Chosen Plain Attack (CPA)

1. **Define the security game-** To prove the CPA (Chosen-Plaintext Attack) security of an encryption scheme, we define a security game between an attacker and a defender. The attacker's goal is to recover the plaintext from the ciphertext, while the defender's goal is to prevent the attacker from doing so.
2. **Assume the attacker's ability-** We assume that the attacker has the ability to choose two plaintext messages of their choice, and then receive the encryption of one of those messages from the defender. The attacker is also allowed to make a limited number of queries to an encryption oracle that encrypts any plaintext message of their choice.
3. **Analyze the encryption scheme-** We analyze the encryption scheme and observe that it uses a secure PRP (Pseudorandom Permutation) or PRF (Pseudorandom Function) to encrypt the plaintext message. The security of the encryption scheme is dependent on the security of the PRP or PRF.
4. **Assume the attacker's strategy-** We assume that the attacker has a strategy to distinguish between the encryption of the two plaintext messages that they have chosen. This strategy can be used to create a distinguisher algorithm that can distinguish between the encryption of a random plaintext message and the encryption of a chosen plaintext message.
5. **Construct a new message-** Using the distinguisher algorithm, the attacker can construct a new message that is not one of the original plaintext messages. The attacker then sends this new message to the encryption oracle to obtain its encryption.
6. **Analyze the new message-** We analyze the new message and observe that it is indistinguishable from the encryption of a

random message, because the encryption oracle uses a secure PRP or PRF to encrypt the message. Therefore, the attacker cannot distinguish between the encryption of a random message and the encryption of the new message.

7. **Conclusion-** We conclude that the **encryption scheme is CPA-Secure** because the attacker cannot distinguish between the encryption of a random message and the encryption of a chosen message. This holds as long as the encryption scheme uses a secure PRP or PRF.

In summary, the CPA-Security of an encryption scheme is based on the attacker's inability to distinguish between the encryption of a random message and the encryption of a chosen message. This inability holds as long as the encryption scheme uses a secure PRP or PRF.