1. Consider the following variant of El Gamal encryption. The private key is \((G, g, q, x)\) and the public key is \((G, g, q, h)\), where \(h = g^x\) and \(x \in \mathbb{Z}_q\) is chosen uniformly. To encrypt a message \(m \in \mathcal{M}\), in the message space \(\mathcal{M}\), choose a uniform \(r \in \mathbb{Z}_q\), compute \(c_1 := g^r \mod p\) and \(c_2 := h^r \cdot g^m\), and let the ciphertext be \((c_1, c_2)\). For which message spaces \(\mathcal{M}\) will the above scheme be a good encryption scheme?

2. Consider the following variant of El Gamal encryption. Let \(p = 2q + 1\), let \(G\) be the group of squares modulo \(p\), and let \(g\) be a generator of \(G\). The private key is \((G, g, q, x)\) and the public key is \((G, g, q, h)\), where \(h = g^x\) and \(x \in \mathbb{Z}_q\) is chosen uniformly. To encrypt a message \(m \in \mathbb{Z}_q\), choose a uniform \(r \in \mathbb{Z}_q\), compute \(c_1 := g^r \mod p\) and \(c_2 := h^r + m \mod p\), and let the ciphertext be \((c_1, c_2)\). Is this scheme CPA-secure? Prove your answer.

3. Consider the following modified version of padded RSA encryption: Assume messages to be encrypted have length exactly \(||N||/2\). To encrypt, first compute \(\hat{m} := 0x00||r||0x00||m\) where \(r\) is a uniform string of length \(||N||/2 - 16\). Then compute the ciphertext \(c := [\hat{m}^e \mod N]\). When decrypting a ciphertext \(c\), the receiver computes \(\hat{m} := [c^d \mod N]\) and returns an error of \(\hat{m}\) does not consist of 0x00 followed by \(||N||/2 - 16\) arbitrary bits followed by 0x00. Show that this scheme is not CCA-secure. Why is it easier to construct a chosen-ciphertext attack on this scheme than on PKCS #1 v1.5?

4. In Section 12.4.1 we showed an attack on the plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a single signing query.