Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1. Man in the Middle
Read this story.

Suppose the Iranian secret police launched the man in the middle attack. Once they had procured a bogus certificate, what would they have technically done to monitor Gmail users in Iran using a man in the middle attack?

Problem 2. Man in the Middle: El-Gamal

(a) Describe a man-in-the-middle attach on the El-Gamal cryptosystem. Please use the notation from the Hoffstein textbook used in Table 2.3 (p. 72), and in Example 3.13 (p. 126).

(b) Discuss how the use of public key certificates could solve the attack (assume there is a secure way for a certificate authority to authenticaet Alice).

(c) What prevents Eve from using a second MITM attack to pretend to be the certificate authority and issuing a bogus certificate?

Taken from Hoffstein 3.12

Problem 3. Discrete Logs and RSA
Explain how to attack RSA if you are able to compute arbitrary discrete logs $(mod\ N)$. That is, explain how to recover d from $s = hash(M)^d\ (mod\ N)$, or from $c = M^e\ (mod\ N)$.

Problem 4. Proof: Primite roots and discrete logs
Let p be an odd prime and let g be a primitive root modulo p.
Prove that a has a square root modulo p if and only if its discrete logarithm $(log_g(a)\ (mod\ p-1))$ is even.

Taken from Hoffstein 2.5

Note: "primitive root" means "generator", and that this question is asking you to prove two statements:

1. Assume that a has a square root $(mod\ p)$, then show that it's discrete log must be even, and
2. Assume that the discrete log of a is even, then show that a must have a square root $(mod\ p)$.