

METHOD AND APPARATUS FOR ENCRYPTING/DECRYPTING DATA ON MOBILE TERMINAL

Abstract

The present invention relates to a method and apparatus for encrypting/decrypting data on a mobile terminal. The method comprises: pre-generating a key pair including a first public key and a first private key; acquiring identification information about a mobile terminal; encrypting the key pair including the first public key and the first private key using the identification information to obtain a first encrypted public key and a first encrypted private key and saving same; when a service key is encrypted, encrypting the service key using the first private key to obtain an encrypted service key; when the service key is decrypted, decrypting the encrypted service key using the first public key to obtain the service key; acquiring data needing to be encrypted/decrypted of the mobile terminal; and encrypting/decrypting the data using the service key. According to the method and apparatus for encrypting/decrypting data involved in the present invention, hardware protection is not required, and the data protection cost is low. In addition, the security of the data can be protected in an off-line case, so that the data cannot be intercepted and tampered with.

Figure 1