ABSTRACT

For effecting cryptographic communications between entities i, j using a common cryptokey, each of the entities i, j generates a common cryptokey by applying an identifier transformation algorithm and a secret private key, which have previously been distributed from a center, to the identifier of the other entity with which to communicate (step 3). In a transmitting side, one-time pass cryptographic communication random number data are generated and encrypted by the common cryptokey, a plaintext is encrypted using the random number data, and the encrypted random number data and the encrypted plaintext are combined into an encrypted communication text (step 4). In a receiving side, the encrypted random number data in the encrypted communication text are decrypted using the common cryptokey, and the encrypted plaintext is decrypted using the decrypted random number data as a key (step 5).