

**Cat-Cipher**Criptografía y Seguridad

**30 de septiembre de 2012**

Integrantes del equipo:

David Barragán Chávez

Edgard Francisco Caballero Zúñiga

Javier Ángel Castro Rubio

Karla Maribel Zuloaga Sánchez

**Cath-Cipher**

* **Diagrama lógico de interacción de los métodos**

**Nota:** Para descifrar es el mismo proceso pero en sentido opuesto.

* **Cálculo de la difusión (mediante ejemplos)**
* Ciframos el mensaje: “holamundo” con la llave “patata” y nos regresa “mhxvzensi”
* Ciframos el mensaje: “holamunda” con la llave “patata” y nos regresa “wplvzensi”
* Ciframos el mensaje: “PeoplesaynothingisimpossiblebutIdonothingeveryday” con la llave “itsatrap” y nos regresa “udkgoordfhejicrslqnzacvmzwqqaamjwqjeycuanilxnowqphr”
* Ciframos el mensaje: “Isaynothingisimpossiblebutpeopledonothingeveryday” con la llave “itsatrap” y nos regresa “udkgoordfhejicrslrzwvnsnokxmfmtcwpxlnmyfjgvhekpeklj”
* Ciframos el mensaje: “esteesunmensajenomuylargo” con la llave “llave” y nos regresa “avahpxgzmiulyigkchfxoqjjkig”
* Ciframos el mensaje: “esteesunmensajenomuylargo” con la llave “llavo” y nos regresa “jgppbhqrdktrrpiulbmuzfesvpi”
* **Instrucciones de uso y restricciones del texto y llave**

**Uso:**

* Para usar Cat-cipher asegúrese de tener java instalado en su computadora.
* Para cifrar un texto coloque una llave en el campo “llave” coloque el mensaje a cifrar en la caja de texto “texto plano” y revise que el símbolo verde sobre las cajas tenga el mono corriendo hacia la derecha (En caso de que no se encuentre volteando hacia la derecha solo basta con presionar sobre el símbolo).
* Para descifrar coloque la misma llave que usó para cifrar el mensaje sobre el campo “llave” coloque el mensaje cifrado en la caja de texto “texto encriptado” y revise que el símbolo verde sobre las cajas tenga el mono corriendo hacia la izquierda.

**Restricciones texto y llave:**

* El programa no hace distinción entre mayúsculas y minúsculas, todos los procesos se hacen en minúsculas.
* El programa solo acepta caracteres dentro del alfabeto inglés a-z.
* No se aceptan espacios, signos de puntuación etc.
* No hay límite en la longitud de los campos tanto de texto como de llave.