification information of the mobile terminal when needed.

The above is an initialization process. Each mobile terminal needs to be initialized once. Initialization is a prerequisite for encryption and decryption. The purpose of the initialization process is to obtain the first encrypted public key and the first encrypted private key.

S105: generating a service key.

Specifically, the service key is a service key randomly generated by the mobile terminal, and each service uses one service key. A method for generating the service key is the same as that for generating the key pair including the first public key and the first private key, and is not described in detail herein.

S106: encrypting data by using the service key, to obtain encrypted data.

Specifically, to-be-encrypted data on the mobile terminal is acquired, and the data is encrypted by using the service key and a symmetric encryption algorithm, to obtain the encrypted data, thus ensuring the security of the data. The data includes private data, such as a biological feature of a user.

S107: decrypting the first encrypted private key by using the character string, to obtain the first private key.

Before step S107, the root key is not saved; therefore, steps S102 and S103 need to be performed again, to obtain the character string.

The first encrypted private key is decrypted by using the character string and a symmetric decryption algorithm, to obtain the first private key.

S108: encrypting the service key by using the first private key, to obtain an encrypted service key.

Specifically, the service key is encrypted by using the first private key and an asymmetric algorithm, to obtain an encrypted service key.

The asymmetric algorithm may be: a public-key encryption algorithm (RSA), a Digital Signature Algorithm (DSA), and the like.

It should be noted that, steps S105 to S108 are an encryption process, which implements encryption of the private data, to prevent the private data from being stolen or tampered with. Moreover, the encrypted service key obtained in step S108 can be used for

decrypting encrypted private data when private data is used.

S109: decrypting the first encrypted public key by using the character string, to obtain the first public key.

Before step S109, the root key is not saved; therefore, steps S102 and S103 need to be performed again, to obtain the character string.

The first encrypted public key is decrypted by using the character string and a symmetric decryption algorithm, to obtain the first public key.

S110: decrypting the encrypted service key by using the first public key, to obtain the service key.

Specifically, the encrypted service key is decrypted by using the first public key and an asymmetric decryption algorithm, to obtain the service key.

S111: decrypting the encrypted data by using the service key, to obtain the data.

Specifically, the encrypted private data is decrypted by using the service key and a symmetric decryption algorithm, to obtain the private data.

It should be noted that, steps S109 to S111 are a process of decrypting the encrypted data. The character string is generated according to the identifier of the device, and during decryption, the character string may be generated at any time according to the mobile phone device for decryption. Therefore, the encrypted private data can be decrypted in an offline state without accessing a server. Meanwhile, the character string is generated according to a local device for decryption, even if data leakage occurs, the data cannot be decrypted by others using other devices. Therefore, user privacy can be effectively protected from leakage.

The method for encrypting/decrypting data on a mobile terminal provided in Embodiment 1 of the present application implements protection for private data on a mobile terminal by using processes of initialization, encryption, and decryption, wherein a root key is not saved; through information calculation by the mobile terminal, a public-private key pair ensures the security of a service key, and the service key protects the data. Hardware protection is not needed, data protection costs are low, and security of data can be ensured in an offline state, so that the data will not be stolen or tampered with.

Corresponding to the foregoing method for encrypting/decrypting data on a mobile terminal, Embodiment 2 of the present application provides an apparatus for encrypting/decrypting data on a mobile terminal. FIG. 2 is a schematic diagram of an apparatus for encrypting/decrypting data on a mobile terminal according to Embodiment 2 of the present application. As shown in FIG. 2, the apparatus specifically includes: a first generation unit 201, a second generation unit 202, a first acquisition unit 203, a first

encryption unit 204, a first decryption unit 205, a second encryption unit 206, a second decryption unit 207, a third decryption unit 208, a second acquisition unit 209, a third encryption unit 210, and a fourth decryption unit 211.

The first generation unit 201 is configured to generate a service key.

The second generation unit 202 is configured to generate a key pair including a first public key and a first private key.

The first acquisition unit 203 is configured to acquire identification information of the mobile terminal.

The first encryption unit 204 is 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.

The first decryption unit 205 is configured to decrypt the first encrypted private key by using the identification information, to obtain the first private key.

The second encryption unit 206 is configured to encrypt the service key by using the first private key, to obtain an encrypted service key.

The second decryption unit 207 is configured to decrypt the first encrypted public key by using the identification information, to obtain the first public key.

The third decryption unit 208 is configured to decrypt the encrypted service key by using the first public key, to obtain the service key.

The second acquisition unit 209 is configured to acquire data that needs to be encrypted/decrypted on the mobile terminal.

The third encryption unit 210 is configured to encrypt the data by using the service key.

The fourth decryption unit 211 is configured to decrypt the data by using the service key.

Optionally, the first encryption unit 204 is specifically configured to:
generate a character string according to the identification information; and
encrypt the first public key and the first private key separately by using the character string.

Optionally, the first decryption unit 205 is specifically configured to:
generate a character string according to the identification information; and
decrypt the first encrypted private key by using the character string.

Optionally, the second decryption unit 207 is specifically configured to:
generate a character string according to the identification information; and

decrypt the first encrypted public key by using the character string.

Optionally, the generating a character string according to the identification information is specifically:

performing hash algorithm processing on the identification information, to obtain the character string.

Optionally, the identification information includes one or more of the following types:

an International Mobile Equipment Identity (IMEI), an International Mobile Subscriber Identification Number (IMSI), a Media Access Control (MAC) address, and a Universally Unique Identifier (UUID) of the mobile terminal.

The method provided in Embodiment 1 of the present application is implanted in the apparatus provided in Embodiment 2 of the present application. Therefore, a specific working process of the apparatus provided in the present application is not described in detail herein again.

The apparatus for encrypting/decrypting data on a mobile terminal provided in Embodiment 2 of the present application implements protection for private data on a mobile terminal by using processes of initialization, encryption, and decryption, wherein a root key is not saved; through information calculation by the mobile terminal, a public-private key pair ensures the security of a service key, and the service key protects the data. Hardware protection is not needed, data protection costs are low, and security of data can be ensured in an offline state, so that the data will not be stolen or tampered with.

Those of ordinary skill in the art could also be aware that objects and algorithm steps in examples described with reference to the embodiments disclosed herein can be implemented by electronic hardware, computer software, or a combination thereof. To clearly illustrate the interchangeability between hardware and software, the composition and steps of each example have been described in general according to functions in the foregoing description. Whether these functions are executed by using hardware or software depends on a specific application and design constraint conditions of the technical solution. For each specific application, professionals may use a different method to implement the described functions. However, such implementation should not be considered as exceeding the scope of the present application.

Steps of the method or algorithm described with reference to the embodiments disclosed herein may be implemented by hardware, a software module executed by a processor, or a combination thereof. The software module may be disposed in a random access memory (RAM), a memory, a read-only memory (ROM), an electrically

programmable ROM, an electrically erasable programmable ROM, a register, a hard drive, a removable disk, a CD-ROM, or any other form of storage medium commonly known in the technical field.

The foregoing specific implementations provide further detailed description of the objectives, technical solutions, and beneficial effects of the present application. It should be understood that, described above are merely specific implementations of the present application, which are not intended to limit the protection scope of the present application. Any modification, equivalent replacement, improvement, and the like made within the spirit and principle of the present application shall all be included in the protection scope of the present application.

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.