Midterm Review - Asymmetric Cryptography

Question 1 ***True/false*** ()

Q1.1 True or False: If the discrete-log problem is broken (someone finds a way to efficiently calculate a given $g^a \bmod p$), ElGamal encryption is no longer secure.

● True ○ False

> **Solution:** True. ElGamal depends on Diffie-Hellman, which depends on the discrete-log problem. An attacker could learn r from the ciphertext, then calculate $(m \times B^r) \times B^{-r} \bmod p$ to obtain the original message.

Q1.2 True or False: If Eve acquires access to **both** Alice and Bob's private signature keys, the communication channel is no longer confidential.

○ True ● False

> **Solution:** False. Even though Eve can now assume the identity of Alice or Bob, the actual messages sent between the real Alice and Bob remain encrypted, since Eve doesn't have access to either person's private decryption keys.

Q1.3 True or False: To use ElGamal encryption efficiently on very long messages, you should break up the message into small blocks and encrypt each block individually with ElGamal.

○ True ● False

> **Solution:** False. To use asymmetric cryptography with large messages, it is most appropriate to randomly generate a symmetric key, encrypt the message using symmetric encryption, and encrypt the key with asymmetric encryption to protect the confidentiality of the message. Using asymmetric cryptography directly on a very long message is very inefficient.

Question 2 ***ElGamal and friends*** **(15 min)**

Bob wants his pipes fixed and invites independent plumbers to send him bids for their services (*i.e.*, the fees they charge). Alice is a plumber and wants to submit a bid to Bob. Alice and Bob want to preserve the confidentiality of Alice's bid, but the communication channel between them is insecure. Therefore, they decide to use the ElGamal public key encryption scheme in order to communicate privately.

Instead of using the traditional version of the ElGamal scheme, Alice and Bob use the following variant. As usual, Bob's private key is x and his public key is $\mathsf{PK} = (p, g, h)$, where $h = g^x \bmod p$. However, to send a message M to Bob, Alice encrypts M as $\mathsf{Enc}_{\mathsf{PK}}(M) = (s, t)$, where $s = g^r \bmod p$ and $t = g^M \times h^r \bmod p$, for a randomly chosen r.

Q2.1 Consider two distinct messages m_1 and m_2. Let $\mathsf{Enc}_{\mathsf{PK}}(m_1) = (s_1, t_1)$ and $\mathsf{Enc}_{\mathsf{PK}}(m_2) = (s_2, t_2)$. For the given variant of the ElGamal scheme, which of the following is true?

- ○ $(s_1 + s_2 \bmod p, \quad t_1 + t_2 \bmod p)$ is a possible value for $\mathsf{Enc}_{\mathsf{PK}}(m_1 + m_2)$.
- ● $(s_1 \times s_2 \bmod p, \quad t_1 \times t_2 \bmod p)$ is a possible value for $\mathsf{Enc}_{\mathsf{PK}}(m_1 + m_2)$.
- ○ $(s_1 \times s_2 \bmod p, \quad t_1 \times t_2 \bmod p)$ is a possible value for $\mathsf{Enc}_{\mathsf{PK}}(m_1 \times m_2)$.
- ○ $(s_1 + s_2 \bmod p, \quad t_1 + t_2 \bmod p)$ is a possible value for $\mathsf{Enc}_{\mathsf{PK}}(m_1 \times m_2)$.
- ○ None of these

Q2.2 In order to decrypt a ciphertext (s, t), Bob starts by calculating $q = ts^{-x} \bmod p$. Assume that the message M is between 0 and 1000. How can Bob recover M from q?

> **Solution:** If Bob knows the possible set of messages, then he can pre-compute a lookup table for values of $q = g^M \bmod p$.

Q2.3 Explain why Bob cannot efficiently recover M from q if M is randomly chosen such that $0 \leq M < p$.

> **Solution:** Requires solving the discrete log mod$p$, which is thought to be computationally hard.

Q2.4 Suppose Alice sends Bob a bid $M_0 = 500$, encrypted under Bob's public key. We let $C_0 = (s, t)$ be the ciphertext here.

Mallory is an active man-in-the-middle attacker who knows Alice's bid is $M_0 = 500$. Mallory wants to replace Alice's bid with $M_1 = 999$. To do that, Mallory intercepts C_0 and replaces it with another ciphertext C_1. Mallory wishes that when Bob decrypts C_1, Bob sees $M_1 = 999$.

Describe how Mallory creates C_1 in each of the following situations:

1. Mallory didn't obtain C_0, but knows Bob's public key $\mathsf{PK} = (p, g, h)$.

   ⋄ Question: How should Mallory create C_1?

   Solution: Mallory can simply encrypt M of her choice using Bob's public key and replace the ciphertext.

2. Mallory knows Alice's ciphertext C_0, but only knows p and g in Bob's public key $\mathsf{PK} = (p, g, h)$. (That is to say, Mallory does not know h.)

   ⋄ Question: How should Mallory create C_1?

   Solution: Mallory can create $(s', t') = (s, tg^{499}) \pmod p$.