

SYSTEM AND METHOD FOR CONSTRUCTING A SELF-AUTHENTICATING MESSAGE USING IDENTITY-BASED CRYPTOGRAPHY

Abstract

This document discloses a system and method for constructing a self-authenticating message that is to be sent from a first electronic device to a second electronic device. The disclosed system and method constructs a self-authenticating message using identity-based cryptography whereby plaintext is encrypted and decrypted using encryption/decryption keys that were generated using identities of the sender and/or receiver.

FIGURE 4