CPA security alone is not sufficient. The adversary might have access to both encryption as well as a decryption server. In that case we need a CCA secured scheme. Cryptosystem is CCA secured if for all probabilistic polynomial time adversaries A:

$$\mathbf{P[b_{guess} = b] <= 0.5 + negl(n)}$$

For CCA encryption scheme, we will use the *Encrypt then Authenticate* strategy. The message will be encrypted using CPA encryption scheme. MAC will be used on the encrypted result to obtain a tag.

Encryption: On input keys (k1, k2) and plaintext message m, compute c <- Enc_{k1}(m) and t <- MAC_{k2}(c) and output the ciphertext (c,t).

Decryption: On input keys (k1, k2) and a ciphertext (c,t) first check whether Verify_{k2}(c,t) == 1. If yes, output Dec_{k1}(c), else output null.

Having access to the decryption server is of no use if the message is modified.