Chosen Cipher Attack (CCA)

To **prove the security of a CCA-secure** encryption scheme, we need to show that an adversary who has access to a decryption oracle cannot successfully distinguish between two ciphertexts that encrypt different messages.

Proof of security of CCA

1. Assume that we have a CCA-secure encryption scheme with a message space M, a key space K, and a ciphertext space C.
2. Define an adversary A that has access to a decryption oracle O, which allows A to obtain the decrypted message for any ciphertext of its choosing.
3. Assume that A has two messages m0, m1 in the message space M that it wants to distinguish between, and that A has obtained two ciphertexts c0 and c1 such that c0 = Enc_k(m0) and c1 = Enc_k(m1) for some randomly chosen key k in the key space K.
4. A will choose a random bit b and send cb = Enc_k(mb) to the oracle O for decryption, where mb is the message corresponding to b. O will return the decrypted message mb'.
5. A will then compute the value of b' = mb xor b, which is the bit that A wants to guess.
6. A repeats steps 4 and 5 for a number of rounds, where the number of rounds is determined by a security parameter specified by the encryption scheme.
7. A outputs its guess for the value of b based on the values of b' obtained from each round.
8. To prove the security of the encryption scheme, we need to show that the probability that A correctly guesses the value of b is negligible.

9. Assume that there exists an adversary A that can guess b with probability ε that is not negligible. We will use A to construct a new adversary A' that can break the CCA-security of the encryption scheme with probability ε.
10. A' will choose two messages m0 and m1 and receive two ciphertexts c0 and c1 from a challenger.
11. A' will simulate the decryption oracle O by computing the values of mb' for each value of b using the ciphertext cb that it obtained from the challenger, as in steps 4 and 5 above.
12. A' will then use the values of mb' to determine which of the two messages was encrypted in the ciphertext that it received from the challenger.
13. If A' correctly identifies the message that was encrypted, it outputs a guess of 0, otherwise it outputs a guess of 1.
14. The probability that A' correctly guesses the value of b is equal to the probability that A correctly guesses the message that was encrypted in the ciphertext.
15. Since A can guess b with probability ε that is not negligible, A' can break the CCA-security of the encryption scheme with the same probability, which contradicts the assumption that the encryption scheme is CCA-secure.
16. Therefore, the probability that A can correctly guess b is negligible, and the **encryption scheme is CCA-secure.**