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

ciphertext y, describe how to choose a ciphertext $y\left(hat\right)\ne y $such that the knowledge of the

plaintext $x\left(hat\right)=d\_{k}\left(y\left(hat\right)\right) $allows you to compute$ x=d\_{k}(y)$. *Hint*: First prove that in the RSA

Cryptosystem ,$e\_{k}\left(x\_{1}\right)e\_{k}\left(x\_{2}\right)modn=e\_{k}(x\_{1}x\_{2}modn)$.