CCA-Security.

→ If Adversary has access to the decryption server so now the Adversary has both access to encryption & decryption which can decrypt all the ciphertext except the chosen cipher text. (CCA)

Eg Cryptosystem is CCA-Secure if for all PPT adversaries A:

$$P[b_{guess} = b] <= 1/2 + negl(n)$$

Encrypt then Authenticate

$$c = (r, F_{k_1}(r) + m), \; MAC_{k_2}(r, F_{k_1}(r) + m)$$

CCA-Secure Encryption

Construction: Let $\Pi_E = (Gen_E, Enc, Dec)$ be a private key encryption scheme and let $\Pi_M = (Gen_M, Mac, Vrfy)$ be a message authentication code. Define an encryption scheme (Gen', Enc', Dec') as follows:

- Gen': on input 1^n, run $Gen_E(1^n)$ and $Gen_M(1^n)$ to obtain keys k_1, k_2.
- Enc': on input a key (k_1, k_2) and a plaintext message m, compute $C \leftarrow Enc_{k_1}(m)$ and $t \leftarrow Mac_{k_2}(C)$ and output the ciphertext $\langle C, t \rangle$
- Dec': On input a key (k_1, k_2) and a cipher text $\langle C, t \rangle$, first check whether $vrfy_{k_2}(C, t) \stackrel{?}{=} 1$. If yes, then output $Dec_{k_1}(C)$; if no, then output $\perp$.

The above is a CCA-secure private-key encryption scheme.