

```

import java.math.BigInteger;
import java.util.Scanner;
import java.security.SecureRandom;

public class ElGamalShort {
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);

        BigInteger p = new BigInteger("23");
        BigInteger g = new BigInteger("5");

        System.out.println("Using public parameters p=" + p + " and g=" + g);

        System.out.print("Enter your private key (an integer x < p): ");
        BigInteger x = sc.nextBigInteger();

        BigInteger y = g.modPow(x, p);
        System.out.println("Your public key is y=" + y);

        System.out.print("\nEnter the message to encrypt (an integer M < p): ");
        BigInteger M = sc.nextBigInteger();

        BigInteger k = new BigInteger(p.bitLength() - 1, new SecureRandom());
        System.out.println("Using a random ephemeral key k=" + k);

        BigInteger c1 = g.modPow(k, p);
        BigInteger c2 = M.multiply(y.modPow(k, p)).mod(p);

        System.out.println("Encrypted ciphertext (c1, c2) = (" + c1 + ", " + c2 + ")");

        BigInteger s = c1.modPow(x, p);
        BigInteger decryptedMessage = c2.multiply(s.modInverse(p)).mod(p);

        System.out.println("\nDecrypted Message: " + decryptedMessage);

        sc.close();
    }
}

```