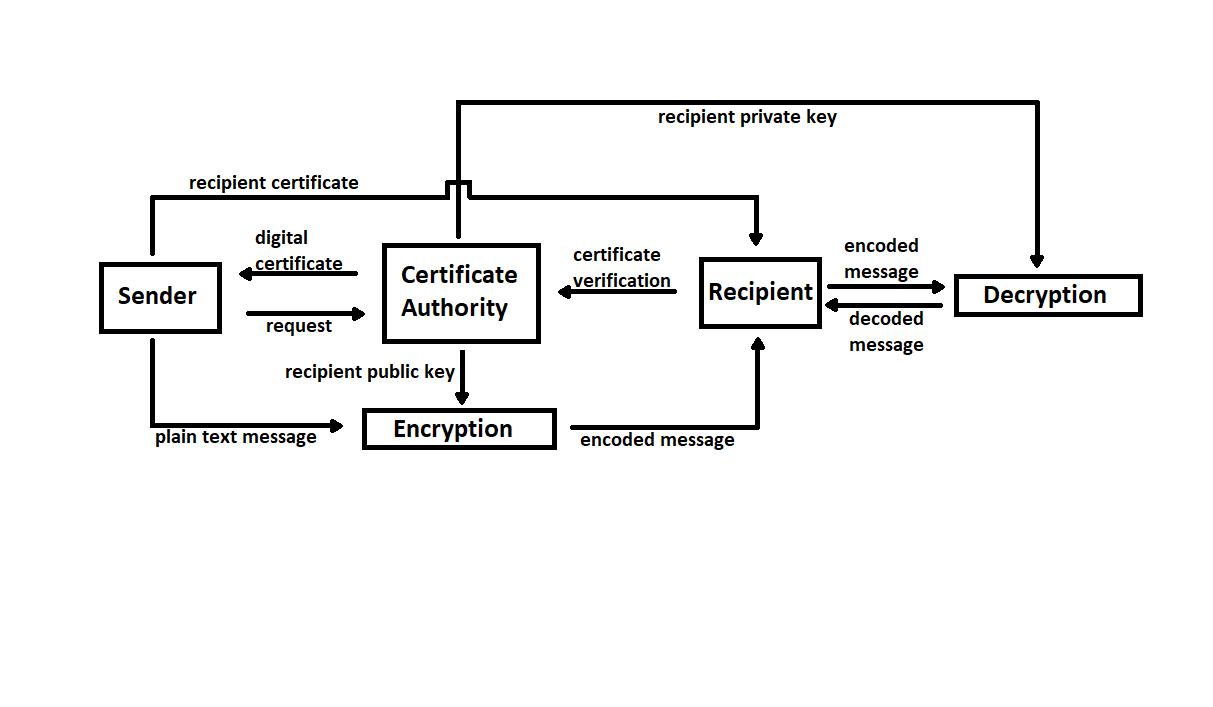
Public Key Infrastructure is used to manage keys and certificates. It is used extensively on Internet today to provide secured communication between client and server, without explicitly establishing prior trust between them. It is important to understand the actual process in the PKI for establishing the secure communication. Create a diagram that shows the establishment of secured communication of a message from sender to recipient, with the following PKI components to provide confidentiality and authentication function:

* Sender
* Recipient
* Recipient private key
* Recipient public key
* Recipient Digital certificate
* Plaintext message
* Encoded message
* Certificate Authority

**Explanation:**

Essentially what’s happening here is the sender is sending an encoded message to the recipient after receiving the digital certificate and public key from the certificate authority. The recipient verifies the certificate with the authority and decrypts the message with the private key. Pretty simple.