Implementación del algoritmo Diffie- Hellman.

DESARROLLO DEL CÓDIGO (20/01/2023)

Resumen del Programa:

Este programa en C implementa el algoritmo de intercambio de claves de Diffie-Hellman para establecer una clave secreta compartida entre dos grupos. Utiliza números primos, generadores y funciones de exponenciación modular para calcular claves privadas, públicas y compartidas. Después, verifica la igualdad de las claves compartidas, asegurando un canal seguro de comunicación entre los grupos.

Código

```c
/**
 *  Autor: Grupo 7
 *  Fecha: 18/01/2024
 *  Asignatura: Algebra y Matematica Discreta
 *  Descripcion: El siguiente programa calcula establecer una
 *  clave secreta compartida mediante el algoritmo Diffie-Hellman
 * */
/*Declaración de las librerías para utilizar ciertas funciones
relevantes para la realización del programa*/
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

// Función para calcular (base^exponente) % modulo
int mod_exp(int base, int exponente, int modulo) {
    int x = 1;
    int power = base % modulo;

    for (int i = 0; i < 8 * sizeof(int); i++) {
        if (exponente & 1) {
            x = (x * power) % modulo;
        }
        exponente >>= 1;
        power = (power * power) % modulo;
    }

    return x;
}
/*
 * Hilo de ejecución principal del programa
 * Generación de las claves privadas
 * */
int main() {
    int p, r, x, y, X, Y, K_1, K_2, A, B;
```

```
    /*Seleccion de los parámetros*/
    p = 761;
    r = 6;
    /*--- 1.Generación de las claves privadas mediante un número
aleatorio ---*/
    srand(time(NULL));
    x = rand() % (p - 1) + 1; // x en el rango [1, p-1]
    printf("\nPaso 1:\n\nGrupo 1, esta es su clave privada: %i\n", x);
    y = rand() % (p - 1) + 1; // x en el rango [1, p-1]
    printf("Grupo 2, esta es su clave privada: %i\n", y);

    /*--- 2.Cálculo de la clave pública del Grupo 1 ---*/
    // Calcular X = r^x mod p

    X = mod_exp(r, x, p);
    printf("\nPaso 2:\n\nGrupo 1, envie el numero: %i al Grupo 2\n",
X);
    /*--- 2.Cálculo de la clave pública del Grupo 2 ---*/
    Y = mod_exp(r, y, p);
    printf("Grupo 2, envie el numero: %i al Grupo 1\n", Y);

    /*--- 3. Cálculo de la clave compartida --- **/
    printf("\nPaso 3:\n\nGrupo 1, introduzca el numero que le ha
enviado el grupo 2\n");
    scanf("%i", &A);
    K_1 = mod_exp(A, x, p);
    printf("Grupo 1, Su clave secreta es %i\n", K_1);
    printf("\nGrupo 2, introduzca el numero que le ha enviado el grupo
1\n");
    scanf("%i", &B);
    K_2 = mod_exp(B, y, p);
    printf("Grupo 2, Su clave secreta es %i\n", K_2);

    /*--- Verificación de la igualdad de las claves compartidas ---
**/
    if (K_1 == K_2)
        printf("\nLas dos claves son identicas, los dos Grupos pueden
conectarse de manera segura con la clave %d\n\n", K_1);
    else
        printf("\nLas claves de sesion no coinciden, alguno de los dos
grupos ha escrito incorrectamente el numero, o alguien está intentando
entrar con sus claves\n\n");
    return 0;
}
```