1. Prove that the RSA Cryptosystem is insecure against a *chosen ciphertext attack*: Given a

ciphertext y, describe how to choose a ciphertext such that the knowledge of the

plaintext allows you to compute. *Hint*: First prove that in the RSA

Cryptosystem ,.