

# ENCRIPTADOR

**Agüero, Santiago Alejandro**

*Universidad Tecnológica Nacional, Facultad Regional Córdoba*

## **Abstract**

*La primera versión del “Encriptador” fue presentada en la cátedra Algoritmo y Estructura de Datos como trabajo final de Investigación. Se buscó desarrollar una utilidad que permitiese a grandes rasgos resguardar información mediante algoritmos diferentes de encriptación. También se incursionó en áreas como Java Swing y Archivos Aleatorios conservando la Programación Orientada a Objetos (P.O.O). En la versión actual se resolvieron ciertos errores y se intenta generalizar su aplicación.*

## **Introducción**

Se partió de la necesidad personal de contar con un programa el cual facilitase la encriptación de texto, para compartirla de una manera segura sin preocupación alguna. Si bien existen muchas utilidades de semejante características, algunas pagas, otras no, éste, el “Encriptador” tiene la ventaja de ser “pequeño” y muy apto para el aprendizaje.

## **Elementos del Trabajo y metodología**

En primera medida se analizó cuales serían las funciones del programa. Se decidió utilizar el lenguaje de programación JAVA™, dada su flexibilidad y modularidad. Luego se procedió a buscar información en diferentes medios (Internet, revistas, libros...) sobre temas relevantes como Algoritmos de Encriptación, Java Swing, Archivos Aleatorios (Temas propiamente de la investigación llevada a cabo). Se diseñó a grandes rasgos el aspecto general del programa (las distintas clases con sus atributos y métodos, tipos de estructuras a utilizar, ya sean listas, matrices, etc.) y se empezó con el desarrollo del mismo conservando el Paradigma de Programación Orientada a Objetos. Se

utilizaron diagramas de flujo sobre todo en algoritmos con matrices (operaciones: matriz cofactores, determinante sarrus, multiplicación de matrices, inversa matriz en determinado módulo, entre otras) y de encriptación (criptosistema Hill, algoritmo “Sustitución Directa” y un algoritmo Poli alfabético)

Finalmente, se probó el programa desarrollado y se realizaron las correcciones, lo cual se sigue haciendo.

## **Resultados**

Se consiguió cumplir con el objetivo planteado, si bien quedan detalles para agregar, corregir, mejorar, su funcionalidad es la que se esperaba según lo expuesto.

## **Discusión**

Una de las posibles aplicaciones sería la encriptación de passwords y datos personales bajo una única contraseña con la posibilidad de utilizarlo en dispositivos móviles.

## **Conclusión**

El programa actualmente responde a los problemas planteados al principio, pero creemos que resulta una base para profundizar más ciertos aspectos del mismo como implementación en diferentes ámbitos.

**Agradecimientos**

A Nafria, Federico quién contribuyó en correcciones del programa y en la generalización de determinados algoritmos

**Referencias**

- [1] Java 2 (Javier Ceballos)
- [2] [www.programacion.net/cursos/swing](http://www.programacion.net/cursos/swing)
- [3] Classical Cryptography Course – “Hill Cipher” (Lanaki)
- [4] [www.textoscientificos.com/criptografia](http://www.textoscientificos.com/criptografia)
- [5] Apunte de Cátedra “Algoritmo y Estructura de Datos” (2006)

**Datos de Contacto**

Santiago Alejandro Agüero. UTN (Córdoba).  
[aguerosantiale@hotmail.com](mailto:aguerosantiale@hotmail.com)  
Federico Nafria. UTN (Córdoba)  
[federiconafria@hotmail.com](mailto:federiconafria@hotmail.com)