1. What is the difference between a message authentication code (MAC) and a digital signature? Where would you use a MAC? What about a signature?

2. Assume that you have a strong one-way function $E_k(x)$ where x can be up to 1024 bits. You decide to encrypt English plaintext by breaking it apart into English words. So, 'this is a dumb idea' would be encrypted as E_k('this'),E_k('is'),E_k('a'),E_k('dumb'),E_k('idea'). You can assume that an attacker does not have the key, k, and that the binary representation of an English word is always less than 1024 bits.

a. Does this scheme provide message security? If not, give at least two different attacks on the scheme.

b. Does it provide integrity for messages? Again, be sure to explain your answer.

3. Recall that DES is a (conjectured) one-way function that maps 64-bit plaintexts to 64-bit ciphertexts under a 56-bit key. Symbolically, $c = DES_K(m)$.

Let $\bar{x}$ be the bitwise complement of x. DES has the additional property that if $c = DES_K(m)$ then $\bar{c} = DES_{\bar{K}}(\bar{m})$ Can you use this fact to mount a choosen-plaintext attack on DES that is better than brute force? In other words, if you are allowed to choose a few m's for which you will receive $c = DES_K(m)$, can you discover K with less than 2^{56} DES encryptions?

4. Consider the following MAC built out of a one-way function, $E_K(x)$. To MAC a message $M = m_1 \circ m_2 \circ \ldots \circ m_n$, let $h_0 = K$ and compute:

$$h_i = E_{m_i}(h_{i-1}) \oplus h_{i-1} \text{ for } i = 1, 2, \ldots, n.$$

The value of the MAC, $MAC_K(M)$, is defined to be $MAC_K(M) = h_n$. Given a message M and $MAC_K(M)$, show that you can construct a message $M' \neq M$ along with $MAC_K(M')$ without knowing the key, K.

5. The RSA function is defined to be $f(m) = m^e \bmod N$. Suppose you know that c_1 is $f(m)$ and c_2 is $f(m+1)$ for some unknown m. Show how you can recover m from $e = 3$, c_1, and c_2. To get started,

$$\begin{aligned} c_1 &= m^3 \\ c_2 &= (m+1)^3 = m^3 + 3m^2 + 3m + 1 = c_1 + 3m^2 + 3m + 1. \end{aligned}$$

Taking square roots in $\mathbb{Z}_N^*$ is **hard**, so that's out. You can however, add, subtract, multiply, exponentiate, and divide (take inverses). Try to write out an equation in c_1 and c_2 that equals m using only these basic operations.