CCA Secure Encryption Scheme

Let (Gen_E, Enc, Dec) be a private key encryption scheme and let (Gen_M, Mac, Vrfy) be a message authentication code.

Gen`: The Gen algorithm takes the input of 1^n and outputs two keys using $Gen_E(1^n)$ and $Gen_M(1^n)$ as k1 and k2 respectively.

Enc`: The Enc algorithms takes the plain message and keys k1 and k2 as input, and calculates Cipher c= Enc(k1,m) and MAC tag t= MAC(k2,c) and outputs the cipher text c,t.

Here Enc is a CPA secure encryption algorithm.

Dec`: On input keys k1,k2 and cipher text c,t. First the tag is verified using Vrfy(k2,c,t). If the output is accept, cipher is decrypted using Dec(k1,c), else there is no output.

Here Dec is a CPA secure decryption algorithm.