ENEE 457: Computer Systems Security
Written Homework 2

1. DH Key Exchange. Describe in detail a man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key k_A with Alice and a different key k_B with Bob, and Alice and Bob cannot detect that anything has gone wrong. What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

2. DH to ElGamal. Diffie Hellman key exchange can be converted to a public key encryption scheme (Gen, Enc, Dec). Describe the algorithms (Gen, Enc, Dec).

Hint: Gen will choose $x \leftarrow Z_q$ and set the secret key to x and the public key to g^x. Notice that this corresponds to the computation/message of the first party in DH key exchange. A ciphertext c produced by Enc will have two parts. The first part will correspond to the second message of the DH protocol and the second part will use the shared DH key to encrypt the message. Dec will use the properties of the DH key exchange (the fact that the first party can recover the shared key) to reconstruct the message, given x and c.

3. RSA Encryption. We mentioned in the lecture that plain RSA Encryption cannot be CPA-secure since it is deterministic. In this problem, we will consider specific attacks on plain RSA Encryption. Assume $e = 3$ and $m < N^{1/3}$. Show that given the ciphertext, the entire message can be recovered.

ENEE 457: Computer Systems Security

4. RSA Signatures. Consider plain RSA signatures. Assume the adversary wants to forge a signature on a target message m^*. Show how the adversary can do this using a single signing query.

5. **Putting it together.** Please respond to each of the following questions using a few sentences:

a. How does a certificate authority (CA) use digital signature schemes to generate certificates?

b. How are public key cryptography and symmetric key cryptography combined in order to communicate securely over the internet?

c. Give two examples of ways cryptographic schemes can be misused in practice.