1. Chapter 9: problems 2, 5
2. Chapter 10: problems 5, 9
3. Chapter 11: problems 5, 6
4. With RSA signatures, it is tempting to use a small verification exponent $e$ to speed up the verification algorithm. Suppose we use $e = 3$ with plain RSA signatures (no padding, no hashing). Suppose that the RSA modulus is $N$ and you have a signature on a message $m$, where $0 \leq m < N/8$. Show how to efficiently forge a signature on the message $8m$. 