

***PROYECTO COMPUTACIONAL***  
***CONTROL DEL CIBERCRIMEN***



El cibercrimen se ha convertido en una poderosa y organizada rama de la delincuencia moderna. Se basa en el uso de la Internet para la realización de fechorías, aprovechando el beneficio que otorga una identidad enmascarada. Una actividad común consiste en la venta/alquiler de bienes y/o servicios ficticios a personas, a quienes se les solicita transferir dinero a ciertas cuentas bancarias (usualmente creadas con datos falsos). Para despistar, ese dinero se hace circular entre múltiples cuentas a través de una sucesión de transferencias, hasta que finalmente llega a manos de uno o más destinatarios finales, en una especie de “lavado virtual de dinero” dentro de la red de crimen constituida.

Ante esta situación, los cuerpos policiales del Estado trabajan arduamente para resolver los casos de cibercrimen reportados, partiendo del análisis del mapa de transferencias. Para ello cuentan con la información suministrada por la Superintendencia de las Instituciones del Sector Bancario, conocida como SUDEBAN, que incluye:

- La lista de todas las cuentas del sistema bancario nacional, especificando aquellas cuentas de las cuales ha salido dinero presuntamente robado, estas últimas denominadas cuentas fuente.
- El mapa de todas las transferencias ejecutadas en el sistema bancario nacional en un periodo de tiempo dado y el monto asociado a cada una de esas transacciones.

Luego de la revisión de los datos facilitados por la SUDEBAN, se ha determinado que toda sucesión de transferencias que inicia en una cuenta fuente es considerada una transacción sospechosa. Además, durante el periodo de tiempo estudiado, nunca hay más de una transferencia directa entre un par de cuentas cualesquiera. Finalmente, algunas cuentas podrían retener parte del dinero recibido por transferencias, para conocer el monto total retenido por una cuenta se debe calcular la diferencia entre el monto total que ha recibido por transferencias y el que ha traspasado a otras cuentas.

Los objetivos inmediatos que los cuerpos policiales desean alcanzar a través de sus investigaciones son:

1) Determinar la lista de cuentas involucradas en una transacción sospechosa, dado el código de una cuenta fuente específica.

2) Determinar el conjunto de cuentas “altamente sospechosas”, es decir, aquellas cuentas que retienen el 5% o más del total del dinero que ha salido de todas las cuentas fuente identificadas en el mapa de transferencias.

Ahora bien, a fin de avanzar en sus investigaciones, los cuerpos policiales junto a la SUDEBAN desean contratar los servicios de su equipo de trabajo, encomendándoles la misión de implementar un sistema para el control del cibercrimen. En este sentido, se pide:

- a) Modelar el problema usando Teoría de Grafos.
- b) Diseñar la solución algorítmica de alto nivel que dé respuesta a los requerimientos planteados.
- c) Implementar la solución algorítmica en un programa de computación, utilizando el lenguaje de programación ANSI C y que ejecute exitosamente bajo ambiente Linux distribución CentOS.
- d) El programa debe permitir la entrada/salida de datos por archivo. Las especificaciones de la secuencia de datos de entrada/salida serán proporcionadas oportunamente.

***PRIMERA ENTREGA: Viernes 09-10-2015 (Publicación de Enunciado Martes 22-09-2015)***

- (1) Modelado del problema usando las herramientas Teoría de Grafos.
- (2) Diseño de las estructuras de datos (Matrices, vectores, registros, entre otras).
- (3) Análisis del problema (¿Qué se tiene? ¿Qué se pide? ¿Cómo se resuelve?)
- (4) Diseño de la solución algorítmica en alto nivel.

La documentación especificada en los puntos anteriores debe ser cargada en el Entorno Virtual, en un sólo archivo .pdf, a través del link que estará disponible para tal fin.

***SEGUNDA ENTREGA: Semana del 19-10 al 23-10-2015***

Cargar en el Entorno Virtual, en un sólo archivo .zip, el código fuente, archivos de entrada y salida generados para la prueba del sistema y la documentación que se describe en el documento anexo: *Documentación de la Segunda Entrega.pdf*, que será suministrado oportunamente.

***DEFENSA DEL PROYECTO: Semana del 19-10 al 23-10-2015***

Oportunamente se publicará el día y hora que corresponda a cada equipo.

**OBSERVACIONES:**

- (1) Los equipos de trabajo son de dos (2) o tres (3) personas, no se permiten trabajos individuales ni de más de tres personas.
- (2) Los equipos debe mantenerse durante la primera y segunda entrega. En la primera entrega se dará por entendida la conformación de los mismos.
- (3) Se sugiere revisar el material correspondiente a los algoritmos de la Teoría de Grafos (disponible en el entorno) para poder abordar el proyecto. El tiempo para la primera entrega se cuenta desde la publicación del enunciado, es por esto que, se recomienda que cada equipo comience la revisión de los algoritmos con antelación a la presentación de las exposiciones.