CS 380/525: Intro to Crypto
Fall 2022
Assignment 5, due 11/22, before class

Please see class written notes and class slides for examples. Total: 100 points.

1. (25 points) Find discrete logarithm using Baby-Step-Giant-Step algorithm. Show your work:
   (a) Given cyclic group $\mathbb{Z}_{29}^*$, and $2^x \bmod 29 = 27$. Find $x = \log_2 27$ in $\mathbb{Z}_{29}^*$.
   (b) Given cyclic group $\mathbb{Z}_{37}^*$, and $2^x \bmod 37 = 6$. Find $x = \log_2 6$ in $\mathbb{Z}_{37}^*$.
   (c) Given cyclic group $\mathbb{Z}_{17}^*$, and $3^x \bmod 17 = 7$. Find $x = \log_3 7$ in $\mathbb{Z}_{17}^*$.
2. (25 points) Find discrete logarithm using Pohlig-Hellman algorithm. Show your work:
   (a) Given cyclic group $\mathbb{Z}_{11}^*$, and $2^x \bmod 11 = 10$. Find $x = \log_2 10$ in $\mathbb{Z}_{11}^*$.
   (b) Given cyclic group $\mathbb{Z}_{31}^*$, and $3^x \bmod 31 = 12$. Find $x = \log_3 12$ in $\mathbb{Z}_{31}^*$.
   (c) Given cyclic group $\mathbb{Z}_{23}^*$, and $5^x \bmod 23 = 15$. Find $x = \log_5 15$ in $\mathbb{Z}_{23}^*$.
3. (25) Consider a group $\mathbb{Z}_{23}^*$, and a message $M = 10$. Encrypt M using ElGamal encryption scheme (you'll have to pick the PK, SK before encryption) to obtain ciphertext C. Now decrypt C to verify you get M back. Show your steps.
4. (25 points) Compute $4^{23} \bmod 187$, and $9^{36} \bmod 101$, using square-and-multiply method.