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

Final

Instructor: Prof. Amir Rezapour

1. Discuss why DL-based identification scheme is better than traditional password-based identification scheme? Which one is more efficient in terms of computation and communication complexities? (10 points)

2. This problem is about ElGamal encryption and signature schemes. (30 points)

   (a) Show that ElGamal encryption scheme is not secure against the chosen ciphertext attack.

   (b) Is ElGamal signature scheme secure against the chosen plaintext attack (allowing to ask the signing oracle) if the hash-then-sign paradigm is used.

   (c) Assume that the hash-then-sign paradigm is not used. Can we forage a signature for any given message m by asking the signing oracle. You cannot ask the oracle about the signature of m.

3. Assume that Alice and Bob know the common (p, g), where p is a large prime and g is a generator of Z_p. (30 points)

   (a) If they want to exchange a large amount of messages through the Internet securely, what can they do?

   (b) If an attacker wants to break the communication, what can he do?

   (c) Assume that $p = 107$ and $g = 2$. Show examples for (a) and (b).

4. Show that the regular RSA signature scheme is "arbitrarily forgeable" (forging the signature of any challenge message m) if the attacker is allowed to ask the signing oracle. Note that the challenge message m cannot be queries to the signing oracle. (10 points)

5. We consider the multi-authority secure electronic voting scheme without a trusted center. How do the authorities $A_1, A_2, \ldots, A_n$ collaboratively construct the public and private keys? (20 points)