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

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

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 $e = 3$.

Solution. The attacker will query $m_1 = 0^{\ell-1}||1$ to obtain signature σ_1. Note that the encoding of m_1 is $\mathrm{E}(m_1) = 0x00||0^{\ell-1}||1||0^{\kappa/10}$.
Now, consider $\mathrm{E}(m_1)\cdot\mathrm{E}(m_1)$. Note that this is a valid encoding of a message $m_2 = 0^{\ell-1-\kappa/10}||1||0^{\kappa/10}$.
Thus, we have that $\sigma_1 \cdot \sigma_1 = \mathrm{E}(m_1)^d \cdot \mathrm{E}(m_1)^d = (\mathrm{E}(m_1) \cdot \mathrm{E}(m_1))^d = \mathrm{E}(m_2)^d$.
Thus, the attacker can output the forgery $(m_2, \sigma_1 \cdot \sigma_1)$.

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 $e = 3$.

Solution. The attacker will query $m_1 = 0^{\ell-1}||1$ to obtain signature σ_1. Note that the encoding of m_1 is $\mathrm{E}(m_1) = 0||0^{\ell-1}||1||0||0^{\ell-1}||1$.
Now, consider $\mathrm{E}(m_1) \cdot 8$. Note that this is a valid encoding of a message $m_2 = 0^{\ell-4}||1||000$. Moreover, note that since $2^3 = 8$, we have that $8^d = 2$.
Thus, we have that $\sigma_1 \cdot 2 = \mathrm{E}(m_1)^d \cdot 8^d = (\mathrm{E}(m_1) \cdot 8)^d = \mathrm{E}(m_2)^d$.
Thus, the attacker can output the forgery $(m_2, \sigma_1 \cdot 2)$.