## Cifrado de Vigenère

by Canek García (kaan.ek@ciencias.unam.mx)

# Agenda

- Breve historia
- Algoritmo
- Implementación

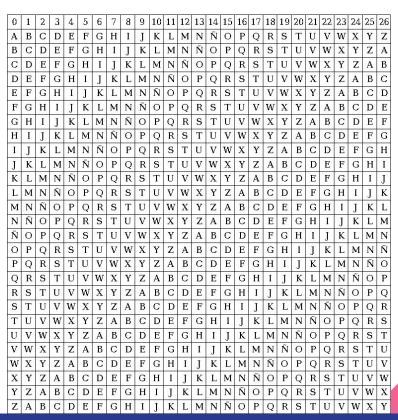
## Breve historia

- Es un cifrado de sustitución simple polialfabético.
- El método original fue descrito por Giovan Battista Belasso en su libro de 1553 La cifra del Sig. Giovan Battista Belasso.
- Fue incorrectamente atribuido más tarde a Blaise de Vigenère, (siglo XIX).
- El escritor y matemático Charles Lutwidge Dodgson (Lewis Carroll) dijo que el cifrado Vigenère era irrompible en el artículo "The Alphabet Cipher".



# Algoritmo

### 1) Tabla de Vigenère



#### Función de cifrado

En términos matemáticos puede expresarse la función de cifrado como:

$$E(X_i) = (X_i + K_i) \mod L$$

Donde:

Xi es la letra en la posición i del texto a cifrar.

**Ki** es el carácter de la clave correspondiente a **Xi** pues se encuentran en la misma posición.

L es el tamaño del alfabeto.

# Implementación

### Java (beta)

```
static String encrypt(String text, final String key) {
   String res = "";
   text = text.toUpperCase();
   for (int i = 0, j = 0; i < text.length(); i++) {
        char c = text.charAt(i);
        if (c < 'A' || c > 'Z') continue;
        res += (char)((c + key.charAt(j) + 'A') % 27 + 'A');
   }
   return res;
}
```

# Código fuente

https://github.com/kanekko/cryptography\_2019-1/tree/master/Lab 02