PRÁCTICA: INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN

Objetivo: Implementar el algoritmo de intercambio de claves de Diffie-Hellman

Desarrollo:

1. Implementa el generador el algoritmo de intercambio de claves de Diffie-Hellman según el diagrama que se incluye a continuación

A	**B**
escoge secreto $\mathbf{x_A}$	escoge secreto $\mathbf{x_B}$
calcula $\mathbf{y_A=\alpha^{xA}\ (mod\ p)}$	calcula $\mathbf{y_B=\alpha^{xB}\ (mod\ p)}$
genera $\mathbf{k= y_B^{xA}\ (mod\ p)}$	genera $\mathbf{k= y_A^{xB}\ (mod\ p)}$

2. El programa debe solicitar el número primo p, el número $\alpha<p$, y los secretos x_A y x_B, y mostrar la traza completa del algoritmo, es decir, los números intermedios generados y_A e y_B, y la clave compartida k.

Ejemplos:

$p = 13,\ \alpha = 4,\ x_A = 5, x_B = 2,\ y_A = 10, y_B = 3, k = 9$

$p = 43, \alpha = 23\ x_A = 25, x_B = 33, y_A = 40, y_B = 16, k = 4$

$p = 113, \alpha = 43\ x_A = 54, x_B = 71, y_A = 11, y_B = 29, k = 61$