

Cifrado de Hill

Agenda

Proyecto 1

Proyecto 1

Especificaciones:

Elaborar **un** programa con **dos** métodos: uno que **cifre** y otro que **descifre** texto en español, usando el criptosistema de Hill.

La función relacionada con **cifrar**, debe recibir como parámetros:

- N - la dimensión de la matriz
- Array `[][]` - Arreglo bidimensional con la matriz, con los coeficientes de la matriz

En el método **main** del programa incluir un texto en español (utilizando en pequeño diccionario de caracteres que hemos visto en clase) para ejecutar la función de cifrado y esta función debe de ser capaz de generar un texto cifrado utilizando el criptograma de Hill.

Tips para la parte de cifrado:


- Leer la dimensión de la matriz A , leer la matriz y verificar que sea invertible en Z_{27} . Si no lo es, terminar el programa con una señal de error a la entrada.
- Introduce un texto en español limpiando el texto de espacios, signos de puntuación y acentos. (como se ha hecho en los ejemplos de clase)



La función relacionada con **decifrar**, debe recibir como parámetros:

- N - la dimensión de la matriz
- Array `[][]` - Arreglo bidimensional con la matriz (con los coeficientes de la matriz usados para encriptar)
- String - Texto previamente cifrado con el primer método de esta práctica.

Incluir en el método main (método principal del programa) la llamada a esta función e imprimir en pantalla el texto en claro después de aplicar el algoritmo de descifrado.



Tips para la parte de descifrado:

- Leer la dimensión de la matriz A , leer la matriz y verificar que sea invertible en Z_{27} . Si no lo es, terminar el programa con una señal de error a la entrada.
- Calcular A^{-1} la inversa de la matriz A (análogo a como se vio en cifrado afín)



Notas adicionales

Considerar el alfabeto con 27 caracteres (Z27).

Desarrollar la práctica en equipos de dos integrantes (que no se pueden repetir en proyectos futuros).

El código fuente puede ser entregado en: **Java, C/C++ o Python.**

La entrega del código es el día **17 de septiembre de 2018.**

Enviar el código fuente a: kaan.ek@ciencias.unam.mx. Y también adjuntarlo en la plataforma **ClassRoom**.

Documentar el código fuente de **ambos** métodos e incluir el **nombre completo** de ambos integrantes en el método **main** del programa.

