

24-9-2024

**Nombre:** Álvarez García Brandon Azarael

**Nombre de la materia:** Selected topics in cryptography

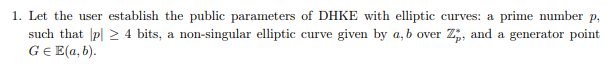
**Grupo:** 7CM1

**Nombre de la profesora:** Dra. Sandra Díaz Santiago

Session 4:

DHKE with elliptic curves

**Ejercicios de programación**

****

Para la resolución de este ejercicio, simplemente implemento una clase como en las practicas pasadas, en donde pueda definir todos los parámetros de la curva elíptica

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Cree una función llamada main() en donde creo una instancia y aquí solicito el valor de k\_a y pueda computar el proceso de DHKE, las funciones son reutilizadas de practicas pasadas, como algoritmo de Euclides, suma de puntos.

**Ejecución y pruebas**

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Este proceso fue visualizado por la profesora de forma presencial, las imágenes presentadas es una simulación del proceso que se realizo