Assignment 3

Introduction

This assignment is given to solve problems based on the Diffie Hellman theory learned in class. All programs is done in Java language.

Question 2

This problem implements the Diffie Hellman key exchange algorithm. Public keys are exchanged between two parties and a secret key is calculated. message is encrypted and decrypted using the shared secret key.

decimal_to_binary.java

This program is a program that returns the binary representation of a decimal number. It starts by counting the number of bits of the decimal number and use it to convert to binary with the help of `Integer.toBinaryString`.

square_and_multiply.java

This program returns the calculated shared secret key by computing power for large prime numbers. The program starts by defining and initializing fix p, alpha and private key. It also prints the generated public key, prompts for an exchanged key and finally prints the shared secret key.

Using the pre defined p, alpha, and private key, this program computes the power of the numbers to calculate the generated public key. This public key is then exchanged to the other party. The exchanged key will need to be input as the prompted exchange key for the program to again compute the power and calculate the shared secret key.

encrypt_Diffie.java

This program connect to both programs mentioned above and prompted for message to decrypt and encrypt. It assumes that the user will received an encrypted message first.

Both the text and secret key will be converted to binaries. The program will then xor both binaries and display the result.

Output

The output of all programs is attached in the folder. Problem2_output shows the output from the compiler side while emai_output shows the email exchange screenshot.