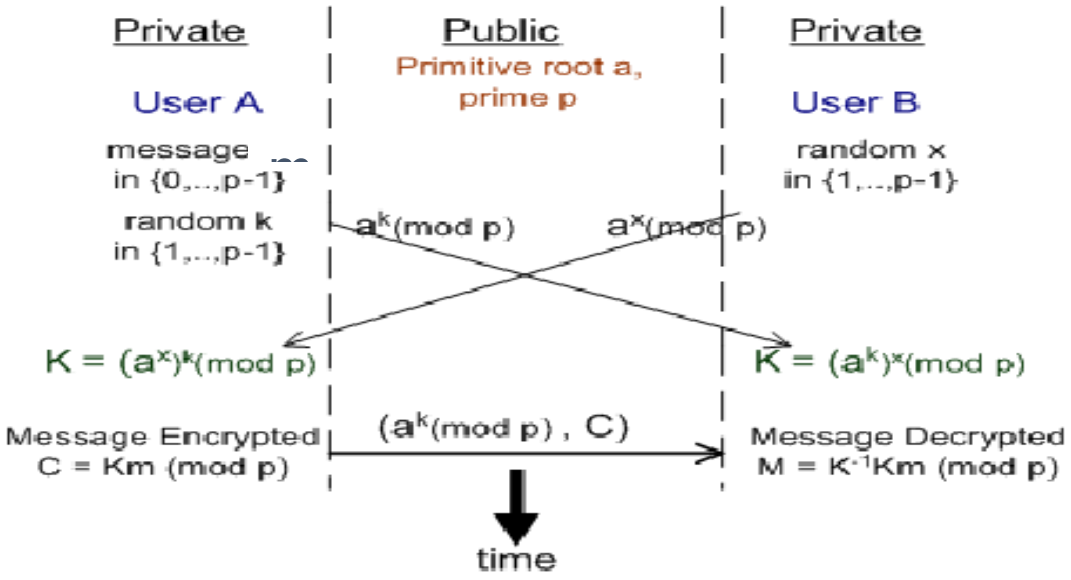
PRÁCTICA: INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN Y CIFRADO DE ELGAMAL

Objetivo: Implementar el algoritmo de intercambio de claves de Diffie-Hellman y el Cifrado de ElGamal.

Desarrollo:

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



Ejemplo:

El programa debe solicitar como entrada el número primo py el número entero a, y los secretos k y x de Alice y Bob respectivamente, y el mensaje m a cifrar. Debe mostrar como salida la traza siguiente del cifrado de ElGamal, incluyendo los entero intermedios generados y_A e y_B, la clave secreta compartida K, su inversa K^{-1}, el mensaje cifrado C y el mensaje descifrado M:

Entrada: p = 13, a = 4, k = 5, x = 2, m= 8
Salida: y_A =10, y_B =3, K = 9, C= 7, K^{-1}= 3, M=8

Entrada: p = 43, a = 23, k = 25, x = 33, m=18
Salida: y_A =40, y_B =16, K = 4, C=29, K^{-1}=11, M=18

Entrada: p = 113, a = 43, k = 54, x= 71, m=28
Salida: y_A =11, y_B =29, K = 61, C=13, K^{-1}=63, M=28