CS161 Summer 2025 — Introduction to Computer Security — MT Review: Asym Crypto

Q1 *ElGamal and friends* **(15 points)**

Bob wants his pipes fixed and invited 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 $\text{PK} = (p, g, h)$, where $h = g^x \bmod p$. However, to send a message M to Bob, Alice encrypts M as $\text{Enc}_{\text{PK}}(M) = (s, t)$, where $s = g^r \bmod p$ and $t = g^M \times h^r \bmod p$, for a randomly chosen r.

Q1.1 (3 points) Consider two distinct messages m_1 and m_2. Let and . 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 $\text{Enc}_{\text{PK}}(m_1 + m_2)$
- ○ $(s_1 \times s_2 \bmod p, \quad t_1 \times t_2 \bmod p)$ is a possible value for $\text{Enc}_{\text{PK}}(m_1 + m_2)$
- ○ $(s_1 \times s_2 \bmod p, \quad t_1 \times t_2 \bmod p)$ is a possible value for $\text{Enc}_{\text{PK}}(m_1 \times m_2)$
- ○ $(s_1 + s_2 \bmod p, \quad t_1 + t_2 \bmod p)$ is a possible value for $\text{Enc}_{\text{PK}}(m_1 \times m_2)$
- ○ None of these

Q1.2 (3 points) 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?

Q1.3 (3 points) Explain why Bob cannot efficiently recover M from q if M is randomly chosen such that $0 \leq M < p$.

This content is protected and may not be shared, uploaded, or distributed.

Q1.4 (6 points) 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 $PK = (p, g, h)$

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

This content is protected and may not be shared, uploaded, or distributed.

Q2 *Bob's Birthday* **(11 points)**

It's Bob's birthday! Alice wants to send an encrypted birthday message to Bob using ElGamal.

Recall the definition of ElGamal encryption:

- b is the private key, and $B = g^b \bmod p$ is the public key.
- $\text{Enc}(B, M) = (C_1, C_2)$, where $C_1 = g^r \bmod p$ and $C_2 = M \times B^r b \bmod p$
- $\text{Dec}(b, C_1, C_2) = C_1^{-b} \times C_2 \bmod p$

Q2.1 (2 points) Mallory wants to tamper with Alice's message to Bob. In response, Alice decides to sign her message with an RSA digital signature. Bob receives the signed message and verifies the signature successfully. Can he be sure the message is from Alice?

- ◯ Yes, because RSA digital signatures are unforgeable.
- ◯ Yes, because RSA encryption is IND-CPA secure.
- ◯ No, because Mallory could have blocked Alice's message and replaced it with a different one.
- ◯ No, because Mallory could find a different message with the same hash as Alice's original message.

As we discussed in class, ElGamal is malleable, meaning that a man-in-the-middle can change a message in a *predictable* manner, such as producing the ciphertext of the message $2 \times M$ given the ciphertext of M.

Q2.2 (3 points) Consider the following modification to ElGamal: Encrypt as normal, but further encrypt portions of the ciphertext with a block cipher E, which has a block size equal to the number of bits in p. In this scheme, Alice and Bob share a symmetric key K_{sym} known to no one else.

Under this modified scheme, C_1 is computed as $E_{K_{\text{sym}}}(g^r \bmod p)$ and C_2 is computed as $E_{K_{\text{sym}}}(M \times B^r \bmod p)$. Is this scheme still malleable?

- ◯ Yes, because block ciphers are not IND-CPA secure encryption schemes
- ◯ Yes, because the adversary can still forge $k \times C_2$ to produce $k \times M$
- ◯ No, because block ciphers are a pseudorandom permutation
- ◯ No, because the adversary isn't able to learn anything about the message M

The remaining parts are independent of the previous part.

For Bob's birthday, Mallory hacks into Bob's computer, which stores Bob's private key b. She isn't able to read b or overwrite b with an arbitrary value, but she can multiply the stored value of b by a random value z known to Mallory.

Mallory wants to send a message to Bob that appears to decrypt as normal, but **using the modified key** $b \cdot z$. Give a new encryption formula for C_1 and C_2 that Mallory should use. Make sure you only use values known to Mallory!

Clarification during exam: For subparts 3 and 4, assume that the value of B is unchanged.

This content is protected and may not be shared, uploaded, or distributed.

Q2.3 (3 points) Give a formula to produce C_1, encrypting M.

Q2.4 (3 points) Give a formula to produce C_2, encrypting M.

This content is protected and may not be shared, uploaded, or distributed.