CSE 40622 Cryptography, Spring 2018
Written Assignment 03 (Lecture 05-07)

Name: **Jasmine Walker**

1. (10 pts, Page 3) Prove that $x^k = x^{k \mod |\mathbb{G}|}$ for $x \in \mathbb{G}$ for any integer k.

   Answer:
   From Theorem 1, we know that $x^{|\mathbb{G}|} = e$. k can be described as some remainder r plus some quotient q times $|\mathbb{G}|$. So,
   $x^k = x^{r+q|\mathbb{G}|} = x^r x^{q|\mathbb{G}|} = x^r e^q = x^r$
   We know that $k \mod |\mathbb{G}|$ will equal r,
   $x^{k \mod |\mathbb{G}|} = x^r$
   $x^k = x^r = x^{k \mod |\mathbb{G}|}$

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:
   I will prove that $e \notin x\mathbb{H}$, so $x\mathbb{H}$ cannot be a group under the same operator as $\mathbb{G}$ because the identity value e for the operation does not exist in $x\mathbb{H}$.
   Proof by contradiction:
   If $e \in x\mathbb{H}$, then some element $h_1 \in \mathbb{H}$ must exist such that $x \cdot h_1 = e$. By definition, h_1 is the inverse of x, and x is the inverse of h_1. This means that, because all elements in $\mathbb{H}$ also have their inverses in $\mathbb{H}$, $x \in \mathbb{H}$. This is false because x is defined $x \in \mathbb{G} - \mathbb{H}$, meaning necessarily that $x \notin \mathbb{H}$. Then there cannot exist an x such that $x \cdot h_1 = e$. So, $x\mathbb{H}$ cannot exist such that $e \in x\mathbb{H}$

3. (15 pts, Page 4-5) In the proof of Lagrange's Theorem, I said $\mathbb{H} \cap x\mathbb{H} = \varnothing$. Formally prove it.

   Answer:
   Proof by contradiction:
   If $\mathbb{H} \cap x\mathbb{H} \neq \varnothing$, then there is some element that is shared by $x\mathbb{H}$ and $\mathbb{H}$. Then there must be some h_2 that exists in both $\mathbb{H}$ and $x\mathbb{H}$ such that, for $\exists h_1 \in \mathbb{H}$, $xh_1 = h_2$. Then $xh_1 = h_2 \Rightarrow x = h_1^{-1}h_2$. Since $h_1, h_2 \in \mathbb{H}$, then $x \in \mathbb{H}$, which is false because x is defined as $x \in \mathbb{G} - \mathbb{H}$. There does not exist any h_2 that exists in both $\mathbb{H}$ and $x\mathbb{H}$, so $\mathbb{H}$ and $x\mathbb{H}$ are disjoint.

4. (15 pts, Page 6) Prove that any $x \in (\mathbb{G} - \{e\})$ generates $\mathbb{G}$ if $|\mathbb{G}|$ is a prime number.

   Answer:
   From Theorem 1, we know that $x^{|\mathbb{G}|} = e$. From Proposition 3, we know that for some $x \in \mathbb{G}$, if $x^k = e$, then $ord(x)|k$. Since $x^{|\mathbb{G}|} = e$, we can set $k = |\mathbb{G}|$. Since $|\mathbb{G}|$ is prime, the only element that divides $k = |\mathbb{G}|$ that is also less than or equal to $k = |\mathbb{G}|$ is $|\mathbb{G}|$. So, $ord(x)$ must be $|\mathbb{G}|$ for all $x \in \mathbb{G}$.

5. (15 pts, Page 7) Describe an algorithm for finding a generator in $\mathbb{Z}_p^*$ when p is a prime number such that $p = 2q + 1$ for a prime q.

   - Hint: You may use the following proposition without proving it – An element $x \in \mathbb{G}$ is a generator of $\mathbb{G}$ if and only if $\mathsf{ord}(x) = |\mathbb{G}|$

   Answer:
   We know that the order of $\mathbb{Z}_p^*$ is $2q$ because the order is equal to $p - 1 = (2q + 1) - 1 = 2q$. So we must find an element $x \in \mathbb{Z}_p^*$ that has an order of $2q$, as stated by the proposition above. From the lecture notes and Lagrange's Theorem, we know that any element in $\mathbb{Z}_p^*$ can only produce sets with an order of 1, 2, q, and $2q$. So the algorithm to find x is as follows:

Pick a number x in $\mathbb{Z}_p^*$.
Calculate x^1.
If $x^1 \neq 1$, calculate x^2.
If $x^2 \neq 1$, calculate x^q.
If $x^q \neq 1$, then x is a generator of $\mathbb{Z}_p^*$.
If x failed any of the above tests, pick a different x and try the tests again.

6. (5pts, Page 8) Explain why x, r should be non-zero in ElGamal encryption.

   Answer:
   If $x = 0$, then the attacker automatically knows because the public key h will be equal to $g^0 = 1$. The attacker then can know the cipher c_2 will equal the message m because $c_2 = m * h^r = m * 1 = m$.
   If $r = 0$, the attacker will automatically knows because c_1 will equal $g^r = 1$. Then the attacker will know the cipher c_2 will equal the message m because $c_2 = m * h^r = m * 1 = m$.

7. (15 pts, Page 11) 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:
   If the DLOG algorithm works, this is how it can be used to find the result g^{ab} of the CDH problem given g, g^a, and g^b:
   First, find $\mathbb{G}$ from g. This can be done because g is a generator of $\mathbb{G}$.
   Then, insert $\mathbb{G}$, g, and g^a into the DLOG algorithm to get a.
   Then, raise g^b to a to get $g^{ba} = g^{ab}$.

8. (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:
   The encryption of m_1 yields $c_{11} = g^{r_1}$ and $c_{21} = g^{m_1} g^{r_1 x}$. The encryption of m_2 yields $c_{12} = g^{r_2}$ and $c_{22} = g^{m_2} g^{r_2 x}$. We can get the encryption of $m_1 + m_2$ from the encryption of m_1 and the encryption of m_2 by computing $c_{11} \cdot c_{12}$ and $c_{21} \cdot c_{22}$.
   $c_{11} \cdot c_{12} = g^{r_1} \cdot g^{r_2} = g^{r_1 + r_2}$, and $c_{21} \cdot c_{22} = g^{m_1} g^{r_1 x} \cdot g^{m_2} g^{r_2 x} = g^{m_1+m_2} g^{(r_1+r_2)x}$
   Then the decryption can be computed by computing $(c_{11} c_{12})^x = g^{(r_1+r_2)x}$, then computing $g^{(-1)(r_1+r_2)(x)}$, then computing $(c_{21} c_{22}) \cdot g^{(-1)(r_1+r_2)(x)} = g^{m_1+m_2} g^{(r_1+r_2)x} g^{(-1)(r_1+r_2)(x)} = g^{m_1+m_2}$. Then compute DLOG on $g^{m_1+m_2}$ to get $m_1 + m_2$.