

Proyecto 1

(Criptosistema de Vigenère y Hill)

Canek García [kaan.ek@ciencias.unam.mx]



Parte 1

(Vigenère)

Especificaciones generales

Elaborar **un** programa con **dos** métodos principales uno que **cifre** (obtener un texto cifrado usando el criptosistema de Vigenère) y otro que **descifre** (recuperar el texto en claro obtenido a partir del texto cifrado) texto en español (Z/27), usando el **criptosistema de Vigenère (implementando recorridos con la tabla de Vigenère, no utilizar la versión con función lineal vista en clase).**



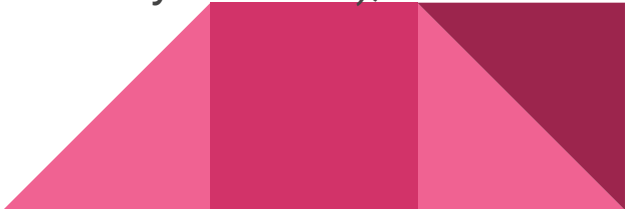
Detalles de la implementación

Los **métodos** de cifrar y descifrar, se deben mandar a llamar desde la función **main** de su programa.

El método relacionado con **cifrar**, debe recibir como parámetros:

- *String* - Texto con la **clave** que se utilizará para el cifrado de Vigenère.
- *String* - **Texto plano** al cual se le va a aplicar el criptosistema de Vigenère.

Los textos en español relacionados con los parámetros se incluirán en la función main, ambos **pueden** ir **normalizados** (sin signos de puntuación y acentos), **sin espacios en blanco** y en **mayúsculas**.



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

- *String* - Texto con la **clave** que se utilizó para cifrar.
- *String* - Texto del **criptograma** obtenido con el método de cifrado de esta práctica.



Recomendaciones:

- Declarar una constante global que sea un arreglo bidimensional para representar la tabla de Vigenère.
- Para los textos de los parámetros pueden considerar longitudes adecuadas, es decir, claves de longitud menor o igual que el mensaje.
- Incluir funciones auxiliares relacionadas con operaciones o recorridos de matrices.
- Se recomienda utilizar un **atributo de clase** para hacer referencia al **alfabeto en español**, debido a que **ASCII** y **UTF-8** utilizan un código para la letra **Ñ** que no está en los rangos de los códigos de la **A** a la **Z**.



Parte 2

(Hill)

Especificaciones generales

Elaborar **un** programa con **dos** métodos principales uno que **cifre** (obtener un texto cifrado usando el criptosistema de Hill) y otro que **descifre** (recuperar el texto en claro obtenido a partir del texto cifrado) texto en español ($\mathbb{Z}/27$), usando el **criptosistema de Hill**.



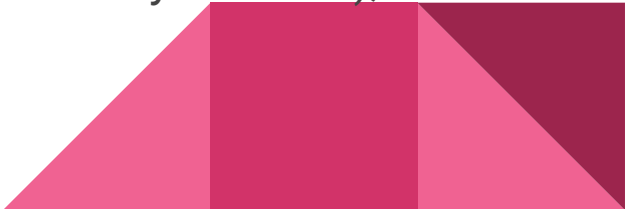
Detalles de la implementación

Los **métodos** de cifrar y descifrar, se deben mandar a llamar desde la función **main** de su programa.

El método relacionado con **cifrar**, debe recibir como parámetros:

- *String* - Texto con la **clave** que se utilizará para el cifrado de Hill.
- *String* - **Texto plano** al cual se le va a aplicar el criptosistema de Hill.

Los textos en español relacionados con los parámetros se incluirán en la función main, ambos pueden ir **normalizados** (sin signos de puntuación y acentos), **sin espacios en blanco** y en **mayúsculas**.



Recomendaciones para el cifrado:

- Calcular la matriz de la clave (primer parámetro), obtener la dimensión de esta y verificar que sea invertible en $Z/27$; si no lo es, lanzar una excepción debido a que no va a ser posible procesar el descifrado.
- Para los textos de los parámetros pueden considerar longitudes adecuadas, es decir, la **longitud de la clave** debe de generar un matriz de **$N \times N$** y la **longitud de texto plano** debe ser **múltiplo de N** , para que el criptosistema de Hill se pueda llevar a cabo.
- Incluir funciones auxiliares relacionadas con operaciones matrices.
- Se recomienda utilizar un **atributo de clase** para hacer referencia al **alfabeto en español**, debido a que **ASCII** y **UTF-8** utilizan un código para la letra **Ñ** que no está en los rangos de los códigos de la **A** a la **Z**.



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

- *String* - Texto con la **clave** que se utilizó para cifrar (**K**).
- *String* - Texto del **criptograma** obtenido con el método de cifrado de esta práctica.

Para calcular \mathbf{K}^{-1} (la inversa de la matriz **K**) recuerda: Generar la matriz de **K**, leer la dimensión de esta, leer la matriz y verificar que sea invertible en $\mathbb{Z}/27$; si no lo es, terminar el programa indicando que no se puede calcular \mathbf{K}^{-1} .



Recomendaciones para el descifrado:

- Descomponer el **criptograma** (segundo parámetro) en **N-gramas** que sean de longitud **$K \times 1$** , para aplicar la transformación usando la matriz **K^{-1}** .





Notas adicionales

Notas adicionales

- Considerar el alfabeto con 27 caracteres ($Z/27$), es decir: **$N \neq \tilde{N}$** .
- Para el criptosistema de Hill, la dimensión de la matriz clave (**K**) se considera como: **$K \in 2$ y $K \in 3$**
- El código fuente puede ser entregado en: **Java, C/C++ o Python** (para esta práctica NO se pueden utilizar bibliotecas externas de matrices) y entregar SOLO el código fuente.
- Desarrollar la práctica en equipos de **uno, dos o tres integrantes** (consideren trabajar en equipos de dos o tres integrantes).
- **Documentar** el código fuente e incluir el **nombre completo** de los integrantes en el método **main** del programa.
- Enviar el código el día **20 de septiembre de 2021**.
- Enviar el código fuente por medio de la plataforma **ClassRoom**. (al menos un integrante, pero de preferencia todos los miembros del equipo).