Manual de usuario

Índice

[Introducción 2](#_Toc309948058)

[Instalación y Compilación 3](#_Toc309948059)

[Pre-requisitos 3](#_Toc309948060)

[Generación de ejecutable 3](#_Toc309948061)

[Generación de archivos de texto: Run Script. 3](#_Toc309948062)

[Ejemplos de uso 4](#_Toc309948063)

[Menú Principal 5](#_Toc309948064)

[Generación de archivos 6](#_Toc309948065)

[Votación 8](#_Toc309948066)

[Reportes 8](#_Toc309948067)

[Recuperación de reporte 10](#_Toc309948068)

[ABM 11](#_Toc309948069)

[Romper RSA 14](#_Toc309948070)

# Introducción

Este documento explica el correcto uso y funcionamiento de la aplicación del simulador de voto electrónico, creado para la materia de Organización de Datos 75.06 de la **Facultad de Ingeniería de Buenos Aires**, y debe ser usado como guía para la ejecución del programa.

A continuación encontrará los pasos explicativos para la instalación y compilación del paquete, la generación de archivos de texto con toda la información de votantes y elecciones relacionadas, y por último, su ejecución y casos principales de uso.

|  |
| --- |
| **Nota**: Para la prueba de este paquete se utilizó un ambiente limpio de Ubuntu 10.10 versión Home sobre una máquina virtual, solamente instalando los prerrequisitos necesarios para la correcta compilación, que se detallan en la siguiente sección de Instalación y Compilación.  (***Sitio de descarga***: <http://releases.ubuntu.com/10.10/> ) |

# 

# Instalación y Compilación

## Pre-requisitos

La aplicación hace uso de los siguientes prerrequisitos los cuales son necesarios para poder realizar una correcta instalación de la misma:

* tar; necesario para la descompresión del paquete. De no estar previamente instalado, puede instalarse con el siguiente comando:

|  |
| --- |
| **Shell** |
| sudo apt-get install tar |

* g++; necesario para la correcta compilación de las librerías del proyecto. De no estar previamente instalado, puede instalarse con el siguiente comando:

|  |
| --- |
| **Shell** |
| sudo apt-get install g++ |

* python; necesario para la ejecución del script generador de archivos de texto. Debería venir ya instalado en el sistema operativo de Linux.

|  |
| --- |
| **Nota**: En ambas instalaciones son necesarios los permisos de root. |

## Generación de ejecutable

Luego de haber instalado los prerrequisitos necesarios se deberán correr los siguientes comandos para la creación del archivo ejecutable, con previo posicionamiento en el directorio donde se encuentra el paquete:

* Descomprimir el paquete:

|  |
| --- |
| **Shell** |
| tar xfvz ElectronicElections.tar.gz |

* Compilación del proyecto con el archivo makefile que se encuentra en la carpeta Release:
  + Posicionamiento a la carpeta Release:

|  |
| --- |
| **Shell** |
| cd ElectronicElections/Release |

* + Compilación:

|  |
| --- |
| **Shell** |
| make all |

Luego de varios segundos compilando el proyecto, ya está listo el archivo ejecutable ***ElectronicsElections*** para ser ejecutado.

# Generación de archivos de texto: Run Script.

Esta sección explica el uso de un script desarrollado en el lenguaje **Python**, para una mejor experiencia del usuario a la hora de generar los archivos de texto con toda la información respectiva a las elecciones, padrón electoral, listas comprometidas, candidatos y cargos. Además, se generará un archivo de administradores con las cuentas de los integrantes del grupo y del tutor responsable.

Este script genera los archivos de texto para votantes aleatoriamente, 50.000 personas uniformemente distribuidas entre 10.000.000, y 99.999.999 de número de DNI; distritos tomados de una lista, 1.000 intendencias, 200 gobernaciones y 5 presidencias; y cargos, listas y elecciones tomando valores válidos respecto a los archivos de votantes y distritos, y generando las fechas al azar.

Para correr el script ejecutamos lo siguiente, desde la carpeta de *ElectronicElections/Files,* la cual se encuentra en el root del programa:

|  |
| --- |
| **Shell** |
| python data.py |

|  |
| --- |
| **Nota**: Para este comando es necesario tener instalado python, como fue nombrado en la sección de prerrequisitos, pero por lo general ya viene instalado en el sistema operativo de Linux. |

# Ejemplos de uso

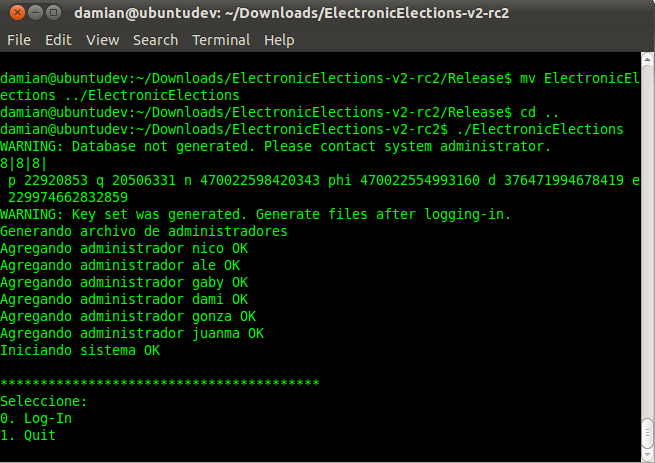
La ejecución del programa es necesario correrlo desde el directorio raiz del proyecto (*/ElectronicElections*). Para esto, ejecutamos la siguiente instrucción que copiará el archivo ejecutable al directorio deseado, de la siguiente forma:

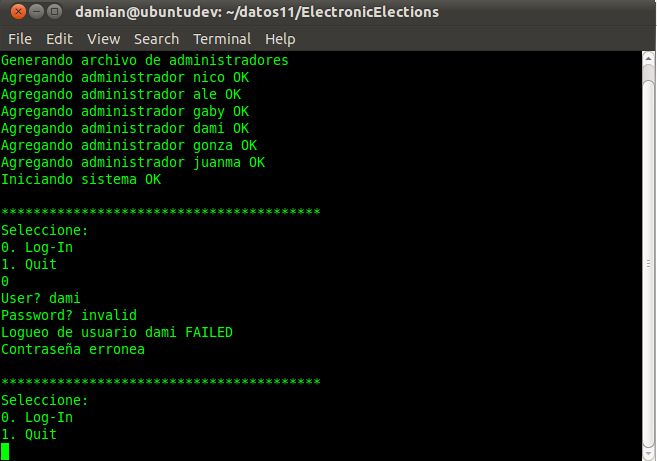
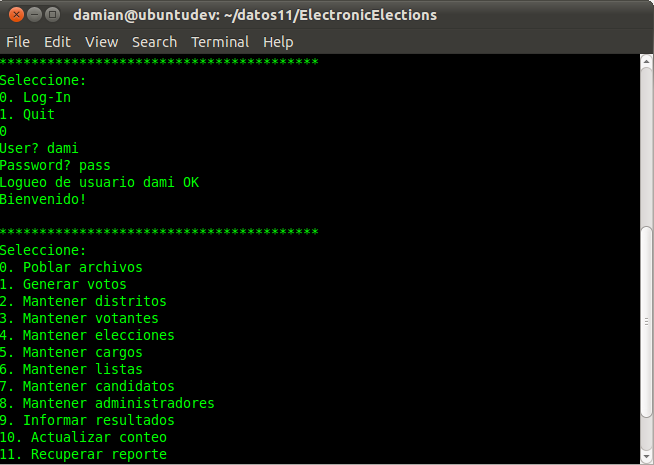
|  |
| --- |
| **Shell** |
| mv ElectronicElections ../ElectronicElections |

Ahora sí, se puede ejecutar la aplicación:

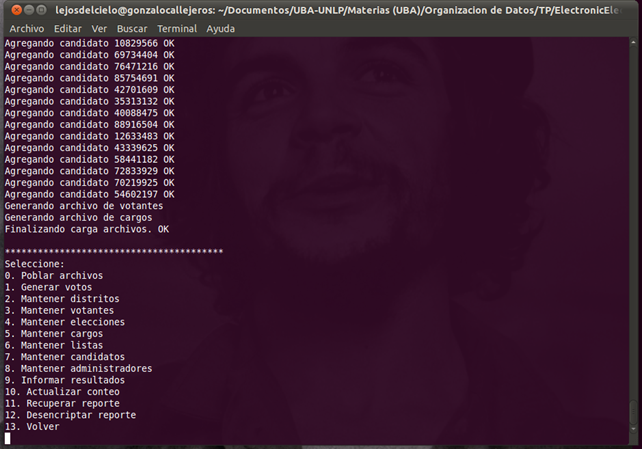
|  |
| --- |
| **Shell** |
| ./ElectronicElections |

## Menú Principal

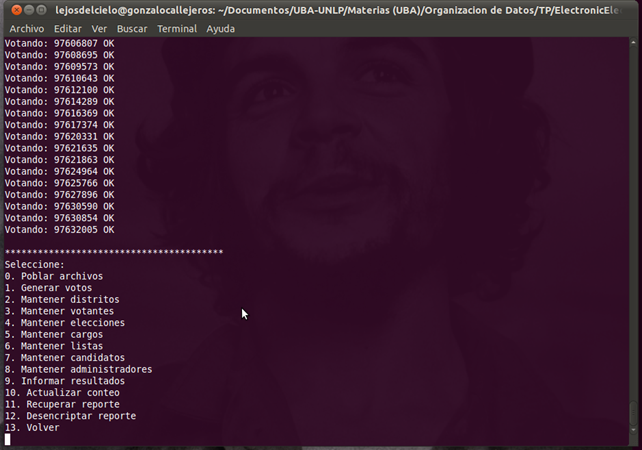
Se ejecuta la aplicación y se muestra el siguiente menú (observar que la primera vez se genera el conjunto de claves RSA):  


1. Seleccionamos la opción 0 “*Log-In*”, para loguearse en la aplicación y poder generar los archivos. Pruebo con un usuario falso:  
   
2. Se puede ver que falló el log-in. Se prueba con un usuario real:  
   

## Generación de archivos

Seleccionamos la opción 0 “Poblar archivos”, para la lectura de los archivos de texto y carga inicial de los árboles y hash. Al finalizar podemos ver que la carga de los datos fueron logueados en el log.  
  
**Los archivos están cargados.**

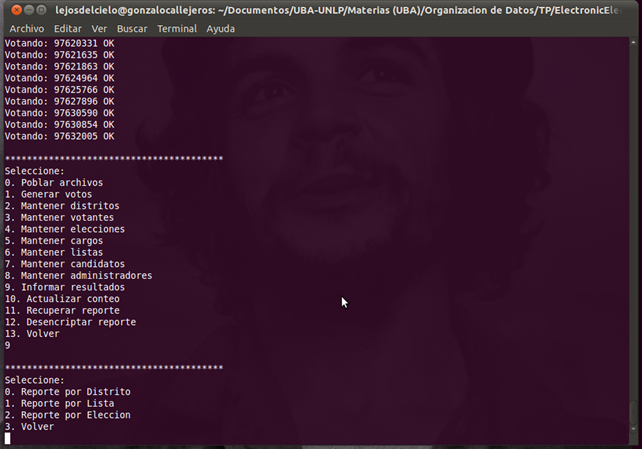
## Votación

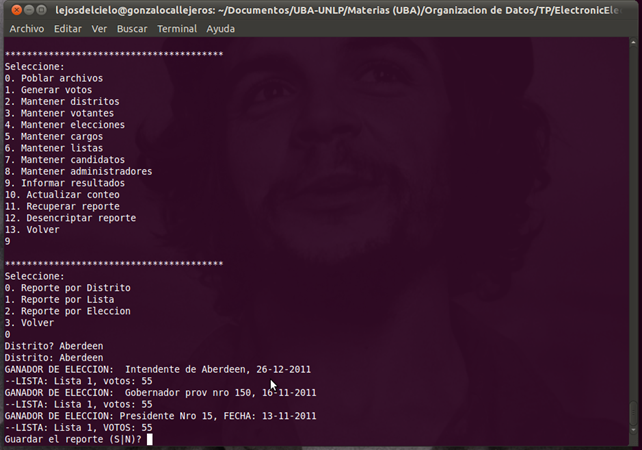
En la pantalla principal de la aplicación, se selecciona la opción 1, “*Generar Votos*”. De la misma forma que en la carga de archivos, la votación de cada persona fue logueado en el log.  


**Una vez generados los votos ya se puede acceder a los reportes.**

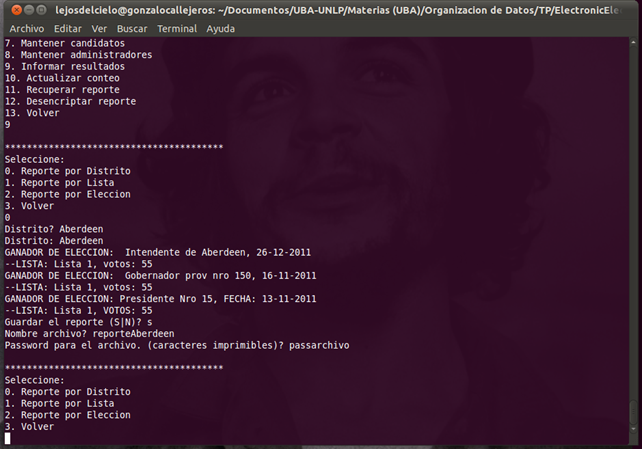
## Reportes

Para ver los resultados de las elecciones, se selecciona la opción de ver los reportes (9):



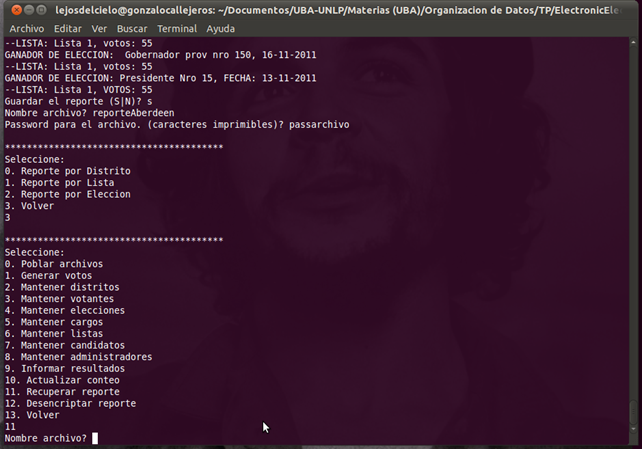
En el nuevo menú se elige la opción deseada. Por ejemplo, reporte por Distrito (opción 0). Se completan las opciones y se obtiene el reporte:  


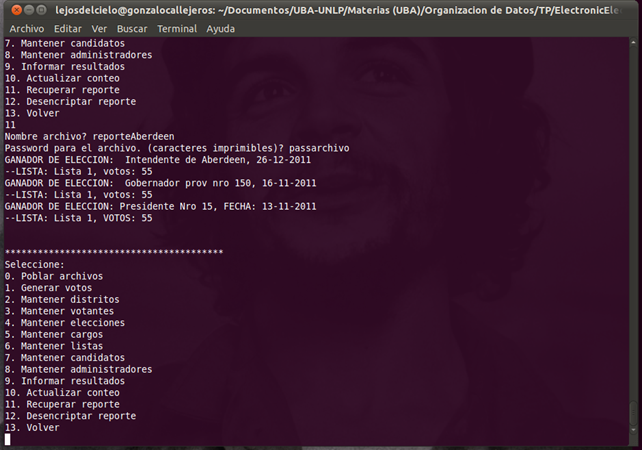
Se puede ver que muestra los votos que obtuvo cada lista en la elección pedida. Note que pudo haber listas las cuales no obtuvieron votos. En ese caso, la lista no es mostrada.

Aparece la opción de guardar o no el reporte. Si se selecciona guardar el reporte, el sistema pide un nombre de archivo y una clave que se debe recordar para luego poder recuperar el archivo (los reportes se guardan en el directorio **/Files/Reports**):  


Se selecciona la opción 3 para volver al menú anterior.

## Recuperación de reporte

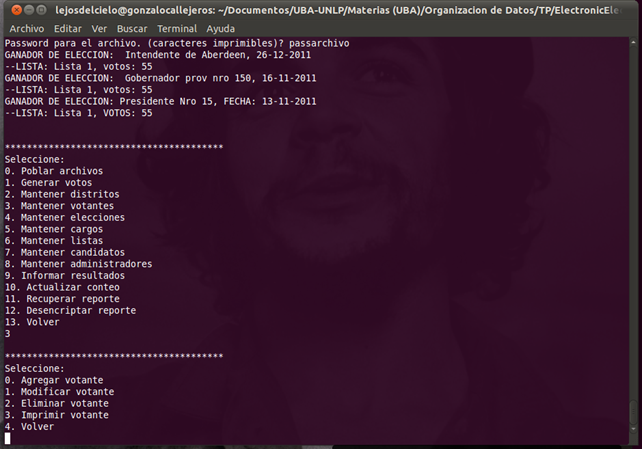
Para recuperar un reporte se elige la opción correspondiente (11) en el menú:  


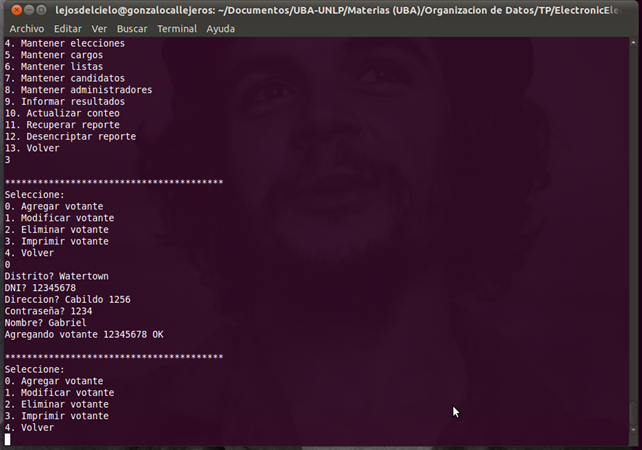
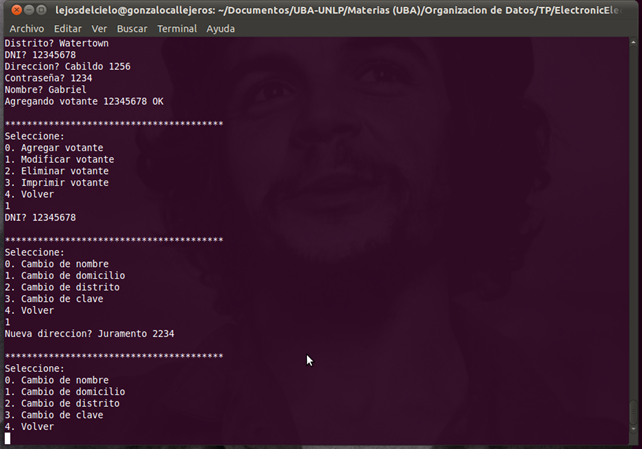
Se ingresan los datos del archivo guardado previamente.  


**El reporte se recuperó correctamente.**

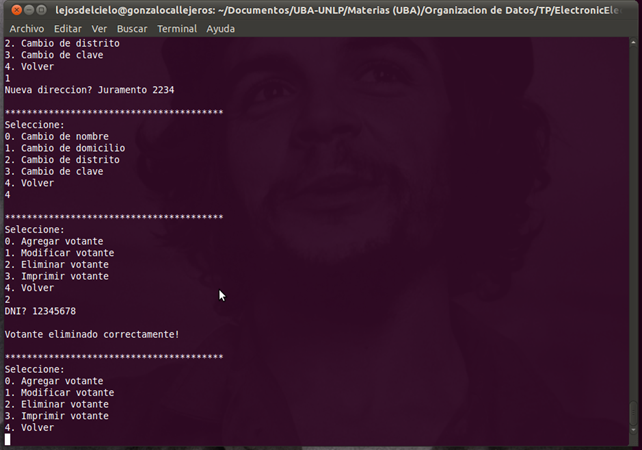
## ABM

Ahora se explicará el funcionamiento de los ABM. Para ejemplificar se utilizará el ABM de votante:

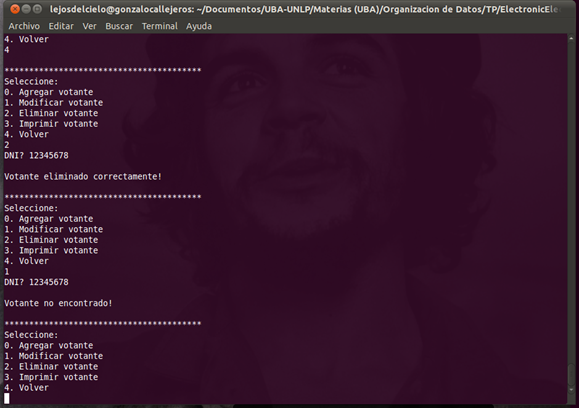


1. Agregar votante “12345678”. Se selecciona la opción 0 y se completan los datos que solicita. Al querer ingresarlo, vemos que no se produjo ningún error:  
   
2. Modificar votante “12345678” recién ingresado. Se modificará el domicilio:  
   

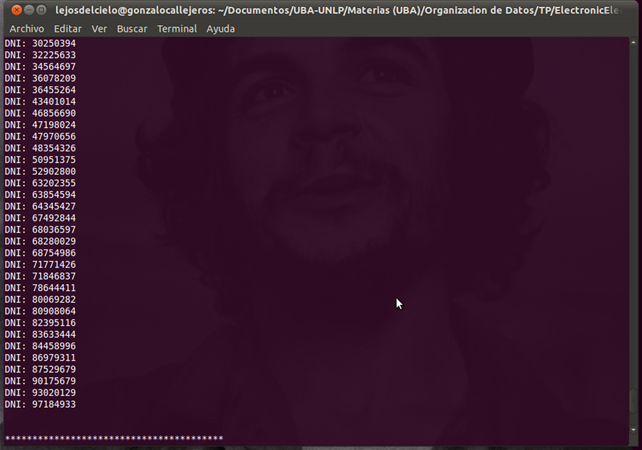
**Cambio correctamente el domicilio.**

1. Eliminar el votante “12345678” (recientemente creado en el paso 1):  
   

Se eliminó correctamente el votante “12345678”, de modo que si ahora quisiera modificarlo, me debería mostrar un error:



**Efectivamente, el votante ya no se encuentra en el archivo.**

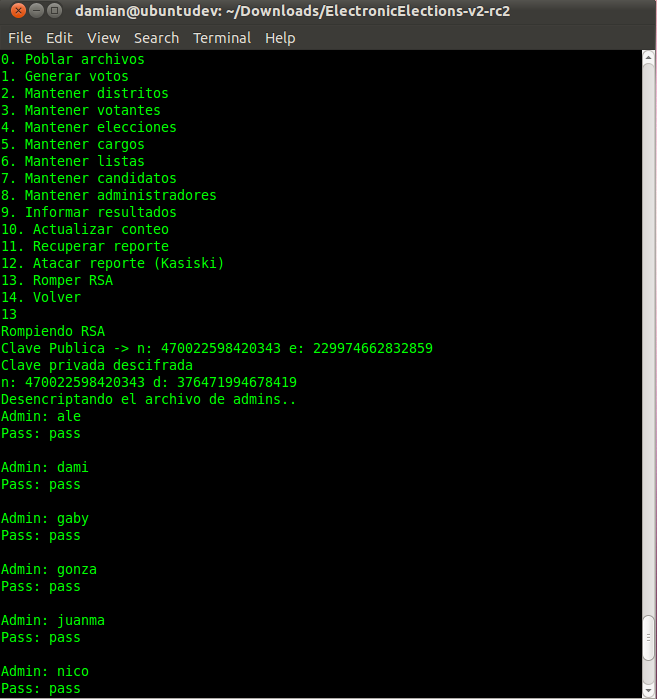
1. Imprimo al votante:  
   

**Imprime todos los votantes del archivo.**

## Romper RSA

Para romper el sistema criptográfico RSA, se debe seleccionar la opción 13 del menú. En ese momento se comienza el proceso de descomposición del número **n** de la clave pública en los números **p** y **q** que los componen.

Finalmente, se obtiene d, que junto con n conforma la clave privada y se muestra cómo se pueden desencriptar las passwords del archivo de administradores usando esta clave privada.



**Output al romper RSA**