ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
REDES DE COMPUTADORES
SEGUNDA EVALUACIÓN
I TÉRMINO 2013

Nombre: _____ ***Matrícula:*** _____

Sección A

1. Ilustre y explique brevemente en qué consisten los ataques ***sniffing***, ***spoofing*** y ***hijacking***. Identifique la violación de seguridad y el objetivo del intruso en cada caso. ***[12%]***
2. Explique brevemente qué es el ***process-to-process delivery*** indicando la capa en la que toma lugar y el papel desempeñado por los sockets. ¿Cuántos sockets se necesitan? ***[6%]***
3. ¿Para qué sirve el ***domain name system***? Ilustre y describa los tipos de *resolución* existentes. ***[8%]***
4. ¿Qué es una arquitectura de red ***peer-to-peer***? Explique brevemente cuatro tipos de redes ***P2P*** que usted conozca. Liste tres redes P2P para compartir archivos. **[8%]**

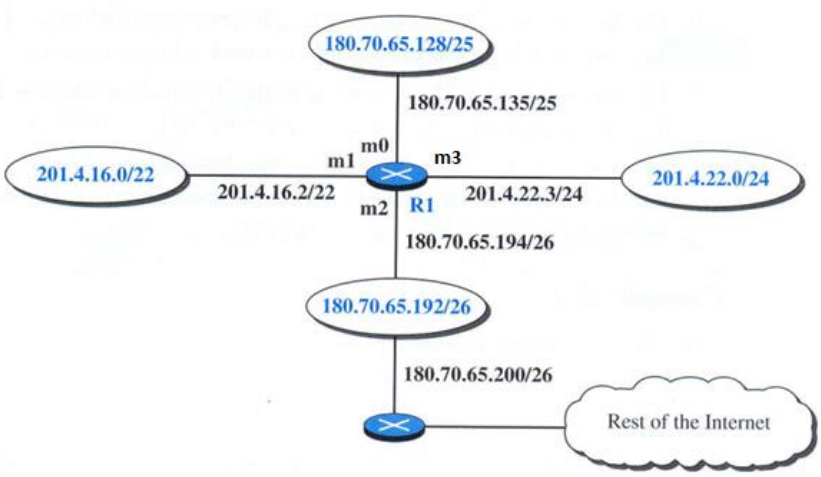
Sección B

5. Carlos, el profesor de Redes de Computadores está viajando a una conferencia y acaba de elaborar el examen en el camino. Necesita enviar el examen a Francisco, que será quien tome el examen. Desafortunadamente, Carlos sabe que algunos de sus estudiantes podrían tener acceso a los routers de la Facultad. Por esta razón, se encuentra preocupado en vista que el examen podría caer en manos de los estudiantes o podría ser reemplazado por uno falso. A buena hora, Carlos tiene varias opciones para uso de criptografía por seguridad. Al inicio del curso, Carlos y Francisco intercambiaron una llave simétrica compartida ***k***. Además, ambos usan PGP y saben la llave pública PGP del otro (PK_{Carlos} y $PK_{Francisco}$), correspondiente al par de llaves pública y privada (PK_{user}/SK_{user}). Asuma que las llaves no han sido comprometidas. Para cada uno de los siguientes casos, considere si el examen puede ser robado o reemplazado.
    a. Carlos firma el examen con SK_{Carlos} y lo envía ***[6%]***
        i. ¿Puede ser robado?
        ii. ¿Puede ser reemplazado?
    b. Carlos encripta y MACs el examen con la clave secreta ***k*** ***[6%]***
        i. ¿Puede ser robado?
        ii. ¿Puede ser reemplazado?
    c. Carlos se da cuenta que ha perdido la llave pública de Francisco, así que va al sitio Web de este y descarga la llave pública ***PK*** de Francisco. Luego, Carlos encripta el examen con esta llave ***PK***, lo firma con su llave privada SK_{Carlos} y lo envía. ***[6%]***
        i. ¿Puede ser robado?
        ii. ¿Puede ser reemplazado?
    d. Carlos decide ser un poco más sofisticado y crea su propio protocolo criptográfico. Así, antes que Carlos envíe el examen M a Francisco, calcula ***H = Hash (M)*** usando una función hash conocida como *SHA-1*. Luego el transmite el conjunto ***(M, H)*** a Francisco. Al recibir el conjunto, Francisco calcula ***H' = Hash (M)*** y acepta el examen como válido si y solo si ***H'== H***. Usted puede asumir que la función Hash es criptográficamente fuerte (es decir, es de una sola vía, resistente a colisiones y pre-image) ***[6%]***

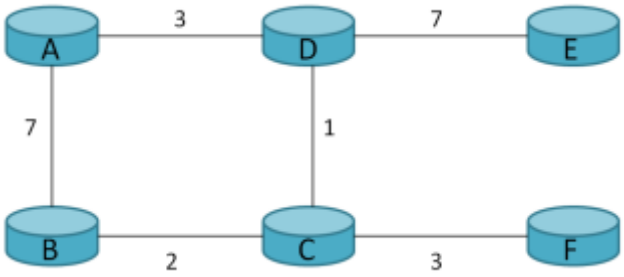
MSc. Carlos Mera Gómez

i. ¿Puede ser robado?
ii. ¿Puede ser reemplazado?

6. En la configuración de red que se muestra en la figura ***m0, m1, m2*** y ***m3*** son las interfaces del router ***R1***.
   a. Elabore la tabla de ruteo del router ***R1***. ***[6%]***
   b. ¿Cuál sería el proceso de reenvío si un paquete arriba a ***R1*** con la dirección de destino ***18.24.32.78***? ***[10%]***



7. Considere la red mostrada en la figura. Los nodos en esta red corren el algoritmo sincrónico de distance-vector usando intervalos de tiempo. En un determinado intervalo, todos los nodos reciben los vectores de distancia de sus vecinos, actualizan sus propios vectores de distancia y notifican los cambios en sus vectores de distancia a sus vecinos.
   a. Usando el algoritmo distance-vector, calcule los vectores de distancia del nodo D en cada slot de tiempo hasta que no haya más intercambio entre routers de actualizaciones de vectores de distancia. Asuma que inicialmente los nodos solo conocen los vectores de distancia a sus vecinos directos. ***[20%]***



   b. El incremento del costo de los enlaces toma mucho tiempo para ser reportado. Explique brevemente al menos dos soluciones que se podrían implementar para resolver este problema. ***[6%]***