**Final Project:**

**(Simplified) El Gamal Encryption System**

The purpose of the project is to create a program in Java that can decrypt a ciphertext encrypted with a simplified version of El Gamal (with p limited to less than 100000). The system is built based on basic Java compiler with standard libraries and is not included Crypto or BigInteger libraries. The program consisted of three main components: The input processor, the ciphertext solver and the plaintext converter; with each of them contain multiple modules.

**The Input Processor**

Modules included:

* Method: getPositions(File file)
  + This method take in input as a .txt file that contained multiple pairs of C1,C2 under the format: (C1,C2); and store them as an array list of “positions” or points.
* Class: Point()
  + Class created for the purpose of storing values of C1, C2

**The Ciphertext Solver**

Modules included:

* Method: modExp(int a, int x, int p)
  + Perform modular exponentiation using the form a^x (mod p)
* Method: extendedEuclidean(int a, int p)
  + Perform extended Euclidean algorithm on a mod p: Used by the modInverse function to find the modular multiplicative inverse
* Method: modInverse(int a, int p) (used extendedEuclidean method)
  + Obtains the coefficients of ax+py=gcd(a,p). Assumes a is the base and p is the modular value, calculates the inverse for a.
* Method: findKey( int alpha, int beta, int p) (used modExp method)
  + Solves the discrete log problem. The key is found when beta = alpha^secretKey (mod p)
* Method: modpow(int value, int power, int mod)
  + Custom method works similar to modPow() in BigInteger library. It takes in a value, raise the value to the defined power then take mod of the result.
* Method: findMessage(int p, int x, int C1, int C2) (used modpow method)
  + Perform decryption on the cipher text with x being the key knows from findKey and p, C1, C2 are known variables.

**The Plaintext Converter:**

* Method: matchWord(int a)
  + This method take in an integer a and match such integer with the alphabet (with 0 matched with A) and return a String of such letter.
* Method: findWord(int message) (used matchWord)
  + This method takes in a decrypted result of pair of C1, C2 and print out group of three letters that matched with them. The process is as followed:
    - Let a= 26^2\*x + 26\*y + 1\*z be the decrypted integer and x, y, z the position of the letters that need to be matched
    - a mod 26 = z
    - Thus y = (a-z)/26 mod 26
    - Substitute z and y to the original function to find x
    - Run x, y, z to matchWord and print them out

**Outstanding method:** decrypt(List<Point> cipher, int p, int secret)

* This method acts as a loop that loop through the entire stored arrayList of pairs of C1, C2 to decrypt and print out the plaintext.