Answer the following questions (choose 6 from 7)

1. (2 points) Given a Hamming distance protocol between Alice and Bob, what notions of security are important in the semi-honest model?

2. (4 points) In the setup for ElGamal, we used a prime $p$ of size (at least) 3248 bits and a prime $q$ of size (at least) 256 bits, and all operations were done in $\mathbb{Z}_p$.

   (a) What is the relationship between $p$ and $q$?
   (b) Why not just use $\mathbb{Z}_q^*$, without relying on $p$?

3. (4 points) Explain the relations between the DL, CDH, DDH assumptions. What can be the motivations for introducing each one?

4. (5 points) Let Alice and Bob have private boolean inputs $\vec{a} = (a_1, a_2, a_3)$ and $\vec{b} = (b_1, b_2, b_3)$ respectively, corresponding to their choices in a voting of three issues. They want to determine whether or not any of their choices are the same for at least one of these issues (and output 1 in this case).

   - Create a boolean function that computes the desired result and works for arbitrary $\vec{a}, \vec{b}$.
   - Create a BDD for this function that works for arbitrary $\vec{a}, \vec{b}$.

5. (6 points) In a simple instantiation of Damgård-Jurik, we have $N = 15$.

   (a) Give an example of a valid public key and secret key.
   (b) What value of $s$ should we use to encrypt $m = 2016$? How big will the ciphertext be?

6. (5 points) Let $f$ be a function such that $f(s, (n + 1)^x \mod n^{s+1}) = x \mod n^s$.

   (a) What is $f(1, (n + 1)^x)$?
   (b) Let $\alpha \in \mathbb{Z}_n^*$, $r \in \mathbb{Z}_n^*$ be such that $r^{\alpha n^s} \equiv 1 \pmod{n^{s+1}}$. Let $g(x) = (n + 1)^x r^{n^s} \mod n^{s+1}$. Determine $g^{-1}(c)$ such that $g^{-1}(g(x)) \equiv x \pmod{n^s}$. 
7. (4 points)

(a) What is the difference between multi-party and multi-round protocols? Compare both to 2-party, 2-round protocols in number of rounds, communication, computation, and trust requirements.

(b) In a \((n, t)\)-secret sharing scheme, what is the significance of the value \(t\)?