HTTP：

1、是什么？

Http是超文本协议，是一种详细的规定了客户端和服务器之间互相通信的规则。

是应用层的协议，常基于TCP/IP协议传输数据。

2、特点？

a、简单快速：客户端向服务器请求服务时，只需要发送请求方法和路径。由于Http协议简单，使得Http的服务规模小，因而通信速度很快。

b、可以传输任一类型的数据对象。正在传输的类型由Content-Type加以标记。

c、客户端与服务器使用持续连接，不必为每一个web对象创建一个新的连接，一个连接可以传送多个对象，可以节省传输时间。

d、Http是无状态协议。无状态是指：协议对于事务处理是没有记忆能力的。

e、支持B/S模式【浏览器/服务器 模式】 和 C/S模式【客户端/服务器 模式】

3、Http的工作流程？

a、客户端与服务器建立连接。

b、建立连接后，客户端向服务器发送请求。

c、服务器接受请求，并发出响应。

d、客户端接收响应，并在浏览器页面显示。

4、客户端与服务器是如何建立连接的？

客户端与服务器之前的通信都是建立在有通信连接的基础上。

a、当客户端输入URL后，会进行DNS域名解析，将域名转为对应的IP地址。当获取IP后，TCP连接会通过三次握手建立连接。

【DNS】:是一个域名系统，存储的是域名 与 IP地址 的映射。

b、TCP的三次握手，建立连接， 四次挥手，断开连接。

c、使用三次握手建立连接，能有效的保证不会建立无效的连接，从而浪费资源。同时也能避免无效的请求报文段又突然传递到了服务器，从而产生错误。

HTTPS：对于请求数据都是都是加密的。

基于HTTP协议，通过SSL或TLS提供加密处理数据、验证对方身份一级数据完整性保护。

特点：

a、内容加密：采用混合加密技术，中间这无法直接查看明文内容。

b、验证身份：通过证书认证客户端访问的是自己的服务器。

c、保护数据完整性： 防止传输的内容被中间人冒充或篡改

HTTP和HTTPS的不同点：

1. HTTP是明文传输， HTTPS是密文传输

1、为什么需要使用TPS进行数据加密？

答：因为HTTP使用的是明问传输，如果请求信息别人拦截，则请求信息就会别人就会被人知晓。同时，还能修改请求不被发现，再次发送给服务器。这就是“中间人攻击”。所以需要对数据进行加密。

加密方式有两种：对称加密 和 非对称加密。

2、对称加密和非对称加密？

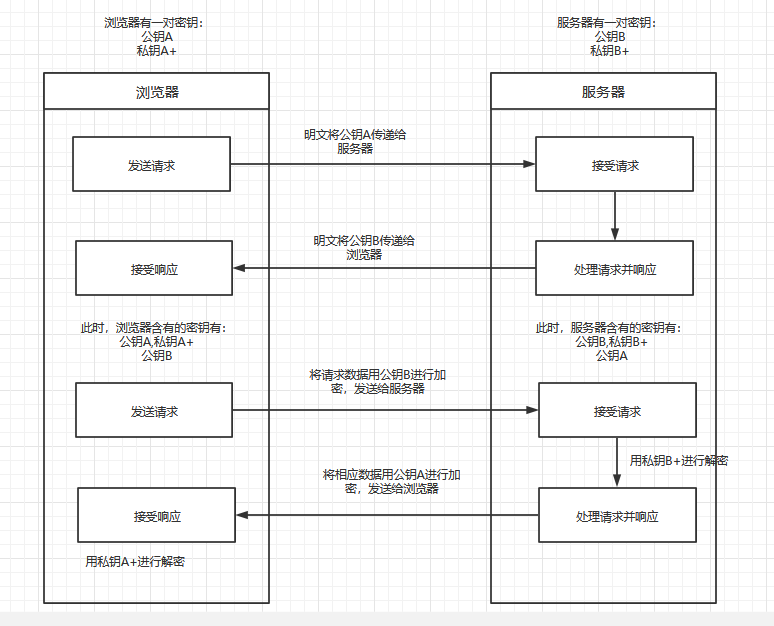
答：对称加密：加密的密钥 和 解密的密钥密钥是同一个。

非对称加密：加密的秘钥 和 解密的密钥不是同一个。简单的说就是有两把密钥，一把公钥，一把私钥。用公钥加密的数据只能用私钥进行解开，同样，用私钥加密的数据数据只能用私钥进行解开。

3、HTTPS使用的加密方式是非对称加密 + 对称加密，为什么要用这种方式？

答：a、能否用非对称加密完成HTTPS的加密？

可以通过两组公钥和私钥进行非对称性加密，实现HTTPS的加密方案。但是由于非对称加密很耗时，所以这种方式不是特别好。而对称加密就快很多，能否用对称加密加密实现呢？



b、能否用对称加密，通过两组密钥实现HTTPS的加密？

答：不行，因为对称加密的公钥和私钥是同一个，一但明文传递公钥，相当于私钥也传递了，所以，不能只用对称加密实现HTPPS的加密。

c、对称加密 + 非对称加密 如何实现HTPPS的加密？

答：将浏览器生成的对称密钥X 加密发送给 服务器，这样浏览器和服务器之间的交互就可以通过该密钥X进行。

这种方式只有在第一次请求的时候需要进行非对称加密，后续可以通过对称加密进行交互。

