实验 5：编写一个安全通信的 HTTP 独立服务程序

实验目的：熟悉 HTTP 协议、掌握安全通信原理的运用。

实验内容：编写一个不需要 WEB 服务器的独立 HTTP 服务程序，并为该程序增加安全通信机制，防止网络攻击行为

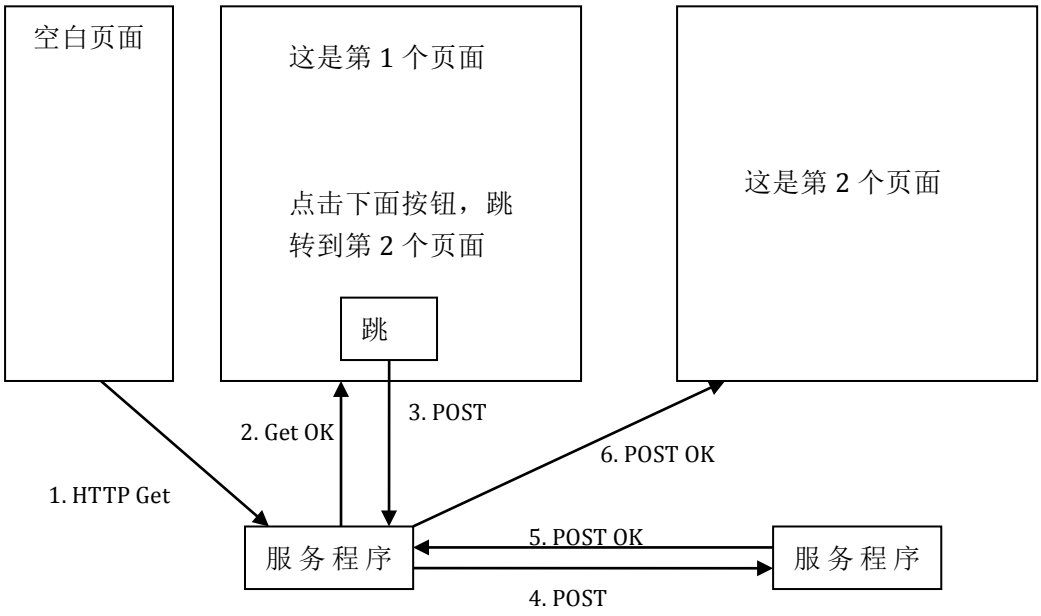
实验环境：PC 机、C++、C#或 Java 编程环境

实验要求：

- 不使用任何封装 HTTP 接口的类库或组件，也不使用任何服务端脚本程序如 JSP、ASP、PHP 等
- 按照标准的 HTTP 协议实现基本的 GET 和 POST 功能
- 服务端程序界面不做要求，使用命令行或最简单的窗体即可
- 本实验应组成小组来完成，2 个服务程序应由不同人完成
- 功能要求如下：

  第一部分：

  1. 应用层协议采用标准的 HTTP
  2. 开发 2 个独立的服务程序，既能接受 HTTP 请求，也能发出 HTTP 请求，其中一个服务程序监听在 80 端口，另 1 个监听在 81 端口
  3. 每个服务程序输出 2 个页面，第 1 个页面是本服务程序所在机器的静态 HTML 页面（采用 Get 方法），第 2 个页面是采用 Post 方法从另外 1 个服务程序获得的 HTML 页面。第 1 个页面有一个跳转按钮，在浏览器上点击它可以从让服务程序发出 HTTP 请求给另外一个服务程序，获得其页面内容，然后输出到浏览器（不是把 URL 地址发给浏览器，让浏览器直接访问另外一个服务程序），如图所示（按数字顺序发生）：

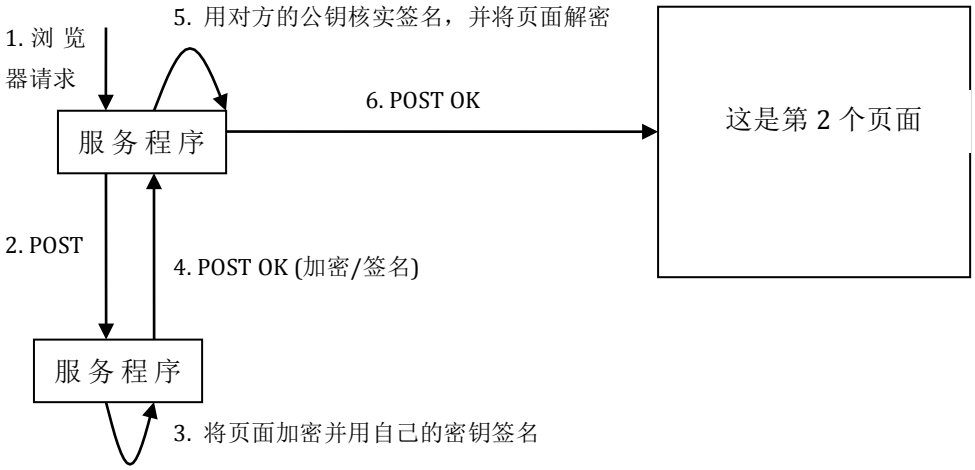


  4. 使用标准的 IE 浏览器可以正常打开每个服务程序所在端口的第 1 个页面，并能互相跳转

  第二部分：

  5. 在服务程序之间能正常访问后，给服务程序之间的 HTTP 访问接口增加加密和

数字签名功能，页面返回时必须使用 DES 加密算法将页面内容加密，并且带上 RSA 数字签名，接收端的服务程序必须先核实数字签名是否正确，如果不正确，就在浏览器上显示错误信息，如果正确，则将页面解密后输出到浏览器，如图所示：



实验步骤：

第一部分：

- 阅读相关标准文档，详细了解 HTTP 协议标准的细节，有必要的话按照实验 2 的方法研究真实网络协议
- 结合选择的编程环境，了解 TCP 服务类的使用
- 小组讨论：根据功能要求设计程序模块，并写出程序设计文档
- 小组分工：1 个人负责编写 HTTP 协议的实现，1 个人负责编写请求响应和页面解析
- 每个人负责编程实现自己那部分应用软件的功能
- 编程结束后，将 2 个服务程序同时运行
- 使用 IE 浏览器访问服务程序的 URL 地址，检查页面输出是否实现功能要求，如果有问题，查找原因，并修改，直至满足功能要求
- 使用多个客户端同时连接 1 个服务端，检查并发性

第二部分：

- 阅读相关加密/解密、数字签名原理文档，详细了解加密/解密过程和数字签名过程
- 结合选择的编程环境，了解加密解密类、数字签名类的使用
- 小组分工：1 人负责编写加密和数字签名，1 人负责编写解密和核实签名
- 每个人负责编程实现自己那部分应用软件的功能
- 使用 IE 浏览器访问服务程序的监听端口，点击按钮跳转到第 2 个服务程序的页面，检查输出是否正确
- 直接访问第 2 个服务程序的 URL 地址，检查是否能正确访问

实验时间：6 机时。

实验报告：提交源代码和程序设计文档（包括分工说明、编程环境说明、功能模块划分、程序运行效果的屏幕截图）