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