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.

Batería de Pruebas 1: Prueba de igualdad de claves compartidas

- Objetivo: Comprobar que el código funciona correctamente con parámetros válidos.
- Verifica que las claves compartidas (K_1 y K_2) resultantes sean iguales. Este caso imprime un mensaje indicando que las claves son compartidas son iguales.
- Resultado: La prueba se pasa correctamente. Ejecución en consola:

```
Paso 1:
Grupo 1, esta es su clave privada: 477
Grupo 2, esta es su clave privada: 91

Paso 2:
Grupo 1, envie el numero: 51 al Grupo 2
Grupo 2, envie el numero: 424 al Grupo 1

Paso 3:
Grupo 1, introduzca el numero que le ha enviado el grupo 2:
424
Grupo 1, Su clave secreta es 52
Grupo 2, introduzca el numero que le ha enviado el grupo 1:
51
Grupo 2, Su clave secreta es 52
Las dos claves son identicas, los dos Grupos pueden conectarse de manera segura con la clave 52
```

Batería de Pruebas 2: Prueba de manejo de entrada inválida

- Objetivo: Introduce caracteres no numéricos o valores que excedan los límites de los parámetros.
- Verifica que el programa maneje correctamente estas situaciones y proporcione mensajes de error o solicite la entrada nuevamente.
- Resultado: La prueba se pasa correctamente

Ejecución en consola:

```
Paso 1:
Grupo 1, esta es su clave privada: 529
Grupo 2, esta es su clave privada: 661

Paso 2:
Grupo 1, envie el numero: 123 al Grupo 2
Grupo 2, envie el numero: 206 al Grupo 1

Paso 3:
Grupo 1, introduzca el numero que le ha enviado el grupo 2:
123
Grupo 1, Su clave secreta es 11
Grupo 2, introduzca el numero que le ha enviado el grupo 1:
206
Grupo 2, Su clave secreta es 631
Las claves de sesion no coinciden, alguno de los dos grupos ha escrito incorrectamente el numero, o alguien est i intent
ando entrar con sus claves
```

Conclusión de Baterías de pruebas:

De acuerdo con las pruebas realizadas, el código proporcionado no produce cálculos incorrectos. Sin embargo, es posible que los cálculos sean incorrectos si se producen errores en la implementación o ejecución del código, o si se utilizan parámetros no seguros.

Se ha realizado una exhaustiva batería de pruebas, abarcando diversos escenarios, incluyendo parámetros válidos e inválidos, así como un generador aleatorio seguro. La implementación de la función mod_exp y la generación de claves privadas y públicas ha demostrado ser precisa.

Es esencial destacar que, aunque no se han identificado errores en las pruebas realizadas, siempre es crucial mantener una implementación y parámetros seguros para evitar posibles vulnerabilidades. Para mitigar estos riesgos, es importante utilizar un código bien implementado y probado, y utilizar parámetros seguros.

Nota: Para pruebas hasta llegar a la implementación correcta del ejercicio se han utilizado páginas web y el cálculo a papel de las claves privadas y públicas. URL: www.irongeek.com/diffie-hellman.php

¿Se ha encontrado algún ejemplo en el que los cálculos obtenidos no son correctos?

No se ha encontrado ningún ejemplo en el que los cálculos obtenidos por el código sean incorrectos. El código ha sido probado con una batería de pruebas que cubre determinados de escenarios, incluyendo parámetros válidos e inválidos, y un generador aleatorio seguro.

A pesar de la precisión y seguridad del algoritmo Diffie-Hellman, **se debe tener en cuenta su vulnerabilidad ante ataques Man In the Middle (MITM)**. En estos escenarios, un atacante podría situarse entre los dos equipos, haciéndose pasar por cada uno de ellos y acordando claves secretas. Este tipo de ataque permite al atacante interceptar la comunicación cifrada entre los equipos sin que estos lo detecten. Aunque Diffie-Hellman es efectivo, es fundamental complementarlo con protocolos adicionales para mitigar amenazas como los ataques MITM. La fortaleza del algoritmo a lo largo del tiempo demuestra su eficacia, pero su implementación segura y consciente del contexto es esencial en entornos críticos de seguridad.