CSE 40622 Cryptography
Writing Assignment 04 (Lecture 06-08)

Name & netID: Walker Bagley (wbagley)

1. (10 pts, Page 4) Prove that $x^k = x^{k \mod |\mathbb{G}|}$ for $x \in \mathbb{G}$ for any integer k.

   Answer:

   Proof. Remember that $k \mod |\mathbb{G}| = k + m|\mathbb{G}|$ for any integer m. So, we have the equality $x^k = x^{k+m|\mathbb{G}|} = x^k x^{m|\mathbb{G}|} = x^k (x^{|\mathbb{G}|})^m$. Knowing that in any group, $x^{|\mathbb{G}|} = e$, we can say $x^k = x^k (e)^m = x^k e = x^k$. □

2. (15 pts, Page 4) In the proof of Lagrange's Theorem, I said the set $x\mathbb{H}$ cannot form a group under the same operator as in $\mathbb{G}$. Formally prove it.

   Answer: You may use the following codes.

   - $x \in \mathbb{H}$, $x \notin \mathbb{H}$, $x \neq y$
   - x^{-1}

   Proof. Consider two arbitrary elements $a, b \in \mathbb{H}$. Then there exist two elements in $x\mathbb{H}$ that are equal to xa and xb. Suppose, towards a contradiction, that $x\mathbb{H}$ has the same binary operator as $\mathbb{G}$. Then by closure of groups, $xaxb \in x\mathbb{H}$, meaning $xaxb = xc$ for some $c \in \mathbb{H}$. Applying left cancellation leaves $a(xb) = c$, and since $a, c \in \mathbb{H}$, then $xb \in \mathbb{H}$. But we know $x \notin \mathbb{H}$, so xb cannot be an element of $\mathbb{H}$. Thus, the subgroup formed by $x\mathbb{H}$ cannot have the same binary operator as $\mathbb{G}$. □

3. (15 pts, page 5) In the proof of Lagrange's Theorem, I said $\mathbb{H} \cap x\mathbb{H} = \varnothing$. Formally prove it.

   Answer:

   Proof. Consider some group $\mathbb{G}$ and a subgroup $\mathbb{H}$. Take some $x \in \mathbb{G} - \mathbb{H}$ and form a new subset $x\mathbb{H}$. Towards a contradiction, suppose $\mathbb{H} \cap x\mathbb{H} \neq \varnothing$. This means $\mathbb{H}$ and $x\mathbb{H}$ share at least one element. Let's take an arbitrary element $a \in \mathbb{H}$, so we know $xa \in x\mathbb{H}$. But since $x \notin \mathbb{H}$ and because $\mathbb{H}$ is a subgroup and therefore closed under the operation of $\mathbb{G}$, then $xa \notin \mathbb{H}$. As a was arbitrary, we can say without loss of generality that this applies for all $a \in \mathbb{H}$. So, $\mathbb{H}$ and $x\mathbb{H}$ cannot possibly share any elements, meaning $\mathbb{H} \cap x\mathbb{H} = \varnothing$. □

4. (15 pts, page 5) In the proof of Lagrange's Theorem, what part becomes false if $\mathbb{H}$ is a subset but not a subgroup? Why can we no longer conclude $|\mathbb{H}|$ divides $|\mathbb{G}|$ if $\mathbb{H}$ is a subset but not a subgroup?

   Answer:

   You may use the following code.

   $\mathbb{H} \cap x\mathbb{H}$

   $\mathbb{G} = \{1, 2, 3, 4\}$

   If $\mathbb{H}$ is only a subset of $\mathbb{G}$ and not a subgroup, then we don't necessarily have the uniqueness of $\mathbb{H}$ and $x\mathbb{H}$. That means we don't know that $\mathbb{H} \cap x\mathbb{H} = \varnothing$. Without closure, there can exist some $x \in \mathbb{G} - \mathbb{H}$ such that $xa \in \mathbb{H}$ for some $a \in \mathbb{H}$. But also, $xa \in x\mathbb{H}$, so then $xa \in \mathbb{H} \cap x\mathbb{H}$. For example with the group $\mathbb{Z}_5^*$ under modular multiplication, meaning $\mathbb{G} = \{1, 2, 3, 4\}$ and subset $\mathbb{H} = \{1, 2, 3\}$, when we take $x = 4$, we get that $4 \cdot 2 = 8 = 3 \in \mathbb{H}$. With this overlap, we are unable to divide the group $\mathbb{G}$ into equally sized disjoint subsets and therefore cannot say that $|\mathbb{H}|$ divides $|\mathbb{G}|$.

5. (10 pts, Page 6) Prove that any $x \in (\mathbb{G} - \{e\})$ generates $\mathbb{G}$ if $|\mathbb{G}|$ is a prime number.

Answer:

Use may use the following codes.

- $x \neq e$, $\mathsf{ord}(x)$.
- $|\langle x \rangle|$.

Proof. Choosing some $x \in \mathbb{G}$ such that $x \neq e$, then we know $x^k = e$ for some integer k. We also know that the order of x divides k, that is, $\mathsf{ord}(x)|k$. In any group, $x^{|\mathbb{G}|} = e$, so we say that $k = |\mathbb{G}|$. So the order of x divides the order of $\mathbb{G}$, and since $|\mathbb{G}|$ is prime, $|\langle x \rangle|$ can only be either 1 or $|\mathbb{G}|$. $|\langle x \rangle|$ cannot possibly be 1, because that would mean $x = e$, so we know the order of x is equal to the order of $\mathbb{G}$. Thus, x must generate $\mathbb{G}$. □

6. (10 pts, Page 12) An algorithm solving DLOG problem can be used to solve CDH problem. Explain how this can be done.

   - Hint: Imagine that you have an algorithm which solves the DLOG problem: It outputs x given g^x. Even though we do not know the mechanism of that algorithm, we can still use that algorithm to as a black box (*i.e.,* only see the output when we give something as input) and solve CDH problem.

Answer:

You may use the following codes.

Given (g, g^a, g^b) where $g, g^a, g^b \in \mathbb{G}$, ... $a \in \mathbb{Z}$...

Using the DLOG algorithm, generate a, b from g^a, g^b. Then calculate $ab \mod |\mathbb{G}|$, since we proved in question 1 that $x^k = x^{k \mod |\mathbb{G}|}$. From here it should be trivial to calculate g^{ab} and thus the CDH problem is solved.

7. (10 pts, Page 12) Analyze why the variant of ElGamal encryption is an additive homomorphic encryption. Please explicitly show how decryption can be done after computation is conducted on the ciphertext.

Answer:

You may use the following codes.

$$C_1 = (g^{r_1}, g^{m_1} h^{r_1}) \qquad C_2 = (g^{r_2}, g^{m_2} h^{r_2})$$

As the ElGamal variant is operational in a multiplicative group, we see that $C_1 \cdot C_2 = (g^{r_1} \cdot g^{r_2}, g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2}) = (g^{r_1+r_2}, g^{m_1+m_2} h^{r_1+r_2})$. This would be the same encryption as $m_1 + m_2$, thus meaning that the ElGamal encryption variant is an additive homomorphism.

Decryption would work very similarly, using the same private key x. Notice that $c_1 = g^{r_1+r_2}$ and $c_2 = g^{m_1+m_2} h^{r_1+r_2}$. So, computing $[(g^{r_1+r_2})^x]^{-1} = [(g^x)^{r_1+r_2}]^{-1} = h^{-(r_1+r_2)}$. Then, $c_2 \cdot (c_1^x)^{-1} = g^{m_1+m_2} h^{r_1+r_2} h^{-(r_1+r_2)} = g^{m_1+m_2}$, so we once again compute DLOG to recover the original message, $m_1 + m_2$.