

Cifrado de Hill

(Proyecto 1)

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



Parte 1

(Código)

Especificaciones generales

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



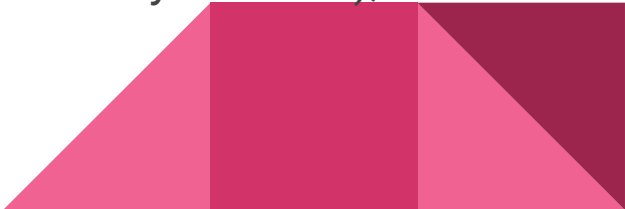
Detalles de la implementación

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}** .



Parte 2

(Reporte)

Especificaciones del reporte

En clase vimos las herramientas: whois, nslookup, google hacking y traceroute. Elaborar un breve reporte escrito con capturas de pantalla referente a estas herramientas.



Detalles del reporte

- Para **whois**, incluir una captura de pantalla que muestre la siguiente información de algún dominio: fecha de creación, fecha de expiración, datos de contacto del administrador y direcciones IP de los DNS.
- Para **nslookup**, una captura de pantalla que muestre toda la información disponible de algún dominio: Nombre del host, dirección IP de los servidores DNS y demás detalles del servidor.



- Para **Google Hacking**, incluir una captura de pantalla que muestre sitios vulnerables e información sensible de organizaciones por medio de los **operadores** vistos en clase, por ejemplo obtener esquemas de bases de datos; adicionalmente buscar **cámaras sin protección** con la ayuda del portal **shodan.io**.
- Para **traceroute**, una captura de pantalla que muestre el trazado de ruta hacia el dominio **gmail.com**.





Notas

Notas adicionales

- Considerar el alfabeto con 27 caracteres (Z27), es decir: $\mathbf{N} \neq \tilde{\mathbf{N}}$.
- La dimensión de la matriz clave (\mathbf{K}) se puede considerar como: $2 \leq \mathbf{K} \leq 3$. (Pero es un plus $\mathbf{K} \in \mathbb{N}$ que te ayuda a omitir el reporte escrito de herramientas)
- El código fuente puede ser entregado en: **Java**, **C/C++** o **Python**. El reporte debe ser entregado en formato **PDF**.
- 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, así mismo como en el reporte escrito.
- Enviar el código y el reporte el día **18 de marzo de 2020**.
- Enviar el código fuente y reporte por medio de la plataforma **ClassRoom**. (al menos un integrante, pero de preferencia todos los miembros del equipo sin importar que se repita esta entrega).