11120IIS/500400 Applied Cryptography, Spring 2023 **Due: 14-Jun-2023**

Homework 2 & 3

Instructor: Prof. Amir Rezapour

1. This problem is about ElGamal encryption and signature schemes. (30 points)
   (a) Let $p = 83$ and $g = 16$ be a generator of Z_{83}^*. Assume that the public key is $(p, g, 59)$ and the secret key $(p, g, 29)$. Encrypt the plaintext $m = 25$ and decrypt the ciphertext $(56, 13)$.
   (b) Use the secret key as the signing key to sign the message $m = 25$. The randomly chosen k is 23. You don't need to do hashing before signing.

2. For DSA, let the public key be $(p = 149, q = 37, g = 41, y = 144)$, and the secret key be $(p = 149, q = 37, g = 41, x = 26)$. Assume that the hash function is $h(m) = m^{21} \bmod 37$. (30 points)
   (a) Compute the signature of $m = 9876543210$.
   (b) Is $(12, 25)$ a valid signature for $m = 3248$?

3. Why is the "sequential" DL interactive proof system zero-knowledge? Why isn't the "parallel" FS interactive proof system zero-knowledge? (20 points)

4. We consider the multi-authority secure electronic voting scheme without a trusted center, discussed in classes. How does the authority A_i assures A_j that the sent share $s_{i,j} = f_i(x_j)$ is indeed consistent with all other shares sent to the other authorities? (20 points)