Universidad de Alcalá

Fecha: 18 de mayo de 2015

DEPARTAMENTO DE AUTOMÁTICA
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Grado en Ingeniería Informática

REDES DE COMPUTADORES

Prueba de conjunto. Test

- **Cada afirmación correctamente contestada vale 0,05 puntos y cada fallo descuenta 0,025.**

Contestar las siguientes cuestiones marcando V (verdadero) o F (falso):

1. En las redes de circuitos virtuales, dos routers pueden establecer una conexión al nivel de la capa de red.
2. La técnica de la *inversa envenenada* consiste en que si un nodo z enruta hacia el nodo x a través de su vecino y, entonces x anuncia a y que su distancia a z es ∞.
3. Uno de los problemas de tener una red detrás de un router NAT es que no es útil para instalar servicios en ella, pues no es técnicamente posible encaminar el tráfico desde internet hacia dichos servicios.
4. Si un router anuncia la ruta `188.45.18.0/23`, otro distinto puede anunciar simultáneamente la ruta `188.45.16.0/20` y es correcto.
5. Los paquetes de descubrimiento DHCP lanzados por un cliente conectado a Ethernet llevan `255.255.255.255` como dirección IP destino en el datagrama y `00:00:00:00:00:00` como dirección MAC en la trama.
6. En el anuncio de una ruta mediante el protocolo BGP, el atributo AS-PATH contiene una lista de los sistemas autónomos que esa ruta ha atravesado hasta el momento.
7. Si el polinomio generador en un código CRC tiene grado r entonces el código corrector que se añade a los datos tiene $r+1$ bits.
8. Los protocolos de acceso al medio por división en tiempo (TDM) y por división en frecuencia (FDM) tienen iguales ventajas e inconvenientes, excepto que en FDM todos los nodos pueden enviar datos a la vez, mientras que TDM no lo permite.
9. Las tramas de Ethernet 10BASE-T, 100BASE-T y Gigabit no se diferencian en nada.
10. El espacio de direcciones MAC tiene un tamaño de 2^{46} direcciones.
11. Para que dos vectores-código en CDMA sean ortogonales es condición necesaria y suficiente que, al comparar bit a bit los dos vectores, se encuentre que el número de bits que tienen igual signo es igual al número de bits que tienen signo opuesto.
12. El diseño del protocolo CSMA/CA que se utiliza en IEEE 802.11 establece que para minimizar colisiones, se podrán utilizar opcionalmente tramas de tipo RTS/CTS.

13. Cuando un nodo, que está asociado a un punto de acceso AP_1 mediante el protocolo IEEE 802.11, se desplaza puede llegar a captar con más intensidad la señal de otro punto de acceso AP_2 y cambiar su asociación de uno a otro, pero a resultas de ese proceso se «caerán» todas las conexiones que tenga activas en ese momento.

14. En el ámbito de los enlaces por radio, el *problema del terminal oculto* consiste en que puede haber terminales asociados a un punto de acceso que, sin embargo, no detectan la presencia de ese punto de acceso, muchas veces a causa de obstáculos interpuestos.

15. En un enlace inalámbrico, es muy importante disponer de un buen código de detección de errores.

16. El formato de la trama en IEEE 802.11 es idéntico al de Ethernet, con la diferencia de que admite una carga útil de hasta 2312 bytes.

17. La cuarta dirección MAC que incluye la trama IEEE 802.11 se emplea únicamente para redes *ad hoc*.

18. En el protocolo IEEE 802.11i están separados el servidor de autenticación y el punto de acceso.

19. El servicio de autenticación mutua entre emisor y receptor significa que ambos pueden estar seguros de la identidad de su interlocutor.

20. Los sistemas de clave pública han de ser resistentes a los ataques al texto claro elegido.

21. Cuando se usa el modo CBC en un criptosistema de cifrado en bloque, no es posible obtener el descifrado de un determinado bloque sin haber previamente descifrado todos los bloques anteriores a él.

22. En la fase de acuerdo de una conexión SSL, el cliente y el servidor intercambian sus certificados.

23. Un criptosistema de clave pública se puede utilizar directamente para generar firma electrónica si se verifica que
$$\mathcal{K}^+\left(\mathcal{K}^-(m)\right) = \mathcal{K}^-\left(\mathcal{K}^+(m)\right)$$
para cualquier mensaje m y cualquier pareja de claves pública y privada $(\mathcal{K}^+, \mathcal{K}^-)$.

24. Sea H una función resumen. Para autenticar al emisor de un mensaje m, basta con que el receptor reciba el par $(m, H(m))$.

25. El uso de un *número distintivo* (es decir, de usar y tirar) en una conexión es condición necesaria y suficiente para evitar el ataque por interposición.

26. El protocolo SSL/TLS actúa a nivel de aplicación mientras que IPsec lo hace a nivel de red.

27. El protocolo IPsec en modo ESP establece un canal único de conexión entre dos pares por el que circulan los datagramas cifrados y autenticados mediante unas claves comunes.

28. Dado un resumen r generado mediante la función resumen H, encontrar una colisión en H equivale a encontrar un m tal que $H(m) = r$.

29. El sistema DES de cifrado en bloque utiliza una clave de 56 bits y se considera vulnerable a día de hoy.

30. La confianza de un certificado firmado por una cadena de autoridades de certificación viene marcada en última instancia por la confianza depositada en la autoridad de certificación raíz.

Universidad de Alcalá

Nombre:

Fecha: 18 de mayo de 2015

DEPARTAMENTO DE AUTOMÁTICA
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Grado en Ingeniería Informática
REDES DE COMPUTADORES

Prueba de conjunto. Problemas

- **Cada problema o cuestión vale 0,5 puntos.**

Problema 1

Sean dos nodos, A y B, conectados a un concentrador por sendos cables de longitudes respectivas d_A y d_B. La velocidad de propagación de la señal por esos cables es v. La velocidad de transmisión de los sistemas es R y la longitud de las tramas es L. Al atravesar el concentrador, la señal sufre un retardo adicional fijo de valor t_c.

Se utiliza el protocolo puro CSMA/CD donde cada nodo solo empieza a transmitir si el canal ha estado inactivo durante un tiempo de, al menos, t_r. Si durante la transmisión detecta una colisión, interrumpe instantáneamente la transmisión.

Supongamos que A y B tienen cada uno una trama para transmitir.

En estas condiciones, se pide:

1. Si el nodo A empieza a transmitir en el instante t_0, calcúlese en función de los parámetros citados más arriba a partir de qué instante de tiempo puede comenzar B el protocolo de transmisión sin que se produzcan colisiones.

2. La longitud L de la trama ¿ha de tener un valor mínimo para que funciones bien el protocolo? De ser así, ¿cuál es?

3. Suponiendo un perfecto acuerdo en las transmisiones de A y de B, de forma que no se produzcan colisiones, ¿cuál sería la eficiencia del canal, es decir, qué porcentaje de tiempo está realizando un trabajo de transmisión útil? Expresarlo en función de los parámetros del sistema.

Problema 2

Para calcular el resumen H de un mensaje, M, Alicia y Benito acuerdan utilizar la función iterativa

$$x_i = a \cdot (x_{i-1} + m_i) + b \pmod{m}$$

en donde se supone que el mensaje se divide en octetos (es decir, en grupos de ocho bits), $M = (m_1, m_2, \ldots, m_t)$, y se aplica iterativamente la función, de tal manera que el resumen del mensaje M es $H(M) = x_t$.

La clave pública RSA de Benito, bien conocida por Alicia, es $\{n = 667, e = 17\}$. Supongamos que Benito quiere mandar un mensaje firmado a Alicia y para ello, acuerda con ella que los parámetros de la función iterativa que usarán para firmar serán $m = 521$, $a = 17$, $b = 45$, y $x_0 = 27$.

Ahora, el mensaje que Benito manda a Alicia es su cuenta corriente, compuesta de los siguientes números: $M = 5482783192$. Cada número se codifica de como un octeto de acuerdo a la siguiente tabla

'0' $\Rightarrow$ 48	'1' $\Rightarrow$ 49	'2' $\Rightarrow$ 50	'3' $\Rightarrow$ 51	'4' $\Rightarrow$ 52
'5' $\Rightarrow$ 53	'6' $\Rightarrow$ 54	'7' $\Rightarrow$ 55	'8' $\Rightarrow$ 56	'9' $\Rightarrow$ 57

y empezando por el octeto menos significativo, es decir, $m_1 =$ '2', $m_2 =$ '9', etc.

Se pide:

1. Reproducir los pasos que tiene que dar Benito para enviar a Alicia dicho mensaje junto con la firma generada usando la función resumen y los parámetros citados, y el sistema RSA.

2. Reproducir los pasos que Alicia debe dar para decidir si el mensaje ha sido firmado verdaderamente por Benito o no.

Problema 3

Supongamos que el conjunto de las letras del alfabeto es {A, B, C, D, E, F, G, H, I, J, K, L, M, N, Ñ, O, P, Q, R, S, T, U, V, W, X, Y, Z}, que cada letra se codifica con su ordinal correspondiente (es decir, la A con 1, la B con 2, hasta las 27 letras y el espacio en blanco es el 0) usando 5 bits. Supongamos que se utiliza un cifrador de bloque con tamaño de bloque igual a 5 y trabajando en modo CBC. La tabla del cifrador en bloque es la siguiente:

$0 \Rightarrow 19$	$1 \Rightarrow 23$	$2 \Rightarrow 14$	$3 \Rightarrow 11$	$4 \Rightarrow 8$	$5 \Rightarrow 10$	$6 \Rightarrow 29$	$7 \Rightarrow 30$
$8 \Rightarrow 4$	$9 \Rightarrow 17$	$10 \Rightarrow 5$	$11 \Rightarrow 3$	$12 \Rightarrow 25$	$13 \Rightarrow 15$	$14 \Rightarrow 2$	$15 \Rightarrow 13$
$16 \Rightarrow 24$	$17 \Rightarrow 9$	$18 \Rightarrow 31$	$19 \Rightarrow 0$	$20 \Rightarrow 26$	$21 \Rightarrow 22$	$22 \Rightarrow 21$	$23 \Rightarrow 1$
$24 \Rightarrow 16$	$25 \Rightarrow 12$	$26 \Rightarrow 20$	$27 \Rightarrow 28$	$28 \Rightarrow 27$	$29 \Rightarrow 6$	$30 \Rightarrow 7$	$31 \Rightarrow 18$

La tabla significa que el 0 se cifra en 19, el 1 en 23, el 2 en 14, etc. Un receptor recibe, por orden, los siguientes bloques cifrados:

```
17, 27, 20, 20, 24, 12, 25, 6, 13, 11, 2, 9, 12
```

Descifrar el mensaje transmitido.

Cuestión 1

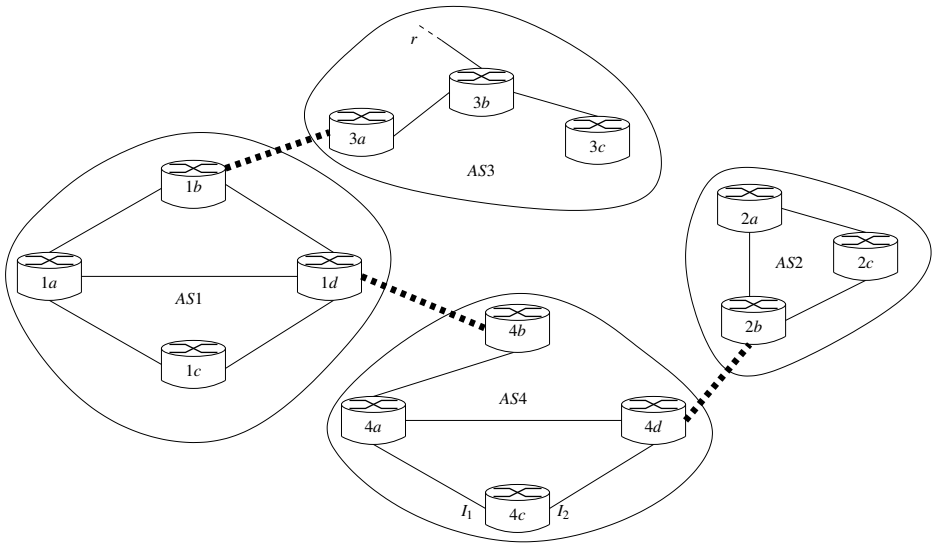
Supóngase que en un determinado espacio (una biblioteca, por ejemplo) existen dos puntos de acceso WiFi, AP_1 y AP_2, tales que cada uno permite acceder a distintas subredes IP. Contestar razonadamente las siguientes preguntas.

1. En el supuesto de que AP_1 y AP_2 estén funcionando en el mismo canal (por ejemplo, en el canal 1), ¿dejaría de funcionar el protocolo IEEE 802.11? Explicar qué ocurre si dos nodos, asociados cada uno con distinto punto de acceso, emiten una trama simultáneamente.

2. Si existe algún problema en el caso anterior, ¿se arreglaría utilizando el protocolo CDMA?

3. ¿Habría alguna otra posibilidad?

Cuestión 2



Se muestra en la figura un conjunto de sistemas autónomos cada uno de los cuales ejecuta el protocolo de enrutamiento interno RIP y se utilizan los protocolos iBGP y eBGP para el enrutamiento entre sistemas autónomos. El router 3*b*, situado en el *AS*3, conoce cómo enrutar hacia el prefijo de subred *r*. Contestar las siguientes preguntas, justificando claramente cada respuesta.

1. ¿Qué protocolo(s) se necesita(n) para que los routers 1*b*, 4*d* y 2*a* se enteren de la existencia del prefijo *r* y cómo enrutar hacia él?

2. ¿Cuál de las dos interfaces, I_1 o I_2, usará el router 4*c* para encaminar los datagramas con destino a *r*?

3. Cuando el router 2*b* reciba el anuncio de la ruta hacia *r*, ¿qué valor tendrá el atributo AS-PATH? ¿Y el atributo NEXT-HOP?

4. Si ahora aparece una nueva conexión (no dibujada) entre 2*a* y 3*c*, ¿cuál de sus interfaces usará 4*c* para encaminar los datagramas con destino a *r*?