Examen de Introducción a las Redes de Computadoras y Comunicación de Datos (ref: eirc0403.doc) 19 de febrero de 2004

***Atención**: para todos los ejercicios, suponga que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).*

Ejercicio 1

Se considera la siguiente variante del método de Vigenere: cuando se llega al final de la clave, cada letra de ésta se sustituye por la siguiente (A por B, ... Z por A).

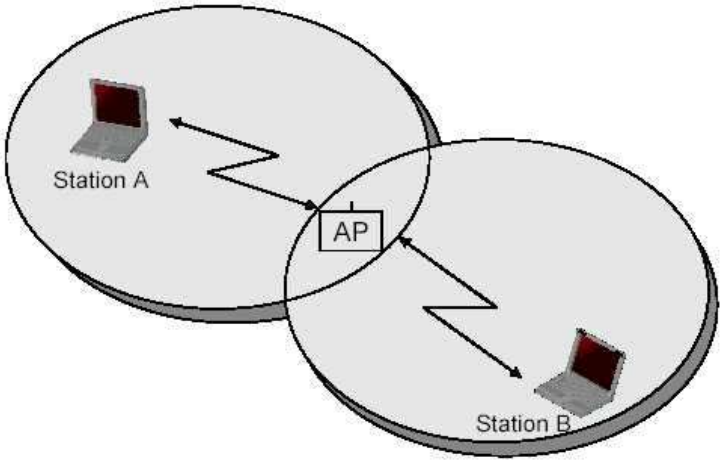
Se pide.

a) Dados : texto original: ”ABAD DE ABADIA”; clave ”ZAB”, determinar el texto cifrado (sugerir cómo se debe proceder con los caracteres espacio).
b) Especificar en un lenguaje de alto nivel, el algoritmo de encriptado.
c) Especificar en un lenguaje de alto nivel, el algoritmo de desencriptado.

Ejercicio 2

Se dispone de un medio simplex (unidireccional), tipo broadcast (inalámbrico). El dispositivo que transmite es capaz de determinar si, en un instante, el medio está siendo utilizado; pero al realizar un envío, no compara lo transmitido con lo recibido (como realiza ethernet). Para estos medios, se propone una política de acceso llamada CSMA/CA, (Carrier Sense Multiple Access/Collision Avoidance).

La comunicación entre las diferentes estaciones, se realiza a través de un AccessPoint (AP), el que se supone tiene un alcance que le permite escuchar los frames de todas las estaciones.



El esquema de utilización para el envío de información a través del medio, en resumen es el siguiente:

- Si el medio está libre, se envía un RTS (Request To Send), indicando dirección origen y destino, y duración del envío de todas las tramas involucradas (RTS, CTS, data y ACK).
- El equipo destino del mensaje, siempre que el medio esté disponible enviará un CTS (Clear To Send), donde incluirá la información del tiempo de reserva del medio, (para todas las tramas involucrada, incluyendo información obtenida del RTS recibido)
- Al recibir el equipo el CTS, se envía el frame con los datos.
- Si el frame se recibe en forma correcta se enviará un mensaje de ACK dando por finalizado el envío. En caso de no recibirse el ACK, se procederá a realizar nuevamente el procedimiento.

El resto de las estaciones escuchan todos los mensajes disponibles en su zona de cobertura del medio, y deben realizar una política que intente no interferir con la transmisión que se está realizando.

Se dispone de las siguientes funciones:

function medio_utilizado(): *boolean;* devuelve TRUE si el medio se está utilizando

function enviar_medio (data): integer; envía los bytes indicados en data por el medio, si la operación es exitosa devuelve 0.

function recibir_medio (): data; función bloqueante que devuelve la información recibida en el medio.

function calcular_tiempo_del_medio (data): integer; dado un mensaje pasado en data, devuelve el tiempo que consume el medio para su envío.

Se pide:

a) Especifique formato y tipo de frames requeridos por el protocolo, en especial RTS, CTS, data y ACK.
b) Especifique en un lenguaje de alto nivel el CSMA/CA propuesto.

Ejercicio 3

Se tiene un servidor DHCP (Dynamic Host Configuration Protocol) simplificado, el cual se encarga de asignar a los hosts una dirección IP al iniciar, y además de autenticar a los hosts respectivos.

El protocolo entre el cliente y el servidor funciona asi:

- El cliente envia un paquete DHCPDISCOVER vía broadcast, para ser encontrado por el servidor.
- El servidor determina la configuración y le contesta un DHCPOFFER que incluye la dirección IP.
- El cliente, en base a la oferta hecha por el servidor, hace un DHCPREQUEST, con lo cual el cliente acepta los datos generados para él.
- Posteriormente el servidor contesta DHCPACK.
- Antes de apagarse todo cliente debe hacer un DHCPRELEASE.

En el protocolo modificado para autenticar, el cliente incluye en el mensaje DHCPDISCOVER su clave pública para que el servidor envíe los posteriores mensajes encriptados con ella. En el mensaje de respuesta del servidor (encriptado), estará además de los datos correspondientes, la clave pública del servidor, que el cliente deberá utilizar para encriptar futuros mensajes.

El servidor mantiene una tabla con las IP asignadas hasta el momento asociadas al tiempo que resta de “alquiler” de esta IP. Además, antes de asignar por primera vez una IP (es decir, no está en su tabla de asignaciones) debe verificar que no haya un host que responda a la dirección IP que intenta asignar. Esto lo hace mediante un mensaje ECHO_REQUEST, y esperará un respuesta ECHO_RESPONSE por ECHO_TIMEOUT segundos. Si la recibe, es que esa IP está asignada. En caso contrario, reserva la dirección para el cliente que recién hizo el pedido. No hay a priori una asignación fija de IP's y cada IP nueva es dada por la función get_IP_from_pool() que devuelve una IP no asignada del pool de IP's. Además, el servidor deberá, cada TIMEOUT_LEASES segundos, verificar que los hosts a los cuales le asignó la dirección IP estén encendidos (mediante la forma ECHO_REQUEST), y darlos de baja en caso de no responder.

Se cuenta con las funciones:

function crypt_public_key(clave_pub,mensaje):mensaje_cifrado;

function decrypt_private_key(clave_priv,mensaje_cifrado):mensaje;

para utilizar en el caso del protocolo modificado.

Se pide:

a) Justifique brevemente para qué casos sirve la extensión al protocolo DCHP, para que acepte autenticación, en el caso de una LAN pública. Indique si permite autenticar en todos los casos, o puede tener fallas.
b) Escribir las estructuras de datos necesarias para el servidor de DHCP autenticado.
c) Especificar en un lenguaje de alto nivel el servidor DHCP autenticado.