

# Manual de Ganzúa 1.01

Jesús Adolfo García Pasquel

4 de octubre de 2004

# Índice general

<b>1. Introducción</b>	<b>3</b>
1.1. ¿Qué es Ganzúa?	3
1.2. Listado de Características	3
<b>2. Instalación</b>	<b>5</b>
2.1. Requisitos	5
2.2. Plataformas Recomendadas	5
2.3. Instalando Ganzúa	6
2.3.1. GNU/Linux	6
2.3.2. Mac OS X (10.3 o superior)	8
2.3.3. Windows	9
2.4. Configurando Ganzúa	11
2.4.1. Archivos y Directorios de Ganzúa	11
2.4.1.1. Paquetes Binarios	11
2.4.1.2. Paquete de Código Fuente	12
2.4.2. Archivos y Directorios Indispensables	13
2.5. Acerca del Paquete de Código Fuente	14
<b>3. Cómo Usar Ganzúa</b>	<b>16</b>
3.1. Interfaz	16
3.2. Barras de Título y de Menús	19
3.2.1. Menú Archivo	19
3.2.2. Menú Edición	21
3.2.3. Menú Visualización	23
3.2.4. Menú Ventana	24
3.3. Área de Substitución	24
3.4. Panel de Estadísticas del Criptotexto	25
3.5. Área de Selección de Cifrado y Herramientas	27
3.5.1. Monoalfabéticos	27
3.5.2. Polialfabéticos	28
3.6. Ajustando el Idioma y Convenciones	30
3.7. Detalles a Considerar	31

<i>ÍNDICE GENERAL</i>	2
<b>4. Frecuencias Relativas de Lenguajes</b>	<b>32</b>
4.1. Documentos XML de Reglas para Alfabetos . . . . .	33
4.2. Usando langFreq.jar . . . . .	36
<b>5. Contribuya</b>	<b>37</b>
5.1. Traduciendo Ganzúa . . . . .	37
5.2. Notas Sobre el Código Fuente . . . . .	38

# Capítulo 1

## Introducción

### 1.1. ¿Qué es Ganzúa?

Ganzúa es una herramienta para el criptoanálisis de cifrados clásicos (monoalfabéticos y polialfabéticos) que permite al usuario definir alfabetos arbitrarios de cifrado y planos, ayudando al criptoanálisis de criptogramas obtenidos de textos en diversos idiomas.

Ganzúa es una aplicación Java internacionalizada, con interfaces en inglés y español. Dicho de otro modo, Ganzúa es un programa de computadora independiente de plataforma que puede ser adaptado a varias regiones y lenguas sin tener que hacer cambios estructurales al programa, que para esta versión ha sido adaptada para las lenguas inglesa y española. Ganzúa fue escrita para ser usada como herramienta en un curso de introducción a la criptología y provee un entorno para el criptoanálisis de textos cifrados con esquemas monoalfabéticos y polialfabéticos.

Ganzúa es software libre distribuido bajo la licencia GPL (General Public License), que da al usuario muchos más derechos que la mayoría de las licencias, incluyendo acceso al código fuente y libertad para modificarlo.

Ganzúa fue escrito en el lenguaje de programación Java con el editor de texto GNU EMACS en los sistemas operativos GNU/Linux y Mac OS X.

### 1.2. Listado de Características

- Características presentes para todos los cifrados:
  - Uso de alfabetos de cifrado y planos casi totalmente arbitrarios.
  - Obtención y visualización de las frecuencias relativas estándar de caracteres, digramas y trigramas de varias lenguas.
  - Obtención y visualización del índice de coincidencias de criptogramas y lenguas.

- Estimado del número de alfabetos usados para obtener el criptograma, basado en el índice de coincidencias del criptograma y el de la lengua.
  - Substitución inyectiva de caracteres
  - Capacidad de guardar y cargar proyectos de criptoanálisis
- Características presentes para los cifrados monoalfabéticos:
    - Herramientas para manipular la substitución de caracteres a nivel alfabeto. Útiles en el cifrado de César y otros cifrados monoalfabéticos.
    - Obtención y visualización de las frecuencias relativas de caracteres, digramas y trigramas del criptograma.
  - Características presentes para los cifrados polialfabéticos:
    - Herramientas para manipular la substitución de caracteres a nivel alfabeto. Útiles en los cifrados de Vigenère o Alberti.
    - Obtención y visualización de las frecuencias relativas de los caracteres cifrados con cada alfabeto.
    - Realiza la prueba de Kasiski al criptograma.

# Capítulo 2

## Instalación

### 2.1. Requisitos

Para usar Ganzúa necesitará una implementación completa de la edición estándar del entorno de tiempo de ejecución de Java 2 (o JRE por sus siglas en inglés<sup>1</sup>) versión 1.4 o superior, que cuente con una implementación de las interfaces para procesamiento de XML de Java (o JAXP por sus siglas en inglés<sup>2</sup>) versión 1.2 o superior.

### 2.2. Plataformas Recomendadas

Dado que Ganzúa es una aplicación Java, es independiente-de-plataforma. Debe correr sin ningún problema en cualquier plataforma con una implementación completa del JRE versión 1.4 o superior con una implementación de JAXP versión 1.2 o superior.

Ganzúa ha sido ejecutada satisfactoriamente en las siguientes plataformas:

- GNU/Linux, usando la implementación de Sun Microsystems de la edición estándar de la plataforma Java 2 (J2SE) 5.0 JRE.
- GNU/Linux, usando la implementación de Sun Microsystems del JRE versión 1.4.2 y Xerces2 Java Parser versión 2.6 para la implementación de JAXP 1.2.
- Mac OS X 10.3 Panther, usando la implementación de Apple del JRE versión 1.4.1 (incluida en Mac OS X 10.3) y Xerces2 Java Parser versión 2.6 para la implementación de JAXP 1.2.
- Windows 98/ME/XP usando la implementación de Sun Microsystems de J2SE 5.0 JRE.

---

<sup>1</sup>Java 2 Runtime Environment, Standard Edition

<sup>2</sup>Java API for XML Processing

- Windows 98/ME/XP usando la implementación de Sun Microsystems del JRE versión 1.4.2 y Xerces2 Java Parser versión 2.6 para la implementación de JAXP 1.2.

Si logra ejecutar Ganzúa en alguna otra plataforma, por favor contácteme (vea el capítulo 5), para que pueda añadirla al listado.

## 2.3. Instalando Ganzúa

Esta sección indica cómo instalar Ganzúa en las distintas plataformas en las que ha sido ejecutado satisfactoriamente. No es necesario que lea todas las secciones, basta con que consulte la que trata sobre la plataforma que quiere usar.

### 2.3.1. GNU/Linux

#### Preparando la Instalación

Para ejecutar Ganzúa, necesitará una implementación completa de la edición estándar del entorno de tiempo de ejecución de Java 2 (JRE) versión 1.4 o superior. Si no tiene una instalada en su sistema, tendrá que conseguir una de las implementaciones para GNU/Linux. La que se usó para probar Ganzúa, fue la de Sun Microsystems, que puede encontrarse en <http://java.sun.com>, pero podría usar la de IBM (<http://www.ibm.com>), la de Blackdown (<http://www.blackdown.org>) o alguna otra. De ser posible, instale un JRE para la versión 5.0 o superior de la edición estándar de la plataforma Java 2 (J2SE), así podrá evitar actualizar el JAXP que se incluye con su JRE.

#### Instalando Ganzúa

Una vez que tiene instalada una implementación del JRE versión 1.4 o superior, siga los siguientes pasos para instalar Ganzúa:

1. Descargue el paquete binario del sitio de Ganzúa: <http://ganzua.sourceforge.net>
2. Expanda el paquete y ponga los archivos extraídos donde usted quiera que Ganzúa quede instalado. Asegúrese de que la ruta al directorio de instalación no contenga directorios cuyos nombres incluyan caracteres fuera del alfabeto inglés o 0-9 (por ejemplo: caracteres acentuados o ñ), de lo contrario el programa puede funcionar de manera incorrecta.

Ahora debe poder ejecutar Ganzúa usando el comando `java -jar ganzua.jar` desde el directorio en el que instaló el programa.

### Pruebe su Instalación

Ejecute Ganzúa y seleccione la opción Abrir del menú Archivo. Ahora elija un proyecto de criptoanálisis de entre los que se incluyen como ejemplo en `GANZÚA/examples/projects/es` donde `GANZÚA` representa al directorio en el que instaló el programa.

Si logró abrir el proyecto sin ningún problema, felicidades, puede saltarse el resto de este capítulo. Si, por el contrario, apareció un mensaje de error indicando que debe actualizar su versión de JAXP, salga del programa y lea la siguiente sección, que le indicará cómo hacerlo.

### Actualizando su Versión de JAXP

Si su implementación del JRE no incluye una implementación de las interfaces para procesamiento de XML de Java (JAXP) versión 1.2 o superior, tendrá que instalar una. Xerces2 Java Parser (versión 2.6 o superior) provee tal implementación. Para instalarlo haga lo siguiente:

1. Descargue la aplicación `findEndorsedDirs.jar` de <http://ganzua.sourceforge.net>. Este JAR ejecutable le indicará cuáles son los directorios de estándares respaldados de Java (donde puede colocar la implementación de JAXP) en su JRE.
2. Descargue la versión más reciente de Xerces2 Java Parser de <http://xml.apache.org/xerces2-j/>
3. Extraiga los archivos del paquete comprimido
4. Ejecute `findEndorsedDirs` con el comando  
`java -jar findEndorsedDirs.jar`
5. Copie todos los archivos JAR (aquellos que terminan en `.jar`) del paquete de Xerces2 a cualquiera de los directorios listados por `findEndorsedDirs`. Si el directorio no existe, créelo.
6. Salga de cualquier Ganzúa que tenga en ejecución.
7. Vuelva a hacer la prueba de la sección anterior para confirmar que ha actualizado la versión de JAXP.

No necesitará `findEndorsedDirs.jar` ni el paquete de Xerces2 en adelante, así que puede borrarlos.

Si tiene algún problema, contácteme (ver capítulo 5) para poder darle solución en versiones futuras de la documentación de Ganzúa.



### 2.3.2. Mac OS X (10.3 o superior)

#### Preparando la Instalación

Mac OS X 10.3 (o superior) incluye la implementación de Apple del JRE versión 1.4.1 (o superior), pero descargar cualquier actualización disponible para la plataforma Java con Actualización de Software puede mejorar el rendimiento de Ganzúa y hacer la instalación más fácil. Para ejecutar Actualización de Software seleccione esa opción del menú Apple o elija Preferencias del Sistema, después Actualización de Software del menú Visualización y ahora pulse el botón Buscar.

#### Instalando Ganzúa

Ahora está listo para instalar Ganzúa. Para ello siga los siguientes pasos:

1. Descargue el paquete para Mac OS X del sitio de Ganzúa: <http://ganzua.sourceforge.net>
2. Abra el paquete y arrastre el directorio que contiene a Ganzúa y otros archivos y directorios (carpetas) al lugar donde quiera que quede instalado. De preferencia póngalo dentro de la carpeta *Aplicaciones*, pues de lo contrario el programa puede funcionar de manera inadecuada. Algunos de los archivos y directorios en la carpeta de Ganzúa son importantes para el funcionamiento del programa y no debe moverlos o borrarlos del directorio de instalación. Esto se explica con mayor detalle en la sección 2.4.

Eso es todo. Ahora puede ejecutar Ganzúa haciendo doble clic en su icono.

#### Pruebe su Instalación

Ejecute Ganzúa y seleccione Abrir en el menú Archivo. Ahora elija uno de los proyectos de criptoanálisis que se incluyen como ejemplo en el directorio `GANZÚA/examples/projects/es` donde `GANZÚA` representa al directorio donde instaló el programa.

Si logró abrir el proyecto satisfactoriamente, felicidades, puede saltarse el resto de este capítulo. Si, por el contrario, apareció un mensaje de error indicando que debe actualizar su versión de JAXP, salga del programa y lea la siguiente sección, que le indicará cómo hacerlo.

#### Actualizando su Versión de JAXP

Si el JRE no incluye una implementación de las interfaces para procesamiento de XML de Java (JAXP) versión 1.2 o superior, tendrá que instalar una, como Xerces2 Java Parser (versión 2.6 o superior). Para instalarlo haga lo siguiente:

Descargue la aplicación `findEndorsedDirs.jar` de <http://ganzua.sourceforge.net>. Este JAR ejecutable le indicará cuales son los directorios de estándares respaldados de Java (donde puede colocar la implementación de JAXP) en su implementación del JRE.

1. Descargue la aplicación `findEndorsedDirs.jar` de <http://ganzua.sourceforge.net>. Este JAR ejecutable le indicará cuáles son los directorios de estándares respaldados de Java (donde puede colocar la implementación de JAXP) en su implementación del JRE.
2. Descargue la versión más reciente de Xerces2 Java Parser de <http://xml.apache.org/xerces2-j/>
3. Extraiga los archivos del paquete comprimido.
4. Ejecute `findEndorsedDirs` haciendo doble clic en el archivo `findEndorsedDirs.jar`
5. Copie todos los archivos JAR (aquellos que terminan en `.jar`) del paquete de Xerces2 a cualquiera de los directorios listados por `findEndorsedDirs`. Si el directorio no existe, créelo.  
Note que los nombres de los directorios que muestra `findEndorsedDirs.jar` están en inglés, así que el directorio `System` en su computadora puede llamarse `Sistema`, o `Libraries` llamarse `Librería`.
6. Salga de cualquier Ganzúa que tenga en ejecución.
7. Vuelva a hacer la prueba de la sección anterior para confirmar que ha actualizado la versión de JAXP.

No necesitará `findEndorsedDirs.jar` ni el paquete de Xerces2 en adelante, así que puede borrarlos.

Si tiene algún problema, contácteme (ver capítulo 5) para poder indicar la solución en versiones futuras de la documentación de Ganzúa.

### 2.3.3. Windows

#### Preparando la Instalación

Para ejecutar Ganzúa, necesitará una implementación completa de la edición estándar del entorno de tiempo de ejecución de Java 2 (JRE) versión 1.4 o superior. Si no tiene una instalada en su sistema, o sólo tiene un programa llamado Microsoft Java Virtual Machine (que **no** es una implementación del JRE), tendrá que conseguir una de las implementaciones para Windows. La que se usó para probar Ganzúa, fue la de Sun Microsystems, que puede encontrarse en <http://java.sun.com>, pero podría usar la de IBM (<http://www.ibm.com>), o alguna otra. De ser posible, instale un JRE para la versión 5.0 o superior de la edición estándar de la plataforma Java 2 (J2SE), así podrá evitar actualizar el JAXP que se incluye con su JRE.

#### Instalando Ganzúa

Una vez que tiene instalada una implementación del JRE versión 1.4 o superior, siga los siguientes pasos para instalar Ganzúa:

1. Descargue el paquete binario del sitio de Ganzúa: <http://ganzua.sourceforge.net>
2. Expanda el paquete y ponga los archivos extraídos donde quiera que Ganzúa quede instalado. Asegúrese de que la ruta al directorio de instalación no contenga directorios cuyos nombres incluyan caracteres fuera del alfabeto inglés o 0-9 (por ejemplo: caracteres acentuados o ñ), de lo contrario el programa puede funcionar de manera incorrecta. Algunos de los archivos y directorios en la carpeta de Ganzúa son importantes para el funcionamiento del programa y no debe moverlos o borrarlos del directorio de instalación. Esto se explica con mayor detalle en la sección 2.4.

Ahora debe poder ejecutar Ganzúa haciendo doble clic en **ganzua.jar** o usando el comando `java -jar ganzua.jar` desde el directorio en que instaló el programa.

### Pruebe su Instalación

Ejecute Ganzúa y seleccione la opción Abrir del menú Archivo. Ahora elija un proyecto de criptoanálisis de entre los que se incluyen como ejemplo con Ganzúa en **GANZÚA/examples/projects/es** donde **GANZÚA** representa al directorio donde instaló el programa.

Si logró abrir el proyecto sin ningún problema, felicidades, puede saltarse el resto de este capítulo. Si, por el contrario, apareció un mensaje de error indicando que debe actualizar su versión de JAXP, salga del programa y lea la siguiente sección, que le indicará cómo hacerlo.

### Actualizando su Versión de JAXP

Si el JRE no incluye una implementación de las interfaces para procesamiento de XML de Java (JAXP) versión 1.2 o superior, tendrá que instalar una, como Xerces2 Java Parser (versión 2.6 o superior). Para instalarlo haga lo siguiente:

1. Descargue la aplicación **findEndorsedDirs.jar** de <http://ganzua.sourceforge.net>. Este JAR ejecutable le indicará cuáles son los directorios de estándares respaldados de Java (donde puede colocar la implementación de JAXP) en su implementación del JRE.
2. Descargue la versión más reciente de Xerces2 Java Parser de <http://xml.apache.org/xerces2-j/>
3. Extraiga los archivos del paquete comprimido.
4. Ejecute **findEndorsedDirs** haciendo doble clic en el archivo **findEndorsedDirs.jar** o con el comando `java -jar findEndorsedDirs.jar`

5. Copie todos los archivos JAR (aquellos que terminan en .jar) del paquete de Xerces2 a cualquiera de los directorios listados por findEndorsedDirs. Si el directorio no existe, créelo.
6. Salga de cualquier Ganzúa que tenga en ejecución.
7. Vuelva a hacer la prueba de la sección anterior para confirmar que ha actualizado la versión de JAXP.

No necesitará findEndorsedDirs.jar ni el paquete de Xerces2 en adelante, así que puede borrarlos.

## 2.4. Configurando Ganzúa

Esta sección explica cómo están organizados los archivos de Ganzúa, qué contienen y cómo cambiar su configuración.

### 2.4.1. Archivos y Directorios de Ganzúa

#### 2.4.1.1. Paquetes Binarios

Si descargó un paquete binario, debe de contar con los siguientes archivos y directorios (carpetas). En el caso del paquete para Mac OS X, debe haber una aplicación en lugar de `ganzua.jar`.

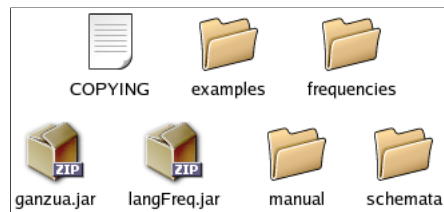


Figura 2.1: Contenido del paquete binario

**COPYING** Archivo con la licencia de Ganzúa (GPL).

**ganzua.jar** el JAR ejecutable que contiene a Ganzúa.

En Mac OS X este archivo se encuentra dentro de la aplicación, y se puede acceder a él seleccionando **Mostrar contenido del paquete** en el menú contextual que aparece al hacer Control-clic en el icono de la aplicación dentro de Finder.

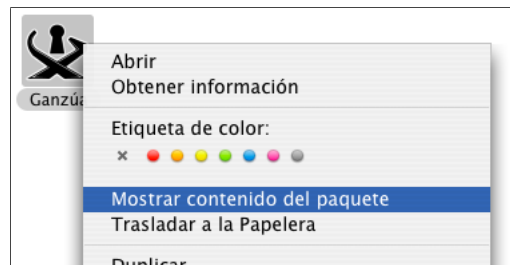


Figura 2.2: ganzua.jar está dentro del paquete de la aplicación en Mac OS X

**langFreq.jar** JAR ejecutable del programa para obtener las frecuencias relativas estándar de caracteres, digramas y trigramas de lenguajes.

**schemata** directorio que contiene esquemas para XML (escritos en el lenguaje para definición de esquemas del W3C) usados para verificar que los archivos XML usados por Ganzúa (con frecuencias relativas estándar de lenguajes, proyectos de criptoanálisis, etc.) estén bien formados.

**frecuencias** directorio con archivos de frecuencias relativas de lenguajes. Este es el directorio en el que Ganzúa busca las frecuencias relativas de lenguajes por omisión.

**examples** directorio con ejemplos.

**manual** directorio donde puede encontrar este manual en formato PDF y la lista de cambios al programa a partir de las versiones previas.

#### 2.4.1.2. Paquete de Código Fuente

Si descargó el paquete de código fuente, debe tener los siguientes archivos y directorios:

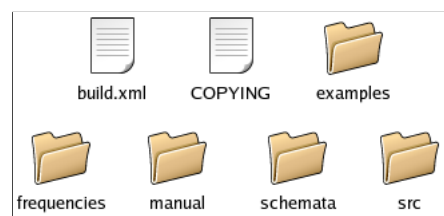


Figura 2.3: Contenido del paquete de código fuente

**COPYING** Archivo con la licencia de Ganzúa (GPL).

**build.xml** un archivo usado para compilar Ganzúa con la herramienta Apache Ant.

**src** directorio con el código fuente de Ganzúa.

**schemata** directorio que contiene esquemas para XML (escritos en el lenguaje para definición de esquemas del W3C) usados para verificar que los archivos XML usados por Ganzúa (con frecuencias relativas estándar de lenguajes, proyectos de criptoanálisis, etc.) estén bien formados. Igual que en el paquete binario.

**frecuencias** directorio con archivos de frecuencias relativas de lenguajes. Este es el directorio en el que Ganzúa busca las frecuencias relativas de lenguajes por omisión. Igual que en el paquete binario.

**examples** directorio con ejemplos. Igual que en el paquete binario.

**manual** directorio donde puede encontrar este manual en formato PDF y la lista de cambios al programa a partir de las versiones previas..

### 2.4.2. Archivos y Directorios Indispensables

Para usar Ganzúa necesita los archivos ganzua.jar, langFreq.jar, los esquemas y las frecuencias de lenguajes. Puede prescindir del resto de los archivos y directorios.

Ganzúa hace uso extensivo de archivos XML (eXtensible Markup Language). Éstos son usados para guardar proyectos, frecuencias de lenguajes y dar instrucciones a la aplicación langFreq.jar. Los archivos XML son similares a los de HTML en que ambos son archivos de texto con etiquetas. Ganzúa verifica la estructura de estos archivos usando esquemas de XML (que a su vez son archivos XML) escritos en el lenguaje para definición de esquemas del W3C. De esta manera, Ganzúa le permite acceder a los datos que ha creado y hacer documentos compatibles con Ganzúa en cualquier editor de texto, y si tiene un editor de XML capaz de usar esquemas de XML, puede verificar su validez mientras los escribe.

Puede renombrar o mover los directorios con los esquemas y frecuencias relativas (**schemata** y **frecuencias**) si gusta, pero tendrá que notificar al programa sobre los cambios editando un par de archivos de configuración.

#### Moviendo los Directorios con Esquemas y Frecuencias Relativas

Si quiere mover o renombrar el directorio con los esquemas de XML y/o el de frecuencias relativas de lenguajes tendrá que cerrar toda Ganzúa en ejecución y editar dos archivos de configuración para notificar al programa sobre los cambios.

Los archivos de configuración están dentro de los archivos JAR, uno dentro de ganzua.jar y el otro dentro de langFreq.jar. Ambos se llaman config.properties y tienen la misma estructura. Para editarlos, hágalo de la misma manera en que editaría archivos de texto dentro de un paquete ZIP (los archivos JAR pueden ser manipulados como archivos ZIP). Si sabe cómo utilizar el editor EMACS, puede abrir los archivos JAR y editar los archivos config.properties directamente.

Si cambia el nombre del directorio con los esquemas o lo mueve, tendrá que cambiar la línea

```
#schemataDir = /usr/local/share/ganzua/schemata/
```

Borre el carácter # al inicio de la línea y cambie el valor después del carácter = por el nombre completo (trayectoria absoluta) del directorio donde puso los esquemas.

Si cambia el nombre del directorio con las frecuencias relativas de lenguajes o lo mueve, tendrá que cambiar la línea

```
#langFreqDir = /usr/local/share/ganzua/frequencies/
```

Borre el carácter # al inicio de la línea y cambie el valor después del carácter = por el nombre completo (trayectoria absoluta) del directorio donde puso las frecuencias relativas.

Recuerde que esto debe hacerse en ambos archivos JAR.

## 2.5. Acerca del Paquete de Código Fuente

Dado que Ganzúa es software libre, el código fuente está disponible en el sitio de Ganzúa (<http://ganzua.sourceforge.net>) para que lo pueda descargar, modificar, distribuir, etc. como se especifica en la licencia GPL.

Para compilar el código fuente, necesitará un compilador para el lenguaje de programación Java versión 1.4 o superior y la herramienta Apache Ant (<http://ant.apache.org>) versión 1.5 o superior.

Durante el desarrollo de Ganzúa versión 1.01 se usaron los siguientes compiladores:

- El que se incluye con el Java 2 SDK, Standard Edition versión 1.4.2 para Linux de Sun Microsystems.
- El que se incluye con la implementación de Apple de la plataforma Java 2, Standard Edition versión 1.4.1 para Mac OS X.

Hay dos archivos con instrucciones para la herramienta Apache Ant en el paquete de código fuente de Ganzúa. El primero está en el directorio raíz del paquete y puede usarse para generar los JARs ejecutables y la documentación. El segundo se encuentra en el directorio `src` y compila el programa dejándolo en la estructura del código fuente (no lo pone en un JAR). Para más información sobre estos archivos use el comando `ant -projecthelp` en los directorios en que se encuentran.

Si quiere ejecutar Ganzúa fuera de un paquete JAR, tendrá que editar el archivo `config.properties` del directorio `src/net/sourceforge/ganzua`, como se explica en la sección 2.4.2, aún si no movió o renombró los directorios de esquemas o frecuencias relativas. Una vez que haya editado el archivo, use el siguiente comando dentro del directorio `src` para ejecutar Ganzúa:

```
java net.sourceforge.ganzua.Analyzer
```

Analyzer es el nombre de la clase que contiene el programa principal de Ganzúa.

Si desea ejecutar el programa para generar las frecuencias relativas de lenguajes use el comando:

```
java net.sourceforge.ganzua.LangFreq
```



## Capítulo 3

# Cómo Usar Ganzúa

Este capítulo describe la interfaz de Ganzúa, cómo está dividida y explica cómo usar las diferentes funciones del programa.

Para que pueda familiarizarse con el programa y entender mejor cómo funciona, se le sugiere que lo abra y pruebe las distintas funciones mientras se describen.

### 3.1. Interfaz

Las siguientes imágenes muestran cómo se ve<sup>1</sup> la ventana principal de Ganzúa en las plataformas en que se ha ejecutado satisfactoriamente (ver sección 2.2).

Las etiquetas en las imágenes representan:

1. Barra de título
2. Barra de menús
3. Lengüetas para el panel principal y las estadísticas del criptograma
4. Área de selección de cifrado
5. Área de herramientas para el cifrado
6. Área de substitución
7. Área de texto plano y cifrado.

---

<sup>1</sup>La apariencia del programa puede variar, dependiendo del valor por omisión que tenga el JRE para el Look And Feel.

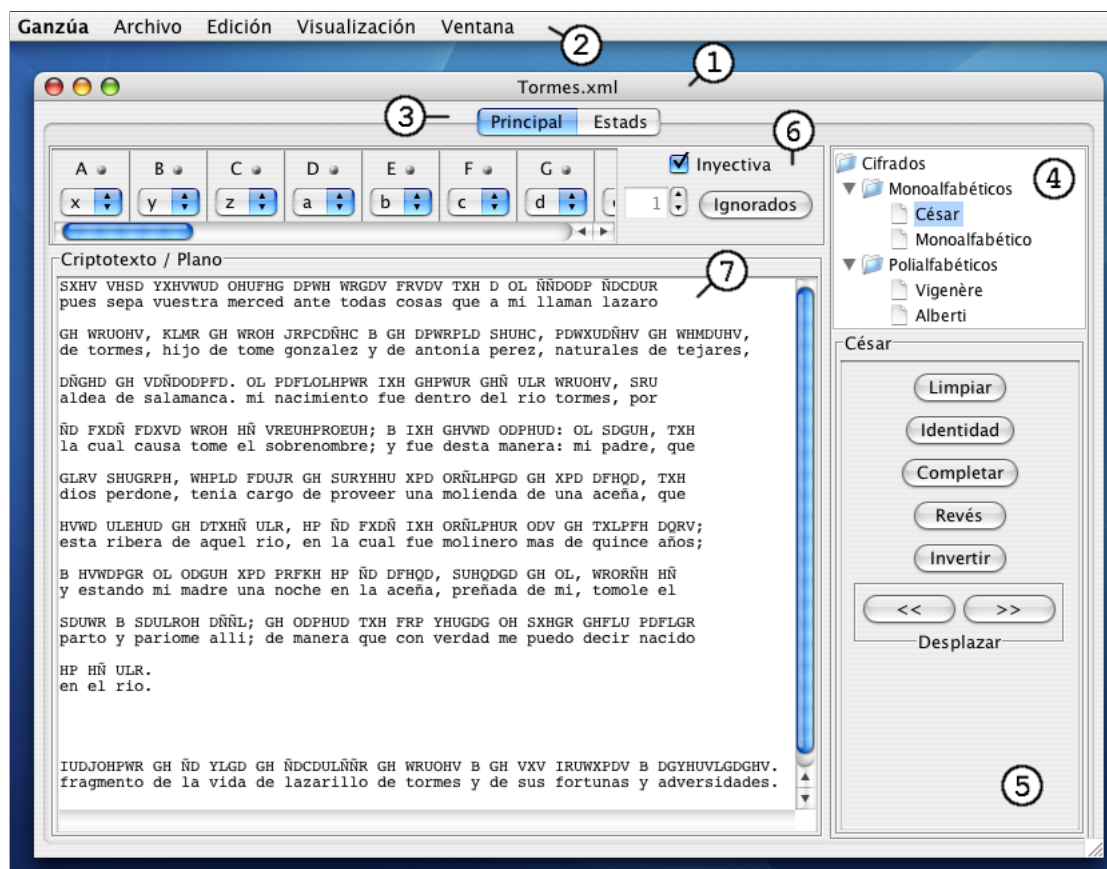


Figura 3.1: Ganzúa en Mac OS X

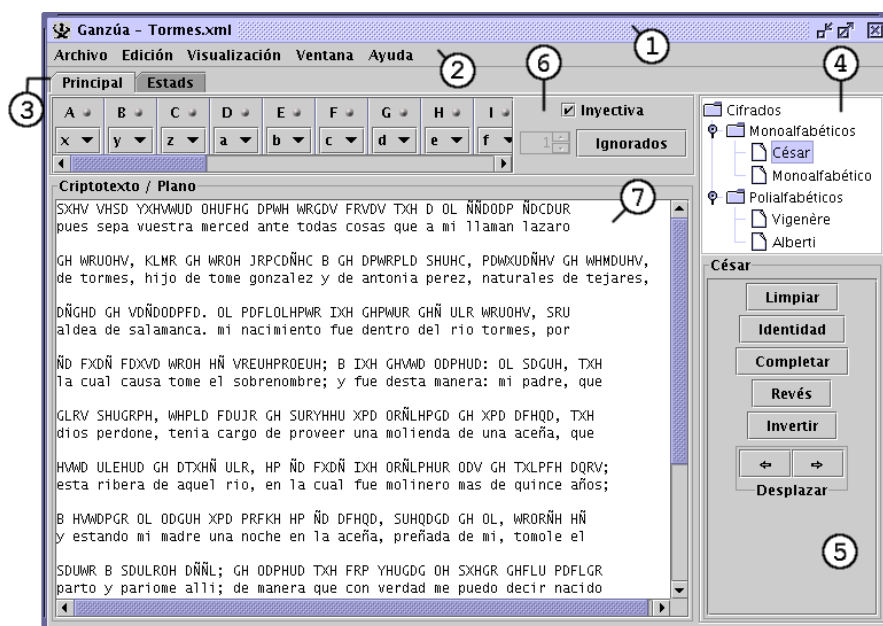


Figura 3.2: Ganzúa en GNU/Linux usando la apariencia de Java (Metal)

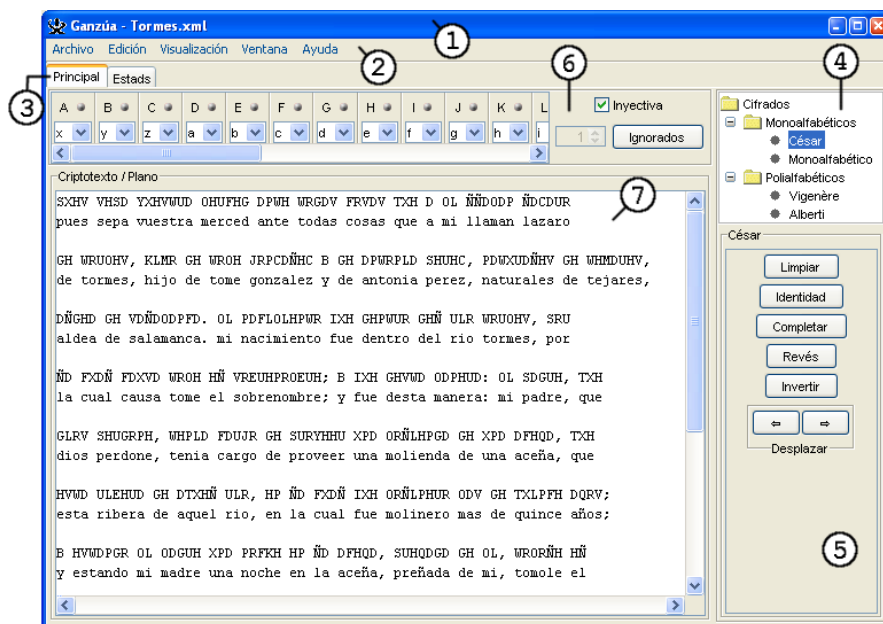


Figura 3.3: Ganzúa en Windows XP usando la apariencia de Windows

## 3.2. Barras de Título y de Menús

La barra de título muestra el nombre del archivo en el que se encuentra el proyecto de criptoanálisis actual. Si no ha guardado el proyecto, entonces se muestra **Sin título**.

La barra de menús muestra cinco menús, que no son los mismos para todas las plataformas. El menú Ganzúa (disponible sólo en Mac OS X) contiene opciones relacionadas con el programa, como *Acerca de*, que muestra información sobre la versión de Ganzúa que está usando. En el resto de las plataformas, *Acerca de* se encuentra en el menú Ayuda y es la única opción de ese menú. Esta es la razón por la que Ganzúa no contiene un menú Ayuda en Mac OS X. Dado que prácticamente cada plataforma maneja los documentos de ayuda de una manera diferente y Ganzúa no fue hecho para una plataforma en particular, sino para ser independiente de éstas; los documentos de ayuda como este manual están disponibles en formatos estándar como HTML y PDF que puede leer en la plataforma que guste. La única ayuda que puede encontrar dentro del programa son etiquetas con descripciones de la sección que está apuntando con el cursor, las cuales aparecen cuando deja el cursor inmóvil sobre la sección de interés por unos segundos.

La siguiente sección explica las opciones de los menús que aparecen en todas las plataformas.

### 3.2.1. Menú Archivo

#### Abrir

Le permite abrir proyectos de criptoanálisis. Usó esta opción en la sección 2.3, cuando probó la instalación de Ganzúa.

**Intente:** Abra el archivo `Tormes.xml`, que se encuentra en `GANZÚA/examples/projects/es` donde `GANZÚA` representa al directorio donde instaló el programa.

#### Abrir criptotexto

Le permite abrir criptogramas de archivos de texto. Cuando selecciona esta opción aparece una ventana de diálogo donde puede seleccionar el archivo de texto y su codificación. La codificación define un conjunto de caracteres y la relación entre el conjunto de caracteres y su representación en el archivo. Si no conoce qué codificación está usando en sus archivos de texto, probablemente sea la que su sistema elige por omisión. Esta codificación es seleccionada automáticamente cada vez que abre Ganzúa. Si cambia la codificación seleccionada en esta ventana de diálogo, ese cambio será reflejado en el resto de las ventanas de diálogo relacionadas con archivos de texto (aquellas usadas por *Guardar criptotexto* y *Guardar texto plano*) y permanecerá hasta que salga de Ganzúa o seleccione otra codificación.

**Intente:** Abra un archivo de texto como la licencia de Ganzúa, que es el archivo llamado `COPYING` en el directorio donde instaló Ganzúa. Si tenía

abierto el proyecto `Tormes.xml`, note cómo cambia el contenido del área de sustitución y la barra de título.

**IMPORTANTE:** Ganzúa se escribió para ser usado como herramienta en un curso de introducción a la criptología y no está hecho para manejar documentos de más de un par de páginas.

### Abrir idioma

Le permite abrir un archivo con las frecuencias relativas estándar de caracteres, digramas y trigramas de un lenguaje. Estos archivos por lo general se encuentran en el directorio `frecuencias` de Ganzúa (ver sección 2.4.1). Por convención las primeras dos letras de los nombres de los archivos de frecuencias son el código ISO 639 de la lengua a la que pertenecen.

Cuando abre un idioma, define el alfabeto plano a usar, la manera en que se ordenan los caracteres (incluyendo los del alfabeto de cifrado) y los datos a mostrar en la ventana de Frecuencias Relativas del Idioma (ver sección 3.2.4).

**IMPORTANTE:** Cuando abre un idioma, el alfabeto plano anterior es descartado, al igual que toda sustitución seleccionada.

**IMPORTANTE:** Cuando abre un criptograma, los datos sobre la lengua que estaba usando hasta antes de abrirlo permanecen hasta que abra una nueva lengua o algún proyecto de criptoanálisis.

### Guardar

Le permite guardar el proyecto de criptoanálisis sobre el que está trabajando en un archivo similar al de `Tormes.xml` mencionado previamente en esta sección. Si el proyecto ha sido guardado en un archivo previamente se actualizan los datos de dicho archivo.

Los datos guardados incluyen el cifrado seleccionado, los datos del idioma (incluyendo las frecuencias de caracteres, digramas y trigramas), la sustitución y el criptotexto.

### Guardar como...

Le permite guardar el proyecto actual en un archivo nuevo.

### Guardar criptotexto

Con esta opción puede guardar el criptotexto de su proyecto en un archivo de texto. Cuando elige esta opción aparece una ventana de diálogo similar al que se muestra al seleccionar *Abrir criptograma*. Desde ésta puede escoger la codificación del archivo y si la cambia, su decisión se reflejará en las ventanas de diálogo relacionadas con archivos de texto (aquellas usadas por *Abrir criptograma* y *Guardar texto plano*).

### Guardar texto plano

Le permite guardar el texto plano del proyecto (el texto que resulta de aplicar la substitución al criptograma) en un archivo. Como con *Abrir criptograma* y *Guardar criptograma*, puede seleccionar la codificación del archivo en la ventana de diálogo y los cambios también se verán reflejados en las las ventanas de esas opciones.

### 3.2.2. Menú Edición

#### Copiar

Copia el texto seleccionado del área de texto plano y cifrado. Si desea copiar selecciones de otros lugares, como las tablas con frecuencias relativas de la ventana de estadísticas del idioma, use el atajo que se muestra junto a esta opción (por ejemplo, Comando-C en Mac OS X) después de hacer la selección. También puede arrastrar su selección y soltarla donde desee pegarla. Note que algunos programas no soportan operaciones de arrastrar-soltar.

#### Añadir caracteres al alfabeto de cifrado

Cuando abre un criptograma desde un archivo de texto (ver sección 3.2.1) el alfabeto de cifrado a usar se obtiene a partir de los caracteres que aparecen en el criptotexto. La mayoría de las veces, los criptogramas no contienen apariciones de todos los caracteres que desea tener en el alfabeto de cifrado. Por ejemplo, si el carácter K no aparece en el archivo de texto, el alfabeto de cifrado generado al abrir dicho archivo, no lo contendrá.

**IMPORTANTE:** Ganzúa considera los siguientes caracteres como especiales y no pueden ser usados en los alfabetos de cifrado o plano: caracteres de espacio, retorno de carro, fin de línea o caracteres de control.

Para incluir los caracteres faltantes en el alfabeto de cifrado, insértelos uno a la vez<sup>2</sup> en la ventana de diálogo que se muestra cuando selecció esta opción (figura 3.4). El botón Cancelar cierra la ventana y cancela la inserción del carácter que se muestre en el área de texto al momento de pulsar.

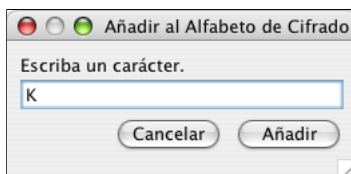


Figura 3.4: Ventana de diálogo de *Añadir caracteres al alfabeto de cifrado*

---

<sup>2</sup>Escriba el carácter y pulse la tecla de retorno o el botón Añadir

**Intente:** Si abre el proyecto `Tormes.xml` y hace clic en la lengüeta de estadísticas, podrá ver que los caracteres A, N y Z no aparecen en el criptograma y se añadieron al alfabeto de cifrado usando este comando. Haga clic en la lengüeta del panel principal y añada algunas letras minúsculas al alfabeto de cifrado.

### Añadir caracteres al alfabeto plano

Si no encuentra el alfabeto plano que desea usar entre los archivos de frecuencias relativas de idiomas incluidos con Ganzúa o le faltan algunos caracteres, puede añadirlos con esta opción. Note que esto es únicamente para propósitos de la substitución y no obtendrá los demás beneficios como las frecuencias relativas de esos caracteres. En el capítulo 4 se explica cómo hacer sus propios archivos de frecuencias relativas de lenguajes.

Para incluir los caracteres faltantes, insérteles uno a la vez, como haría al agregarlos al alfabeto de cifrado.

### Eliminar caracteres del alfabeto de cifrado

Esta opción le permite eliminar caracteres del alfabeto de cifrado y el criptograma. Cuando selecciona esta opción, se muestra una ventana con un listado de todos los caracteres en el alfabeto de cifrado. Una vez que haya seleccionado<sup>3</sup> los que desea quitar, pulse el botón Eliminar. Esto quitará del alfabeto de cifrado todos los caracteres seleccionados y borrará todas sus apariciones en el criptograma.

**IMPORTANTE:** Ganzúa no incluye un comando para revertir cambios, así que tenga cuidado cuando realice operaciones como eliminar caracteres y guarde su trabajo frecuentemente.

**Intente:** Abra el proyecto `Tormes.xml` y elimine los caracteres de puntuación.

### Agrupar caracteres del criptotexto

Le permite agrupar los caracteres del criptograma en bloques separados por un espacio. Esta es una de las razones por las que los caracteres de espacio se consideran especiales y no pueden formar parte del alfabeto de cifrado. Si fueran parte del alfabeto de cifrado, esta operación alteraría el criptograma.

**Intente:** Agrupe los caracteres del proyecto `Tormes.xml`

### Criptotexto en mayúsculas

Convierte todos los caracteres del criptograma a mayúsculas. Esta operación es equivalente a abrir un nuevo criptograma con el mismo texto que el

---

<sup>3</sup>Para seleccionar más de un carácter, use las teclas convencionales para su plataforma. Por ejemplo Control-clic en GNU/Linux.

actual, pero en mayúsculas. Esto implica que perderá toda la información sobre la substitución, incluyendo los caracteres que haya añadido al alfabeto de cifrado. Si el criptotexto del proyecto actual ya está compuesto exclusivamente por mayúsculas (como en `Tormes.xml`), entonces el proyecto no sufrirá cambios.

### Criptotexto en minúsculas

Convierte todos los caracteres del criptograma a minúsculas. Como *Criptotexto en mayúsculas*, esta operación es equivalente a abrir un nuevo criptograma con el mismo texto que el actual pero en mayúsculas, por lo que perderá toda la información sobre la substitución. Si el criptotexto del proyecto actual ya está compuesto exclusivamente por minúsculas, entonces el proyecto no sufrirá cambios.

### Asignar texto plano como criptotexto

Hace que el texto plano del proyecto actual se convierta en el criptotexto. Esta operación es equivalente a abrir un criptograma que contenga el texto plano de este proyecto. Como en los casos de *Criptotexto en mayúsculas* y *Criptotexto en minúsculas*, perderá toda la información sobre la substitución.

Esta operación puede ser útil si está usando Ganzúa para cifrar en lugar de hacer criptoanálisis.

**Intente:** Abra el proyecto `Tormes.xml` y use esta operación.

### 3.2.3. Menú Visualización

Este menú contiene opciones que le permiten cambiar la manera en que el área de texto plano y cifrado muestra su contenido. También puede acceder a estas opciones desde el menú contextual que puede activar en esta área (por ejemplo, con un Control-clic en Mac OS X o un clic con el botón derecho del ratón en otras plataformas)

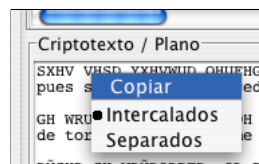


Figura 3.5: Área de texto plano y cifrado

#### Intercalados

En este modo, las líneas de texto plano se muestran debajo de las correspondientes líneas cifradas.



### Separados

En este modo, el criptotexto y el texto plano se muestran en áreas separadas.

### 3.2.4. Menú Ventana

Este menú le permite abrir las ventanas secundarias de Ganzúa.

#### Mostrar Estadísticas del idioma

Abre la ventana de estadísticas del idioma, que contiene tablas con las frecuencias relativas estándar de caracteres, digramas y trigramas; las cuales corresponden a las del último archivo que se haya abierto para el proyecto actual.

Los datos presentados en las tablas pueden ser ordenados alfabéticamente o por frecuencia haciendo clic en los encabezados de las columnas. Por ejemplo, si está viendo la tabla de frecuencias relativas de caracteres y hace clic en la etiqueta de la columna que contiene a los caracteres, la tabla se ordenará alfabéticamente y si hace clic en la etiqueta de la columna de frecuencias, la tabla será ordenada por frecuencia de mayor a menor. También puede ordenar los datos en orden inverso si hace clic mientras presiona la tecla de mayúsculas.

**Intente:** Abra el proyecto `Tormes.xml` y ordene las distintas tablas de frecuencias relativas del lenguaje.

#### Mostrar caracteres ignorados

Abre la ventana de caracteres ignorados, que contiene un listado de los caracteres del alfabeto de cifrado que están siendo ignorados. Cómo hacer que un carácter sea ignorado y lo que esto significa se explica en la sección 3.3.

## 3.3. Área de Substitución

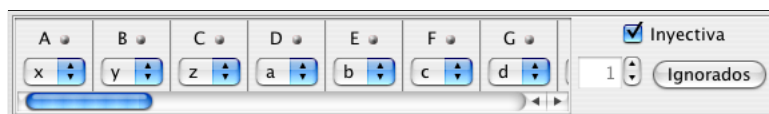


Figura 3.6: Área de substitución

El área de substitución es la sección que muestra la relación entre los caracteres del alfabeto de cifrado y los del alfabeto plano. Contiene una región con controles para la substitución de caracteres, una casilla que controla que sea uno-a-uno (inyectiva), un botón que abre la ventana de caracteres ignorados y un control para elegir la substitución a mostrar dado el número del alfabeto al que corresponde (habilitado sólo para cifrados polialfabéticos).

Los controles de substitución de caracteres muestran el carácter del alfabeto de cifrado a reemplazar en su parte superior, a la derecha un botón que permite añadirlo al conjunto de caracteres ignorados y abajo una lista desplegable para seleccionar un carácter de reemplazo de entre los caracteres del alfabeto plano.

Cuando un carácter está en el conjunto de ignorados, es casi como haberlo eliminado del criptograma y del alfabeto de cifrado. Se quita del área de substitución y las frecuencias relativas del criptotexto se calculan como si no existiera; pero se incluye en el texto plano como aparece en el cifrado. Por ejemplo, en el proyecto `Tormes.xml` los caracteres de puntuación son ignorados.

La casilla determina si la substitución es inyectiva (uno-a-uno) o no. Si está seleccionada, el usuario únicamente puede elegir caracteres de reemplazo de entre los caracteres que no han sido previamente seleccionados para sustituir algún otro carácter. Si la casilla no está seleccionada, todos los caracteres del alfabeto plano están disponibles.

El botón Ignorados hace lo mismo que la opción *Mostrar los caracteres ignorados* del menú Ventana; abre la ventana que muestra los caracteres ignorados del alfabeto de cifrado y permite al usuario eliminarlos de ese conjunto.

### 3.4. Panel de Estadísticas del Criptotexto

El panel de estadísticas del criptotexto contiene el índice de coincidencias del criptograma, tablas con las frecuencias relativas del criptograma y un estimado del número de alfabetos usados en el cifrado para obtener el criptograma.

El estimado del número de alfabetos se obtiene usando el índice de coincidencias del criptograma y el del lenguaje. Si el índice de coincidencias del lenguaje no está disponible o el número de caracteres en el alfabeto de cifrado es mayor al del lenguaje, no se muestra el estimado.

**Intente:** Abra el proyecto `Tormes.xml`, vea el estimado del número de alfabetos, incluya los caracteres que se encuentran en la ventana de caracteres ignorados y revise el estimado de nuevo.

Las tablas de frecuencias relativas del criptotexto muestran diferentes datos dependiendo del cifrado elegido. Para los monoalfabéticos, las tablas muestran las frecuencias relativas de caracteres, digramas y trigramas; mientras que para los polialfabéticos se muestran las frecuencias relativas de los caracteres cifrados con cada alfabeto.

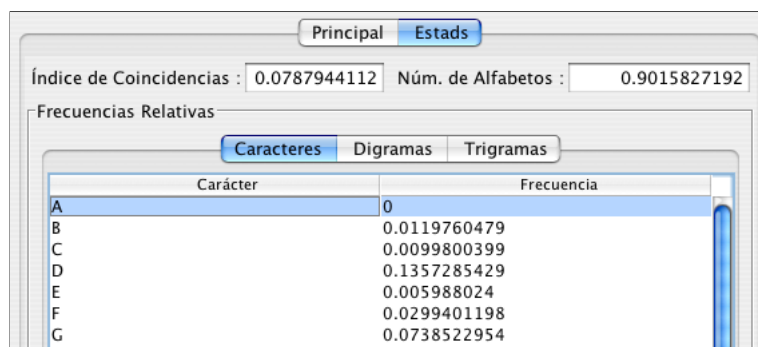


Figura 3.7: Estadísticas del criptotexto (cifrados monoalfabéticos)

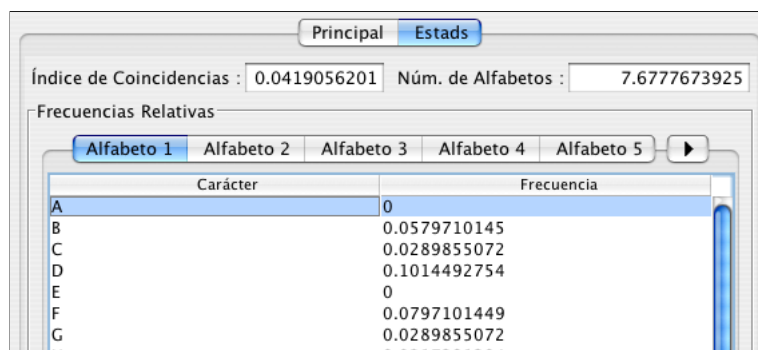


Figura 3.8: Estadísticas del criptotexto (cifrados polialfabéticos)

**Intente:** Abra el proyecto `Tormes.xml` y haga clic en la lengüeta de estadísticas del criptotexto. Regrese al panel principal y seleccione un cifrado polialfabético en el área de selección de cifrado. Vuelva a hacer clic en la lengüeta de estadísticas del criptotexto y note los cambios.

**Recuerde:** Los datos de las tablas pueden ser ordenados alfabéticamente o por frecuencia como se explicó en la sección 3.2.4. El contenido de las tablas puede ser copiado (por ejemplo a una hoja de cálculo) seleccionando los renglones que le interesan, arrastrando su selección y soltándola donde desea pegarla o usando el atajo de teclado (ver sección 3.2.2). Para seleccionar todo el contenido de la tabla, puede usar el atajo de teclado convencional de su plataforma, por ejemplo Comando-A en Mac OS X, o Control-A en GNU/Linux.

### 3.5. Área de Selección de Cifrado y Herramientas

El área de selección de cifrado le permite elegir las herramientas específicas del cifrado a usar en su proyecto de criptoanálisis, si tendrá uno o más alfabetos y la información a mostrar en el panel de estadísticas del criptotexto.



Figura 3.9: Área de selección de cifrado y herramientas

#### 3.5.1. Monoalfabéticos

Ganzúa tiene dos grupos de herramientas para cifrados monoalfabéticos: el general y el del cifrado de César.

##### Herramientas para el cifrado de César

El tipo de substitución en la que el alfabeto es simplemente desplazado un número de posiciones es llamado cifrado de César. En Ganzúa, las herramientas para criptogramas obtenidos con este cifrado se encuentran en la categoría César. A continuación se describe la función de los controles disponibles en el área de herramientas para el cifrado de César.

**Limpiar:** Pone en blanco todos los caracteres de substitución.

**Identidad:** Limpia la substitución actual y selecciona una tan cercana a la substitución identidad como sea posible. Esto es, si el alfabeto plano contiene el carácter del alfabeto de cifrado, se elige ése como su reemplazo, si no está precisamente ese carácter pero está su versión en mayúscula/minúscula, entonces ése queda seleccionado.

**Completar:** Asigna arbitrariamente caracteres de reemplazo a aquellos a los que no se les ha asignado uno. Los reemplazos se seleccionan en orden alfabético de entre los caracteres que no han sido previamente seleccionados.

**Revés:** Toma la substitución actual e invierte el orden en que aparecen los caracteres de reemplazo. En otras palabras, el carácter que reemplaza al primer carácter, reemplazará al último, etc.

**Invertir:** Selecciona una substitución tan cercana a la inversa de la actual como sea posible. Toma aquellos caracteres del alfabeto de cifrado que aparecen también en el alfabeto plano y cuyos reemplazos se encuentran en el alfabeto de cifrado e invierte la relación (asigna el carácter siendo substituido como substitución y la substitución como el que es substituido). Las mayúsculas y minúsculas se consideran en la misma manera que en el botón identidad.

**Desplazar:** Este control le permite desplazar los caracteres de reemplazo hacia la derecha o izquierda.

**Intente:** Abra el proyecto `Tormes.xml` y pulse el botón Limpiar. Si no recuerda por qué permanecen los símbolos de puntuación en el texto plano, lea la sección 3.3. Ahora pulse el botón Identidad y desplace la selección a la izquierda tres posiciones. Esta es la substitución que se usó para obtener el criptograma, así que si pulsa el botón Invertir, obtendrá el texto original.

### Herramientas para los cifrados monoalfabéticos en general

Las herramientas para cifrados monoalfabéticos en general son las mismas que las disponibles para el cifrado de César, con excepción de la herramienta para desplazamiento.

Si está trabajando en este modo y llega a necesitar la herramienta de desplazamiento, elija César en el área de selección de cifrado. No perderá datos en el cambio, lo mismo aplica para cambiar de César a monoalfabéticos en general.

#### 3.5.2. Polialfabéticos

Cuando escoge un cifrado polialfabético, aparece un control llamado Núm. Alfabetos en la parte superior de la sección de herramientas. Este control le permite seleccionar el número de alfabetos a usar. No confunda la función de este control con la del control del área de substitución.

Ganzúa tiene dos grupos de herramientas para cifrados polialfabéticos: el del cifrado de Vigenère y el del cifrado de Alberti.

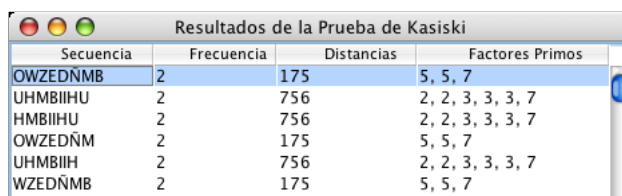
### Herramientas para el cifrado de Vigenère

En el cifrado de Vigenère cada alfabeto usado difiere de los demás por un desplazamiento, así que muchas de las herramientas disponibles para este cifrado se parecen a las del cifrado de César.

Abra el proyecto `Quijote.xml` y vea cómo lucen las diferentes secciones de Ganzúa cuando usa un cifrado polialfabético. Fíjese en el área de substitución, el panel con estadísticas del criptotexto y pruebe las herramientas para el cifrado de Vigenère mientras lee sus descripciones.

**Núm. Alfabetos:** Esta herramienta le permite seleccionar el número de alfabetos con los que va a trabajar.

**Kasiski:** Realiza la prueba de Kasiski al criptograma. Encuentra todas las secuencias de caracteres de longitud dos o más que se repitan en el criptotexto, el número de veces que aparecen, la distancia entre apariciones y los factores primos de esas distancias. Una vez terminada la prueba, se abre la ventana de resultados de la prueba de Kasiski y se muestran los datos en una tabla. La tabla puede ser ordenada por longitud de las secuencias o frecuencia haciendo clic en los encabezados de las columnas.



Secuencia	Frecuencia	Distancias	Factores Primos
OWZEDÑMB	2	175	5, 5, 7
UHMBIIHU	2	756	2, 2, 3, 3, 3, 7
HMBIIHU	2	756	2, 2, 3, 3, 3, 7
OWZEDÑM	2	175	5, 5, 7
UHMBIIH	2	756	2, 2, 3, 3, 3, 7
WZEDÑMB	2	175	5, 5, 7

Figura 3.10: Ventana de resultados de la prueba de Kasiski

**Agrupar:** Agrupa los caracteres del criptotexto en bloques igual que la opción *Agrupar caracteres del criptotexto* del menú Edición

**Subst 1:** Copia la substitución del primer alfabeto al alfabeto seleccionado actualmente.

**Limpiar:** Limpia los caracteres de reemplazo del alfabeto seleccionado actualmente.

**Identidad:** Limpia la substitución del alfabeto actual y selecciona una tan cercana a la identidad como sea posible. Hace la selección de la misma manera que su homólogo monoalfabético.

**Completar:** Asigna arbitrariamente caracteres de reemplazo a aquellos a los que no se les ha asignado uno en el alfabeto actual. La selección se hace de la misma manera que en su homólogo monoalfabético.

**Revés:** Toma la substitución del alfabeto actual e invierte el orden en que aparecen los caracteres de reemplazo.

**Invertir:** Selecciona una substitución tan cercana a la inversa de la del alfabeto actual como sea posible. La selección se hace de la misma manera que en su homólogo monoalfabético.

**Desplazar:** Desplaza los caracteres de reemplazo de el alfabeto actual a la izquierda o derecha.

### Herramientas para el cifrado de Alberti

Las herramientas para el cifrado de Alberti son las mismas que las disponibles para el cifrado de Vigenère, con excepción de la herramienta para desplazamiento.

Si está trabajando en este modo y llega a necesitar la herramienta de desplazamiento, elija Vigenère en el área de selección de cifrado. No perderá datos en el cambio, lo mismo aplica para cambiar de Alberti a Vigenère.

**IMPORTANTE:** Si cambia de un cifrado polialfabético a uno monoalfabético perderá todas las substituciones excepto la del primer alfabeto.

## 3.6. Ajustando el Idioma y Convenciones

La interfaz de Ganzúa emplea el idioma y convenciones regionales preferidos por el sistema por omisión. Si Ganzúa aún no puede manejar la lengua<sup>4</sup> que usted desea, usará el idioma inglés.

Si quiere que Ganzúa emplee algún otro lenguaje o convenciones regionales<sup>5</sup> sin cambiar las preferencias de su sistema, puede especificarlos como opciones en la línea de comandos. Para esto tendrá que ejecutar Ganzúa desde una terminal de línea de comandos.

Por ejemplo, para ejecutar el programa con una interfaz en español y con las convenciones de México, usaría el comando:

```
java -jar GANZÚA/ganzua.jar -l es -c MX
```

Donde GANZÚA es el directorio en que se instaló Ganzúa. `-l` se usa para indicar el lenguaje usando su código ISO 639 y `-c` para indicar las convenciones regionales a usar con el código ISO 3166 del país. No es necesario que use ambas opciones, puede usar `-l` y omitir `-c` y vice versa.

En Mac OS X puede especificar estos argumentos en el paquete de la aplicación. Para hacer esto, abra el archivo `Info.plist` con un editor de texto e inserte las siguientes dos líneas en la línea 29, debajo de `<string>1.4+</string>`.

```
<key>Arguments</key>
<string>-l es -c MX</string>
```

Reemplace `es` y `MX` con los códigos del lenguaje y país que quiera usar. Como con las opciones de la línea de comandos, puede usar sólo `-l` o `-c`, no necesita usar ambos.

<sup>4</sup>La versión 1.01 de Ganzúa puede usar inglés o español en su interfaz.

<sup>5</sup>Las convenciones regionales indican cómo se deben presentar los datos numéricos. Por ejemplo si se separan la parte entera y fraccionaria de un número con un punto o una coma (1.234 ó 1,234).

### 3.7. Detalles a Considerar

Esta sección lista algunos puntos que debe considerar cuando use Ganzúa además de los resaltados en las secciones anteriores.

Cuando abre un criptograma de algún archivo de texto, el alfabeto de cifrado se obtiene a partir de los caracteres que aparecen en él y no son considerados caracteres especiales<sup>6</sup>. Lo primero que debe hacer después de abrir un criptograma es verificar que el alfabeto de cifrado contenga todos los caracteres que desea usar y sólo esos, dado que es común que los criptogramas carezcan de algún carácter del alfabeto. De no hacerlo puede complicar innecesariamente el proceso de criptoanálisis. Las secciones 3.2.2 y 3.3 explican cómo añadir, eliminar e ignorar caracteres del alfabeto de cifrado.

Si piensa usar Ganzúa para cifrados polialfabéticos, también debe recordar que los resultados de la prueba de Kasiski incluyen todas las secuencias repetidas de caracteres con longitud dos o más. Esto implica que las subsecuencias de hasta longitud dos se incluyen en los resultados. Por ejemplo, si ve que la secuencia ABCDE tiene frecuencia 2 y que la secuencia BCD tiene frecuencia 3, entonces, dos de esas apariciones son como subsecuencias en las apariciones de ABCDE.

Revise el sitio de Ganzúa (<http://ganzua.sourceforge.net>) para actualizaciones y respuestas a preguntas frecuentes. También lea el capítulo 5 si encuentra algún error en el programa, documentación, etc. y necesita contactar al autor.

---

<sup>6</sup>Los espacios, retornos de carro, saltos de línea y caracteres de control se consideran caracteres especiales.



## Capítulo 4

# Frecuencias Relativas de Lenguajes

Ganzúa incluye algunos archivos con frecuencias relativas estándar de lenguajes, pero probablemente no las incluye para el idioma o alfabeto que usted desea usar. Todos esos archivos fueron generados con el programa langFreq.jar. Este programa de línea de comandos puede obtener frecuencias relativas estándar para alfabetos arbitrarios a partir de un archivo de texto. Dado que es un programa de línea de comandos, tendrá que ejecutarlo desde una terminal<sup>1</sup>.

Para que las frecuencias relativas sean representativas del idioma, el archivo del que las obtiene debe ser lo más grande posible. Las las frecuencias incluidas con Ganzúa fueron obtenidas de novelas que puede encontrar en el sitio de Project Gutenberg (<http://www.promo.net/pg/>). En particular las estadísticas para el idioma inglés se obtuvieron de *David Copperfield*, de Charles Dickens y las de la lengua española de *El Ingenioso Hidalgo Don Quijote de la Mancha* de Miguel de Cervantes Saavedra. A diferencia de Ganzúa, que no está hecho para manejar documentos extensos, langFreq.jar puede usar documentos muy grandes.

La información sobre el archivo de texto y el alfabeto que quiera usar se coloca en un documento XML como los que se encuentran en el directorio `examples/alphabetRules/en` de Ganzúa. Estos documentos XML son casos particulares de el esquema `AlphabetRules.xsd`. Se les llama documentos de reglas para alfabetos (alphabet rules) porque especifican los caracteres a incluir en el alfabeto y cómo se deben manejar aquellos que no se encuentran dentro de éste.

Si encuentra la siguiente sección complicada o le gustaría saber algo sobre XML antes de empezar a escribir sus propios documentos XML, hojee alguna de las muchas lecciones sobre XML disponibles en Internet, como la que se encuentra en <http://www.w3schools.com>.

---

<sup>1</sup>En Mac OS X puede encontrar el programa Terminal en Aplicaciones/Utilidades

## 4.1. Documentos XML de Reglas para Alfabetos

Abra uno de los documentos de reglas para alfabetos (`examples/alphabetRules/es`) con su editor de texto (o XML) favorito para que pueda ver un ejemplo completo mientras se explican las diferentes secciones de este tipo de documento XML.

```
<?xml version="1.0" encoding="UTF-8"?>
```

La primera línea debe indicar la codificación usada por el archivo XML. Si no sabe qué codificación está usando, probablemente sea la que usa por omisión su sistema. Puede usar Ganzúa para averiguar cuál es la codificación por omisión de su plataforma (vea *Abrir criptotexto* en la sección 3.2.1).

```
<alphabetRules xmlns="http://ganzua.sourceforge.net/rules"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ganzua.sourceforge.net/rules
    ../schemas/AlphabetRules.xsd"
  language="en" country="GB"
  source="/home/user/cprfd10.txt" sourceEncoding="ISO-8859-15">
```

Las siguientes líneas contienen la etiqueta de apertura del elemento `alphabetRules` y sus atributos. Los únicos atributos que debe modificar<sup>2</sup> son aquellos que especifican características del archivo de texto del que obtendrá las frecuencias relativas.

**language** Identifica el lenguaje en el que está escrito el archivo de texto usando su código ISO 639 de dos letras.

**country** identifica el país de origen del documento en el archivo de texto con el código ISO 3166 de dos letras del país. Este atributo se usa para identificar las diferencias en el uso de un idioma en distintos países; por ejemplo, el español como se habla en España del que se habla en México. Este atributo puede ser omitido por completo.

**source** Indica el archivo de texto del que se van a obtener las frecuencias relativas. Su valor debe ser el nombre completo del archivo (con su trayectoria absoluta).

**sourceEncoding** Indica la codificación usada en el archivo de texto.

Los siguientes elementos especifican los caracteres que conforman el alfabeto. Esto se puede hacer de dos maneras:

- Liste todos los caracteres que contiene el alfabeto.

---

<sup>2</sup>Cambie el valor entre comillas, cuidando no borrar las comillas.

- Especifique un conjunto de caracteres que debe incluir el alfabeto (aún si no aparecen en el archivo de texto) y un conjunto de caracteres a descartar. Todo carácter en el archivo de texto que no esté entre los ignorados será considerado parte del alfabeto.

Si quiere listar todos los caracteres del alfabeto, que es la manera más sencilla, use el elemento `includeExclusively` (incluir únicamente).

```
<includeExclusively>
  <character char="A" />
  <character char="B" />
  <character char="C" />
  <character char="D" />
  :
</includeExclusively>
```

Cada elemento `character` especifica un carácter a ser incluido en el alfabeto en su atributo `char`. Todo carácter en el archivo de texto que no se encuentre en el elemento `includeExclusively` será ignorado cuando el programa obtenga las frecuencias relativas. `ES_27_Min.xml` y `ES_26_May.xml` son ejemplos de archivos de reglas para alfabetos que usan este elemento.

**Recuerde:** Los caracteres de retorno de carro, espacio y control son considerados especiales por Ganzúa y no deben formar parte del alfabeto plano o de cifrado.

No ponga caracteres especiales dentro de `includeExclusively`.

Para dejar que `langFreq.jar` añada caracteres al alfabeto de cifrado como los va encontrando en el archivo de texto, use los elementos `include` e `ignore`. En el siguiente ejemplo se especifican algunos caracteres haciendo referencia a su valor en el estándar Unicode (por ejemplo `&#10;` para el salto de línea) o usando entidades (como `&quot;` para el carácter "). Las entidades que hacen referencia al valor de Unicode son de la forma `&#NUM;` donde `NUM` es el número decimal (no hexadecimal) del carácter en las tablas de Unicode. Si desea aprender más sobre Unicode, visite <http://www.unicode.org>.

```
<include>
  <character char="A" />
  <character char="B" />
  <character char="C" />
  <character char="D" />
  :
</include>
<ignore>
  <character char=" " /> <!-- espacio -->
  <character char="&#9;" /> <!-- tabulación horizontal -->
```

```

    <character char="#10;" /> <!-- cambio de línea -->
    <character char="#13;" /> <!-- retorno de carro -->
    <character char="#13;#10;" /> <!-- línea nueva -->
    <character char=""" /> <!-- comillas -->
    <character char="-" />
    :
</ignore>

```

Todos los caracteres en el elemento `include`, serán parte del alfabeto aún si no aparecen en el archivo de texto; mientras que los caracteres en el elemento `ignore` no serán añadidos al alfabeto aunque aparezcan en el archivo de texto.

**IMPORTANTE:** Nunca ponga los mismos caracteres tanto en el elemento `include` como en el `ignore`. De hacer esto, esos caracteres estarán en el alfabeto, pero sus apariciones en el texto serán ignoradas, por lo que tendrán frecuencia cero en el archivo de frecuencias relativas y no aparecerán en ningún digrama o trigrama.

Dado que los caracteres de salto de línea, espacio y control son considerados especiales por Ganzúa, no deben aparecer en el elemento `include` y siempre deben ser ignorados. En el ejemplo anterior los caracteres de espacio, tabulación, cambio de línea, retorno de carro y línea nueva son ignorados. Si usa el elemento `include`, al menos esos caracteres deben aparecer dentro del elemento `ignore`.

ES\_26\_May\_Ignr.xml, ES\_27\_Min\_Ignr.xml y el resto de los ejemplos de reglas para alfabetos cuyos nombres incluyen `Ignr` usan los elementos `include` e `ignore`.

El siguiente elemento hace que `langFreq.jar` maneje las apariciones de ciertos caracteres como si fueran otros. El programa no hace esto automáticamente, si su alfabeto contiene únicamente letras mayúsculas (como en un elemento `includeExclusively`), sólo esos caracteres serán considerados y todas las letras minúsculas serán descartadas. Esto es, a menos que el elemento `replace` especifique que las minúsculas deben de ser manejadas como caracteres que forman parte del alfabeto.

```

<replace>
  <occurrences ofChar="a" byChar="A" />
  <occurrences ofChar="b" byChar="B" />
  <occurrences ofChar="c" byChar="C" />
  <occurrences ofChar="d" byChar="D" />
  :
</replace>

```

Los elementos `occurrences` indican el carácter a substituir en su atributo `ofChar` y el carácter de reemplazo en el atributo `byChar`. De esta manera puede hacer que se considere el carácter Ñ como N, etc.

Note que si especifica en **replace** que un carácter debe ser reemplazado por otro a ser ignorado, ambos serán ignorados. También debe considerar que langFreq.jar no reemplaza los caracteres recursivamente. Por ejemplo, si las siguientes líneas están dentro del elemento **replace**:

```
<occurrences ofChar="a" byChar="A" />
<occurrences ofChar="A" byChar="X" />
```

Las apariciones del carácter **a** en el texto contarán como **A**, y aquellas de **A** como **X**, pero **a** no contará como **X**.

Todos los ejemplos de reglas para alfabetos incluidos con Ganzúa usan el elemento **replace**.

## 4.2. Usando langFreq.jar

Para usar langFreq.jar necesita tener el archivo de texto del que va a obtener las frecuencias relativas y el documento XML con las reglas para el alfabeto. Una vez que tenga esto, abra una terminal de línea de comandos y cambie de su directorio actual al que contiene su documento XML. Ahora use el comando:

```
java -jar GANZÚA/langFreq.jar reglas.xml
```

Donde GANZÚA es el directorio que contiene a langFreq.jar y reglas.xml es el nombre del archivo XML que quiere usar. Este comando hará que langFreq.jar analice el documento XML, reporte cualquier error sintáctico que encuentre en él y si no hay ninguno, genere un documento XML con las frecuencias relativas. El programa reporta el nombre del archivo y el directorio donde puso el archivo con las frecuencias relativas al terminar el proceso. Por omisión, tratará de poner el archivo nuevo de frecuencias junto con las demás, en el directorio de frecuencias de Ganzúa, pero si no tiene permisos de escritura para ese directorio, lo pondrá en el directorio de inicio del usuario. El archivo será nombrado usando el código del idioma y un número arbitrario.

Si quiere especificar el directorio y nombre del archivo que quiere que escriba langFreq.jar, use la opción -o. Por ejemplo, si usa el comando:

```
java -jar GANZÚA/langFreq.jar -o frecuencias.xml reglas.xml
```

langFreq.jar escribirá las frecuencias relativas en el archivo frecuencias.xml en el directorio actual.

Si hace archivos de frecuencias nuevos, por favor considere donarlos al proyecto Ganzúa, especialmente si son de lenguajes para los que aún no cuenta con ningún archivo. El capítulo 5 explica cómo contribuir a Ganzúa.

## Capítulo 5

# Contribuya

Hay muchas maneras de contribuir al mejoramiento de Ganzúa.

- **Reporte todo error que encuentre en los programas**, aún si es un problema menor.
- **Reporte errores en la documentación**, aún si es un error ortográfico.
- **Done archivos de frecuencias relativas estándar de lenguajes**, especialmente para idiomas para los que Ganzúa no cuenta con ninguno.
- **Traduzca Ganzúa**. En otras palabras, traduzca los archivos de texto de los que Ganzúa obtiene las etiquetas para su interfaz. Esto es más fácil de lo que suena y estaría dando acceso a personas que no hablan inglés o español. La sección 5.1 explica en mayor detalle cómo hacer esto. Idealmente, cualquiera debe de poder usar Ganzúa sin importar su lengua materna.
- **Traduzca la documentación de Ganzúa**.
- **Implemente mejoras**.

Si desea contribuir de alguna de las maneras citadas anteriormente, por favor contacte al autor de Ganzúa por medio de su dirección de correo electrónico, `agarciap@users.sourceforge.net`. Recuerde que Ganzúa es software libre y sólo puede ser mejorado con su apoyo. Si llega a necesitar ayuda, mejoras o algún arreglo, siéntase con libertad de escribir, pero recuerde ser cortés. Cuando contacte al autor por favor hágalo en español o inglés.

### 5.1. Traduciendo Ganzúa

Ganzúa obtiene las etiquetas de su interfaz de archivos de propiedades. Éstos son archivos de texto codificados en ISO-8859-1 (ISO-Latin-1) que se encuentran dentro del JAR y cuyos nombres tienen extensión `properties`. Puede

extraer el contenido de un JAR con la misma aplicación que usaría para expandir un archivo ZIP. Los archivos de propiedades tienen nombres de la forma `nombre_cl_CP.properties` donde `cl` es el código ISO 639 de la lengua en la que están las etiquetas y `CC` es el código ISO 3166 de dos letras del país.

Cuando traduzca un archivo de propiedades, lo primero que debe hacer es copiar el archivo a traducir a otro con el nombre apropiado para la traducción. Por ejemplo, si quiere traducir `nombre_en.properties` a portugués, entonces el archivo con la traducción debe llamarse `nombre_pt.properties` o `nombre_pt_BR.properties` si la traducción tiene uso de la lengua propio de Brasil.

Los archivos de propiedades contienen líneas como las siguientes:

```
# Un comentario
clave = Algo de texto
```

El carácter `#` marca el inicio de un comentario, el texto que le sigue será ignorado por el programa, así que no hay necesidad de traducirlo. Las líneas importantes para Ganzúa son las que contienen parejas clave-valor separadas por el carácter `=`. La clave es usada por Ganzúa para obtener el texto traducido, así que nunca debe cambiar las claves, sólo el texto a la derecha del carácter `=`. También debe considerar que `\n` representa un cambio de línea, `\t` una tabulación y en algunas ocasiones `FN` y `NUM` funcionan como variables que Ganzúa reemplaza por nombres de archivos y números respectivamente, por lo que no deben ser modificados.

Ganzúa requiere que los archivos de propiedades estén codificados en ISO-8859-1. Para convertir sus archivos puede que necesite la herramienta `native2ascii` que se incluye en la mayoría de los kits para desarrollo de Java (ver sección 2.5).

Para ejecutar Ganzúa con la versión expandida de `ganzua.jar` siga las instrucciones en la sección 2.5 (note que no necesita compilar Ganzúa, dado que `ganzua.jar` contiene el programa compilado). Esto puede ser útil mientras edita/prueba sus archivos de propiedades.

Para que Ganzúa quede traducido para su idioma o región, debe traducir, nombrar apropiadamente y codificar en ISO-8859-1 todos los archivos de propiedades.

Si tiene problemas traduciendo Ganzúa, contácteme explicando su problema.

## 5.2. Notas Sobre el Código Fuente

A continuación se listan algunas cosas que debe saber si quiere editar el código fuente.

- Los archivos con el código fuente usan la codificación UTF-8
- Los archivos de propiedades usan ISO-8859-1.

- El código fuente de Ganzúa está documentado en inglés usando comentarios para la herramienta Javadoc, por lo que puede generar la documentación en formato HTML con dicha herramienta. Puede hacerlo con el comando `ant docs` si está usando Apache Ant.



Copyright © 2004 Jesús Adolfo García Pasquel

Sun, Sun Microsystems, the Sun Logo, Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

W3C is a registered trademark of the World Wide Web Consortium in the United States and other countries.

Apache, Ant and Xerces are trademarks or registered trademarks of The Apache Software Foundation.

Apple and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.

IBM is a registered trademark of International Business Machines Corporation in the United States and other countries.

Project Gutenberg is a registered trademark of the Project Gutenberg Association in the United States and other countries.

Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Other company, product, service names and marks may be trademarks or service marks of others.