Trabajo Práctico - Etapa 1
Voto Electrónico

Martín Hernán Gómez, *Padrón Nro. 85.780*
martinhgomez@yahoo.com.ar

Ignacio Marambio Catán, *Padrón Nro. 82.694*
ignacio.marambio@gmail.com

Martín Eduardo Quiroz, *Padrón Nro. 86.012*
martinedq@yahoo.com.ar

Daniel Shlufman, *Padrón Nro. 88.040*
incorporado@gmail.com

Lucas Damian Tarcetti, *Padrón Nro. 87.165*
lucas.tarcetti@yahoo.com.ar

2do. Cuatrimestre de 2011
75.06 Organización de Datos – Cátedra Lic. Arturo Servetto
Facultad de Ingeniería, Universidad de Buenos Aires

26/10/11

Índice

1. Introducción

El trabajo consiste crear una aplicación capaz de mantener un sistema de voto electrónico.

1.1. Objetivos

El objetivo de este trabajo práctico es que la aplicación sea capaz de mantener información sobre las entidades que componen el sistema de votaciones (votantes, elecciones, candidatos, etc.), y de proveer la posibilidad a un votante de emitir su voto para la correspondiente elección.

2. Documentación técnica

2.1. Elección del lenguaje de programación

La resolución del trabajo práctico debe será realizada en plataforma Linux y en lenguaje C++, aprovechando el uso de la programación orientada a objetos.

2.2. Entidades

- Distrito ((distrito)i)
- Votante ((DNI)i, NombreyApellido, clave, domicilio, (distrito)ie, ((eleccion)ie)*)
- Eleccion ((fecha, (cargo)ie)i, ((distrito)ie)+)
- Lista (((eleccion)ie, nombre)i, cantidadVotos)
- Candidato (((lista)ie, (votante)ie, (cargo)ie)i)
- Cargo ((cargo)i)
- Administrador ((usuario)i, clave)

2.3. Estructuras de datos

Las estructuras principales elegidas para este trabajo han sido elegidas según la necesidad de cada entidad. Las mismas son:

- Árbol B+
- Dispersión Extensible
- Archivos de Bloques
- Registros Variables

2.4. Funcionalidades

En el ámbito del administrador se encuentran las siguientes funcionalidades:

- Mantener Distritos
- Mantener Votantes
- Mantener Elecciones
- Mantener Cargos
- Mantener Listas
- Mantener Candidatos
- Informar Resultados

2.5. Descripción de la arquitectura utilizada

Para una mejor observación de los diagramas de clases de la arquitectura utilizada en el programa, las mismas se encuentran documentadas en un archivo externo junto con su descripción, se puede acceder a el a través del archivo '00 Index.html', el mismo se encuentra en la carpeta 'Documentación'. Desde allí se puede navegar a través de todas las clases existentes.

2.6. Descripción de cada clase utilizada

A continuación se enumeran las principales clases de la aplicación, no refiréndonos a sus nombres de archivo sino con su nombre conceptual.

- Clase ArbolBMas: Se utiliza para guardar las listas de votación y para la confección de informes.
- Clase Dispersión: Se utiliza para almacenar todas las demás entidades que no sean las listas de votación.
- Clase Archivo en Bloques: Se usa para darle un sustento en disco a las clases de Árbol B+ y de Dispesión. Ofrece una persistencia en disco en un archivo de bloques.
- Clases de Entidades: Las mismas se utilizan para instanciar cada entidad necesaria al momento de crear una votación. Las mismas incluyen: Distrito, Votante, Eleccion, Lista, Candidato, Cargo, Administrador.

2.7. Justificación de uso de cada clase utilizada

El uso del *Árbol B+* se eligió principalmente debido a la opción de poder hacer búsquedas parciales y además a la ventaja de poder acceder secuencialmente a los datos de forma ordenada. El uso del *archivo de dispersión* se eligió debido a que usa la menor cantidad de accesos posibles (solo un acceso) haciendo que se optimice el uso de estos archivos, al ser los mas accedidos en disco. El uso del *archivo de bloques* se eligió por ser el más compatible con respecto a la persistencia del Árbol B+ y del archivo de dispersión, haciendo mas efectivo el uso de los mismos.

2.8. Archivos auxiliares

Definiciones lógicas y físicas de todos los archivos que se utilicen (datos maestros, índices, trabajo, control, etc).Descripción de la organización de cada uno de los archivos. Para qué se utiliza. Por qué se utiliza (base teórica).

Dentro de los archivos utilizados para el funcionamiento del programa disponemos de las siguientes estructuras auxiliares:

- Archivo de configuración: El mismo se usa para obtener las rutas de los archivos de dispersión, archivo del árbol, tamaños de cubetas y de nodos.
- Índice: El índice se usa para la obtención de los informes de votaciones por distintos criterios de una misma base de datos.
- Archivo de control: Se utiliza para poder persistir datos referentes a las estructuras de control de las estructuras, como por ejemplo la tabla de dispersión dentro de la estructuras de dispersión.
- Archivo de password: Guarda el *user* y *pass* perteneciente al administrador de votos.

2.9. Planificación de tareas

Planificación (identificación de tareas, estimación de duración y asignación)

A grandes rasgos la planificación del proyecto se realizó dentro de las cinco semanas la siguiente manera:

- Semana 1: Planeamiento del problema, elección de las distintas estructuras para las entidades existentes, configuración del sistema operativo, herramientas de compilación, IDE's, etc. Para su correcto funcionamiento en el sistema Linux. Duración aproximada: 1 semana.
- Semana 2: Construcción de las entidades, creación de sus respectivas clases (1 semana). Creación de la clase encargada del manejo en disco, manejador de archivos (1 semana). Comienzo de creación de la clase de Árbol B+ (4 semanas).
- Semana 3: Comienzo de creación de la clase de Dispersión (3 semanas). Creación de la clase encargada del archivo de bloques (2 semanas). Creación de clase bucket y creación de clase nodo.
- Semana 4: Creación de pruebas individuales e integrales (1 semana). Serialización e hidratación de datos (1 semana). Creación del archivo de buckets (1 semana).
- Semana 5: Integración de los distintos módulos (1 semana). Creación de la lógica de votación (1 semana). Implementación de una interfaz para el usuario (1 semana).

2.10. Bugs conocidos

A continuación se enumeran ciertas situaciones donde el programa podría presentar dificultades en su proceso:

- La fechas deben tener tener el formato: aaaa/mm/dd para poder procesarse correctamente.
- Si el archivo de configuración no tiene el delimitador '//' dentro del archivo, el mismo no parsea ningún dato, ya que toma al archivo entero como comentario
- El archivo de bloques debido a su estructura interna debe tener un tamaño de bloque que sea múltiplo de 4 bytes, si no es de esta forma podría referenciar erroneamente a un bloque. Esto se solucionó validando el tamaño de bloque al iniciar un archivo.
- En una elección determianda se podría agregar cualquier distrito sin que se verifique si realmente existe.
- El borrado de algún archivo de control, configuración y/o datos en tiempo de ejecución llevará a una malfunción del programa.

2.11. Archivos de Control para las Entidades

2.11.1. Archivos de Control

Se encuentran todos dentro de un directorio, especificado a través de un archivo de configuración de la aplicación, y pueden tener jerarquía de subdirectorios interna. Es donde se guarda toda la información necesaria para poder funcionar.

2.11.2. Archivos con resultados

Como respuesta a toda interacción, el sistema generará archivos de registro de operaciones (LOGs) en el directorio donde se llame a la aplicación.

3. Parte teórica

En la siguiente sección se enumeran distintos conceptos teóricos acerca de las estructuras usadas en la resolución del TP.

3.1. Física - Organización

3.1.1. Organización de registros

- La longitud de un registro y/o de un campo variable se delimita con el uso de un indicador de longitud, el cual se antepone a los datos pertenecientes al registro o campo. De esta forma se puede conocer donde termina la sección de datos.
- En todos los casos se guarda como mínimo la información correspondiente a la longitud del segmento de datos pudiendo, en ciertos casos, guardarse mas información, según sea la estructura.

3.1.2. Consideraciones acerca del Archivo de Bloques

1. Los bloques tienen tamaño fijo, determinado por primera y única vez al crearse el archivo.
2. Existen 4 tipos de bloques: Data, Metadata, Removed y Head
3. Head: Existe un solo bloque de este tipo por archivo y siempre se ubica al principo del mismo (en la posición 0).

   El bloque Head tiene en su estructura:

   |currmetadata (int)|maxblocknum(int)|blocksize(int)| Espacio sin uso (int)|... ...|Espacio sin uso (int)|
4. Data: Este bloque se usa íntegramente para guardar datos del usuario

   El bloque Data tiene en su estructura:

   |datos(int)|...|datos(int)|...|datos(int)| (Todo el espacio reservado para datos, sin metadata).
5. Metadata: Bloque que se encarga del control de los bloques de datos borrados (Removed). Aquí se guardan las referencias a bloques removed.

   El bloque de Metadata tiene en su estructura:

   | Metadata Anterior(int)| currPos(int)| ID bloqLibre (int)| ...| ID bloqLibre (int)|
6. Removed: Son bloques de datos que han sido borrados por el usuario, no se utiliza ningún atributo para identificarlos, los mismos están referenciados en el bloque de metadata como 'libre'.
7. Internamente todos los atributos de metadata son manejados como int. En el caso donde desde afuera se piden los bloques de datos el bloque se obtiene como un char*.
8. El currpos empieza desde el primer byte del bloque, incluyendo los bytes cabezeras. O sea que el 1er dato de metadata está en el byte 8 (2*sizeof(int))
9. Cada vez que cambia el 'currmetadata' o 'maxblocknum' se escribe en disco con serializehead (que escribe 2 veces en disco por cada vez que se lo llama)
10. Cada vez que cambia el 'currpos' se escribe en disco (se escribe en el bloque de metadata). Esto sucede al pedir un bloque nuevo o al borrar un bloque de datos
11. Está contemplado el caso donde el metadata actual no tiene bloques libres, y entonces este mismo pasa a ser un bloque disponible (Caso límite).
12. Está contemplado el caso donde borro un data, pero el metadata actual está totalmente lleno, pasando el bloque 'D' a ser un bloque 'M' (Caso límite).
13. Si pido un metadata nuevo tengo que ver si es el 1ro, si esto es así, su valor ."anterior"(posición [1] dentro del bloque de int's) tiene que ser = Cero

14. No hace falta un getblock de 'R' porque esos bloques siempre van a ser accedidos a través de newblock (con parámetro 'D' o 'M')

15. No hace falta un newblock de 'R' porque esos bloques siempre van a ser creados a través de delblock

16. En una primera instancia, se propuso etiquetar cada bloque para su identificación. Pero luego, para simplificar el funcionamiento y para no invadir espacio en el bloque de Datos, se optó por no usar etiquetas en los bloques.

3.2. Índices - Búsqueda

3.2.1. Hashing

Función de hashing utilizada. Criterio de elección.

Para una rápida recuperación de la información se decide organizar dicho archivo con el método de dispersión extensible. Se utiliza un hashing extensible de valores sufijos. La función de hashing utilizada es f(x) = (x) mod (tamaño de tabla)

3.2.2. Árbol B+

Nuestro arbol B+ es relativamente genérico, a excepción de la clave de ordenamiento que es invariablemente un string, los datos son una entidad genérica y en general no me interesa que se guarda ahi.

Está implementado de tal manera que también esta separado casi completamente de la parte que lidia con el almacenamiento teniendo 2 precondiciones ineludibles. el lugar donde se encuentra alojada la raíz debe ser invariante y las estructuras que representan a los punteros a los bloques deben ser representadas como enteros.

La separación se logró mediante la clase ffile y tuvo tanto éxito que con mínimas modificaciones fue posible pasar de un árbol cuyo almacenamiento era la memoria a otro cuyo almacenamiento era un archivo de bloques.

El árbol esta implementado en 4 clases diferentes, la ya mencionada ffile, bplustree, inner _node y leaf_node estando estas ultimas intimamente relacionadas de manera tal que una esta declarada como friend de la otra. Esta decision se tomo para no exponer cosas criticas de las clases que necesariamente tenian que usarse entre inner_node y leaf_node.

En memoria, estas clases utilizan un vector de pares de enteros y cadenas de caracteres para los nodos internos (la clase inner_node) y pares de cadenas y vectores en las hojas (la clase leaf_node). Estas 2 clases, al serializarse se transforman en una cadena larga de caracteres (que se guarda en un vector) representada por pares longitud, datos. Ademas a esto se agrega un entero mas que representa la cantidad de pares, longitud, datos que existen en la cadena en adicion a un encabezado que es una I o una L segun sea el nodo un nodo interno o una hoja y un par de enteros mas que representan el nodo que contiene los datos cuya clave es mayor al nodo actual o el nodo que tiene datos menor al primer par del nodo.

En este momento, el árbol se comporta como un árbol B+ clásico para los agregados pero no hace rebalanceos en caso de los borrados.

Mas alla de los enteros que tienen tamaño fijo, el resto de las estructuras son dinamicas. El objetivo de esta implementacion fue utilizar la mayor cantidad de las funciones de la STL que fueran posible y, como desafortunadamente, la STL, si bien tiene una funcion de busqueda que funciona en contenedores como los vectores utilizados para almacenar los datos en la memoria de este árbol, ésta solo devuelve si un dato se encuentra o no en el contenedor pero no su posición o sus datos por lo que la búsqueda dentro de los nodos es lineal.

Esto también fue una pre condicion para poder implementar la función que luego de una búsqueda devuelva el dato inmediatamente mayor al ultimo devuelto.

Para ordenar los datos en memoria, sin embargo si se utiliza la función sort() del grupo de funciones incluidas en <algorithms>

4. Documentación de usuario

4.1. Instalación del sistema

La instalación usará un archivo makefile, el cual realizará automaticamente toda la operación de compilación de todos los archivos de código fuente, recorriendo todas las subcarpetas necesarias para una operación exitosa.

Para la instalación del sistema debemos descomprimir el archivo conteniendo el código fuente en la carpeta donde se desea realizar la misma. Una vez realizada la descompresión debemos ejecutar por consola, situados en la ruta elegida, el comando *make* el cual compilará todos los archivos fuente y como consecuencia obtendremos el archivo ejecutable listo para usar.

4.2. Ejecución del sistema

Una vez creado el archivo ejecutable debemos iniciar el programa[1] pasando por parámetro la ruta del archivo de configuración, esto es un requisito obligatorio para comenzar con el programa, mediante los argumentos -c <rutaArchivoConfiguración>. De esta forma, desde el directorio donde se creó el ejecutable, se inicia el sistema:

```
./voto -c ../ArchivosAuxiliares/config.txt
```

Nota: -c es el flag para ubicar el archivo de configuración. Para ver las demás opciones podemos ingreasar al programa con -h

A su vez el archivo de configuración proveerá todos los requisitos necesarios para ubicar los demás archivos relativos al programa, ya sean archivos de datos, control, configuración o el archivo de password.

4.2.1. Interfaz de administrador

Al iniciar el programa el administrador de la votación deberá autenticarse para poder entrar al sistema, una vez ingresado tendrá un menú con opciones donde podrá:

[1] Para iniciar el programa, al administrador se debe autentificar. User: undomiel, Pass: aragorn

- Mantener Distritos.
- Mantener Votantes.
- Mantener Elecciones.
- Mantener Cargos.
- Mantener Listas.
- Mantener Candidatos.
- Informar Resultados.

4.2.2. Interfaz de usuario

Una vez iniciada una votación, se dispondrá de una interfaz para el usuario 'votante'. En esta instancia el votante podrá:

- Autenticarse
- Emitir voto
- Corregir voto
- Informar voto

5. Segunda etapa - Seguridad

5.1. Método de Vigènere

5.1.1. Resolución del método

Se empleará el método para cifrar los reportes generados: Listas, Elección, Distrito.

Para la resolución se necesitará generar una clave k de dimensión n. Cada elemento de la clave pertenece al alfabeto sobre el cual se resuelve el método.

Una opción resulta en considerar al alfabeto como todo el conjunto de los elementos representables con 1 byte, es decir 256 elementos. De esta forma se trabaja con aritmética modular de modulo 256.

Desde el punto de vista de la programación se crearía la clase Vigènere que sería la encargada de realizar la encriptación (y desencriptación) de un documento.

El criptosistema es simétrico por lo que al instanciar la clase se le asignaría la clave que podría ser del tipo vector. Se define implícitamente el tamaño del alfabeto que resulta ser de 256, correspondiente al código ASCII.

La clave se pasa por valor de forma tal que el objeto instanciado tenga un copia interna de la clave y pueda manejarse sin riesgo de que en el caso de ser pasado por referencia se elimine accidentalmente.

La encriptación manejaría strings, recibiría en mensaje y lo cifraría devolviendo el correspondiente criptograma. De esta forma haríamos que se desentienda del origen del objeto que está manejando, que podría ser desde memoria o desde disco.

El descrifrador recibe el criptograma, lo descifra con la clave y devuelve el mensaje como un string.

Hay dos situaciones diferentes en las cuales se debe usar Vigeneré. Una es para cifrar un texto plano. La otra es para cifrar un texto plano y a continuación otro texto plano utilizando la misma instancia de Vigeneré y la misma clave.

En el caso que se quiere cifrar un texto plano solamente con la misma clave y la misma instancia de Vigeneré: para el manejo en bloques Vigenere cuenta con dos variables que contienen la última posición de la clave durante el uso del cifrador y del descifrador, de forma tal que no haya que restringir el mensaje que se desea encriptrar/descencriptar a un tamaño múltiplo del tamaño de la clave porque cada vez que se llega a la última posición del cifrador/descifrador se reinicia esta variable.

5.1.2. Criptoanálisis

Para realizar el criptoanálisis una opción es resolverlo empleando el método de Kasiski.

1. Desarrollo del método:

El método consiste en realizar una búsqueda de fragmentos de bits repetidos para luego calcular la distancia que los separa. A partir de ello se obtiene el máximo común divisor MCD para obtener la dimensión de la clave.

Una vez obtenida se procede a realizar un análisis de frecuencia de caracteres en una forma especial. Se tienen tantos vectores (o listas) como lo indique la dimensión de la clave. Se aplica la operación de módulo sobre la posición del elemento en el flujo de caracteres, y se asigna la frecuencia correspondiente

al elemento encontrado en el vector correspondiente, que se identifica por el resultado de la operación módulo.

Luego conociendo previamente el idioma en que se encuentra el criptograma, se procede a buscar los caracteres con mayores frecuencias.

Como tenemos 256 posibilidades, hacemos un prueba sobre un archivo para obtener un histograma de las frecuencias de las apariciones de los códigos ASCII en un texto.

En base a pruebas realizadas por el grupo se obtuvo el siguiente gráfico:

El gráfico que se observa muestra las frecuencias obtenidas en una prueba para los 255 caracteres ASCII. En el gráfico no se puede observar claramente pero se observa que se encuentran entre el 42 y el 126 que corresponde a los caracteres imprimibles. Por otro lado, hay un pico muy elevado que corresponde al caracter 32 que resulta ser el espacio.

Luego se analiza el mismo gráfico pero acotado a los valores imprimibles. En este caso, el caracter con mayor frecuencia es el 32, que resulta ser el espacio, seguido del caracter e (101), el caracter a(97) y por último el caracter o(111). Estos son los más frecuentes y dependiendo del archivo la frecuencia puede variar levemente.

En el texto de prueba se obtuvieron en porcentaje:

- espacio:16 %
- a: 9 %
- e: 10 %
- o: 6,7 %

Es decir que como es esperable las minúsculas son más probables que las mayúsculas, y el caracter espacio es el más probable. Esta información es de suma utilidad al realizar el análisis de frecuencias que requiere el método.

Es destacable que con sólo los caracteres espacio, a, e y o se emplean en el 36 % de un texto.

Finalmente se descifra el mensaje.

5.2. Método RSA

5.2.1. Resolución del método

Se empleará el método para cifrar los datos de los votantes.

El sistema empieza generando por primera y única vez el par de claves privada y pública que son guardadas en un archivo en disco.

Utilizacion de campos finitos en el algoritmo de RSA Se utilizará el algoritmo de euclides extendido para generar el inverso multiplicativo o sea el número que se utilizará para desencriptar y que por lo tanto compondrá la clave privada.

También se usará exponenciación por cuadrados para la operación a^b mod q .

Por esta razón se debe tener especial cuidado en la cantidad de bits que se utilizará para representar los números ya que si se trabaja con números demasiado grandes las operaciones de campos finitos pueden fallar. Por esto el enunciado al pedir que se ingrese el tamaño del número da la posibilidad de limitar este tamaño.

Limitaremos el tamaño de los números primos a entre 3 y 97. Siendo los demás números resultados de operaciones de campos finitos de tamaño manejable por el algoritmo de RSA.

Objeto RSA Desde el punto de vista de la programación se crearía la clase RSA que será la encargada de realizar la encriptación/desencriptación de los datos del votante.

Encriptación El votante instancia un objeto RSA con sus atributos cargados apartir de un archivo.

La encriptación se realiza sobre el string serializado del votante.

Desde serializar se llama al método de encriptación de RSA pasándole el string serializado.

Se toma cada caracter del string y se lo convierte en número entero.

Se realizan las operaciones de campos finitos y se devuelve un numero grande.

Se almacena el número grande en un buffer auxiliar.

Luego de almacenar todos los caracteres transformados en numeros en el buffer auxiliar, se devuelve el string asociado a este buffer de numeros grandes.

Todos los votantes se cifran con la misma clave, ésta se genera una única vez y se almacena en un archivo aparte. Cada vez que se desee encriptar se buscará la clave pública en el archivo. De esta forma al desencriptar se evita tener que realizar una búsqueda de la clave que cifró cada votante ya que es la misma para todos.

Desencriptación El deserializar de votante recibe el string serializado y encriptado.

El deserializar de votante instancia un objeto RSA.

Se inicializan los atributos del RSA apartir de la clave privada y pública guardadas en un archivo.

Se desencripta el string que recibió el deserializar de votante a partir del método desencriptar de RSA.

Desencriptar recibe el string serializado y encriptado y procede a desencriptar cada caracter del string casteado a un numero grande.

Se realizan las operaciones de campos finitos y se devuelve un numero entero.

Cada número entero (caracter desencriptado) se carga en un string. Al final se devuelve este string desencriptado que es el que el deserializar procede a hidratar.

5.2.2. Criptoanálisis

Se genera una lista de números primos entre 3 y 97 dado que hemos decidido acotar los números primos a este rango.

Se realizan multiplicaciones entre todos los numeros hasta lograr encontrar el par que de como resultado el n de las claves.

El ataque por fuerza bruta es el más sencillo y eficaz dado el pequeño rango de números posibles. Por eso se recomienda que los números primos sean de 1024 bits al menos así dificulta la capacidad de la computadora de realizar operaciones matemáticas en un tiempo razonable o útil.

6. Corridas de prueba - 1er Etapa

A continuación se detallan las pruebas realizadas sobre el funcionamiento del programa. Se emplearon las pruebas detalladas en el enunciado del informe, las cuales pasaron con éxito.

Corridas de prueba

```
Ingreso:
INGRESO APROBADO
Bienvenido al sistama de gestion de elecciones
¿ Desea eliminar la base de datos y comenzar de 0? S/N
S

Menú principal:
Opciones:

1) Mantener Distritos
2) Mantener Votantes
3) Mantener Elecciones
4) Mantener Cargos
5) Mantener Listas
6) Mantener Candidatos
7) Informar Resultados
8) Habilitar Elecciones
9) Habilitar Votantes para elección
10) salir
Opcion: 1

Menú de Distrito:
Opciones:

1) Alta Distrito
2) Baja Distrito
3) Modificar Distrito
4) Volver atrás
5) Ver Distritos
Opcion: 1

Ingrese el nombre del distrito:
Misiones

Operacion OK

Menú de Votante:
Opciones:

1) Alta Votante
2) Baja Votante
```

```
3) Modificar Votante
4) Volver atrás
5) Alta Automática
6) Ver votantes
Opcion: 1

Ingrese el DNI del votante: 14254983

Ingrese nombre: Daniel

Ingrese apellido: Martinez

Ingrese la clave: 8754

Clave: 8754
Ingrese el domicilio: San Luis 2728

dom: San Luis 2728
Ingrese el nombre del distrito:
Misiones

Distrito: Misiones
Operacion OK

Opciones:

1) Alta Votante
2) Baja Votante
3) Modificar Votante
4) Volver atrás
5) Alta Automática
6) Ver votantes
Opcion: 5

Ingrese la cantidad de votantes a ingresar: 3
 - Nombre: Mariel Iacub
 - DNI: 1
 - Password: 8335
 - Domicilio: Haiti 2793
 - Distrito: Jujuy
Elecciones Anteriores:
----------------------
El votante no participo de ninguna eleccion a la fecha

 - Nombre: Ivan Lopez
 - DNI: 2
 - Password: 6498
 - Domicilio: Montiel 3061
 - Distrito: Santa Fe
Elecciones Anteriores:
```

```
----------------------
El votante no participo de ninguna eleccion a la fecha

 - Nombre: Fernanda Rodriguez
 - DNI: 3
 - Password: 4940
 - Domicilio: Udaondo 1425
 - Distrito: Ciudad Autonoma de Buenos Aires
Elecciones Anteriores:
----------------------
El votante no participo de ninguna eleccion a la fecha

Menu de Cargo:
Opciones:

1) Alta Cargo
2) Baja Cargo
3) Modificar Cargo
4) Volver atrás
5) Ver cargos
Opcion: 1

Ingrese el nombre del cargo principal:
Presidente

Desea agregar subcargos? (S/N)S

Ingrese el nombre del subcargo:
Vice Presidente

Desea agregar más subcargos? (ingrese 'S' para seguir)N

Operacion OK

Menú de Elección:
Opciones:

1) Alta Eleccion
2) Baja Eleccion
3) Modificar Eleccion
4) Volver atrás
5) Ver elecciones
Opcion: 1

Ingrese la fecha de la elección: 19991010

Ingrese el cargo: Panadero
No existe cargo/cargo no valido
¿ Desea repetir? (S/N): S
```

```
Ingrese el cargo: Presidente
Ingrese el nombre del distrito:
Panaderia

El distrito no existe

Desea agregar más distritos? (ingrese 'S' para seguir)S

Ingrese el nombre del distrito:
Misiones

Distrito agregado

Desea agregar más distritos? (ingrese 'S' para seguir)N

Operacion OK

Opciones:

1) Alta Eleccion
2) Baja Eleccion
3) Modificar Eleccion
4) Volver atrás
5) Ver elecciones
Opcion: 5


tamaño de la tabla de dispersion: 1
2048 B0 :(free=958) : (cant: 1):
Fecha: 19991010
Cargo Principal: Presidente
Distrito: Misiones


Tabla de hash (size: 1):  0
Tabla de dispersion (size: 1):  1

Menú de Lista:
Opciones:

1) Alta Lista
2) Baja Lista
3) Modificar Lista
4) Volver atrás
5) Ver Listas
Opcion: 1

Ingrese la fecha de la elección: 19991110

Ingrese el cargo: Zapatero
```

```
No existe cargo/cargo no valido
¿ Desea repetir? (S/N): S

Ingrese el cargo: Presidente
Ingrese la lista: Datos
Operación exitosa
Opciones:

1) Alta Lista
2) Baja Lista
3) Modificar Lista
4) Volver atrás
5) Ver Listas
Opcion: 5

19991010   Presidente blanco
19991110   Presidente Datos

Menú Candidato:
Opciones:

1) Alta Candidato
2) Baja Candidato
3) Modificar Candidato
4) Volver atrás
5) Mostrar Candidatos
Opcion: 1

Ingrese el numero de DNI: 1

Ingrese la fecha de la elección: 19991010

Ingrese el cargo: Gobernador

Ingrese el nombre de la lista: FIUBA

Operacion OK

Menú Habilitar Elecciones
Opciones:

1) Habilitar Eleccion
2) Ver elecciones habilitadas
3) Salir
Opcion: 1

Ingrese la fecha de la elección: 19991010

Ingrese el cargo: Presidente
Elección habilitada
```

```
Opciones:

1) Habilitar Eleccion
2) Ver elecciones habilitadas
3) Salir
Opcion: 2



ELECCIONES ACTIVAS
------------------
Eleccion 1
Fecha: 19991010
Cargo Principal: Presidente
----------------------------------------

Menú habilitar votante:
Caso Automático:
Ingrese la cantidad de votos a realizar: 4800

Ingrese modo de votación: Automático (a) o Manual (m)a.
Bienvenido Jessica Michel
Ingrese su Password
INGRESO AUTORIZADO

Las elecciones activas en las que usted emitir su voto son las siguientes
Eleccion 1:
Fecha: 19991010
Cargo Principal: Presidente
---------------
Indique el numero de eleccion en la cual desea sufragar
Usted eligio la eleccion 1
Si es correcto presione s sino n

Estas son sus boletas a elegir
Lista 1
Nombre: ARI
Lista 2
Nombre: Izquierda
Lista 3
Nombre: PJ
Lista 4
Nombre: PRO
Lista 5
Nombre: Socialista
Lista 6
Nombre: UCR
Lista 7
Nombre: blanco
```

```
Elija su boleta en base al numero de opcion indicado
La opcion elegida es: 1
LISTA: ARI
Si esta seguro presione s si desea corregir su voto presione n

Caso Manual:
Ingrese la cantidad de votos a realizar: 1

Ingrese modo de votación: Automático (a) o Manual (m)m

Bienvenido al sistema de voto electronico de los Gutierrez

Ingrese su DNI:
5002
Su dni es: 5002
Presione S para confirmar, N para cancelar
s

Bienvenido Daniel Martinez
Ingrese su Password
5002
INGRESO AUTORIZADO

Las elecciones activas en las que usted emitir su voto son las siguientes
Eleccion 1:
Fecha: 19991010
Cargo Principal: Presidente
---------------
Indique el numero de eleccion en la cual desea sufragar
1
Usted eligio la eleccion 1
Si es correcto presione s sino n
s

Estas son sus boletas a elegir
Lista 1
Nombre: Datos
Lista 2
Nombre: blanco

Elija su boleta en base al numero de opcion indicado
1
La opcion elegida es: 1
LISTA: Datos
Si esta seguro presione s si desea corregir su voto presione n
s

Menú de informes:
Opciones:
```

```
1) Informe por elección
2) Informe por lista
3) Informe por distrito
4) Volver atrás
5) Mostrar archivo de conteo
6) Mostrar archivo de conteo ordenado por distrito
Opcion: 1

Ingrese la fecha de la elección: 19991010

Ingrese el cargo: Presidente
********* GENERO EL INFORME POR ELECCION **********

Fecha     Cargo                         Lista                                   Cantidad d
19991010  Presidente                    ARI                                     2533
19991010  Presidente                    Izquierda                               1283
19991010  Presidente                    PJ                                      1267
19991010  Presidente                    PRO                                     1332
19991010  Presidente                    Socialista                              1305
19991010  Presidente                    UCR                                     1280
19991010  Presidente                    blanco                                  0

Ingrese una tecla para continuar

Opciones:

1) Informe por elección
2) Informe por lista
3) Informe por distrito
4) Volver atrás
5) Mostrar archivo de conteo
6) Mostrar archivo de conteo ordenado por distrito
Opcion: 2

Ingrese la fecha de la elección: 19991010

Ingrese el cargo: Presidente
Ingrese la lista: Socialista
********* GENERO EL INFORME POR LISTA **********

Lista a informar: Socialista

Fecha     Nombre de lista                         Cantidad de votos
19991010  Socialista                             1305
Cargo principal Presidente
Subcargo 1 Vicepresidente

Ingrese una tecla para continuar

Opciones:
```

```
1) Informe por elección
2) Informe por lista
3) Informe por distrito
4) Volver atrás
5) Mostrar archivo de conteo
6) Mostrar archivo de conteo ordenado por distrito
Opcion: 3

Ingrese el nombre del distrito: Misiones
********* GENERO EL INFORME POR DISTRITO **********

Distrito a informar: Misiones

Fecha     Cargo                          Lista ganadora                          Cantidad d
19991010  Presidente                     ARI                                     108

Ingrese una tecla para continuar

Opciones:

1) Informe por elección
2) Informe por lista
3) Informe por distrito
4) Volver atrás
5) Mostrar archivo de conteo
6) Mostrar archivo de conteo ordenado por distrito
Opcion: 5

19991010  Presidente          ARI                          Buenos Aires
19991010  Presidente          ARI                          Catamarca
19991010  Presidente          ARI                          Chaco
19991010  Presidente          ARI                          Chubut
19991010  Presidente          ARI                          Ciudad Autonoma de Buenos Aire
19991010  Presidente          ARI                          Cordoba
19991010  Presidente          ARI                          Corrientes
19991010  Presidente          ARI                          Entre Rios
19991010  Presidente          ARI                          Formosa
19991010  Presidente          ARI                          Jujuy
19991010  Presidente          ARI                          La Pampa
19991010  Presidente          ARI                          La Rioja
19991010  Presidente          ARI                          Mendoza
19991010  Presidente          ARI                          Misiones
19991010  Presidente          ARI                          Neuquen
19991010  Presidente          ARI                          Rio Negro
19991010  Presidente          ARI                          Salta
19991010  Presidente          ARI                          San Juan
19991010  Presidente          ARI                          San Luis
19991010  Presidente          ARI                          Santa Cruz
19991010  Presidente          ARI                          Santa Fe
```

```
19991010  Presidente          ARI                       Santiago del Estero
19991010  Presidente          ARI                       Tierra del Fuego
19991010  Presidente          ARI                       Tucuman
19991010  Presidente          Izquierda                 Buenos Aires
19991010  Presidente          Izquierda                 Catamarca
19991010  Presidente          Izquierda                 Chaco
19991010  Presidente          Izquierda                 Chubut
19991010  Presidente          Izquierda                 Ciudad Autonoma de Buenos Aire
19991010  Presidente          Izquierda                 Cordoba
19991010  Presidente          Izquierda                 Corrientes
19991010  Presidente          Izquierda                 Entre Rios
19991010  Presidente          Izquierda                 Formosa
19991010  Presidente          Izquierda                 Jujuy
19991010  Presidente          Izquierda                 La Pampa
19991010  Presidente          Izquierda                 La Rioja
19991010  Presidente          Izquierda                 Mendoza
19991010  Presidente          Izquierda                 Misiones
19991010  Presidente          Izquierda                 Neuquen
19991010  Presidente          Izquierda                 Rio Negro
19991010  Presidente          Izquierda                 Salta
19991010  Presidente          Izquierda                 San Juan
19991010  Presidente          Izquierda                 San Luis
19991010  Presidente          Izquierda                 Santa Cruz
19991010  Presidente          Izquierda                 Santa Fe
19991010  Presidente          Izquierda                 Santiago del Estero
19991010  Presidente          Izquierda                 Tierra del Fuego
19991010  Presidente          Izquierda                 Tucuman
19991010  Presidente          PJ                        Buenos Aires
19991010  Presidente          PJ                        Catamarca
19991010  Presidente          PJ                        Chaco
19991010  Presidente          PJ                        Chubut
19991010  Presidente          PJ                        Ciudad Autonoma de Buenos Aire
19991010  Presidente          PJ                        Cordoba
19991010  Presidente          PJ                        Corrientes
19991010  Presidente          PJ                        Entre Rios
19991010  Presidente          PJ                        Formosa
19991010  Presidente          PJ                        Jujuy
19991010  Presidente          PJ                        La Pampa
19991010  Presidente          PJ                        La Rioja
19991010  Presidente          PJ                        Mendoza
19991010  Presidente          PJ                        Misiones
19991010  Presidente          PJ                        Neuquen
19991010  Presidente          PJ                        Rio Negro
19991010  Presidente          PJ                        Salta
19991010  Presidente          PJ                        San Juan
19991010  Presidente          PJ                        San Luis
19991010  Presidente          PJ                        Santa Cruz
19991010  Presidente          PJ                        Santa Fe
19991010  Presidente          PJ                        Santiago del Estero
19991010  Presidente          PJ                        Tierra del Fuego
```

```
19991010  Presidente          PJ                  Tucuman
19991010  Presidente          PRO                 Buenos Aires
19991010  Presidente          PRO                 Catamarca
19991010  Presidente          PRO                 Chaco
19991010  Presidente          PRO                 Chubut
19991010  Presidente          PRO                 Ciudad Autonoma de Buenos Aire
19991010  Presidente          PRO                 Cordoba
19991010  Presidente          PRO                 Corrientes
19991010  Presidente          PRO                 Entre Rios
19991010  Presidente          PRO                 Formosa
19991010  Presidente          PRO                 Jujuy
19991010  Presidente          PRO                 La Pampa
19991010  Presidente          PRO                 La Rioja
19991010  Presidente          PRO                 Mendoza
19991010  Presidente          PRO                 Misiones
19991010  Presidente          PRO                 Neuquen
19991010  Presidente          PRO                 Rio Negro
19991010  Presidente          PRO                 Salta
19991010  Presidente          PRO                 San Juan
19991010  Presidente          PRO                 San Luis
19991010  Presidente          PRO                 Santa Cruz
19991010  Presidente          PRO                 Santa Fe
19991010  Presidente          PRO                 Santiago del Estero
19991010  Presidente          PRO                 Tierra del Fuego
19991010  Presidente          PRO                 Tucuman
19991010  Presidente          Socialista          Buenos Aires
19991010  Presidente          Socialista          Catamarca
19991010  Presidente          Socialista          Chaco
19991010  Presidente          Socialista          Chubut
19991010  Presidente          Socialista          Ciudad Autonoma de Buenos Aire
19991010  Presidente          Socialista          Cordoba
19991010  Presidente          Socialista          Corrientes
19991010  Presidente          Socialista          Entre Rios
19991010  Presidente          Socialista          Formosa
19991010  Presidente          Socialista          Jujuy
19991010  Presidente          Socialista          La Pampa
19991010  Presidente          Socialista          La Rioja
19991010  Presidente          Socialista          Mendoza
19991010  Presidente          Socialista          Misiones
19991010  Presidente          Socialista          Neuquen
19991010  Presidente          Socialista          Rio Negro
19991010  Presidente          Socialista          Salta
19991010  Presidente          Socialista          San Juan
19991010  Presidente          Socialista          San Luis
19991010  Presidente          Socialista          Santa Cruz
19991010  Presidente          Socialista          Santa Fe
19991010  Presidente          Socialista          Santiago del Estero
19991010  Presidente          Socialista          Tierra del Fuego
19991010  Presidente          Socialista          Tucuman
19991010  Presidente          UCR                 Buenos Aires
```

```
19991010  Presidente          UCR                 Catamarca
19991010  Presidente          UCR                 Chaco
19991010  Presidente          UCR                 Chubut
19991010  Presidente          UCR                 Ciudad Autonoma de Buenos Aire
19991010  Presidente          UCR                 Cordoba
19991010  Presidente          UCR                 Corrientes
19991010  Presidente          UCR                 Entre Rios
19991010  Presidente          UCR                 Formosa
19991010  Presidente          UCR                 Jujuy
19991010  Presidente          UCR                 La Pampa
19991010  Presidente          UCR                 La Rioja
19991010  Presidente          UCR                 Mendoza
19991010  Presidente          UCR                 Misiones
19991010  Presidente          UCR                 Neuquen
19991010  Presidente          UCR                 Rio Negro
19991010  Presidente          UCR                 Salta
19991010  Presidente          UCR                 San Juan
19991010  Presidente          UCR                 San Luis
19991010  Presidente          UCR                 Santa Cruz
19991010  Presidente          UCR                 Santa Fe
19991010  Presidente          UCR                 Santiago del Estero
19991010  Presidente          UCR                 Tierra del Fuego
19991010  Presidente          UCR                 Tucuman
19991010  Presidente          blanco              Buenos Aires
19991010  Presidente          blanco              Catamarca
19991010  Presidente          blanco              Chaco
19991010  Presidente          blanco              Chubut
19991010  Presidente          blanco              Ciudad Autonoma de Buenos Aire
19991010  Presidente          blanco              Cordoba
19991010  Presidente          blanco              Corrientes
19991010  Presidente          blanco              Entre Rios
19991010  Presidente          blanco              Formosa
19991010  Presidente          blanco              Jujuy
19991010  Presidente          blanco              La Pampa
19991010  Presidente          blanco              La Rioja
19991010  Presidente          blanco              Mendoza
19991010  Presidente          blanco              Misiones
19991010  Presidente          blanco              Neuquen
19991010  Presidente          blanco              Rio Negro
19991010  Presidente          blanco              Salta
19991010  Presidente          blanco              San Juan
19991010  Presidente          blanco              San Luis
19991010  Presidente          blanco              Santa Cruz
19991010  Presidente          blanco              Santa Fe
19991010  Presidente          blanco              Santiago del Estero
19991010  Presidente          blanco              Tierra del Fuego
19991010  Presidente          blanco              Tucuman

Cantidad de votos en total: 9000
Ingrese una tecla para continuar
```

```
Opciones:

1) Informe por elección
2) Informe por lista
3) Informe por distrito
4) Volver atrás
5) Mostrar archivo de conteo
6) Mostrar archivo de conteo ordenado por distrito
Opcion: 6

Buenos Aires                              19991010  Presidente                ARI
Buenos Aires                              19991010  Presidente                Izquierda
Buenos Aires                              19991010  Presidente                PJ
Buenos Aires                              19991010  Presidente                PRO
Buenos Aires                              19991010  Presidente                Socialista
Buenos Aires                              19991010  Presidente                UCR
Buenos Aires                              19991010  Presidente                blanco
Catamarca                                 19991010  Presidente                ARI
Catamarca                                 19991010  Presidente                Izquierda
Catamarca                                 19991010  Presidente                PJ
Catamarca                                 19991010  Presidente                PRO
Catamarca                                 19991010  Presidente                Socialista
Catamarca                                 19991010  Presidente                UCR
Catamarca                                 19991010  Presidente                blanco
Chaco                                     19991010  Presidente                ARI
Chaco                                     19991010  Presidente                Izquierda
Chaco                                     19991010  Presidente                PJ
Chaco                                     19991010  Presidente                PRO
Chaco                                     19991010  Presidente                Socialista
Chaco                                     19991010  Presidente                UCR
Chaco                                     19991010  Presidente                blanco
Chubut                                    19991010  Presidente                ARI
Chubut                                    19991010  Presidente                Izquierda
Chubut                                    19991010  Presidente                PJ
Chubut                                    19991010  Presidente                PRO
Chubut                                    19991010  Presidente                Socialista
Chubut                                    19991010  Presidente                UCR
Chubut                                    19991010  Presidente                blanco
Ciudad Autonoma de Buenos Aires           19991010  Presidente                ARI
Ciudad Autonoma de Buenos Aires           19991010  Presidente                Izquierda
Ciudad Autonoma de Buenos Aires           19991010  Presidente                PJ
Ciudad Autonoma de Buenos Aires           19991010  Presidente                PRO
Ciudad Autonoma de Buenos Aires           19991010  Presidente                Socialista
Ciudad Autonoma de Buenos Aires           19991010  Presidente                UCR
Ciudad Autonoma de Buenos Aires           19991010  Presidente                blanco
Cordoba                                   19991010  Presidente                ARI
Cordoba                                   19991010  Presidente                Izquierda
Cordoba                                   19991010  Presidente                PJ
Cordoba                                   19991010  Presidente                PRO
```

Cordoba	19991010	Presidente	Socialista
Cordoba	19991010	Presidente	UCR
Cordoba	19991010	Presidente	blanco
Corrientes	19991010	Presidente	ARI
Corrientes	19991010	Presidente	Izquierda
Corrientes	19991010	Presidente	PJ
Corrientes	19991010	Presidente	PRO
Corrientes	19991010	Presidente	Socialista
Corrientes	19991010	Presidente	UCR
Corrientes	19991010	Presidente	blanco
Entre Rios	19991010	Presidente	ARI
Entre Rios	19991010	Presidente	Izquierda
Entre Rios	19991010	Presidente	PJ
Entre Rios	19991010	Presidente	PRO
Entre Rios	19991010	Presidente	Socialista
Entre Rios	19991010	Presidente	UCR
Entre Rios	19991010	Presidente	blanco
Formosa	19991010	Presidente	ARI
Formosa	19991010	Presidente	Izquierda
Formosa	19991010	Presidente	PJ
Formosa	19991010	Presidente	PRO
Formosa	19991010	Presidente	Socialista
Formosa	19991010	Presidente	UCR
Formosa	19991010	Presidente	blanco
Jujuy	19991010	Presidente	ARI
Jujuy	19991010	Presidente	Izquierda
Jujuy	19991010	Presidente	PJ
Jujuy	19991010	Presidente	PRO
Jujuy	19991010	Presidente	Socialista
Jujuy	19991010	Presidente	UCR
Jujuy	19991010	Presidente	blanco
La Pampa	19991010	Presidente	ARI
La Pampa	19991010	Presidente	Izquierda
La Pampa	19991010	Presidente	PJ
La Pampa	19991010	Presidente	PRO
La Pampa	19991010	Presidente	Socialista
La Pampa	19991010	Presidente	UCR
La Pampa	19991010	Presidente	blanco
La Rioja	19991010	Presidente	ARI
La Rioja	19991010	Presidente	Izquierda
La Rioja	19991010	Presidente	PJ
La Rioja	19991010	Presidente	PRO
La Rioja	19991010	Presidente	Socialista
La Rioja	19991010	Presidente	UCR
La Rioja	19991010	Presidente	blanco
Mendoza	19991010	Presidente	ARI
Mendoza	19991010	Presidente	Izquierda
Mendoza	19991010	Presidente	PJ
Mendoza	19991010	Presidente	PRO
Mendoza	19991010	Presidente	Socialista

Mendoza	19991010	Presidente	UCR
Mendoza	19991010	Presidente	blanco
Misiones	19991010	Presidente	ARI
Misiones	19991010	Presidente	Izquierda
Misiones	19991010	Presidente	PJ
Misiones	19991010	Presidente	PRO
Misiones	19991010	Presidente	Socialista
Misiones	19991010	Presidente	UCR
Misiones	19991010	Presidente	blanco
Neuquen	19991010	Presidente	ARI
Neuquen	19991010	Presidente	Izquierda
Neuquen	19991010	Presidente	PJ
Neuquen	19991010	Presidente	PRO
Neuquen	19991010	Presidente	Socialista
Neuquen	19991010	Presidente	UCR
Neuquen	19991010	Presidente	blanco
Rio Negro	19991010	Presidente	ARI
Rio Negro	19991010	Presidente	Izquierda
Rio Negro	19991010	Presidente	PJ
Rio Negro	19991010	Presidente	PRO
Rio Negro	19991010	Presidente	Socialista
Rio Negro	19991010	Presidente	UCR
Rio Negro	19991010	Presidente	blanco
Salta	19991010	Presidente	ARI
Salta	19991010	Presidente	Izquierda
Salta	19991010	Presidente	PJ
Salta	19991010	Presidente	PRO
Salta	19991010	Presidente	Socialista
Salta	19991010	Presidente	UCR
Salta	19991010	Presidente	blanco
San Juan	19991010	Presidente	ARI
San Juan	19991010	Presidente	Izquierda
San Juan	19991010	Presidente	PJ
San Juan	19991010	Presidente	PRO
San Juan	19991010	Presidente	Socialista
San Juan	19991010	Presidente	UCR
San Juan	19991010	Presidente	blanco
San Luis	19991010	Presidente	ARI
San Luis	19991010	Presidente	Izquierda
San Luis	19991010	Presidente	PJ
San Luis	19991010	Presidente	PRO
San Luis	19991010	Presidente	Socialista
San Luis	19991010	Presidente	UCR
San Luis	19991010	Presidente	blanco
Santa Cruz	19991010	Presidente	ARI
Santa Cruz	19991010	Presidente	Izquierda
Santa Cruz	19991010	Presidente	PJ
Santa Cruz	19991010	Presidente	PRO
Santa Cruz	19991010	Presidente	Socialista
Santa Cruz	19991010	Presidente	UCR

```
Santa Cruz                  19991010  Presidente  blanco
Santa Fe                    19991010  Presidente  ARI
Santa Fe                    19991010  Presidente  Izquierda
Santa Fe                    19991010  Presidente  PJ
Santa Fe                    19991010  Presidente  PRO
Santa Fe                    19991010  Presidente  Socialista
Santa Fe                    19991010  Presidente  UCR
Santa Fe                    19991010  Presidente  blanco
Santiago del Estero         19991010  Presidente  ARI
Santiago del Estero         19991010  Presidente  Izquierda
Santiago del Estero         19991010  Presidente  PJ
Santiago del Estero         19991010  Presidente  PRO
Santiago del Estero         19991010  Presidente  Socialista
Santiago del Estero         19991010  Presidente  UCR
Santiago del Estero         19991010  Presidente  blanco
Tierra del Fuego            19991010  Presidente  ARI
Tierra del Fuego            19991010  Presidente  Izquierda
Tierra del Fuego            19991010  Presidente  PJ
Tierra del Fuego            19991010  Presidente  PRO
Tierra del Fuego            19991010  Presidente  Socialista
Tierra del Fuego            19991010  Presidente  UCR
Tierra del Fuego            19991010  Presidente  blanco
Tucuman                     19991010  Presidente  ARI
Tucuman                     19991010  Presidente  Izquierda
Tucuman                     19991010  Presidente  PJ
Tucuman                     19991010  Presidente  PRO
Tucuman                     19991010  Presidente  Socialista
Tucuman                     19991010  Presidente  UCR
Tucuman                     19991010  Presidente  blanco

Cantidad de votos en total: 9000
```

7. Corridas de prueba - 2da Etapa

A continuación se detallan las pruebas realizadas sobre el funcionamiento del programa para la segunda etapa. Se emplearon las pruebas detalladas en el enunciado del informe, las cuales pasaron con éxito.

Corridas de prueba

```
Ejemplo de vulneración de RSA

(Salida para verificar que realmente fue vulnerada la seguridad)
N en archivo: 3953
D en archivo: 19
E en archivo: 403

Ingrese su nombre de usuario: undomiel

Ahora ingrese su contraseña: aragorn

usuario: <undomiel>
password: <aragorn>
INGRESO APROBADO
Bienvenido al sistama de gestion de elecciones
¿ Desea eliminar la base de datos y comenzar de 0? S/N
S

Opciones:

1) Mantener Distritos
2) Mantener Votantes
3) Mantener Elecciones
4) Mantener Cargos
5) Mantener Listas
6) Mantener Candidatos
7) Informar Resultados
8) Habilitar Elecciones
9) Habilitar Votantes para elección
10) salir
11) Votacion automatica
12) Criptoanalizar informes
13) Atacar RSA
Opcion: 13

Vulnerado!!!
El p es= 59
El q es= 67
N= 3953
D: 19
E= 403
Con estos datos puede crearse el archivo clavePrivada.txt y vulnerarse la seguridad
```

```
(porque las claves se levantan desde el archivo clavePrivada.txt)

================================================================================================
Ejemplo de vulneracion de Vigeneré con Kasiski.

1) Mantener Distritos
2) Mantener Votantes
3) Mantener Elecciones
4) Mantener Cargos
5) Mantener Listas
6) Mantener Candidatos
7) Informar Resultados
8) Habilitar Elecciones
9) Habilitar Votantes para elección
10) salir
11) Votacion automatica
12) Criptoanalizar informes
13) Atacar RSA
Opcion: 12

Opciones:

1) Criptoanalizar informe de Elecciones
2) Criptoanalizar informe de Listas
3) Criptoanalizar informe de Distritos
4) Volver atrás
Opcion: 1

Clave descifrada: EXITO

********* GENERO EL INFORME POR ELECCION **********
Fecha     Cargo                         Lista                                   Cantidad d
19990303  Presidente                    Amarilla                                28
19990303  Presidente                    Azul                                    15
19990303  Presidente                    Blanca                                  13
19990303  Presidente                    Cesleste                                10
19990303  Presidente                    Marron                                  17
19990303  Presidente                    Negra                                   22
19990303  Presidente                    Roja                                    13
19990303  Presidente                    Rosa                                    20
19990303  Presidente                    Turquesa                                17
19990303  Presidente                    Verde                                   12
19990303  Presidente                    Violeta                                 11
19990303  Presidente                    blanco                                  0
Opciones:

1) Criptoanalizar informe de Elecciones
2) Criptoanalizar informe de Listas
3) Criptoanalizar informe de Distritos
4) Volver atrás
```

```
Opcion: 2

Clave descifrada: EXITO

********* GENERO EL INFORME POR LISTA **********

Lista a informar: Roja

Fecha     Nombre de lista                         Cantidad de votos
19990303  Roja                                    13
Cargo principal Presidente
Subcargo 1 Vicepresidente

Opciones:

1) Criptoanalizar informe de Elecciones
2) Criptoanalizar informe de Listas
3) Criptoanalizar informe de Distritos
4) Volver atrás
Opcion: 3

Clave descifrada: EXITO

********* GENERO EL INFORME POR DISTRITO **********

Distrito a informar: Misiones

Fecha     Cargo                       Lista ganadora                      Cantidad d
19830303  Presidente                  empate                              2
19840303  Presidente                  empate                              2
19850303  Presidente                  Negra                               3
19860303  Presidente                  empate                              2
19870303  Presidente                  empate                              2
19880303  Presidente                  Amarilla                            3
19890303  Presidente                  empate                              2
19900303  Presidente                  empate                              1
19910303  Presidente                  empate                              2
19920303  Presidente                  Cesleste                            1
19930303  Presidente                  Turquesa                            3
19940303  Presidente                  empate                              1
19950303  Presidente                  empate                              1
19960303  Presidente                  Roja                                2
19970303  Presidente                  Negra                               3
19980303  Presidente                  Cesleste                            2
19990303  Presidente                  Negra                               2
20000303  Presidente                  empate                              2
20010303  Presidente                  Marron                              3
20020303  Presidente                  empate                              1
20030303  Presidente                  Violeta                             2
20040303  Presidente                  Cesleste                            2
```

```
20050303  Presidente                    Negra                          2
20060303  Presidente                    Rosa                           4
20070303  Presidente                    empate                         1
20080303  Presidente                    Azul                           2
20090303  Presidente                    Amarilla                       2
Opciones:

1) Criptoanalizar informe de Elecciones
2) Criptoanalizar informe de Listas
3) Criptoanalizar informe de Distritos
4) Volver atrás
Opcion:
```

Referencias

[1] Folk, Michael J. Zoellick, Bill. *File Structures.*

[2] Smith, Peter. Barnes, G. *Files and Databases: An Introduction.* Addison-Wesley.

[3] Documentación: Texmaker 3.0.2 (para la redacción de este informe)

`http://www.xm1math.net/texmaker/`

8. Apendice - Enunciado TP Etapa 1

A continuación se agrega el enunciado de la Etapa 1, correspondiente a este Trabajo Práctico.

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERIA

DEPARTAMENTO DE COMPUTACIÓN

75.06 – ORGANIZACIÓN DE DATOS

TRABAJO PRÁCTICO

VOTO ELECTRÓNICO

ETAPA 1

SETIEMBRE 2011

Índice General

1 Introducción

Este documento consiste en el enunciado del trabajo práctico de la asignatura. En el mismo se especifican los requerimientos de cada etapa de entrega, dejando de lado el cronograma de entregas que se encuentran en la página o grupo de correo de comunicación de la cátedra respectivamente.

Toda aclaración, indicación o respuesta a consultas (ofrecidas en clase o mediante el grupo yahoo) serán tomadas como extensión y parte explícita de este enunciado.

La forma de trabajo con los grupos es descripta en el Reglamento de Trabajos Prácticos de la Cátedra (http://materias.fi.uba.ar/7506C/blog/?page_id=9)

El trabajo consistirá en implementar una aplicación capaz de resolver la problemática del voto electrónico.

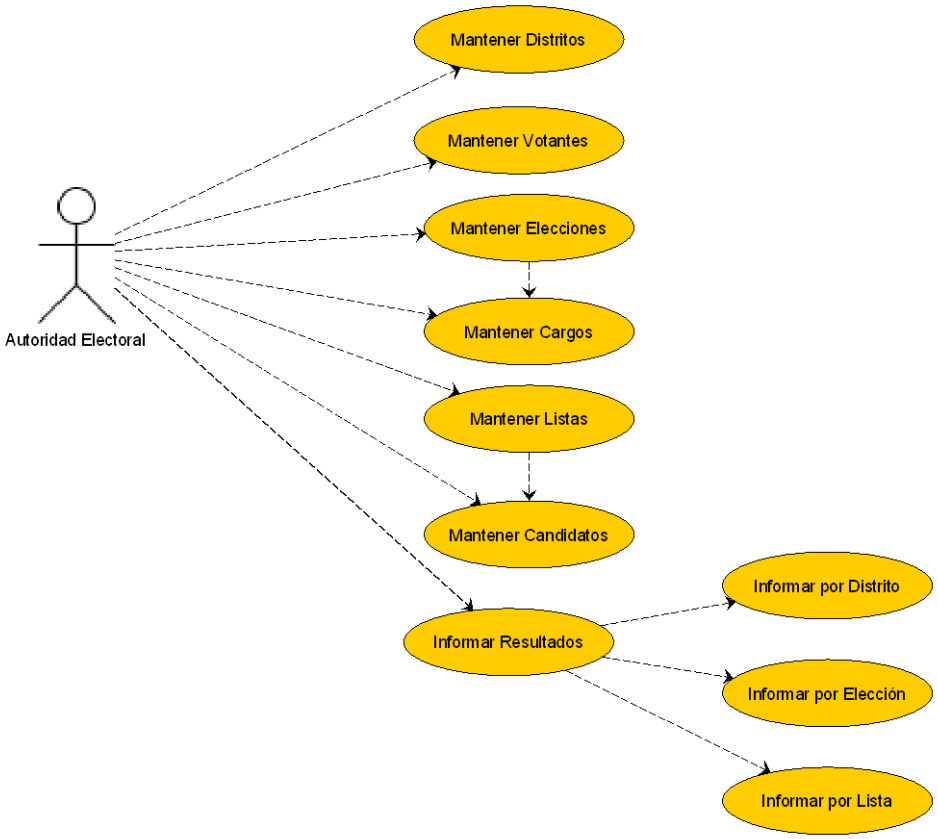
2 Enunciado

La aplicación deberá ser capaz de mantener información sobre las entidades que componen el sistema de votaciones (votantes, elecciones, candidatos, etc.), y de proveer la posibilidad a un votante de emitir su voto para la correspondiente elección.

La Primer Entrega se avocará a la aplicación de los conceptos de Organización de Archivos.

Funcionalidades mínimas

Tipo: URNA ELECTRÓNICA DE REGISTRO DIRECTO



Mantener Distritos: Es el Alta, Baja y Modificación de los Distritos que delimitan las elecciones.

Mantener Votantes: Es el Alta, Baja y Modificación del padrón de votantes en la elección.

Mantener Elecciones: Es el Alta, Baja y Modificación del evento electoral.

Mantener Cargos: Es el Alta, Baja y Modificación de los cargos a ser electos en la Elección.

Mantener Listas: Es el Alta, Baja y Modificación de las listas de candidatos a los cargos a elegirse en un distrito.

Mantener Candidatos: Es el Alta, Baja y Modificación de los Candidatos, que deben ser votantes, a los cargos puestos en juego en la elección distrital.

Informar Resultados: Es el Alta de informes a mostrar por pantalla bajo tres posibles criterios, un Distrito determinado, una Elección determinada o una Lista determinada.

Almacenamiento y Archivos de Control para las Entidades = Se encuentran todos dentro de un directorio, especificado a través de un archivo de configuración de la aplicación, y pueden tener jerarquía de subdirectorios interna. Es donde se guarda toda la información necesaria para poder funcionar.

Comandos por consola = Toda la interacción del usuario con el sistema se realiza a través de comandos por consola.

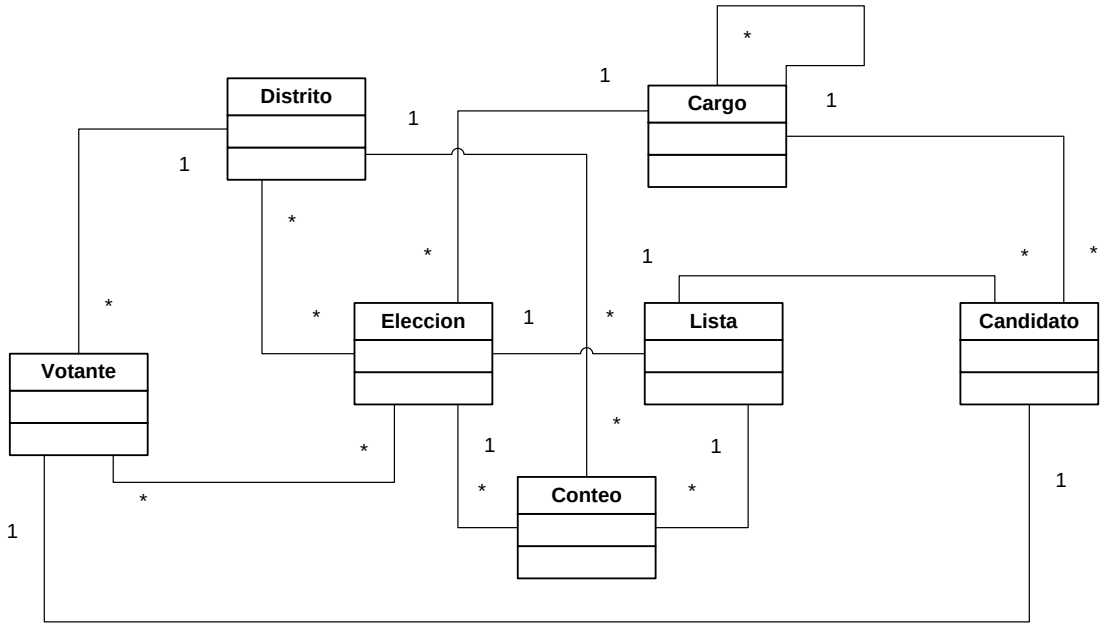
Archivos con resultados = Como respuesta a toda interacción, el sistema generará archivos de registro de operaciones (LOGs) en el directorio donde se llame a la aplicación.

La resolución del trabajo práctico debe ser realizada en plataforma Linux y lenguajes C o C++ (preferentemente respetando el estándar ANSI), y la entrega debe constar de un Makefile para su compilación. Además debe funcionar en calidad de Usuario (user) del sistema operativo.

2.1 *Entidades*

Respecto a las entidades que conformarán la información necesaria para resolver esta problemática, a continuación presentamos un diagrama básico de entidades y sus relaciones.

El objetivo de esta etapa es resolver la aplicación, utilizando las herramientas brindadas por el módulo Organización de Archivos. Por ello se plantea la siguiente relación entre esos conceptos.



Distrito ((distrito)i)
Votante ((DNI)i, NombreyApellido, clave, domicilio, (distrito)ie, ((eleccion)ie)*)
Eleccion ((fecha, (cargo)ie)i, ((distrito)ie)+)
Lista (((eleccion)ie, nombre)i)
Conteo (((lista)ie, (distrito)ie, (eleccion)ie)i, cantidad)
Candidato (((lista)ie, (votante)ie, (cargo)ie)i)
Cargo ((cargo)i, (cargo)*)
Administrador ((usuario)i, clave)

2.2 *Estructuras de Datos*

Para la implementación, deberán elegirse, con criterios bien definidos y explicados por el grupo, las estructuras de datos en disco que se utilizarán para cada uno de los archivos previamente definidos.

Es importante presentar al tutor o docente a cargo del grupo la estrategia a utilizar para resolver el TP para validar que sea correcta y cumpla los requerimientos mínimos de complejidad que requiere el mismo.

Las estructuras a elegir son las siguientes:

- Árbol B
- Árbol B+
- Árbol B#
- Dispersión Extensible
- Dispersión Fija con Zona de Desborde.
- Archivos de Registros Variables
- Archivos de Registros Fijos
- Archivos de Bloques

La resolución del trabajo práctico debe ser realizada en plataforma Linux y lenguajes C o C++ (preferentemente respetando el estándar ANSI).

2.3 *Accesorios*

Deberán, además, crearse votantes aleatorios automatizados para resolver el ingreso de votos de varias elecciones, que muestren la correcta funcionalidad del sistema.

Además, será necesario registrar en un archivo de LOG todas las operaciones del votante: Acceso, Acceso Fallido, voto, voto ingresado, cambio de voto.

3 Criterio de aprobación

Como se especifica en el Reglamento de la materia existe un criterio mínimo para poder acceder a una re-entrega en cada etapa. A continuación se menciona una lista de requerimientos que forman parte de dicho criterio. No cumplir con alguna de ellas implica no cumplir el mínimo requerido. Pero no vale la inversa, es decir, cumplir con ellas no implica cumplir con el criterio mínimo.

3.1 *Entrega*

La entrega debe constar de un Makefile para su compilación, y el sistema debe funcionar en calidad de Usuario (user) del sistema operativo.
Además, deberá entregarse la documentación que se describe en la página de la materia (http://materias.fi.uba.ar/7506C/docs/wiki/doku.php?id=tp:requisitos_de_documentacion)

Los grupos a formar serán de 5 integrantes.

El periodo de resolución de esta etapa del trabajo práctico es de 5 semanas de la fecha de presentación del mismo (Sábado 22/10 00hs).

3.2 *Documentación*

- *General*
  - Diagrama de clases o módulos (según corresponda)
  - Especificación de cada clase o módulo (según corresponda)
  - Diagramas de secuencia o intercambio de mensajes entre capas. Mostrar escenarios.
  - Planificación (identificación de tareas, estimación de duración y asignación)
  - Bugs conocidos
  - Manual de usuario. Indicaciones generales del trabajo práctico, modo de instalación y ejemplos de uso.

- *Física – Organización*

  Organización de registros

  - ¿Cómo delimitan la longitud de un registro y de un campo variable?. Mostrar los campos que posee y cuanto espacio ocupa cada uno.
  - Indicar que información administrativa se utiliza.

- *Índices – Búsqueda*

  Hashing
  - Función de hashing utilizada. Criterio de elección.

- Tamaño de Buckets.
- ¿Cuál es el factor de empaquetamiento que utilizan?

Árbol B+

- *Sequence set*: ¿Cómo delimitan la longitud de un registro y de un campo variable?. Mostrar los campos que posee y cuanto espacio ocupa cada uno. Política utilizada para split / concatenación de bloques. ¿Hacen algún tipo de redistribución?
- *Index set:* Mostrar los campos que posee y cuanto espacio ocupa cada uno. ¿Cómo se generan los separadores? ¿Cómo se eliminan separadores? Indicar que condiciones deben surgir en cada caso. ¿Existe algún tipo de concatenación de separadores dentro de la página? ¿Qué método se utiliza para la búsqueda de un separador dentro de la página? (binaria, secuencial, otro).

4 Referencias

Folk, Michael. Zoellick, Hill. *File Structures*. 724 páginas.

Smith, Peter. Barnes, G. *Files and Databases: An Introduction.* Addison-Wesley.

9. Apendice - Enunciado TP Etapa 2

A continuación se agrega el enunciado de la Etapa 2, correspondiente a este Trabajo Práctico.

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERÍA

DEPARTAMENTO DE COMPUTACIÓN

75.06 – ORGANIZACIÓN DE DATOS

TRABAJO PRÁCTICO

VOTO ELECTRÓNICO

SEGURIDAD

ETAPA 2

NOVIEMBRE 2011

Índice General

1 Introducción

Este documento consiste en el enunciado del trabajo práctico de la asignatura. En el mismo se especifican los requerimientos de cada etapa de entrega, dejando de lado el cronograma de entregas que se encuentran en la página o grupo de correo de comunicación de la cátedra respectivamente.

Toda aclaración, indicación o respuesta a consultas (ofrecidas en clase o mediante el grupo yahoo) serán tomadas como extensión y parte explícita de este enunciado.

La forma de trabajo con los grupos es descripta en el Reglamento de Trabajos Prácticos de la Cátedra (http://materias.fi.uba.ar/7506C/blog/?page_id=9)

El trabajo consistirá en agregar seguridad al voto electrónico, realizado en la primera etapa de este trabajo práctico.

2 Enunciado

En esta etapa, agregaremos algo de seguridad a los datos que queremos que sean confidenciales dentro de nuestro sistema de voto electrónico. Para esto, aplicaremos un algoritmo criptográfico simétrico y otro asimétrico.

En el caso de la información de votantes y administradores, queremos que estos datos se persistan en disco de forma confidencial, debido a que incluyen las claves de estos usuarios en texto plano. Es por esto que utilizaremos el algoritmo RSA para encriptar estos datos.

También sabemos que los datos de reportes podrían necesitar ser intercambiados antes de que se den a conocer los resultados oficiales, por lo que deberían poder ser enviados de forma segura. El método elegido para poder encriptarlos es el de Vigenere. Por lo que los reportes se generaran en archivos encriptados por este método.

2.1 *Detalles técnicos*

Según lo estipulado por enunciado, el algoritmo RSA deberá ser implementado y agregado al trabajo práctico, de modo de proveer una encripción y desencripción transparentes dentro del funcionamiento de los módulos ya desarrollados. Es importante que las claves generadas sean valores aleatorios de n bytes (parametrizable), pudiendo poner un valor de n máximo.

Además, deberá proveerse una funcionalidad adicional al sistema ya desarrollado, agregando la posibilidad de intentar romper el criptosistema RSA, sabiendo que la clave pública que se genere es conocida.

Por otra parte, el algoritmo de Vigenere será implementado para resolver la encripción de los reportes, de modo de generar una copia de los mismos encriptada en disco. La clave utilizada para esto debe ser elegida por el usuario (ingresada en tiempo real o colocada en un archivo de configuración) y deberá contener caracteres imprimibles. La misma también puede ser limitada en su cantidad de caracteres a un valor n.

Por último, el sistema deberá proveer la posibilidad de aplicar el método de Kasiski para romper el criptosistema descripto. Para esto, podrá ser de ayuda el conocer palabras clave de los reportes, como Lista, Elección, Distrito, etc. La idea será que los alumnos puedan generar reportes suficientemente largos y estructurados de forma de poder generar un caso de ejemplo donde el criptosistema se rompa. No siempre será sencillo romper el criptosistema, por lo que el hecho de implementar el método de criptoanalisis y dar un caso donde pueda romperse, será suficiente.

3 Criterio de aprobación

A continuación se menciona una lista de requerimientos que forman parte del criterio de aprobación. No cumplir con alguna de ellas implica no cumplir el mínimo requerido. Pero no vale la inversa, es decir, cumplir con ellas no implica cumplir con el criterio mínimo.

3.1 *Entrega*

La entrega, además de lo estipulado por el enunciado, debe constar de un Makefile para su compilación, y el sistema debe funcionar en calidad de Usuario (user) del sistema operativo.

Además, deberán entregarse las correcciones que queden pendientes, indicadas por el tutor, de la etapa anterior, y la documentación que se describe a continuación.

Los grupos a formar serán los mismos que aprobaron la primera etapa.

El periodo de resolución de esta etapa del trabajo práctico es de 4 semanas de la fecha de presentación del mismo (Sábado 03/12 23:59hs). Dados los tiempos que se manejan, no habrá posibilidad de reentrega.

3.2 *Documentación*

- *General*
  - Diagrama de clases o módulos (según corresponda)
  - Especificación de cada clase o módulo (según corresponda)
  - Diagramas de secuencia o intercambio de mensajes entre capas. Mostrar escenarios.
  - Planificación (identificación de tareas, estimación de duración y asignación)
  - Bugs conocidos
  - Manual de usuario. Indicaciones generales del trabajo práctico, modo de instalación y ejemplos de uso.
  - Casos de ejemplo documentados y repetibles.

4 Referencias

- Criptografía 1: http://f1.grp.yahoofs.com/v1/0ACzTtPXFs1PCfvkCfJdhDq1WqjINWPrpDKTzOHyyAHiKjvPIv0obCkNqeNlDClZJSfwopTg1ClPng1DpIqz1Q/Material%20clases/Criptograf%80%A0%A0%EDa/Sugerido/Criptografia1-2010.pdf

- Criptografía 2: http://f1.grp.yahoofs.com/v1/0ACzTtQHXOdPCfvkzP1a7lGNlH-CaAZiPqD_2vSwoYSQnhMmORxcrSXpAqLd6IfwZYnO7Bj_jycZePhlQ__mWQ/Material%20clases/Criptograf%80%A0%A0%EDa/Sugerido/Criptografia2-2010.pdf