Assignment 2

Due Date: 16:00hr, Monday, Nov 16

1. Implement Shanks's babystep-giantstep method to solve the following discrete logarithm problems:

a $650^x = 2213$ in $\mathbb{F}_{3571}$.

b $106^x = 9999$ in $\mathbb{F}_{1300147}$.

2. Solve the following simultaneous systems of congruences

$$x \equiv 37 \bmod 43, \quad x \equiv 22 \bmod 49, \quad x \equiv 18 \bmod 71.$$

3. Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communication using the ElGamal public key cryptosystem.

a Alice chooses $a = 947$ as her private key. What is the value of her public key A?

b Bob chooses $b = 716$ as his private key, so his public key is

$$B \equiv 2^{716} \equiv 469 \bmod 1373.$$

Alice encrypts the message $m = 583$ using the ephemeral key $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

c Alice decides to choose a new private key $a = 299$ with associated public key A. Bob encrypts a message using Alice's public key and sends her the ciphertexts $(c_1, c_2) = (661, 1325)$. Decrypt the message.

d Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertexts $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission and decrypts the message. What is the message (plaintext)?

4. Use the Pohlig-Hellman algorithm to solve the discrete logarithm problem

a $p = 41022299$, $g = 2$, $a = 39183497$.

b $p = 1291799$, $g = 17$, $a = 192988$.