

# Manual de usuario

---

## Índice

Introducción .....	2
Instalación y Compilación.....	3
Pre-requisitos .....	3
Generación de ejecutable.....	3
Generación de archivos de texto: Run Script. ....	3
Ejemplos de uso.....	4
Menú Principal.....	5
Generación de archivos .....	6
Votación.....	8
Reportes .....	8
Recuperación de reporte.....	10
ABM .....	11
Romper RSA.....	14

## 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 prerequisites 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
<code>sudo apt-get install tar</code>

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

Shell
<code>sudo apt-get install g++</code>

- 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
<code>tar xfvz ElectronicElections.tar.gz</code>

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

Shell
<code>cd ElectronicElections/Release</code>

- Compilación:

Shell
<code>make all</code>

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
<code>python data.py</code>

**Nota:** Para este comando es necesario tener instalado python, como fue nombrado en la sección de prerequisites, 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 raíz del proyecto (*/ElectronicElections*). Para esto, ejecutamos la siguiente instrucción que copiará el archivo ejecutable al directorio deseado, de la siguiente forma:

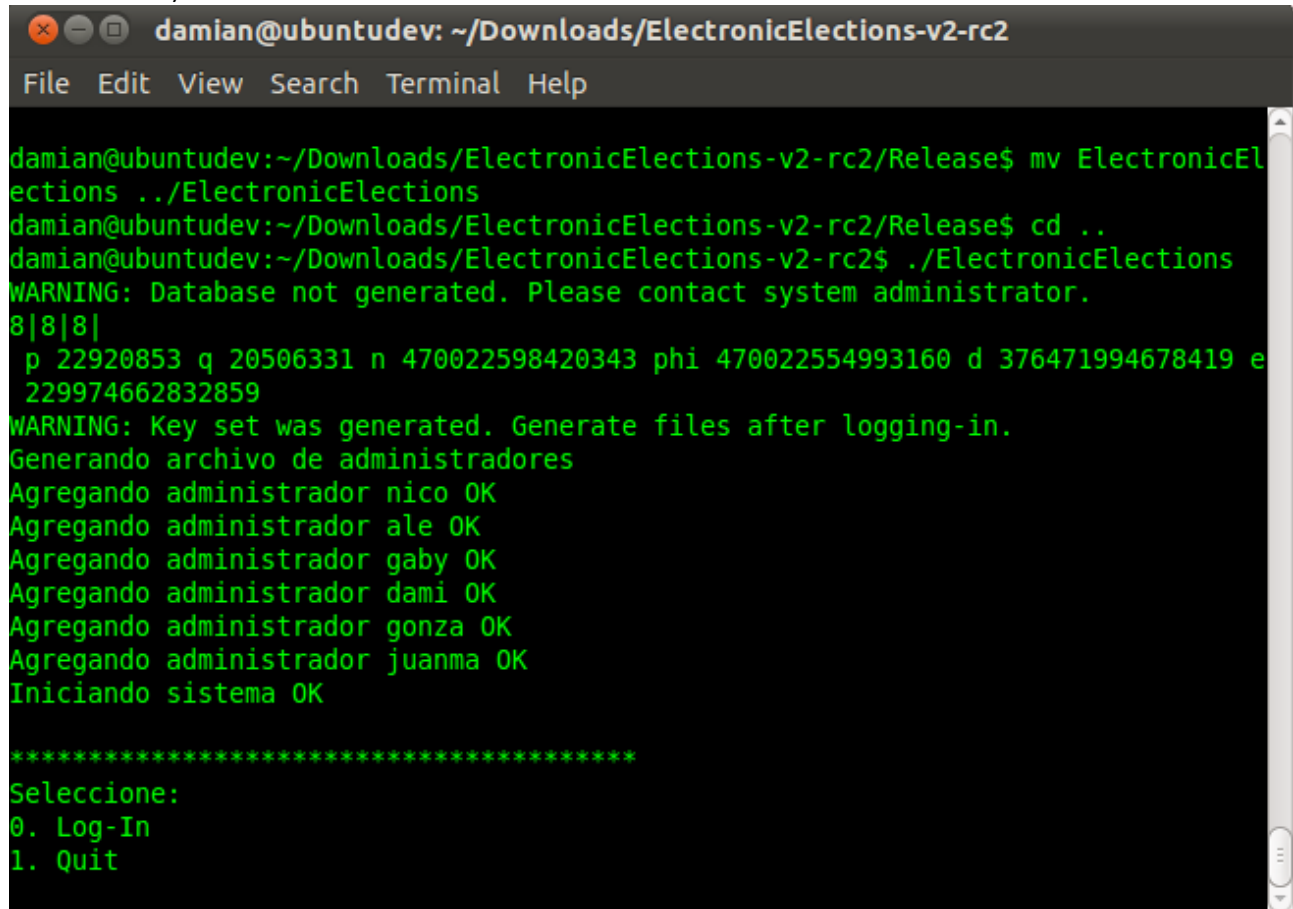
Shell
<code>mv ElectronicElections ../ElectronicElections</code>

Ahora sí, se puede ejecutar la aplicación:

Shell
<code>./ElectronicElections</code>

## Menú Principal

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

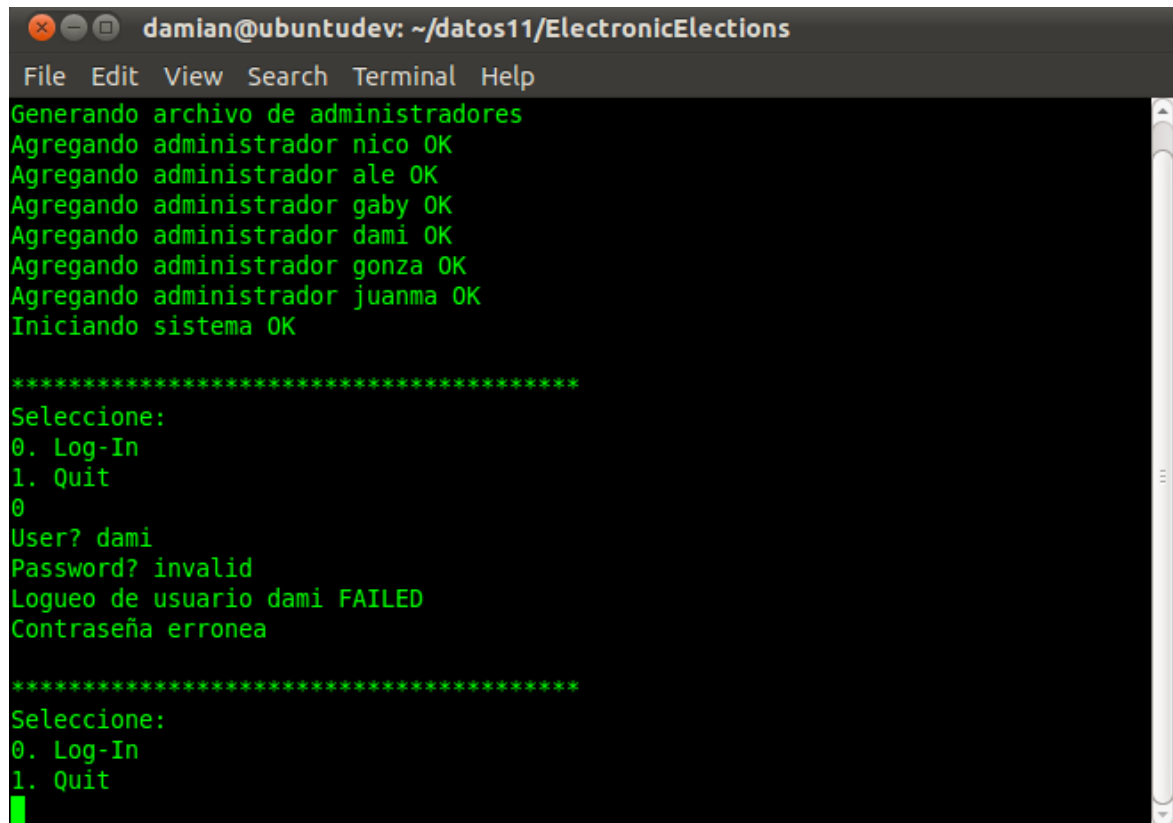


```
damian@ubuntudev: ~/Downloads/ElectronicElections-v2-rc2
File Edit View Search Terminal Help

damian@ubuntudev:~/Downloads/ElectronicElections-v2-rc2/Release$ mv ElectronicEl
ections ../ElectronicElections
damian@ubuntudev:~/Downloads/ElectronicElections-v2-rc2/Release$ cd ..
damian@ubuntudev:~/Downloads/ElectronicElections-v2-rc2$ ./ElectronicElections
WARNING: Database not generated. Please contact system administrator.
8|8|8|
p 22920853 q 20506331 n 470022598420343 phi 470022554993160 d 376471994678419 e
229974662832859
WARNING: Key set was generated. Generate files after logging-in.
Generando archivo de administradores
Agregando administrador nico OK
Agregando administrador ale OK
Agregando administrador gaby OK
Agregando administrador dami OK
Agregando administrador gonza OK
Agregando administrador juanma OK
Iniciando sistema OK

*****
Seleccione:
0. Log-In
1. Quit
```

1. Seleccionamos la opción 0 “Log-In”, para loguearse en la aplicación y poder generar los archivos.  
Pruebo con un usuario falso:

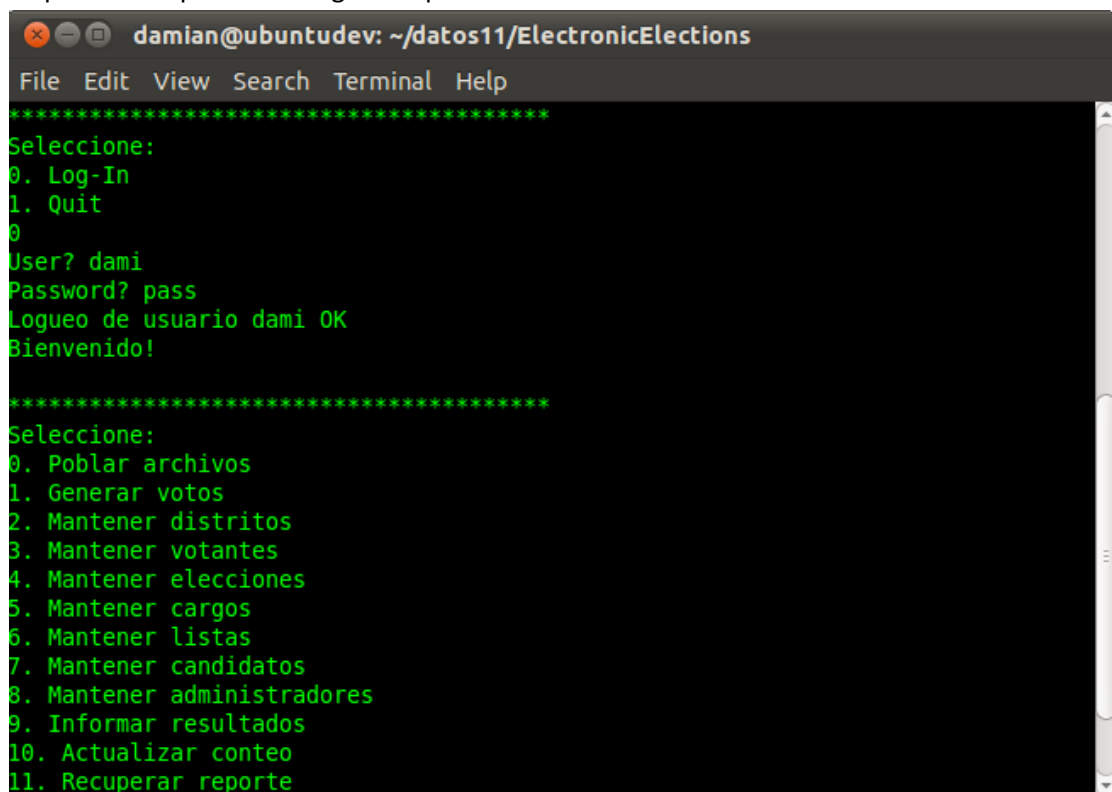


```
damian@ubuntudev: ~/datos11/ElectronicElections
File Edit View Search Terminal Help
Generando archivo de administradores
Agregando administrador nico OK
Agregando administrador ale OK
Agregando administrador gaby OK
Agregando administrador dami OK
Agregando administrador gonza OK
Agregando administrador juanma OK
Iniciando sistema OK

*****
Seleccione:
0. Log-In
1. Quit
0
User? dami
Password? invalid
Logueo de usuario dami FAILED
Contraseña erronea

*****
Seleccione:
0. Log-In
1. Quit
0
```

2. Se puede ver que falló el log-in. Se prueba con un usuario real:



```
damian@ubuntudev: ~/datos11/ElectronicElections
File Edit View Search Terminal Help
*****
Seleccione:
0. Log-In
1. Quit
0
User? dami
Password? pass
Logueo de usuario dami OK
Bienvenido!

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
```

## 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.

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
Agregando candidato 10829566 OK
Agregando candidato 69734404 OK
Agregando candidato 76471216 OK
Agregando candidato 85754691 OK
Agregando candidato 42701609 OK
Agregando candidato 35313132 OK
Agregando candidato 40088475 OK
Agregando candidato 88916504 OK
Agregando candidato 12633483 OK
Agregando candidato 43339625 OK
Agregando candidato 58441182 OK
Agregando candidato 72833929 OK
Agregando candidato 70219925 OK
Agregando candidato 54602197 OK
Generando archivo de votantes
Generando archivo de cargos
Finalizando carga archivos. OK

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
█
```

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.

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
Votando: 97606807 OK
Votando: 97608695 OK
Votando: 97609573 OK
Votando: 97610643 OK
Votando: 97612100 OK
Votando: 97614289 OK
Votando: 97616369 OK
Votando: 97617374 OK
Votando: 97620331 OK
Votando: 97621635 OK
Votando: 97621863 OK
Votando: 97624964 OK
Votando: 97625766 OK
Votando: 97627896 OK
Votando: 97630590 OK
Votando: 97630854 OK
Votando: 97632005 OK

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver

```

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):

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
Votando: 97620331 OK
Votando: 97621635 OK
Votando: 97621863 OK
Votando: 97624964 OK
Votando: 97625766 OK
Votando: 97627896 OK
Votando: 97630590 OK
Votando: 97630854 OK
Votando: 97632005 OK

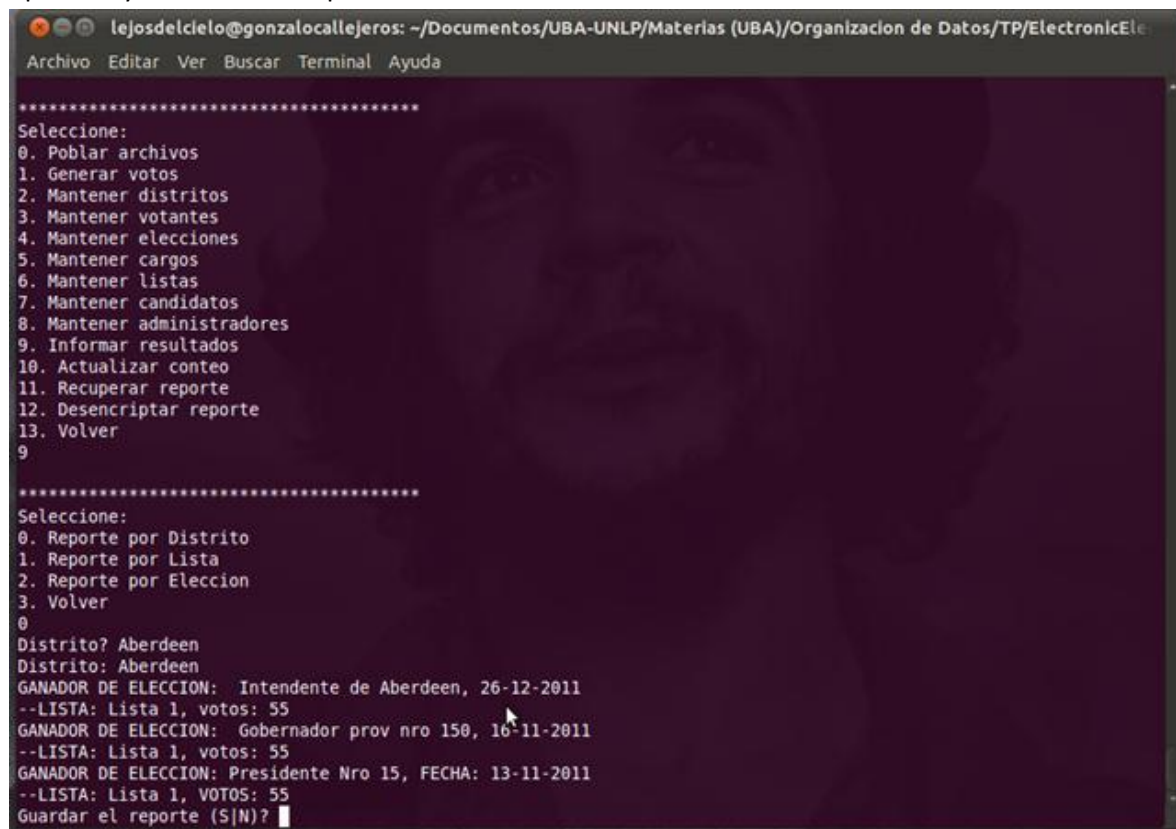
*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
9

*****
Seleccione:
0. Reporte por Distrito
1. Reporte por Lista
2. Reporte por Eleccion
3. Volver

```



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:



```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desenscriptar reporte
13. Volver
9

*****
Seleccione:
0. Reporte por Distrito
1. Reporte por Lista
2. Reporte por Eleccion
3. Volver
0
Distrito? Aberdeen
Distrito: Aberdeen
GANADOR DE ELECCION: Intendente de Aberdeen, 26-12-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Gobernador prov nro 150, 16-11-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Presidente Nro 15, FECHA: 13-11-2011
--LISTA: Lista 1, VOTOS: 55
Guardar el reporte (S|N)?
```

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**):

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
9

*****
Seleccione:
0. Reporte por Distrito
1. Reporte por Lista
2. Reporte por Eleccion
3. Volver
0
Distrito? Aberdeen
Distrito: Aberdeen
GANADOR DE ELECCION: Intendente de Aberdeen, 26-12-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Gobernador prov nro 150, 16-11-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Presidente Nro 15, FECHA: 13-11-2011
--LISTA: Lista 1, VOTOS: 55
Guardar el reporte (S|N)? s
Nombre archivo? reporteAberdeen
Password para el archivo. (caracteres imprimibles)? passarchivo

*****
Seleccione:
0. Reporte por Distrito
1. Reporte por Lista
2. Reporte por Eleccion
3. Volver

```

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:

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Gobernador prov nro 150, 16-11-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Presidente Nro 15, FECHA: 13-11-2011
--LISTA: Lista 1, VOTOS: 55
Guardar el reporte (S|N)? s
Nombre archivo? reporteAberdeen
Password para el archivo. (caracteres imprimibles)? passarchivo

*****
Seleccione:
0. Reporte por Distrito
1. Reporte por Lista
2. Reporte por Eleccion
3. Volver
3

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
11
Nombre archivo? 
```

Se ingresan los datos del archivo guardado previamente.

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectronicEle
Archivo Editar Ver Buscar Terminal Ayuda
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
11
Nombre archivo? reporteAberdeen
Password para el archivo. (caracteres imprimibles)? passarchivo
GANADOR DE ELECCION: Intendente de Aberdeen, 26-12-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Gobernador prov nro 150, 16-11-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Presidente Nro 15, FECHA: 13-11-2011
--LISTA: Lista 1, VOTOS: 55

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver

```

El reporte se recuperó correctamente.

## ABM

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

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectronicEle
Archivo Editar Ver Buscar Terminal Ayuda
Password para el archivo. (caracteres imprimibles)? passarchivo
GANADOR DE ELECCION: Intendente de Aberdeen, 26-12-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Gobernador prov nro 150, 16-11-2011
--LISTA: Lista 1, votos: 55
GANADOR DE ELECCION: Presidente Nro 15, FECHA: 13-11-2011
--LISTA: Lista 1, VOTOS: 55

*****
Seleccione:
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desencriptar reporte
13. Volver
3

*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver

```

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:

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Desenscriptar reporte
13. Volver
3
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
0
Distrito? Watertown
DNI? 12345678
Direccion? Cabildo 1256
Contraseña? 1234
Nombre? Gabriel
Agregando votante 12345678 OK
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
1
```

2. Modificar votante "12345678" recién ingresado. Se modificará el domicilio:

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle
Archivo Editar Ver Buscar Terminal Ayuda
Distrito? Watertown
DNI? 12345678
Direccion? Cabildo 1256
Contraseña? 1234
Nombre? Gabriel
Agregando votante 12345678 OK
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
1
DNI? 12345678
*****
Seleccione:
0. Cambio de nombre
1. Cambio de domicilio
2. Cambio de distrito
3. Cambio de clave
4. Volver
1
Nueva direccion? Juramento 2234
*****
Seleccione:
0. Cambio de nombre
1. Cambio de domicilio
2. Cambio de distrito
3. Cambio de clave
4. Volver
1
```

**Cambio correctamente el domicilio.**

3. Eliminar el votante "12345678" (recientemente creado en el paso 1):



```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectronicEle
Archivo Editar Ver Buscar Terminal Ayuda
2. Cambio de distrito
3. Cambio de clave
4. Volver
1
Nueva direccion? Juramento 2234
*****
Seleccione:
0. Cambio de nombre
1. Cambio de domicilio
2. Cambio de distrito
3. Cambio de clave
4. Volver
4
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
2
DNI? 12345678
Votante eliminado correctamente!
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver

```

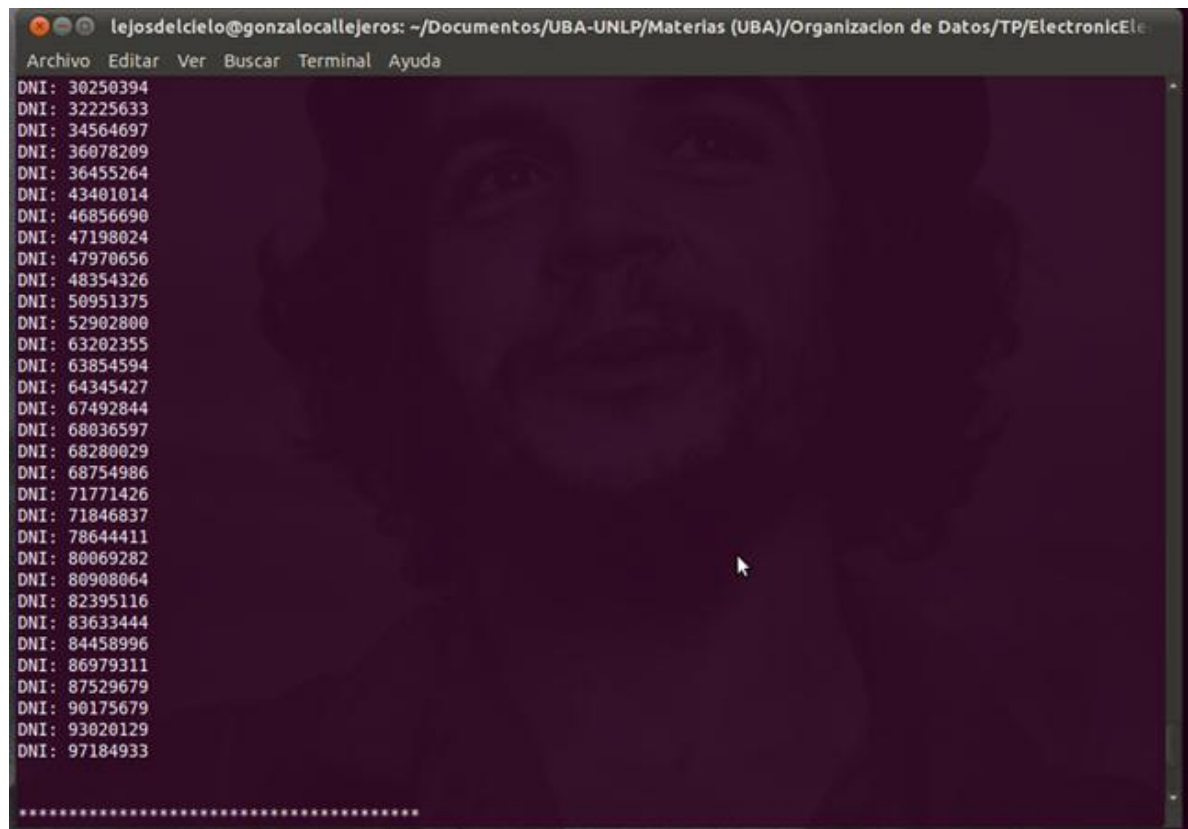
Se eliminó correctamente el votante “12345678”, de modo que si ahora quisiera modificarlo, me debería mostrar un error:

```
lejosdelcielo@gonzalocallejeros: ~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectronicEle
Archivo Editar Ver Buscar Terminal Ayuda
4. Volver
4
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
2
DNI? 12345678
Votante eliminado correctamente!
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver
1
DNI? 12345678
Votante no encontrado!
*****
Seleccione:
0. Agregar votante
1. Modificar votante
2. Eliminar votante
3. Imprimir votante
4. Volver

```

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

4. Imprimo al votante:



A screenshot of a terminal window. The title bar shows the user 'lejosdelcielo@gonzalocallejeros' and the path '~/Documentos/UBA-UNLP/Materias (UBA)/Organizacion de Datos/TP/ElectroncEle'. The menu bar includes 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal content displays a list of 30 DNI numbers, each preceded by 'DNI:'. The numbers are: 30250394, 32225633, 34564697, 36078209, 36455264, 43401014, 46856690, 47198024, 47970656, 48354326, 50951375, 52902800, 63202355, 63854594, 64345427, 67492844, 68036597, 68280029, 68754986, 71771426, 71846837, 78644411, 80069282, 80908064, 82395116, 83633444, 84458996, 86979311, 87529679, 90175679, 93020129, and 97184933. A line of asterisks is visible at the bottom of the list.

```
DNI: 30250394
DNI: 32225633
DNI: 34564697
DNI: 36078209
DNI: 36455264
DNI: 43401014
DNI: 46856690
DNI: 47198024
DNI: 47970656
DNI: 48354326
DNI: 50951375
DNI: 52902800
DNI: 63202355
DNI: 63854594
DNI: 64345427
DNI: 67492844
DNI: 68036597
DNI: 68280029
DNI: 68754986
DNI: 71771426
DNI: 71846837
DNI: 78644411
DNI: 80069282
DNI: 80908064
DNI: 82395116
DNI: 83633444
DNI: 84458996
DNI: 86979311
DNI: 87529679
DNI: 90175679
DNI: 93020129
DNI: 97184933
*****
```

**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.

```
damian@ubuntudev: ~/Downloads/ElectronicElections-v2-rc2
File Edit View Search Terminal Help
0. Poblar archivos
1. Generar votos
2. Mantener distritos
3. Mantener votantes
4. Mantener elecciones
5. Mantener cargos
6. Mantener listas
7. Mantener candidatos
8. Mantener administradores
9. Informar resultados
10. Actualizar conteo
11. Recuperar reporte
12. Atacar reporte (Kasiski)
13. Romper RSA
14. Volver
13
Rompiendo RSA
Clave Publica -> n: 470022598420343 e: 229974662832859
Clave privada descifrada
n: 470022598420343 d: 376471994678419
Desencriptando el archivo de admins..
Admin: ale
Pass: pass

Admin: dami
Pass: pass

Admin: gaby
Pass: pass

Admin: gonza
Pass: pass

Admin: juanma
Pass: pass

Admin: nico
Pass: pass
```

Output al romper RSA