sen Ciphertext Attack (CCA)

e adversary chooses a number of ciphertexts and is then given the responding plaintexts, decrypted with the target's private key

- Thus the adversary could select a plaintext, encrypt it with the target's pu key, and then be able to get the plaintext back by having it decrypted wit private key.
- The adversary exploits properties of RSA and selects blocks of data that, processed using the target's private key, yield information needed for cryptanalysis

counter such attacks, RSA Security Inc. recommends modifying the plaint ng a procedure known as optimal asymmetric encryption padding (OAEP