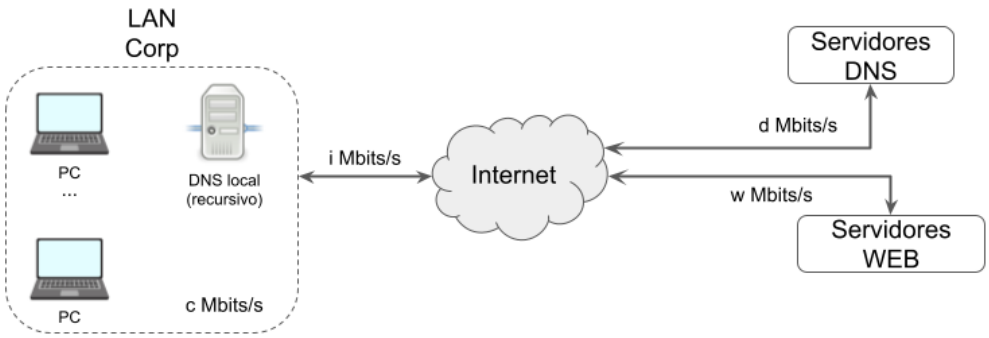
Las respuestas no razonadas, o no que utilicen estrictamente la notación indicada, no serán consideradas como válidas, aunque sean correctas. Recuadra CLARAMENTE tu respuesta a cada apartado. Consigna tu NIA, nombre y apellidos completos en todas las hojas que entregues.

1. **PROBLEMA 1** 3

Imagina el siguiente escenario:



en el que DNS hace referencia a cualquier servidor DNS, y WEB a cualquier servidor Web. En el interior de la LAN, el ancho de banda es c MBit/s. Además,

- Las peticiones y respuestas DNS tienen un tamaño medio de d_1 y d_2 bytes, respectivamente. En este momento, el DNS local solo contiene los registros que se muestran en la tabla inferior.
- Las peticiones y respuestas WEB tienen un tamaño medio de w_1 y w_2 bytes, respectivamente, a no ser que se indique otra cosa.

En esta situación, responde a las siguientes cuestiones, recuadrando claramente la solución a cada apartado:

1. Calcula el tiempo medio de procesamiento o carga para las siguientes acciones:
   a) Un usuario de la LAN desea visitar la URL '`http://www.uam.es`'.
   b) Tras finalizar la carga del recurso anterior, el mismo usuario anterior descarga ahora el fichero '`http://www.uam.es/bienvenida.mp4`', de 300 MBytes de tamaño.
   c) A continuación, el usuario vista la página `http://www.uam.es/info.html`, que contiene a su vez 5 objetos embebidos de t bytes cada uno. El servidor no tiene límite de conexiones simultáneas desde el mismo cliente, y no soporta *pipelining* de recursos.
2. Finalmente, el usuario establece una llamada de videoconferencia con un usuario externo a la institución. Si cada paquete de datos ocupa 1Kbyte, ¿cuál es la máxima tasa de $frames$ por segundo que soportará la comunicación? Supón que en la LAN existe ya un tráfico de v kbit/s en ese momento.

DNS local Corp	
TLD .com	x.x.x.x
TLD .org	y.y.y.y

Solución:

1.
   a) La conexión a la URL, implicará primero su resolución DNS, por lo que podemos distinguir dos grandes tiempos:

$$t_{TOTAL} = t_{DNS} + t_{CARGA}$$

Calculémoslos por partes. Para hacer más legibles las expresiones, realizaremos un cambio de unidades, puesto que los anchos de banda vienen expresadas en Mbits y los tamaños de los paquetes en bytes: $\alpha = 8/10^6$.
El primero de los sumandos anteriores implica la comunicación con el DNS local, en el que comprobamos que no existe el registro asociado al dominio solicitado, ni al TLD necesario (.es):

$$t_{DNS} = t_{LOCAL} + t_{RAIZ} + t_{TLD} + t_{PRI} + t_{RESP}$$

Así, la petición DNS deberá acceder, primero, al DNS local, que al ser recursivo, reenviará las peticiones a los servidores raíz (t_{RAIZ}), TLD .es (t_{TLD}) y primario de UAM (t_{PRI}). Finalmente, la respuesta del DNS deberá volver al PC del usuario (t_{RESP}):

$$t_{LOCAL} = \alpha d_1/c + \alpha d_2/c = \alpha \frac{d_1 + d_2}{c}$$

$$t_{RAIZ} = \alpha d_1/i + \alpha d_1/d + \alpha d_2/d + \alpha d_2/i = \alpha \left(\frac{d_1 + d_2}{i} + \frac{d_1 + d_2}{d} \right)$$

Las expresiones para el TLD .es y el servidor primario del dominio destino, 'uam.es', son idénticas a las de t_{RAIZ}. Por último, claramente ($t_{RESP} = t_{LOCAL}$), por lo que tenemos que:

$$t_{DNS} = 2\alpha \frac{d_1 + d_2}{c} + 3\alpha \left(\frac{d_1 + d_2}{i} + \frac{d_1 + d_2}{d} \right)$$

Una vez la máquina del usuario dispone de la dirección IP adecuada, puede empezar la conexión con el servidor Web y la descarga del recurso. Consideramos que el tiempo de conexión es despreciable (puesto que no se menciona en el enunciado), y pasamos a calcular el tiempo de carga del recurso 'http://www.uam.es'. Como no se nos dice lo contrario, entendemos que tendrá un tamaño w_1 y, su respuesta, w_2. De nuevo, tenemos que:

$$t_{CARGA} = \alpha \left(\frac{w_1 + w_2}{i} + \frac{w_1 + w_2}{w} \right)$$

Finalmente, ya disponemos de todos los sumandos necesarios, y obtenemos que:

$$\begin{aligned} t_{TOTAL} &= t_{DNS} + t_{CARGA} \\ &= 2\alpha \frac{d_1 + d_2}{c} + 3\alpha \left(\frac{d_1 + d_2}{i} + \frac{d_1 + d_2}{d} \right) + \alpha \left(\frac{w_1 + w_2}{i} + \frac{w_1 + w_2}{w} \right) \end{aligned}$$

b) Una vez finalizada la carga del recurso anterior, el DNS local ya dispone de la dirección IP del dominio 'uam.es', por lo que no necesitaremos volver a pedir su resolución en este caso. El tiempo de carga será, ahora, simplemente el tiempo de conexión (que no consideraremos), y el de descarga:

$$\begin{aligned} t_{TOTAL} &= \alpha \frac{w_1}{c} + \alpha \frac{w_1}{i} + \alpha \frac{w_1}{w} + \alpha \frac{300 \cdot 10^6}{w} + \alpha \frac{300 \cdot 10^6}{i} + \alpha \frac{300 \cdot 10^6}{c} \\ &= \alpha \frac{2400 + w_1}{c} + \alpha \frac{2400 + w_1}{i} + \alpha \frac{2400 + w_1}{w} \end{aligned}$$

c) Por último, tenemos la descarga de 5 objetos embebidos en la página 'info.html' del mismo dominio, de t bytes cada uno. Sea t_{INFO} el tiempo de carga de dicha página:

$$t_{INFO} = \alpha \frac{w_1}{c} + \alpha \frac{w_1}{i} + \alpha \frac{w_1}{w}$$

Ahora, comenzará la descarga de los objetos. Como no hay límite de conexiones simultáneas con el servidor, podemos establecer una para cada objeto, que descargará en un tiempo:

$$t_{OBJ} = \alpha\frac{t}{c} + \alpha\frac{t}{i} + \alpha\frac{t}{w}$$

Así que finalmente:

$$\begin{aligned} t_{TOTAL} &= t_{INFO} + t_{OBJ} \\ &= \alpha\frac{w_1}{c} + \alpha\frac{w_1}{i} + \alpha\frac{w_1}{w} + \alpha\frac{t}{c} + \alpha\frac{t}{i} + \alpha\frac{t}{w} \\ &= \alpha\left(\frac{w_1+t}{c} + \frac{w_1+t}{i} + \frac{w_1+t}{w}\right) \end{aligned}$$

2. En este caso, el factor limitante en la comunicación será la LAN, donde ya existe un tráfico previo de v kbits/s. Esto significa que quedan "libres", para su uso en la videollamada, $c-1000v$ Mbit/s (obviamente debe ocurrir que $c > 1000v$).
   Consideraremos que la comunicación tiene lugar con ancho de banda w en Internet. Por tanto, tenemos tres posibles factores limitantes, que son los tres anchos de banda involucrados, $c-1000v$, i y w. Sea f la tasa máxima de frames por segundo, y una nueva transformación α, de Kbytes a Mbit/s, tal que $\alpha = 8/10^3$. Para cada ancho de banda, f tomaría los siguientes valores (teniendo en cuenta que la comunicación es bidireccional y que, por tanto, necesitamos dos paquetes de 1 Kbytes simultáneamente en todo momento para la comunicación):

$$f_{LAN} = \alpha\frac{2}{c-1000v}$$

$$f_{ENLACE} = \alpha\frac{2}{i}$$

$$f_{INET} = \alpha\frac{2}{w}$$

   La tasa máxima estará determinada por el mínimo de estos valores, que hará de cuello de botella. Por tanto, tenemos finalmente que:

$$f_{max} = \text{mín}\{f_{LAN}, f_{ENLACE}, f_{INET}\}$$

2. PROBLEMA 2

1

Sea la siguiente notación:

Notación	Concepto
h(x)	Función hash sobre x
salt	Salt
HMAC(x)	Función HMAC con clave k sobre x
$E_k(x)$	Cifrado simétrico con clave k sobre x
t_s	Tiempo de generación de un byte para el salt
$K[u]_{prv}(x)$	Cifrado sobre x con clave privada del usuario u (p.ej.: $KA_{prv}(x)$ para usuario A)
$K[u]_{pub}(x)$	Cifrado sobre x con clave pública del usuario u
$\|$	Concatenación

Siguiendo estrictamente la notación anterior, escribe expresiones para las siguientes operaciones realizadas entre un emisor A y un receptor B:

A. Cifrado de un fichero f.

B. Firma digital de un fichero f.

C. Firma y cifrado de un fichero f.

Solución:

A. Cifrado de un fichero f:

$$E_k(f)|KB_{pub}(k)$$

B. Firma digital de un fichero f:

$$KA_{prv}(h(f))|f$$

C. Firma y cifrado de un fichero f: f:

$$E_k\left(KA_{prv}(h(f))|f\right)|KB_{pub}(k)$$

3. **PROBLEMA 3** [3]

Hemos establecido una comunicación de audio con protocolo RTP. En el router del emisor se tiene implementado un sistema de balde de fichas (token bucket). El balde de fichas tiene un máximo de 100000 fichas y obtiene una ficha nueva cada 30 ms. Cuando se inicia la comunicación el balde está vacío.

La comunicación consiste en un tramo de silencio de 3s, un tramo de habla de 20s, un tramos de silencio de 10s, y un tramo de habla de 2 min.

- ¿Existe algún momento en el que la comunicación se haga imposible?

  Solución:
  - En determinado periodo t se generan $f_p = 10^2 \cdot t/3$ fichas.
  - En un tramo de silencio no se consume ninguna ficha porque no se envía ningún paquete.
  - En los tramos de habla se consumen $f_c = 10^2 \cdot t/2$ fichas puesto que al ser audio se produce un paquete por cada 20 ms de habla.
  - Como en el primer tramos de habla de 20 s se producen 2000/3 fichas pero se consumen 1000 fichas. Dado que las producidas en el primer tramo de silencio más las que se producirían en este tramo de habla es menor que las fichas que se necesitarían consumir entonces a partir de cierto momento los paquetes de habla de 20 ms se transmitirán cada 30 ms **haciendo imposible la comunicación**.

- Si la respuesta es sí, calcula de forma razonada dicho instante desde el punto de vista del emisor.
- Si la respuesta es no, explica razonadamente el motivo.

  Solución: El instante en el que la comunicación se hace imposible es cuando no queda ninguna ficha en el balde. Como sucede en el primer tramo de habla se produce cuando:

  $$10^2 + 10^2 \cdot t_h/3 - 10^2 \cdot t_h/2 = 0$$

  o lo que es lo mismo cuando

  $$1 + t_h/3 - t_h/2 = 0$$

  es decir $t_h = 6s$.
  Por tanto la comunicación se hace imposible en el segundo 6 de habla o en el segundo 8 desde el inicio de la comunicación.

Supón ahora que el emisor cambia de dispositivo de comunicación y restablece la comunicación a través de una red 5G sin balde de fichas. Si el jitter de la comunicación es de 68 ms, y suponemos que el primer paquete tarda en transmitirse 92 ms y que es un paquete que se ha transmitido a la velocidad media de la comunicación:

- Haz una estimación razonable para el retraso fijo de la comunicación e indica qué problemas puede producir en la comunicación.

Solución: Dado que el jitter es, básicamente la varianza de la distribución de la recepción de los paquetes y el primer paquete se transmite a la velocidad media de la comunicación basta con retrasar la reproducción del primer paquete justo la mitad del tiempo del jitter para tener una confianza de σ para la recepción de los paquetes. También se puede retrasar el jitter completo para tener una confianza mucho mayor, de 2σ. En el primer caso el tiempo de retraso respecto a la emisión del paquete deberá ser 92+34 ms, es decir, 126 ms y en el segundo sería 92+68 ms, es decir 160 ms.
En el caso de confianza de σ el tiempo es levemente superior a 120 ms con lo que podría considerarse comunicación síncrona con unas pérdidas razonables. En el segundo caso, con 160 ms los participantes notarían un pequeño retraso en la comunicación pero la comunicación sería posible y con muchas menos pérdidas que el primer caso.

- En esta situación ¿qué esquema FEC utilizarías y por qué?

  Solución: Utilizaríamos un esquema que no aumente el número de paquetes. El esquema entrelazado permitiría una comunicación con pérdidas despreciables pero, dado que en este problema no hay limitación con el tamaño de los paquetes es aconsejable un esquema con paquetes anteriores en baja resolución.

- Si queremos tener una confianza 8σ para que no se pierda prácticamente ningún paquete. ¿Qué retraso fijo será necesario?. En esta situación indica los problemas que puede haber en la comunicación.

  Solución: Dado que el paquete es el medio, para tener una confianza 8σ es necesario retrasar la reproducción del paquete 4σ. En esta situación el primer paquete se reproduciría 98 + 68*4 ms después de emitirse, es decir, 370 ms. Esta cantidad está muy próxima a los 400 ms que hacen imposible una comunicación síncrona y por tanto aunque sería posible, sería muy molesta y dificultosa.