ABSTRACT

A data-protection system which permits authorized users to use a target data through a simple operation but does not permit unauthorized users to use the program even though they may be able to copy it. A data-protecting system in which a center prepares a special algorithm which is secretly held by the center only, the center prepares a secret algorithm exclusively for the data and for the user by applying the center algorithm to the data and the user identifier which are inherent to the data and the user, and are well-known to the public and are used without any change, and supplies the secret algorithm to the user and to the data supplier and then when it happens that the data supplier must supply a data to the user, the data supplier prepares the same and a specific encryption key between the data that is to be supplied and the user by inputting the user identifier to the secret algorithm of the data that is to be supplied, encrypts part or whole of the data that is to be supplied directly or indirectly based on the encryption key and supplies it to the user, and the user prepares the same encryption key between the data that is supplied and the user based upon the data identifier that is supplied and his own secret algorithm and decrypts the encrypted data directly or indirectly.