DOCUMENT_HEADING

2 files

excension de responsabilidad.c
Diffie_Hellman.c

excension de responsabilidad.c

```
/*

Exención de responsabilidad:

Al descargar y/o utilizar los materiales proporcionados en este archivo (en adelante, "los Materiales"), el usuario (en adelante, "el Usuario") acepta los términos y condiciones que se describen a continuación:

Los Materiales son proporcionados "tal cual" y sin garantías de ningún tipo, ya sean expresas o implícitas. El autor de los Materiales no garantiza la precisión, exhaustividad, actualidad o idoneidad de los mismos para un propósito particular.

Los Materiales se ofrecen únicamente como refuerzo o ayuda para realizar más ejercicios, y no están destinados a ser copiados directamente. El Usuario debe utilizarlos como una guía o recurso de apoyo en su aprendizaje y no como una solución completa para sus tareas o trabajos académicos.

El autor de los Materiales no se hace responsable de ningún error, omisión, inexactitud o malentendido en la información proporcionada.

El Usuario acepta asumir todos los riesgos asociados con la utilización de los Materiales y será el único responsable de cualquier daño, pérdida, perjuicio o inconveniente que pueda surgir como resultado del uso o la incapacidad de usar los Materiales.

El Usuario se compromete a no responsabilizar al autor de los Materiales por cualquier reclamo, demanda, acción, responsabilidad, costo o gasto, incluidos los honorarios legales, que surjan de o estén relacionados con el uso o la dependencia de los Materiales.

Los Materiales no deben ser utilizados como sustituto del asesoramiento, la supervisión o la instrucción de un profesor, tutor u otro profesional cualificado en la materia.

El Usuario no debe compartir, distribuir, modificar, vender, transmitir, copiar o reproducir en cualquier forma, total o parcialmente, los Materiales sin la previa autorización por escrito del autor.

Al descargar y/o utilizar los Materiales, el Usuario confirma que ha leído, comprendido y aceptado los términos y condiciones aquí establecidos.


*/
```

Diffie_Hellman.c

```
/*
Dada una aritmética modular en número primo p=761 y raíz primitiva r=6, implementa un programa que genere un número aleatorio x, calcule X=rx mod p y lo imprima. A continuación, el programa recoge como entrada por consola el
```

```
número Y
que ha generado otro usuario y genera el número K=Yx=rxy.

*/

#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <math.h>

/**
 * @brief
 *
 * @param b
 * @param e
 * @param p
 * @return int
 */
// Funcion `b^e mod p`
int mod_exp(int b, int e, int p)
{
    int i, x, power;
    x = 1;
    power = b % p;

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

    return x;
}

// Programa C para demostrar el algoritmo de Diffie-Hellman
int main()
{
    int p = 761;
    int r = 6;
    srand(time(NULL));

    // Numero aleatorio (Secreto)
    int numeroRandom;

    // X = Clave pública nuestra
    // Y = Clave pública que nos llega
    int X, Y;

    // Calculabmos numero aleatorio
    numeroRandom = rand();

    // Calculamos la X
    X = mod_exp(r, numeroRandom, p);

    printf("X:%d\n", X);
```

```
    // Pedimos que nos introduzcan su clave pública
    printf("Introduce el numero Y generado por otro usuario: ");
    scanf("%d", &Y);

    // Encontrar la clave privada
    int clave = mod_exp(Y, numeroRandom, p);

    printf("Clave privada es: %d\n", clave);
    return 0;
}
```