

# Cifrado de Hill

Canek García ([kaan.ek@ciencias.unam.mx](mailto:kaan.ek@ciencias.unam.mx))

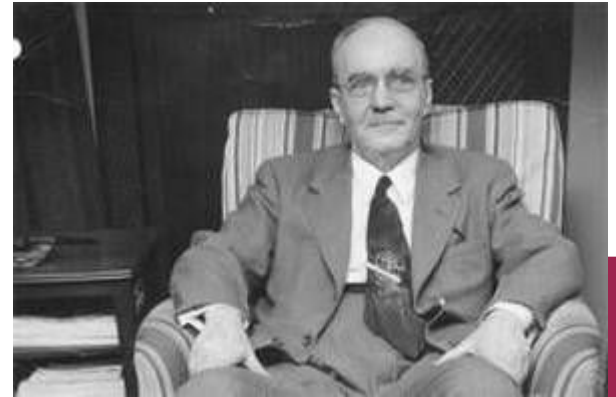
# Agenda

- Breve historia
- Algoritmo
- Proyecto 1

---

# Breve historia

- El algoritmo data de 1929, y fue descrito por Lester S. Hill
- Se basa en el uso del álgebra lineal
- Sistema criptográfico de sustitución polialfabética





# Algoritmo

# Cifrado

1. Asignar un valor numérico a cada letra del alfabeto a utilizar iniciando en 0.
2. La clave a utilizar debe constar de tantas letras como se desee siempre que sea posible calcular los equivalentes numéricos de cada una de ellas en una matriz de  $N \times N$  (K).
3. El mensaje (Mcla) se divide en diagramas, trigramas o N-gramas necesarios tal que sus equivalentes sean colocados en matrices de  $N \times 1$
4. El criptograma se obtiene multiplicando las matrices  $K * Mcla$ , esot es:

$$C(N \times 1) = K (N \times N) * Mcla(N \times 1)$$


# Descifrado

El mensaje en claro se recupera llevando a cabo el proceso inverso.

NOta: Todas las operaciones aritméticas se realizan con módulo  $n$ , donde  $n$  corresponde al tamaño del alfabeto que se esté empleando.



# Ejemplo

N = 27

Mensaje = CONSUL

Clave = FORTALEZA

1. Formar la matriz cuadrada para la clave:

$$K = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix}$$



3. Obtener trigramas de mensaie:

$$M_1 = \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} \quad M_2 = \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix}$$

4.  $K * M_1$  y  $K * M_2$

$$K * M_1 = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} = \begin{pmatrix} 469 \\ 183 \\ 398 \end{pmatrix} = \begin{pmatrix} 10 \\ 21 \\ 20 \end{pmatrix} \text{ mod } 27 = \begin{pmatrix} K \\ U \\ T \end{pmatrix}$$

$$K * M_2 = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix} \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix} = \begin{pmatrix} 608 \\ 501 \\ 622 \end{pmatrix} = \begin{pmatrix} 14 \\ 15 \\ 1 \end{pmatrix} \text{ mod } 27 = \begin{pmatrix} \tilde{N} \\ O \\ B \end{pmatrix}$$

5. Recuperar criptograma: **KUTÑOB**

Descifrando:

$$K^{-1} * C_1 = \begin{pmatrix} 23 & 9 & 21 \\ 11 & 9 & 2 \\ 22 & 23 & 6 \end{pmatrix} \begin{pmatrix} 10 \\ 21 \\ 20 \end{pmatrix} = \begin{pmatrix} 839 \\ 339 \\ 823 \end{pmatrix} = \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} \bmod 27 = \begin{pmatrix} C \\ O \\ N \end{pmatrix}$$

$$K^{-1} * C_2 = \begin{pmatrix} 23 & 9 & 21 \\ 11 & 9 & 2 \\ 22 & 23 & 6 \end{pmatrix} \begin{pmatrix} 14 \\ 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 478 \\ 291 \\ 659 \end{pmatrix} = \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix} \bmod 27 = \begin{pmatrix} S \\ U \\ L \end{pmatrix}$$

# Proyecto 1


# Especificaciones:

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

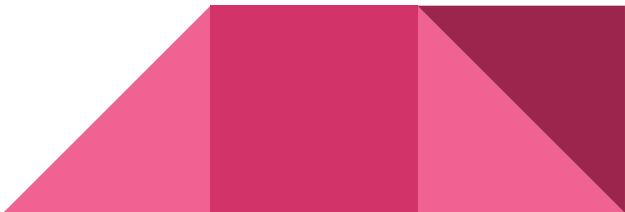
La función relacionada con **cifrar**, debe recibir como parámetros:

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

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)
  - Pueden utilizar funciones auxiliares para calcular la dimensión de la matriz de la clave.
- 

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

- Array `[][]` - Arreglo bidimensional con la matriz de la clave (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 **15 de marzo de 2019**.

Enviar el código fuente por medio de la plataforma **ClassRoom**. (ambos miembros del equipo, sin importar que se repita esta entrega).

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

