Universidad de Alcalá

Redes de computadores

Problemas propuestos

Raúl Durán Díaz

Departamento de Automática
Universidad de Alcalá

Alcalá de Henares, España

Raúl Durán Díaz
Departamento de Automática
Universidad de Alcalá
E-28871 Alcalá de Henares, España
raul.duran@uah.es

El autor, consciente de la debilidad del pensamiento humano, ruega y agradece al piadoso lector que le comunique cualquier error que pueda encontrar en las siguientes páginas.

El presente documento es evolutivo. Los campos de revisión y fecha que aparecen a continuación indicarán cuál es la versión más moderna.

Revisión: 1.9
Fecha: 15 de junio de 2018

Índice general

Capítulo 4

La capa de red

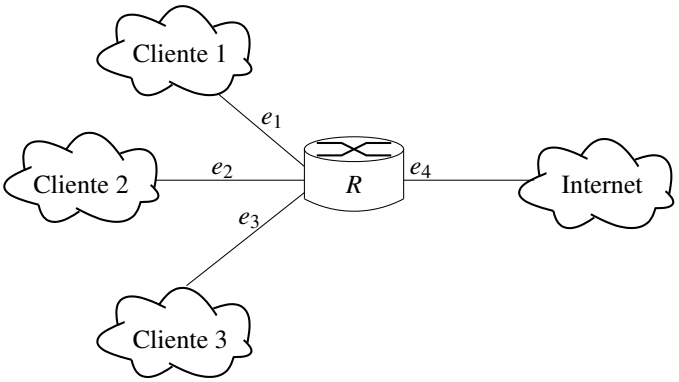
1. Recordemos que en la cabecera de IPv4 existen dos *flags*, a saber, el flag MF (*more fragments*) y el DF (*don't fragment*). Contestar a las siguientes cuestiones.

   a) Explicar qué significa el término MTU (*maximum transmission unit*), por qué existe, y qué es la MTU de una ruta.

   b) Explicar qué influencia puede tener el valor de la MTU en el rendimiento de una red.

   c) Explicar cómo se puede implementar un protocolo que permita a un nodo emisor de un datagrama averiguar la MTU de la ruta hasta el receptor de dicho datagrama. Suponer que se pueden generar las cabeceras a voluntad y están disponibles cualesquiera de los protocolos existentes a nivel de capa de red.

2. Un proveedor de servicios de internet (ISP) tiene tres clientes corporativos, todos ellos conectados al mismo *router R*, administrado por el ISP, según se ve en la figura. El ISP realiza la siguiente asignación de redes a cada cliente:



   - Al primero le asigna las redes:
     `212.128.16.0/24`, `212.128.17.0/24`, `212.128.18.0/24`, `212.128.19.0/24`.
   - Al segundo le asigna las redes:
     `212.128.20.0/24`, `212.128.21.0/24`, `212.128.22.0/24`.

- Por fin, al tercero le asigna la red: `212.128.23.0/24`.

Rellenar las entradas de la tabla enrutamiento de *R* de manera que los datagramas se enruten correctamente y se minimice el número de entradas de dicha tabla.

3. Supongamos un *router* NAT con una dirección IP de `212.128.55.27` en el lado WAN. El lado LAN está conectado a una red con prefijo `192.168.10.0/24` a la que también hay conectados tres equipos terminales con una interfaz de red cada uno.

   a) Dar direcciones IP congruentes a todas las interfaces de la LAN.

   b) Supongamos que cada equipo terminal ha establecido una conexión HTTP con el servidor web `www.uc3m.es`, cuya dirección IP es `213.134.43.166`. Se pide dar valores congruentes para las direcciones IP origen y destino, y puerto TCP origen y destino tanto en el lado LAN como en el lado WAN para tres parejas de datagramas, donde cada pareja va asociada a cada una de esas conexiones.

   c) Más tarde nos encontramos en la tabla NAT del *router* unas entradas como las siguientes:

Lado WAN	**Lado LAN**
`212.128.55.27, 5080`	`192.168.10.10, 3357`
`212.128.55.27, 5081`	`192.168.10.10, 3358`
`212.128.55.27, 5082`	`192.168.10.11, 5439`
`212.128.55.27, 5050`	`192.168.10.10, 80`

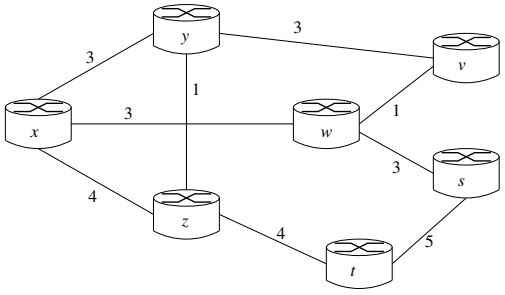
   A la vista de esas entradas, dar una posible interpretación de lo que está pasando.

4. Consideremos la red de la figura. Utilizando el algoritmo de Dijkstra, se pide:

   a) Calcular las rutas de coste mínimo y sus costes desde el nodo *s* a todos los nodos de la red.

   b) Dibujar el árbol de rutas de coste mínimo desde el nodo *s*.

   c) Escribir la tabla de reenvío resultante para el nodo *s*.



5. Se necesita transmitir un mensaje de tamaño M bits a lo largo de una ruta que ha de atravesar L equipos (por ejemplo, en la figura se tiene $L = 3$), troceado en paquetes que contienen k bits de datos y h bits de cabecera (un número fijado) cada uno (supóngase que $M \gg h + k$). El modo de transmitir es *almacenamiento y reenvío*, es decir, cada equipo recibe todo un paquete antes de empezar a transmitirlo al siguiente equipo. Además, cada equipo puede estar emitiendo y recibiendo a la vez. La velocidad de transmisión de todos los enlaces es la misma e igual a R bits por segundo. El tiempo de propagación entre cada equipo es constante y de valor t_p. El tiempo de procesamiento es despreciable.

   a) ¿Cuál será el número total de bits que se necesita transmitir?

   b) ¿Cuál es el retardo total, es decir, el tiempo necesario para conseguir la transmisión de todo el mensaje, en función de los parámetros?

   c) ¿Cuál es el valor de k que minimiza ese retardo total? Aplicarlo al caso particular en que $M = 1$ MB, $L = 5$, $h = 64$ bytes, $t_p = 10^{-3}$ s y $R = 1$ Gb/s. ¿Qué velocidad de transmisión efectiva obtenemos?

6. A lo largo de todo el problema consideramos que la cabecera IP tiene una longitud fija de 20 bytes. En estas condiciones, supongamos que un datagrama IP de 1684 bytes de longitud llega a un enlace cuya MTU es tan solo de 536 bytes.

   Describir los campos *longitud de datagrama*, *identificador*, *indicador* y *desplazamiento* de todos y cada uno de los fragmentos que el router ha de generar para introducirlos en el enlace.

   Nota: Se pueden elegir valores aleatorios cuando se vea necesario.

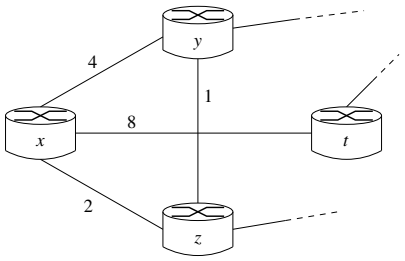
7. Consideremos la red de la figura, con los costes de enlace indicados. Supongamos que se usa el algoritmo de vector distancia para calcular las tablas de reenvío. Los nodos y, z, t han calculado sus vectores de mínima distancia a un cierto nodo u (no visible en la figura) y el resultado es que $d_y(u) = 3$, $d_z(u) = 3$, $d_t(u) = 1$. En ese mismo instante, x tan solo conoce las distancias a sus vecinos (expresadas en la figura) y está inicialmente a distancia infinita de u.

   a) Cuando los nodos vecinos de x le entreguen sus vectores de distancia mínima, ¿qué distancia mínima calculará x para ir a u? ¿Qué entrada registrará en su tabla de reenvío?

   b) Cuando x calcule su distancia mínima a u y la difunda a sus vecinos, ¿cambiarán estos sus respectivas distancias a u? Justificar la respuesta.

   c) Si de repente z se desconecta de u (suponemos que x, w no enrutan a través de z y por tanto no se ven afectados), de modo que $d_z(u) = \infty$, ¿cuál será la nueva distancia mínima de x a u? ¿Cambia la tabla de reenvío de x? ¿Qué le ocurrirá al nodo z?

d) ¿Qué valores debieran tener $d_y(u)$, $d_z(u)$ y $d_t(u)$ para que la ruta desde x hasta u tuviera el mismo coste enrutando a través de cualquiera de los vecinos y este coste fuera el mínimo? Suponer que $d_y(u)$, $d_z(u)$ y $d_t(u)$ han de tener como mínimo el valor 1.



8. En una determinada red se ha ejecutado el algoritmo de Dijkstra, obteniéndose la tabla que se ve más abajo. Basándose en ella, se pide

   a) Reproducir en un dibujo todo lo que se pueda deducir acerca de la estructura de esa red, anotando también los costes de cada enlace que puedan inferirse de la tabla.

   b) ¿Cuál es el nodo origen de las rutas? Proporcionar la tabla de enrutamiento partiendo de dicho nodo origen.

   c) Dibujar el árbol de rutas de coste mínimo a los demás nodos, indicando el coste de cada enlace.

   d) Calcular ahora mediante el algoritmo de Dijkstra las rutas mínimas en esa misma red pero tomando como nodo origen el *w*. Se pide también para este caso, el árbol de coste mínimo y la tabla de enrutamiento.

Paso	**valor N′**	$D(x), p(x)$	$D(z), p(z)$	$D(w), p(w)$	$D(v), p(v)$	$D(s), p(s)$	$D(t), p(t)$
0	y	3, y	**1, y**	—	3, y	—	—
1	yz	**2, z**		—	3, y	—	5, z
2	yzx			4, x	**3, y**	—	5, z
3	yzxv			**4, x**		—	5, z
4	yzxvw					8, w	**5, z**
5	yzxvwt					**6, t**	
6	yzxvwts						

Capítulo 5

La capa de enlace

1. Sea una codificación tal que la distancia de Hamming mínima entre sus códigos es H. Supongamos que tal codificación se usa en un enlace y que en ese enlace se produce un error en un bit con probabilidad p, independiente para cada bit. ¿Cuál es la probabilidad de que se transmita un código erróneo y pase inadvertido al receptor? Justificar adecuadamente la respuesta.

2. Un enlace punto a punto emplea el código de redundancia cíclica (CRC) para detectar errores, con un polinomio generador $g(x) = x^6 + x^5 + x^3 + x^2 + x + 1$. El receptor ha recibido una trama que lleva los datos junto con el CRC concatenado al final (es decir, son los bits de menor peso). Dicha trama resulta ser: $(1,0,1,1,0,0,0,1,1,0,1,1,0,1,1,0,0,1,0,0,1,1)$. Contestar las siguientes cuestiones.

   a) ¿Cuáles son los bits que corresponden a los datos y cuáles los que corresponden al CRC?

   b) Comprobar si la trama ha llegado bien o si ha habido algún error, justificando la respuesta.

   c) Justificar si el CRC así definido proporciona o no el chequeo de paridad par.

3. En una red de área local con medio compartido se utiliza el protocolo ALOHA ranurado. A dicha red se encuentran conectados tres nodos, A, B y C. Las tramas que todos transmiten son de longitud fija, L, y el canal tiene un ancho de banda R. Supongamos que las probabilidades de transmisión respectivas de cada nodo son p_A, p_B y p_C, distintas en general.

   a) ¿Cuál será la probabilidad de que A consiga transmitir una trama con éxito?

   b) ¿Cuál será la probabilidad de que cualquier nodo transmita una trama con éxito?

   c) Si $p_A = 20\,\%$, $p_B = p_C = 30\,\%$, $L = 1500$ bytes, $R = 100$ Mb/s, cuál será la tasa media de transmisión de todo el sistema?

   d) ¿Qué probabilidad de transmisión tendría que tener A para que su tasa media de transmisión fuera el doble que la de B y C, supuestas estas igua-

les? Obtener una expresión general y aplicarlo después al caso en que $p_B = p_C = 30\,\%$.

4. Supongamos una red Ethernet tipo cable coaxial con velocidad de transmisión R. Para ese tipo de red modelamos la eficiencia, η, como

$$\eta = \frac{1}{1 + 2e\frac{t_{\text{prop}}}{t_{\text{trans}}}},$$

siendo e la base de los logaritmos neperianos, t_{prop} el tiempo de propagación de la señal y t_{trans} el tiempo de transmisión.

Sean ahora dos nodos conectados a esa red y separados por una distancia d. Si la velocidad de propagación de la señal en el cable es v, se pide

a) ¿Cuál será la longitud de trama L que proporciona una eficiencia η_0 en función de los parámetros anteriores?

b) Si $R = 100$ Mb/s, $v = 2 \times 10^8$ m/s, $L = 1500$ bytes, ¿qué rango de distancias de separación entre los nodos proporciona una eficiencia de al menos 0,7?

5. Sea un medio compartido en el que están presentes solamente dos nodos, A y B, separados una distancia d. La velocidad de propagación de la señal en ese medio es v. Cada nodo emite a una velocidad de transmisión R. La longitud de las tramas es igual a L.

Se utiliza el protocolo puro CSMA/CD donde cada nodo sondea el canal antes de transmitir y, si está libre, empieza la transmisión de manera inmediata. Si durante la transmisión detecta una colisión, interrumpe instantáneamente la transmisión.

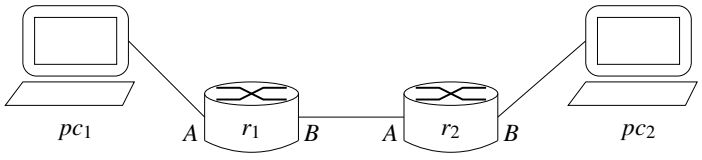
En estas condiciones, se pide:

a) Si el nodo A empieza a transmitir en el instante t_0, ¿durante qué periodo de tiempo debiera B estar en silencio para que la transmisión se termine sin colisiones?

b) Si B detecta señal en el canal antes de transmitir, ¿cuánto tiempo debería esperar para tener cierta garantía de encontrar el canal libre?

c) 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 d, v, L y R.

6. Considere la red Ethernet de la figura en donde los routers están correctamente configurados para enrutar paquetes desde pc_1 a pc_2 y viceversa:



Los datos para cada interfaz de red son:

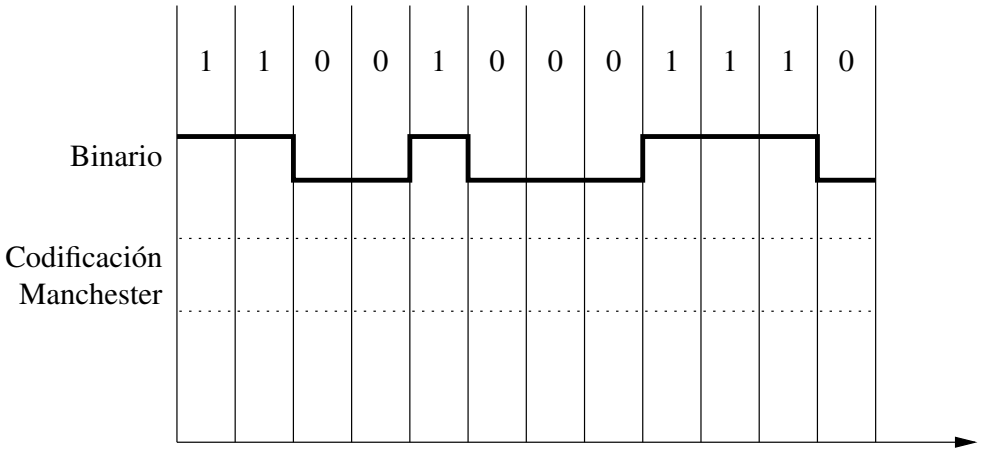
Equipo	Interfaz	Dirección IP	Dirección MAC
pc_1		212.100.1.10	C1:C1:C1:C1:C1:C1
pc_2		159.23.1.10	C2:C2:C2:C2:C2:C2
r_1	*A*	212.100.1.1	A1:A1:A1:A1:A1:A1
r_1	*B*	12.10.1.1	B1:B1:B1:B1:B1:B1
r_2	*A*	12.10.1.2	A2:A2:A2:A2:A2:A2
r_2	*B*	159.23.1.1	B2:B2:B2:B2:B2:B2

Inicialmente supondremos que las tablas ARP de todos los equipos están vacías. En estas condiciones pc_1 quiere enviar un segmento TCP a pc_2.

Se pide dibujar cronológicamente todo el tráfico de tramas que van a circular por cada uno de los enlaces presentes en la figura. Para las tramas que encapsulen datagramas IP, se pide dar los valores de los campos *dirección IP origen*, *dirección IP destino* correspondientes a la cabecera IP y los campos *MAC origen*, *MAC destino* correspondientes a la cabecera Ethernet.

Para las tramas que encapsulen ARP, se piden los campos *MAC origen*, *MAC destino* de la cabecera Ethernet y los valores de *dirección fuente hardware*, *dirección fuente del protocolo IP*, *dirección destino hardware*, *dirección destino del protocolo IP*, encapsulados en esa trama.

7. Obtenga la codificación Manchester de la siguiente señal binaria dibujándola sobre el diagrama.



   a) Indique alguna razón que, a su juicio, haga aconsejable este tipo de codificación.

   b) Sabemos que el preámbulo de una trama Ethernet está constituido por una ráfaga de 7 bytes, cada uno de ellos con esta estructura: $(1,0,1,0,1,0,1,0)$. ¿Qué aspecto tendrá la señal codificada en codificación Manchester correspondiente a tal preámbulo? ¿Qué frecuencia base tendrá, en relación con la velocidad de transmisión en bits por segundo?

8. Supongamos una red de área local que ejecuta el protocolo MAC propio de Ethernet. Contestar las siguientes cuestiones.

a) Tras la quinta colisión, ¿cuál es la probabilidad de que un nodo espere un número $k = 7$ de periodos?

b) Si la velocidad de la red es 100 Mb/s, ¿a cuántos segundos equivale una espera de $k = 7$ periodos?

Capítulo 8

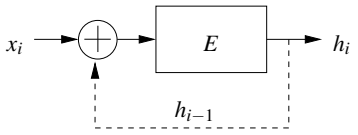
Criptografía y seguridad de redes

1. Tomemos el conjunto de las letras del alfabeto {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}, y codifiquemos cada letra 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 dispone de un cifrador de bloque, E, con tamaño de bloque igual a 5 bits con la siguiente tabla de cifrado:

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

   La tabla significa que el 0 se cifra en 19, el 1 en 23, el 2 en 14, etc. Con dicho cifrador en bloque, se construye una función resumen de acuerdo al esquema CBC:



   es decir, $h_i = E(x_i \oplus h_{i-1})$, $1 \leq i \leq n$

   con un valor fijo inicial de $h_0 = 1$. De este modo, si un mensaje está compuesto de n bloques, $m = (x_1, x_2, \ldots, x_n)$, su resumen se construye calculando los sucesivos valores h_1, h_2, $\ldots$, de modo que, finalmente, $H(m) = h_n$ (obsérvese que, en realidad, cada bloque es del tamaño de una letra).

   En un criptosistema de clave pública, Begoña tiene como clave pública los valores $(n = 253, e = 13)$ y Alicia, otra usuaria, tiene como clave pública $(n = 323, e = 11)$. Para la realización de la firma, ambas acuerdan públicamente usar como resumen del mensaje el esquema CBC explicado más arriba.

   Alicia envía a Begoña un mensaje cifrado (considerando que cada letra es un bloque, y cifrando letra por letra) y firmado. El criptograma, c, y la firma, f, son:

$$c = (144, 136, 26, 126), \quad f = 118.$$

Naturalmente, Eva está espiando y captura el criptograma c y la firma f. Se pide explicar cómo debe atacar Eva el sistema para quebrantar las claves de Alicia y Begoña, de modo que consiga

- averiguar cuál era el mensaje original,
- y si realmente ese mensaje está firmado por Alicia o no.

2. La siguiente función iterativa

$$x_{i+1} = x_i^2 \pmod{n}$$

se puede usar como generadora de bits aleatorios de la siguiente manera:

a) se da un valor inicial x_0, que es la clave;

b) se aplica la función anterior iterativamente cuantas veces se quiera para obtener los valores $x_1, x_2, \ldots$

c) la secuencia de bits aleatorios está constituida por el $\mathsf{LSB}(x_i)$, con $i = 1,2,\ldots$, es decir, por el bit menos significativo de cada valor x_i (exceptuando x_0).

Dos usuarias, Alicia y Begoña, quieren intercambiarse un mensaje secreto mediante un sistema criptográfico con cifrado en flujo, utilizando el anterior generador con un valor del módulo, previamente acordado, $n = 437$.

Para intercambiarse la clave (que es el valor inicial x_0) usan el método de intercambio de clave de Diffie-Hellman, cuyos parámetros son los siguientes: el grupo es $\mathbb{Z}_{257}^* = \{1,2,\ldots,256\}$, (con la operación de multiplicar módulo 257), y el generador del grupo es $g = 3$ (es decir, todos los elementos del grupo son potencias de 3 módulo 257).

Al comenzar el protocolo, Alicia elige como exponente aleatorio $a = 108$ y recibe de Begoña el elemento $46 \in \mathbb{Z}_{257}^*$.

Con estos datos, se pide

a) ¿Cuál es el valor de la clave x_0 intercambiada mediante el protocolo Diffie-Hellman?

b) Begoña ha enviado a Alicia una cadena de bits cifrada con la clave secreta intercambiada, que resulta ser $(0,1,1,1,1,1,1,0)$ (donde el bit menos significativo es el primero que se ha transmitido). ¿Qué cadena obtendrá Alicia cuando descifre la cadena enviada por Begoña?

3. En un criptosistema de clave pública, Begoña tiene como clave pública los valores $(n = 323, e = 67)$ y Alicia, otra usuaria, tiene como clave pública $(n = 187, e = 103)$. Para la realización de la firma, ambas acuerdan usar como resumen del mensaje la suma de comprobación en 8 bits. Acuerdan también usar el conjunto de las letras del alfabeto, {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}, codificando cada letra con su ordinal correspondiente (es decir, la A se codifica como 1, la B como 2, etc., hasta las 27 letras).

Se pide simular un ataque que haría Eva para conseguir:

a) Quebrantar la clave pública de Begoña y averiguar cuál es su clave privada correspondiente.

b) Enviar a Alicia el mensaje `LEON`, cifrando cada letra por separado de acuerdo a la codificación explicada arriba.

c) Firmar un resumen (generado como se indica arriba) del anterior mensaje, para hacer creer a Alicia que realmente se lo está mandando Begoña.

d) Reproducir los pasos que dará Alicia para verificar la firma que ella cree procedente de Begoña.

4. Supongamos que la clave pública RSA de una autoridad de certificación *AC* es $(n = 899, e = 817)$.

   En un momento dado, *AC* recibe una petición de un cliente *C* para que le genere un certificado de clave pública. El certificado consta de dos campos de tamaño 1 byte cada uno, que contienen la clave pública de *C*: el primer campo almacena el valor $n = 221$ y el segundo campo almacena $e = 133$.

   El cometido de la autoridad *AC* es generar la firma RSA del resumen de la clave pública de *C* y añadirla al certificado. Dicho resumen consiste en generar la suma de comprobación (hecha en 8 bits) de los dos campos descritos en el párrafo anterior.

   Se pide:

   a) Suplantar a *AC* y generar el certificado de la clave pública del cliente *C*, reproduciendo para ello los cómputos que realizaría *AC* para crear tal certificado.

   b) Justificar, a la vista de los resultados anteriores, si la clave pública de *AC* es segura o no.

5. 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:

a) 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.

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

6. 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.

7. Supongamos que la clave pública RSA de una autoridad de certificación *AC* es $(n = 899, e = 11)$. Esta clave es perfectamente conocida por un determinado cliente.

   En un momento dado, este cliente recibe un certificado de clave pública de un servidor *S*. El servidor *S* indica al cliente que tal certificado ha sido firmado por la autoridad *AC*. El certificado consta de dos campos de tamaño 1 byte cada uno, que contienen la clave pública de *S*: el primer campo almacena el valor $n = 221$ y el segundo campo almacena $e = 133$. Además, el certificado contiene la firma realizada por la autoridad de certificación *AC* sobre la suma de comprobación (hecha en 8 bits) de los dos campos anteriores: el valor de dicha firma es $f = 99$.

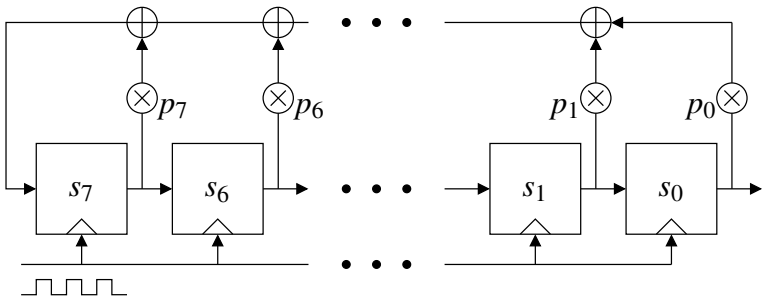
   Se pide reproducir los cómputos que ha de realizar el cliente para asegurarse de que el certificado del servidor es válido. Según tal cómputo, ¿es válido ese certificado?

8. Utilizando la siguiente tabla ASCII parcial:

"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

generar la firma RSA del mensaje que consta de los caracteres “1215”, usando como función resumen la suma de comprobación de 8 bits. La clave privada del usuario que va a firmar es $p = 13$, $q = 17$, $d = 7$.

9. Supóngase que dos usuarias, Alicia y Begoña, disponen de un generador de bits aleatorios LFSR como el de la figura:



Recordemos que la ecuación que nos da el valor del bit que se va a insertar sobre el registro s_7 es

$$s_7 \Leftarrow p_7 s_7 + p_6 s_6 + \cdots + p_1 s_1 + p_0 s_0 \pmod 2.$$

Supóngase que este LFSR particular está implementado de modo que $p_0 = p_2 = p_3 = p_4 = 1$, mientras que el resto está a 0; esto no es modificable por un usuario. Por otro lado, la clave es el valor inicial de los registros, es decir, $s = (s_7, \ldots, s_0)$ que, obviamente, sí es configurable. Al empezar a funcionar, el LFSR emite en primer lugar los ocho bits de la clave y, a partir del noveno, empieza la secuencia cifrante utilizable.

Alicia y Begoña quieren intercambiarse un mensaje secreto mediante un sistema criptográfico con cifrado en flujo, utilizando el anterior generador. Para intercambiarse la clave, s, que es el valor inicial de los registros, usan el método de intercambio de clave de Diffie-Hellman, configurado de modo que usa el grupo constituido por el conjunto de números $\mathbb{Z}_{257}^* = \{1, 2, \ldots, 256\}$ con la operación de multiplicar módulo 257. El generador del grupo es $g = 3$ (es decir, todos los elementos del grupo son potencias de 3 módulo 257).

Al comenzar el protocolo, Alicia elige como exponente aleatorio $a = 49$ y Begoña elige como exponente aleatorio $b = 170$.

   a) ¿Cuál es el valor de la clave s intercambiada entre Alicia y Begoña mediante el protocolo Diffie-Hellman?

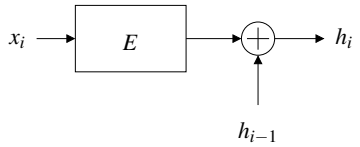
   b) Begoña genera una secuencia cifrante de 10 bits de longitud usando la clave intercambiada. Se pide dar dicha secuencia cifrante.

   c) Por último, Begoña cifra el número $n = 815$ usando la secuencia cifrante del apartado anterior. Se pide dar dicho criptograma.

10. Supongamos que se dispone de un cifrador de bloque, E, con tamaño de bloque igual a 5 bits con la siguiente tabla de cifrado:

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

La tabla significa que el 0 se cifra en 19, el 1 en 23, el 2 en 14, etc. Con dicho cifrador en bloque, se construye una función resumen de acuerdo al siguiente esquema:



es decir, $h_i = E(x_i) \oplus h_{i-1}$, para $1 \leq i \leq n$

con un valor fijo inicial de $h_0 = 1$. De este modo, si un mensaje está compuesto de n bloques, $m = (x_1, x_2, \ldots, x_n)$, su resumen se construye calculando los sucesivos valores h_1, h_2, ..., de modo que, finalmente, $H(m) = h_n$ (obsérvese que, en realidad, cada bloque es del tamaño de una letra).

Con la función resumen anterior, H, se construye un código de autenticación e integridad, *HMAC*, definido de la siguiente manera:

$$HMAC(m) = H(s||H(s||m)),$$

donde $||$ representa el operador de concatenado y s es un secreto compartido.

En lo que sigue, supondremos que cada letra del conjunto de las letras del alfabeto {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} 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.

Alicia y Begoña se intercambian un secreto, $s = \{L, M\}$, que comparten entre ellas. Begoña recibe de Alicia el mensaje $m = \{R, I, S, A\}$ y un código de autenticación $HMAC = \{S\}$. Se plantean las siguientes cuestiones.

a) La función resumen tal como ha sido definida, ¿presenta grandes cambios en la salida cuando cambia poco la entrada? Justificar la respuesta mediante un ejemplo.

b) El mensaje que recibe Begoña, ¿procede realmente de Alicia y está íntegro? Dar todos los pasos para comprobarlo.

Bibliografía

Básica

- ☐ James F. Kurose, Keith W. Ross. *Redes de computadoras: un enfoque descendente*. 7ª edición. Pearson Educación, Madrid, 2017.

Complementaria

- ☐ William Stallings. *Comunicaciones y Redes de Computadores*. 7ª edición traducida. Prentice Hall, 2004.
- ☐ Andrew S. Tanenbaum. *Redes de computadoras*. 4ª edición traducida. Prentice Hall, 2003.
- ☐ Alberto Leon-Garcia, Indra Widjaja. *Redes de comunicación, conceptos fundamentales y arquitecturas básicas*. McGraw-Hill, 2002.
- ☐ Dimitri P. Bertsekas, Robert G. Gallager. *Data Networks*. Second edition. Prentice Hall, 1992.
- ☐ F. Halsall. *Redes de computadoras e Internet*. 5ª edición traducida. Pearson Educación, 2006.
- ☐ Behrouz A. Forouzan. *Transmisión de datos y redes de comunicaciones*. 4ª edición traducida. McGraw-Hill, Madrid, 2007.
- ☐ W. Richard Stevens. *TCP/IP Illustrated, Volume 1: The Protocols*. First edition. Addison-Wesley, 1994.
- ☐ Francisco Manuel Márquez García. *UNIX programación avanzada*. 3ª edición. Ra-Ma, 2004.
- ☐ Paul Deitel, Harvey M. Deitel. *C: how to program*. Sixth edition. Prentice Hall, 2009.
- ☐ Bruce Eckel. *Thinking in Java*. Third edition. Prentice Hall, 2003.

Complementaria (equivalente en inglés)

- ☐ James F. Kurose, Keith W. Ross. *Computer networking: a top-down approach*. Seventh edition. Pearson Education, 2017.
- ☐ William Stallings. *Data and Computer Communications*. Ninth edition. Prentice Hall, 2010.
- ☐ Andrew S. Tanenbaum. *Computer networks*. Fourth edition. Prentice Hall, 2003.

□ Alberto Leon-Garcia, Indra Widjaja. *Communication Networks. Fundamental concepts and key architectures*. McGraw-Hill International Editions, Singapore, 2000.