ENEE 457
RSA Signatures Class Exercise

Consider the "Plain" RSA Signature scheme covered in the lecture.

1. Show how an adversary can create a forgery with a "no-message attack." I.e. the adversary makes no queries to the signing oracle.

2. Assume the adversary wants to forge a signature on a target message m^***.** Show how the adversary can make 2 queries to the signing oracle to create a forgery on m^*. Can this be done with less than 2 signing queries?