

## Quiz 8

Name:

In this quiz you will discover attacks on plain RSA digital signatures. Recall that plain RSA works as follows:

$Gen(1^n)$ :  $(N, e, d) \leftarrow GenRSA(1^n)$ ,  $pk = (N, e)$ ,  $sk = (N, d)$

$Sign_{sk}(m)$ : For  $m \in \mathbb{Z}_N^*$ ,  $\sigma = [m^d \bmod N]$

$Vrfy_{pk}(m, \sigma)$ : For  $m \in \mathbb{Z}_N^*$ , and  $\sigma \in \mathbb{Z}_N^*$ , output 1 iff  $m = [\sigma^e \bmod N]$

1. The no-message attack:

(a) Consider a signature  $\sigma \in \mathbb{Z}_N^*$ , show how to find a message  $m$  such that  $\sigma$  is a valid plain RSA signature on  $m$ .

(b) How can you use this to break the unforgeability of plain RSA signatures?

2. Forging a signature on any message  $m$

(a) Let  $(m_1, \sigma_1)$  and  $(m_2, \sigma_2)$  be two valid plain RSA message, signature pairs. How can you use these to produce a valid signature on a 3rd message  $m' \neq m_1, m_2$ ?

(b) Show how to use this observation to forge a signature on any chosen message  $m$ . (Hint: think of how you can choose  $m_1$  and  $m_2$  and remember to use the  $Sign_{sk}(\cdot)$  oracle.)