Question 1

Consider the following encryption scheme for a one-bit message $M \in \{0, 1\}$. Let $g$ be a quadratic residue modulo a safe prime $q$. The secret key is a random $X \in \mathbb{Z}_q^*$ and the public key is $h = g^X$. To encrypt a 0 output $(g^R, h^R)$ for a random $R$ in $\mathbb{Z}_q^*$. To encrypt a 1 output $(g^R, h^{R'})$ where $R$ and $R'$ are independent random elements in $\mathbb{Z}_q^*$.

(a) Show that it is not possible to decrypt ciphertexts with probability 1.

(b) Describe and analyze a decryption algorithm that succeeds with probability $1 - \Omega(1/q)$.

(c) Show that the encryption is message indistinguishable assuming the $(s, \varepsilon)$-DDH assumption in base $g$. Work out the parameters.

Question 2

In this question you will analyze the following LWE-based public-key identification protocol. The secret key is a random $x \sim \{-1, 1\}^m$. The public key is $(A, z = xA)$ where $A$ is a random $m \times n$ matrix over $\mathbb{Z}_q$. All arithmetic is modulo $q$.

1. Prover chooses a random $r \sim \{-b, \ldots, b\}^m$ and sends $h = rA$.

2. Verifier sends a random bit $c \sim \{0, 1\}$.

3. Prover sends $y = r + cx$.

4. Verifier accepts if $yA = h + cz$ and $y \in \{-b - 1, \ldots, b + 1\}^m$.

(a) Show that if $m = 1$ then $r$ conditioned on $|r| \leq b - 1$ is identically distributed to $r + x$ conditioned on $|r + x| \leq b - 1$.

(b) Now let $m$ be arbitrary as in the protocol. Show that $r$ and $r + x$ are $O(m/b)$-statistically close.

(c) Show that the view of an eavesdropper who sees $q'$ protocol transcripts is $O(q'm/b)$-statistically close to some random variable that can be efficiently sampled by a simulator that is given only the public key.

(d) Let $H_A(x) = xA$, where the entries of $x$ are of magnitude at most $2(b + 1)$. Show that if $H$ is a collision-resistant hash function then no efficient cheating prover can handle both challenges $c = 0$ and $c = 1$. Conclude that, if repeated sufficiently many times, the protocol is secure against eavesdropping. (Work out the dependencies between the security parameters.)

(e) (Optional) Prove that the protocol is secure against impersonation.
Question 3

Assume \( F_K : \{0,1\}^{n+1} \rightarrow \{0,1\}^n \) is an \((s, \varepsilon)-\)pseudorandom function. Which of the following is a secure MAC tagging algorithm for message length \( 2n \)? Justify your claim.

(a) \( \text{Tag}(K, M_0 M_1) = (F_K(M_0, 0), F_K(M_1, 1)), \) 
\( \text{Ver}(K, M_0 M_1, T_0 T_1) \) accepts iff \( F_K(M_0, 0) = T_0 \) and \( F_K(M_1, 1) = T_1. \)

(b) \( \text{Tag}(K, M_0 M_1) = F_K(M_0, 0) + F_K(M_1, 1), \) 
\( \text{Ver}(K, M_0 M_1, T) \) accepts iff \( F_K(M_0, 0) + F_K(M_1, 1) = T. \)

Question 4

In this question you will show that using an obfuscator, an adversary can plant a collision in a hash function that makes it insecure against him, but secure against everyone else. Let \( h : \{0,1\}^m \rightarrow \{0,1\}^n \) be a collision-resistant hash, \( \text{Obf} \) an obfuscator, and \( A \) the following algorithm:

1. Sample a random key \( K \) and a random input \( \hat{x} \sim \{0,1\}^m \setminus \{0\}. \)
2. Construct a circuit \( h' \) that implements the function
   \[
   h'(x) = \begin{cases} 
   h_K(0), & \text{if } x = \hat{x}; \\
   h_K(x), & \text{if not.}
   \end{cases}
   \]
3. Output \( H = \text{Obf}(h'). \)

Then \( A \) knows a collision for \( H \), namely the pair \((0, \hat{x})\). We can view \( H \) both as a random key and the function described by it, so \((s, \varepsilon)-\)collision-resistance means that the probability that \( C(H) \) outputs a collision for \( H \) is at most \( \varepsilon \) for every \( C \) of size at most \( s \).

(a) Show that the views \( D^{hK} \) and \( D^{h'} \) are \( q/(2^m - 1) \)-statistically close for any distinguisher \( D \) that makes at most \( q \) queries to its oracle.

(b) Show that if \( h \) is \((s, \varepsilon)-\)collision resistant and \( \text{Obf} \) is \((s + 2t + O(n), \varepsilon')-\)VBB secure, \( H \) is \((s - tt', \varepsilon + \varepsilon' + q/(2^m - 1))-\)collision resistant, where \( t \) and \( t' \) are the sizes \( h \) and the VBB simulator, respectively.

(c) Show that the MAC from Theorem 5 in Lecture 6 is insecure against a forger that knows \( \hat{x}. \)