**Pregunta 1.** Explica los conceptos de servicio, arquitectura orientada a objetos y sistema distribuido.

**Servicio:** Mecanismo que habilita el acceso a uno o más recursos, este acceso se provee usando una interfaz prefijada con limitaciones y políticas especificadas por la descripción del servicio.

**Arquitectura orientada a objetos:** Paradigma para organizar y utilizar recursos distribuidos que están bajo el control de diferentes dominios.

**Sistema distribuido:** Consiste en diversos agentes de software que trabajan conjuntamente para realizar algunas tareas. Los agentes de un sistema distribuido no operan en el mismo entorno así que se tienen que comunicar mediante un protocolo HW/SW a través de la red.

**Pregunta 2.** Explica brevemente el rol del protocolo WSDL (Web Services Description Language) en un servicio Web y cómo se estructura un servicio web con WSDL.

Lenguaje basado en XML que provee un modelo para describir un servicio que se ofrece, su localización, los parámetros y métodos que soporta.

Se estructura con los siguientes elementos:

* Tipos de dato
* Mensajes
* Tipo de puerto
* Bindings
* Servicios

**Pregunta 3.** Explica el rol de SOAP (Simple Object Access Protocol) en un servicio Web y describe el tipo de encapsulamiento que usa

Intercambia la estructura de la información entre clientes y servidores de un web service.

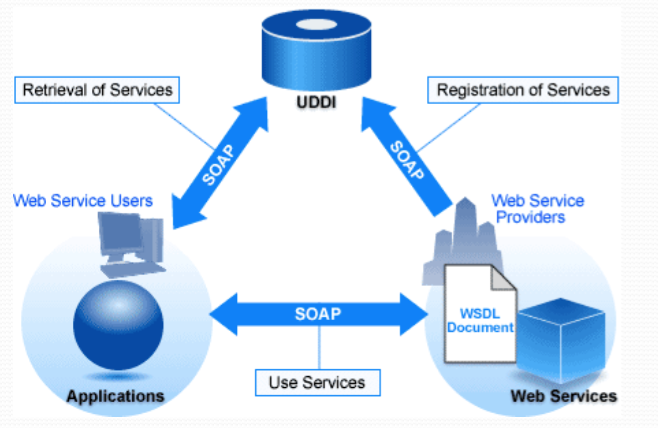
Encapsulamiento del SOAP:

* Envelope
  + Header -> Contiene las opciones del mensaje a procesar.
  + Body -> Contiene la petición/respuesta del mensaje.
  + Faults -> Señales de error en el procesamiento de la petición.

**Pregunta 4.** Explica qué diferencias hay en usar RPC, RPC-XML y SOAP.

* RPC -> Ejecuta funciones en el host remoto, sin definir lenguaje.
* RPC-XML -> Llamada serializada en XML.
* RPC-JSON -> Llamada serializada en JSON.
* SOAP -> Modo de encapsulamiento con etiquetas predefinidas.

**Pregunta 5.** Dibuja un esquema que defina la arquitectura de referencia de los Web Services y explica su funcionamiento básico.



El solicitante hace una petición de ejecución al web service, el proveedor la procesa.

Discovery agency -> Es la agencia a través de la cual la descripción de un web service se hace publica y accesible.

Los proveedores son los responsables de publicar una descripción de los servicios de los que proveen.

Los clientes deben ser capaces de encontrar dicha descripción.

**Pregunta 6.** Explica que diferencias hay entre usar una arquitectura basada en XML o en JSON.

XML, dispone de más opciones, pero también es mucho mas pesado y por tanto menos eficiente que JSON, y en esencia cumplen con el mismo fin, trasportar datos. JSON utiliza clave – valor, mientras que XML, define un espacio de nombres (etiquetas) para diversas opciones.

**Pregunta 7.** Explica el funcionamiento básico de la criptografía de llave simétrica y como se asegura el intercambio de la llave.

Con la criptografía en llave simétrica, se usa la misma llave tanto para cifrar como para descifrar. Si esta es interceptada al compartirse las comunicaciones se pueden ver comprometidas.

Para conseguir intercambiar la llave de forma segura, se hace a través de una KDC (Key Distribution Center), un ente fiable que sabes las llaves de los participantes en las comunicaciones. De forma que cuando A quiere comunicarse con B, A pide la clave para comunicarse con B, y este genera una llave simétrica para dicha comunicación.

El intercambio de la llave se asegura mediante el uso de certificados.

**Pregunta 8.** Explica el funcionamiento básico de la criptografía de llave pública. Explica en un ejemplo como podemos firmar un documento y a continuación encriptarlo.

En la criptografía de llave publica, disponemos de 2 claves por cada parte de la comunicación, es decir A, tendrá una llave publica y una privada, igual que B.

A compartirá con B su clave publica, y B con A hará lo mismo (todas las llaves son distintas). Cuando A se quiera comunicar con B cifrara el mensaje usando la llave publica de B, y cuando B se quiera comunicar con A, cifrara el mensaje usando la llave publica de A. Después de hacer esto el mensaje solo podrá ser descifrado usando la llave privada, que no ha sido compartida, de forma que podemos asegurar que nadie será capaz de leer los mensajes.

Aunque no podemos asegurar que nadie pueda suplantar a A o B, aquí es donde entran las firmas.

**Pregunta 9.** Explica cómo se puede firmar digitalmente con criptografía de llave pública.

Firmando digitalmente, evitamos que alguien se pueda hacer pasar por nosotros.

Esto se hace mediante un intercambio de la clave publica y privada, de forma que en vez de encriptar un mensaje con la llave publica, lo haremos con la llave privada, y el destino lo des encripta con la llave publica. Esto tiene la ventaja de que, al solo poder descifrarse con la llave pública del emisor, solo podrá haber sido generado por este.

**Pregunta 10.** Explica mediante un ejemplo como funciona un KDC (Key Distribution Center) en la criptografía simétrica.

A, escoge una clave de sesión (Ks), y le indica a la KDC que quiere hablar con B usando como llave Ks, este mensaje A lo envía a B utilizando la llave de A para hablar con KDC, Ka.

El KDC descifra el mensaje y extra la identidad de B y Ks, mediante su llave para comunicarse con B (Kb), le envía los datos a este.

Ahora A conoce la clave con la que hablara con B i B conoce la clave con la que hablar con A y con la que este le hablara.

**Pregunta 11. Explica para qué sirve y cuál es el mecanismo de funcionamiento de una** **Autoridad de Certificación (CA), indicando si se usa con criptografía de llave simétrica o** **asimétrica.**

Sirve para poder asegurar que el que nos envía un mensaje es el que dice ser.

Se usa criptografía de llave asimétrica.

A, se identifica ante una CA, esta le proporciona un certificado, al negociar las llaves de sesión con B, B se lo pedirá, y se lo enviara de nuevo a la CA, esta certificara que A es A. A también hará lo mismo con el certificado de B.

Al saber que cada uno es quien dice ser todo funcionara de forma normal. Utilizando las llaves publicas y privadas (que se envían con el certificado).

**Pregunta 12.** Explica la diferencia de funcionamiento entre un KDC (Key Distribution Center) y una Autoridad de Certificación (CA) y con qué tipo de criptografía se usa cada uno de ellos.

Una KDC, se utiliza como un paso intermedio para intercambiar la llave de sesión de forma segura y utiliza llave simétrica.

Una CA, se utiliza para emitir y verificar certificados, y así comprobar la autenticidad de la identidad del receptor/emisor y utiliza llave asimétrica.