CCA Security Theory

For CCA Security, previously built CPA security and secure MAC can be used.
The following is a simple formulation of the same:

1. Create 2 keys, k_{cpa} and k_{mac} for cpa encryption and Variable Length MAC verification respectively.
2. $c = CPAEncrypt(m, k_{cpa})$
3. $t = MAC(c, k_{mac})$
4. $c' =< c, t >$

Thus c' gives us the new encrypted cipher text.

This encryption scheme where encryption is done using CPA and then verification is done using a VLMAC improves on the limitations of both individual methods. The MAC scheme in in itself had the drawback of revealing the contents of the message to 3rd parties, whereas the CPA scheme was vulnerable to CCA, i.e., obfuscation of the encrypted message for the benefit of the adversary.

The decryption is also simple, in that, a verification is first done to check for tampering in the ciphertext. If the verification is successful, $CPADecrypt$ is applied on the ciphertext to get back the message.