Homework 4

Due Thursday, October 1

Implementation Part

1. Let's begin by implementing the Elgamal cryptosystem. Fix a prime p and an element $g \in \mathbb{F}_p^*$ and save them as global variables.

   (a) Write Alice's algorithms: `generatePublicKey(a)` which takes as input Alice's private key and returns her public key; and `elgamalDecrypt(c1,c2,a)` which takes as input ciphertext (c_1, c_2) as well as Alice's private key and returns a message.

   (b) Write Bob's algorithm: `elgamalEncrypt(m,A)` which takes as input Alice's public key A and a message m and returns ciphertext (c_1, c_2). (Recall that Bob needs to choose a random exponent to encrypt with. `ZZ.random_element(lowerBound,upperBound)` should come in handy).

   (c) Test it out. Let $p = 9787$ and $g = 34$. Pick any exponent you like and generate a public key as Alice. Then put on your Bob hat and encrypt a message (secret number). Finally decrypt it as alice and make sure you got what you started with. Do this for various values of a and messages.

   (d) I'm trying to send you a message. Let

   $$\begin{aligned} p &= 7530222359743975912426835638868420091\,17 \\ g &= 47393028462819284673. \end{aligned}$$

   Suppose further that your secret key is $a = 31415926535897932384 6$. I send you the following ciphertext:

   $$\begin{aligned} (c_1, c_2) = \;& (449164960684688587557185888310931655332, \\ & 608713686463403616105013668689979824341). \end{aligned}$$

   Decode my message. (Use `intToText` to read it!)

   (e) You're welcome to respond to my message. With the same prime and generator, I have a public key of

   $$A = 418194837551245918495968754919547251501.$$

   Encode me a message. You can just post in on discord and it should still be well enough encrypted so that only I can read it!

Written Part

In class we showed that an Elgamal oracle can solve the Diffie-Hellman problem. Let's show the other direction, and conclude that Elgamal and Diffie-Hellman are equally difficult.

2. Suppose you have access to an oracle who can solve the Diffie-Hellman problem. That is, for any prime p, given g^a and $g^b \mod p$, the oracle can tell you $g^{ab} \mod p$. Show that you can use this oracle to crack the Elgamal Public Key Cryptosystem. Precisely, suppose Alice publishes a prime p, an element $g \in \mathbb{F}_p^*$, and a public key A, and Bob sends the cipher text (c_1, c_2). Consult with the oracle to find the message Bob sent.

Problem 2.10 in [HPS] gives an example of a cryptosystem where Alice and Bob need to send two rounds of messages back and forth to communicate. We reproduce it here. It might be fun to follow along on cocalc!

3. Alice and Bob decide on a prime $p = 32611$. The rest is secret. But any information crossing the middle channel (via the arrows) should be assumed to be intercepted by Eve.

	Alice	Eve	Bob
1.	Alice has message $m = 11111$		
2.	Alice chooses random $a = 3589$		
3.	Alice computes $u = m^a \mod p = 15950$	$\longrightarrow$	Bob recieves u
4.			Bob chooses random $b = 4037$.
5.	Alice recieves v	$\longleftarrow$	Bob Computes $v = u^b \mod p = 15422$
6.	Alice knows $a' = 15619$		
7.	Alice computes $w = v^{a'} \mod p = 27257$	$\longrightarrow$	Bob recieves w.
8.			Bob knows $b' = 31883$
9.			Bob computes $w^{b'} \mod p = 11111$. That's m!

(a) Notice how Alice knows a second exponent $a' = 15619$ in step 6. Where does this number come from and how does this relate to $a = 3589$ from step 2? Similarly how do Bob's exponenets $b = 4037$ and $b' = 31883$ relate? Use this information to explain how the algorithm works.

(b) Formulate a general version of this algorithm using variables and show that it works in general.

(c) Can a solution to the DLP break this cryptosystem? Justify your answer.

(d) Can a solution to the DHP break this cryptosystem? Justify your answer.

The following exercises are adapted from 2.12-2.15 [HPS], and cover important properties and examples from group theory.

4. Let G be a group, and N a positive integer. The *N-torsion* of G is the set:

$$G[N] := \{g \in G : g^N = 1\}.$$

(a) Prove that if $g \in G[N]$, then so is g^{-1}.

(b) Suppose that G is commutative. Prove that if $a, b \in G[N]$, then so is $a * b$

(c) Suppose that G is commutative. Prove that $G[N]$ is a group.

5. Let G and H be groups, and denote their multiplication rules by $*_G$ and $*_H$ respectively. A function $\varphi : G \to H$ is called a *homomorphism* if for all $a, b \in G$:

$$\varphi(a *_G b) = \varphi(a) *_H \varphi(g).$$

Homomorphisms have some nice properties:

(a) Let e_G be the identity of G and e_H the identity of H. Show that if φ is a homomorphism then $\varphi(e_G) = e_H$

(b) Show that $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

(c) Let G be a commutative group, show that the function $\varphi(g) = g^2$ is a homomorphism. Do the same for the function $\psi(g) = g^{-1}$. Highlight the steps whereyou needed G to be commutative.

(d) Suppose $\varphi : G \to H$ is a homomorphism and is bijective. Show that the inverse $\varphi^{-1} : H \to G$ is a homomorphism as well. Such a map is called an *isomorphism*.

6. Prove that the following maps are homomorphisms.

(a) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ taking $a \in \mathbb{Z}$ to $a \mod N \in \mathbb{Z}/N\mathbb{Z}$.

(b) The map $\iota : \mathbb{R}^* \to GL_2(\mathbb{R})$ defined by $r \mapsto \begin{pmatrix} r & 0 \\ 0 & -r \end{pmatrix}$.

(c) Show that the discrete log map $\log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$ is an isomorphism.

7. Matrix groups over finite fields are very interesting examples of finite groups, and essential in the study of linear algebra over finite fields. Recall that $GL_2(\mathbb{F}_p)$ is the set of 2 by 2 matrices with entries in $\mathbb{F}_p$ and nonzero determinant.

(a) Prove $GL_2(\mathbb{F}_p)$ is a group under matrix multiplication.

(b) Prove $GL_2(\mathbb{F}_p)$ is noncommutative for every p.

(c) Write down all the elements of $GL_2(\mathbb{F}_2)$ and the multiplication.

(d) Compute this size of $GL_2(\mathbb{F}_p)$ in terms of p. (*Hint:* How many choices are there for the first column? Once you fix this first column how many choices are there left for the second?)

8. Let's play with big $\mathcal{O}$ notation.

(a) Show that $x^3 + 2x + 5 = \mathcal{O}(x^3)$

(b) Let $f(x)$ be a polynomial of degree n. Show that $f(x) = \mathcal{O}(x^n)$.

(c) Show that $(\ln x)^{500} = \mathcal{O}(x^{.01})$.

(d) Show that $k^2 2^k = \mathcal{O}(3^k)$