

# Universidad Nacional de San Agustín Ciencia de la Computación

Codificacion de Alberti

Basurco Cayllahua, Eduardo Apaza Torres, Alexander Del Castillo Ramirez, Kevin



### Índice

Introducción

Cifrado

Resultado





# Algoritmo de Albert

- Los discos de Alberti son artilugios que sirven de herramienta para realizar el cifrado de Alberti.
- El anillo móvil tiene 24 celdas iguales y en cada una de ellas hay grabada un símbolo del alfabeto latino en minúscula o los símbolos '&', 'y', 'k' y 'h'. El orden de las celdas puede ser cualquiera. Este alfabeto se usará para el texto cifrado.
- Por tanto el número de alfabeto distintos usables para un disco de Alberti determinado es de 24, sin embargo nuestro disco es variable



#### Cifrado

- Para adaptar el texto plano a las posibilidades de nuestro cifrador es necesario realizar un proceso de preprocesado.
- Texto a cifrar : 'LAGVER2RASIFARA'
  Clave: El orden del disco móvil es

'gkInprtuz&xysomqihfdbace'

 Se elige una letra del disco móvil como índice, únicamente conocido por el emisor y el receptor. Supongamos que es la 'g'. Se hace coincidir la 'g' con la letra del disco móvil que queramos, por ejemplo la 'A'. Por tanto los discos quedan así:

ABCDEFGILMNOPQRSTVXZ1234 Anillo fijo gklnprtuz&xysomqihfdbace Anillo móvil



#### Resultado

\_LAGVER2RA\_SIFARA texto a cifrar AzgthpmamgQlfiyky texto cifrado

Observar que cuando realizó el giro los discos quedan en la posición relativa:

QRSTVXZ1234ABCDEFGILMNOP Anillo fijo gklnprtuz&xysomqihfdbace Anillo móvil