ENEE/CMSC/MATH 456
RSA Signatures Class Exercise

Another approach (besides hashing) that has been tried to construct secure RSA-based signatures is to encode the message before applying the RSA permutation. Here the signer fixes a public encoding function $E : \{0,1\}^{\ell} \to Z_N^*$ as part of its public key, and the signature on a message m is

$$\sigma := \left[E(m)^d \bmod N\right]$$

1. Show that encoded RSA is insecure if we define $E(m) = 0\text{x}00\|m\|0^{\kappa/10}$ (where $\kappa = \|N\|, \ell = |m| = 4\kappa/5$, and m is not the all-0 message). Assume $e = 3$.

ENEE/CMSC/MATH 456
RSA Signatures Class Exercise

2. Show that encoded RSA is insecure if we define $E(m) = 0||m||0||m$ (where $\ell = |m| = (||N|| - 1)/2$ and m is not the all-0 message). Assume $e = 3$.