Tema 2a:

¿Qué cifrador en flujo elegirías en la actualidad, atendiendo a la seguridad y el rendimiento?

Salsa20 o ChaCha, claramente. Porque no hay ataques conocidos capaces de romperlos y por el buen rendimiento.

Tema 2b:

¿Qué cifrador en bloque elegirías en la actualidad, atendiendo a la seguridad y el rendimiento? ¿Con qué modo de operación?

AES en cifrado rápido (y Salsa también son bastante rápidos y se parecen mucho). Modo contador, es el único que garantiza que va a recorrer todos los estados posibles sin repetición, consiguiendo el periodo máximo posible. No hay descifrado, sino que se usa el mismo cifrado. Permite acceder de forma secuencial al segmento cifrado.

¿Hay situaciones en las que sería preferible un cifrador en bloque a uno en flujo o viceversa?

Un cifrador en bloque produce latencia y es más lento que el cifrador en flujo, porque como va bit a bit no hay que esperar y lo podemos ir cifrando a tiempo real. Pero en la mayoría de los casos son intercambiables.

Tema 2c:

¿Qué ventajas aporta un esquema PBKDF frente a un sistema de contraseñas basado en hash convencional?

En general se puede configurar el coste para evitar ataques por GPU. Por otro lado me permite usar “sal” para que los hashes no se repitan.

¿Qué aplicaciones se benefician de protocolos como SSL/TLS, HTTPS o SSH?

1. Solo aquellas que tengan elementos que requieran seguridad/privacidad.
2. Todas, tengan arquitectura C/S o no, porque escribir en disco y volver a leer es como hacer C/S contigo mismo.

Respuesta: Lo normal es pensar el 1, pero es el 2, que garantiza confidencialidad.

Tema 2d:

¿Por qué no usamos criptografía de clave pública para propósito general y qué alternativas tenemos a nuestra disposición?

Porque la criptografía asimétrica es tan lenta. Alternativa: criptografía simétrica.

¿Qué papel tienen las funciones hash en los protocolos de firma digital?

El rendimiento.

¿Qué diferencia hay entre un certificado y un par de claves pública/privada?

En realidad un certificado es un fichero con un formato estándar y tiene el par de claves pública/privada(esta última cifrada por AES con una clave pin, para que si roban el fichero no esté expuesta) además está firmado por una firma de autenticidad certificadora. Entonces la diferencia es que ese par de claves es solo parte del certificado, pero tiene más cosas.