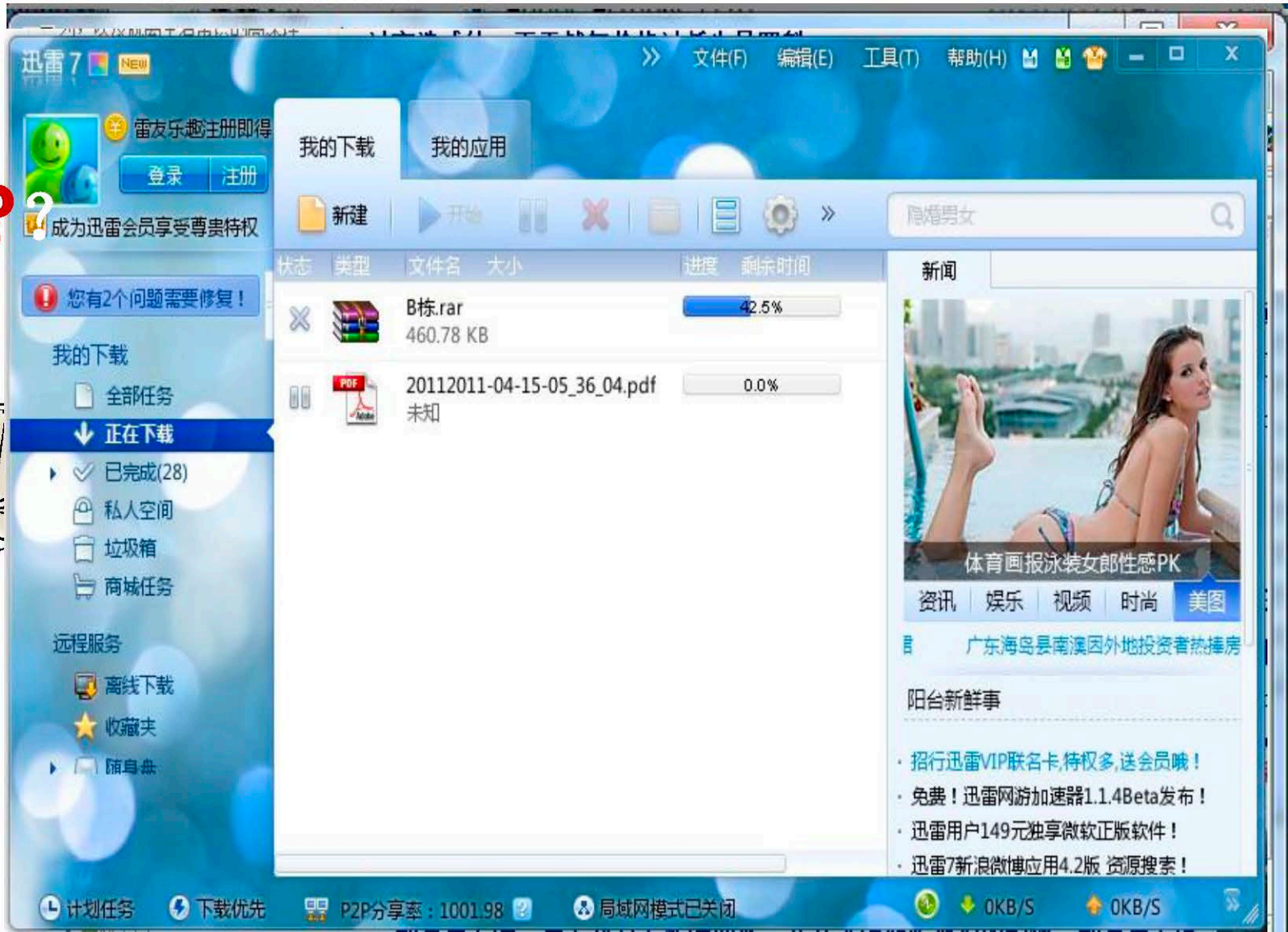
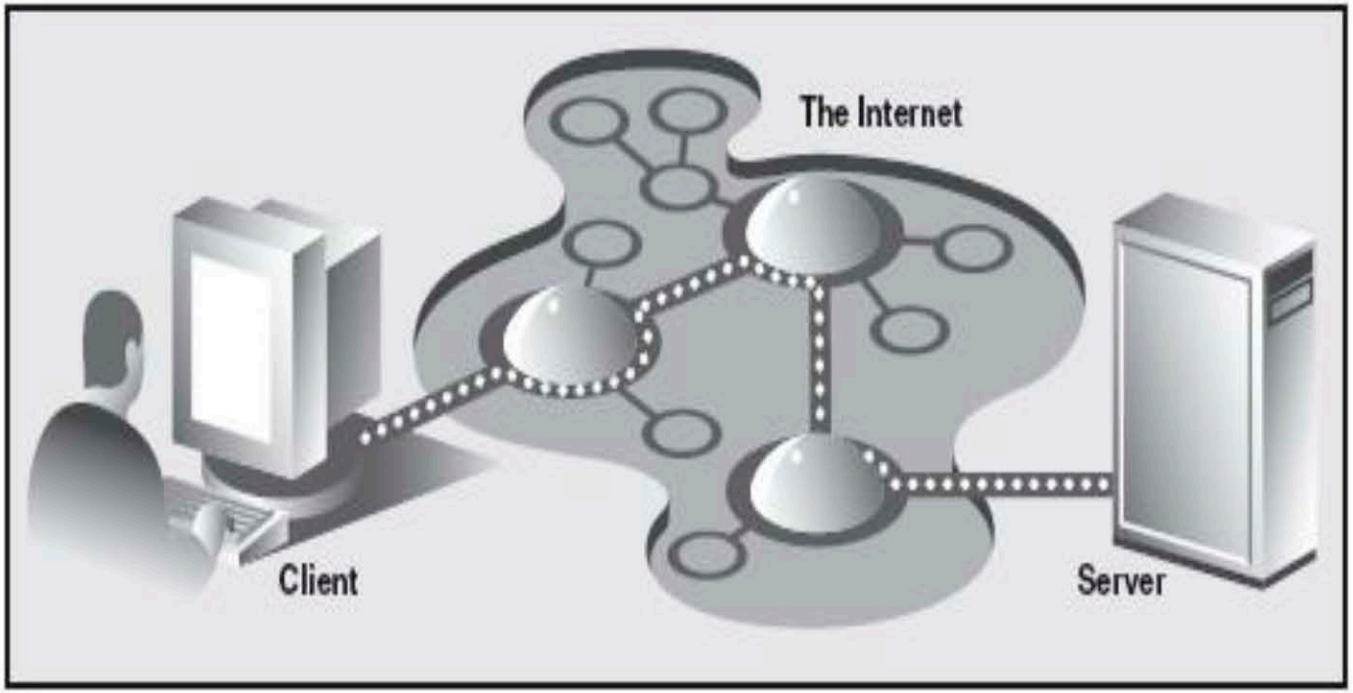
加密通信

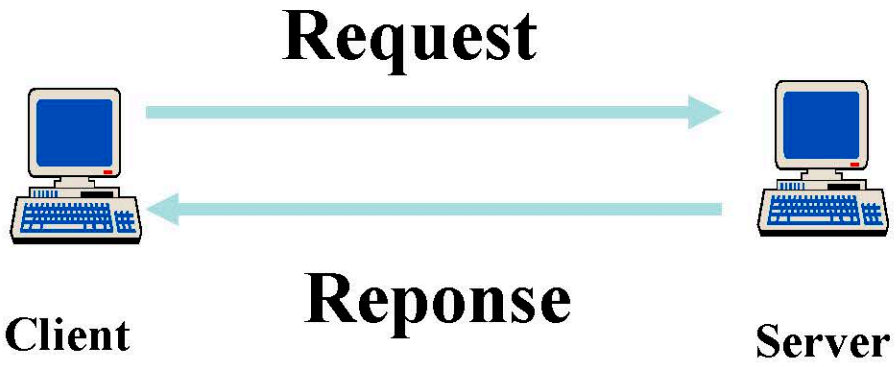
Introduction

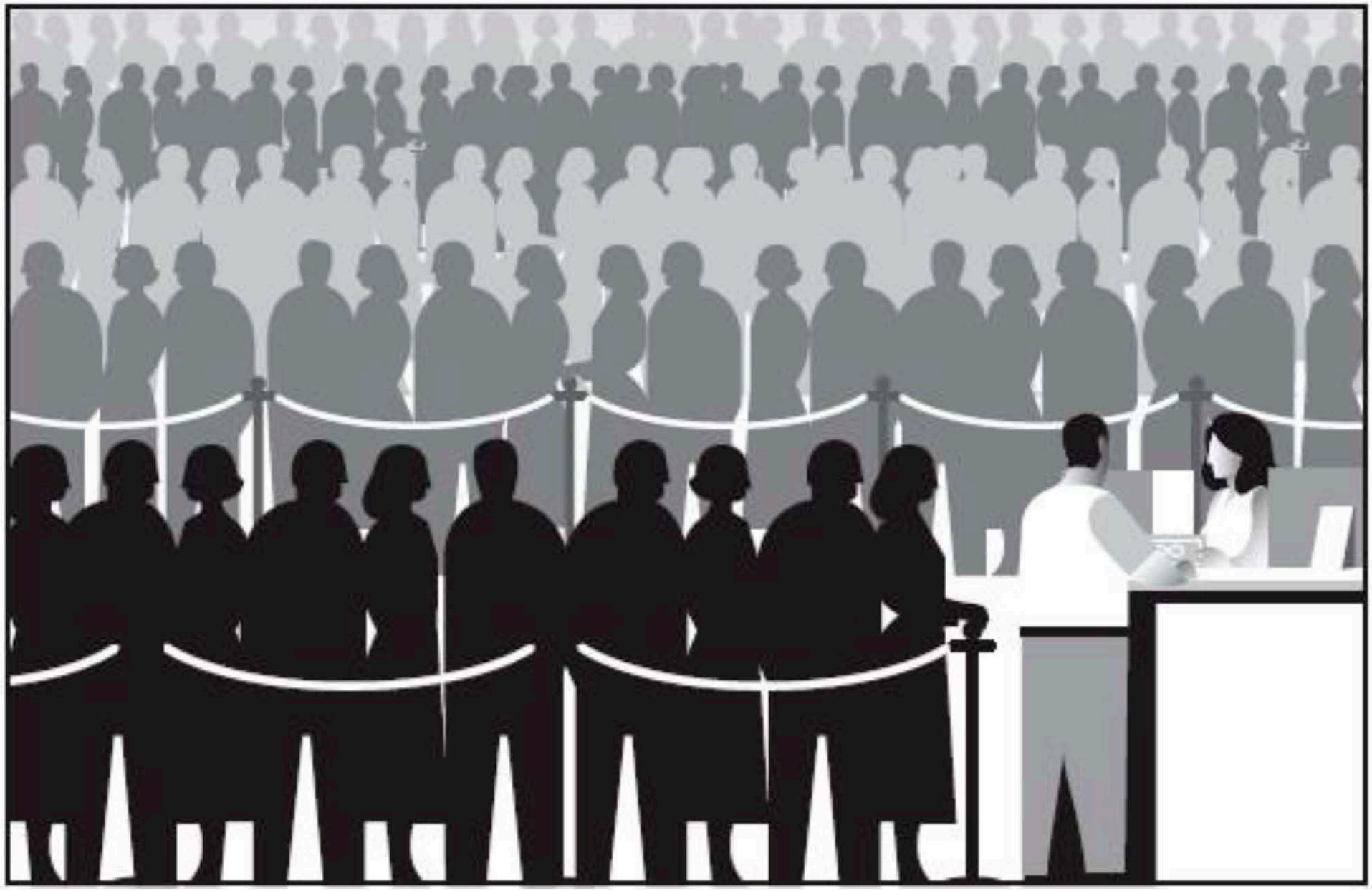
How??



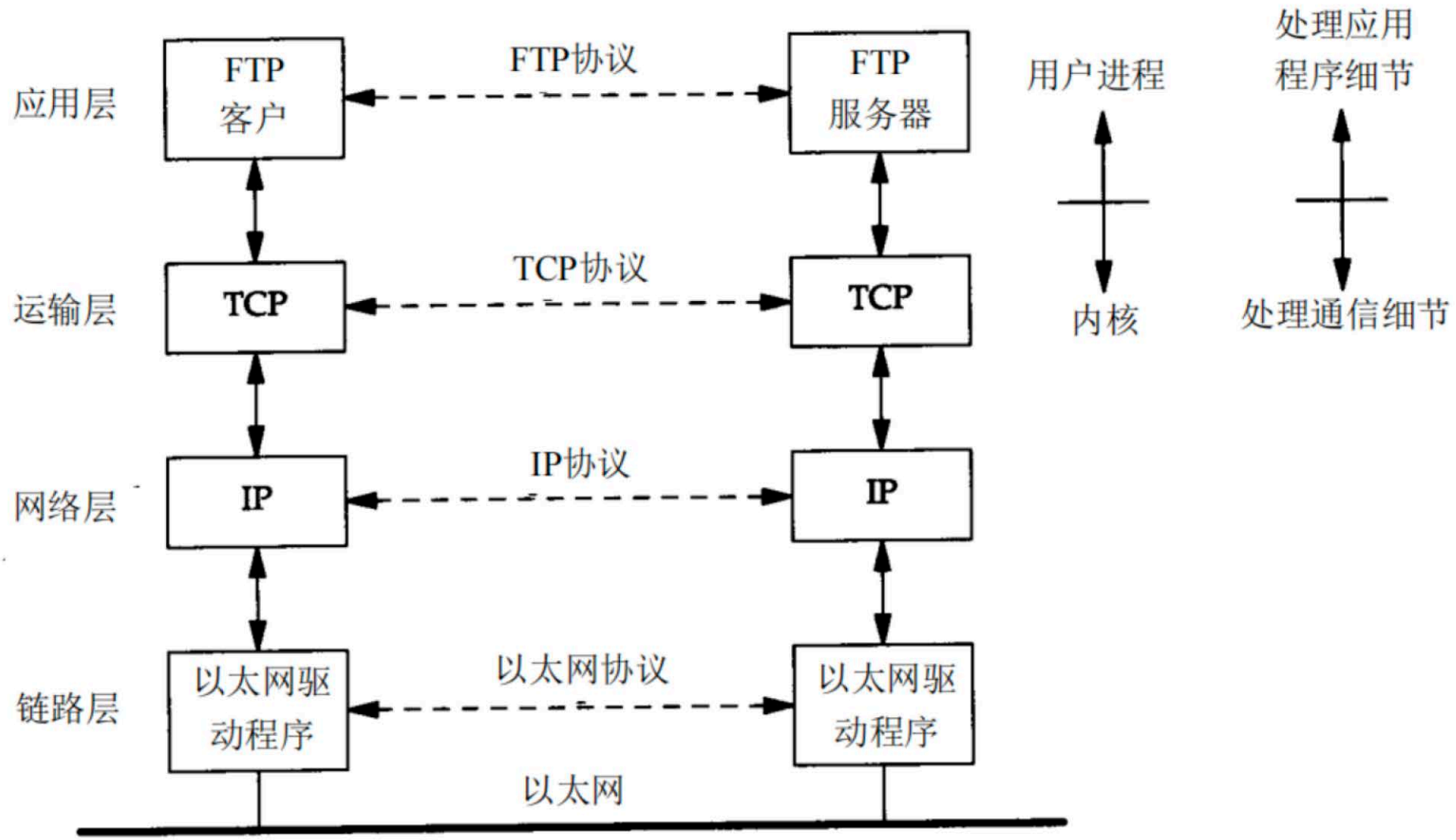
Client and Server



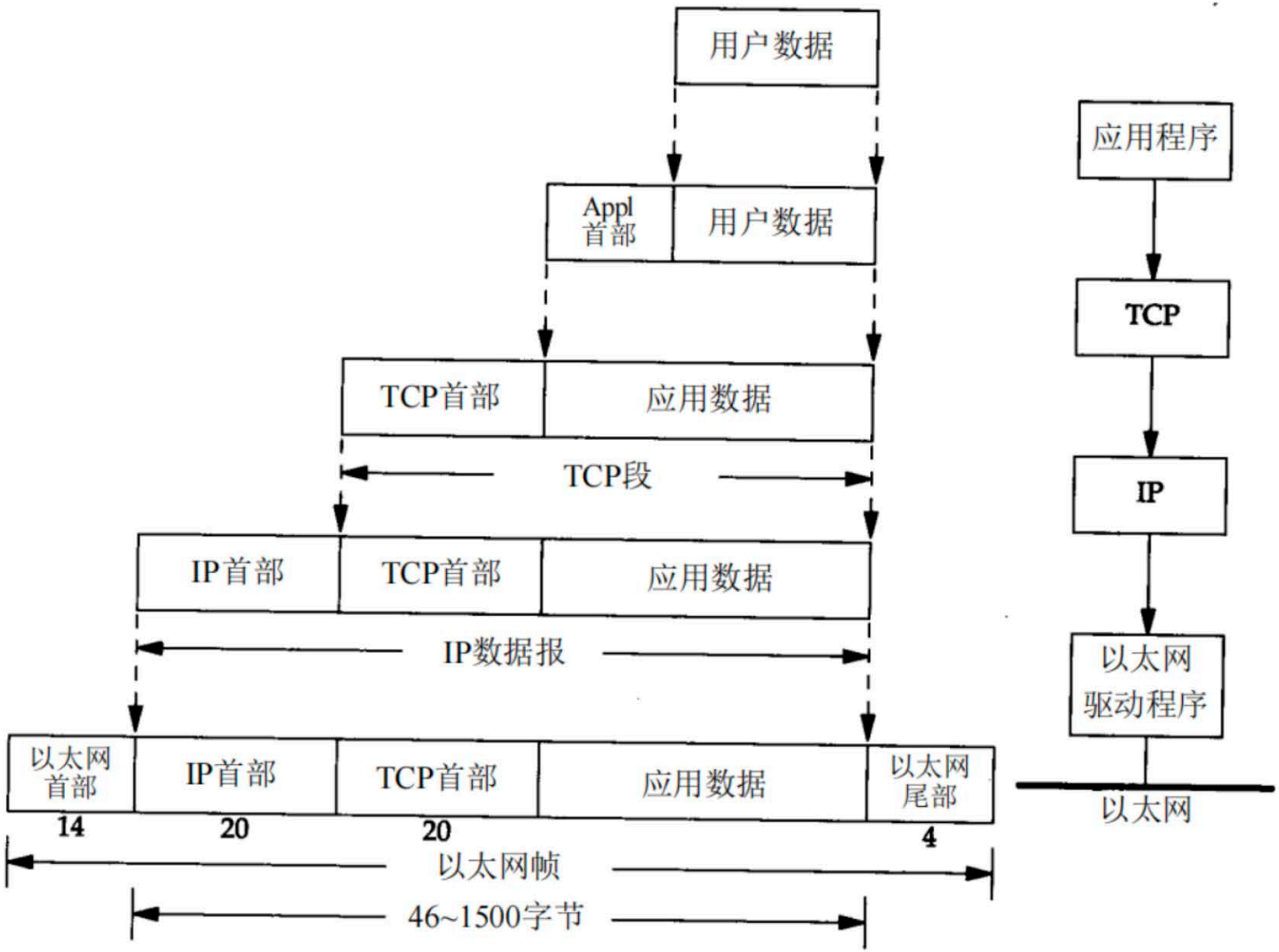




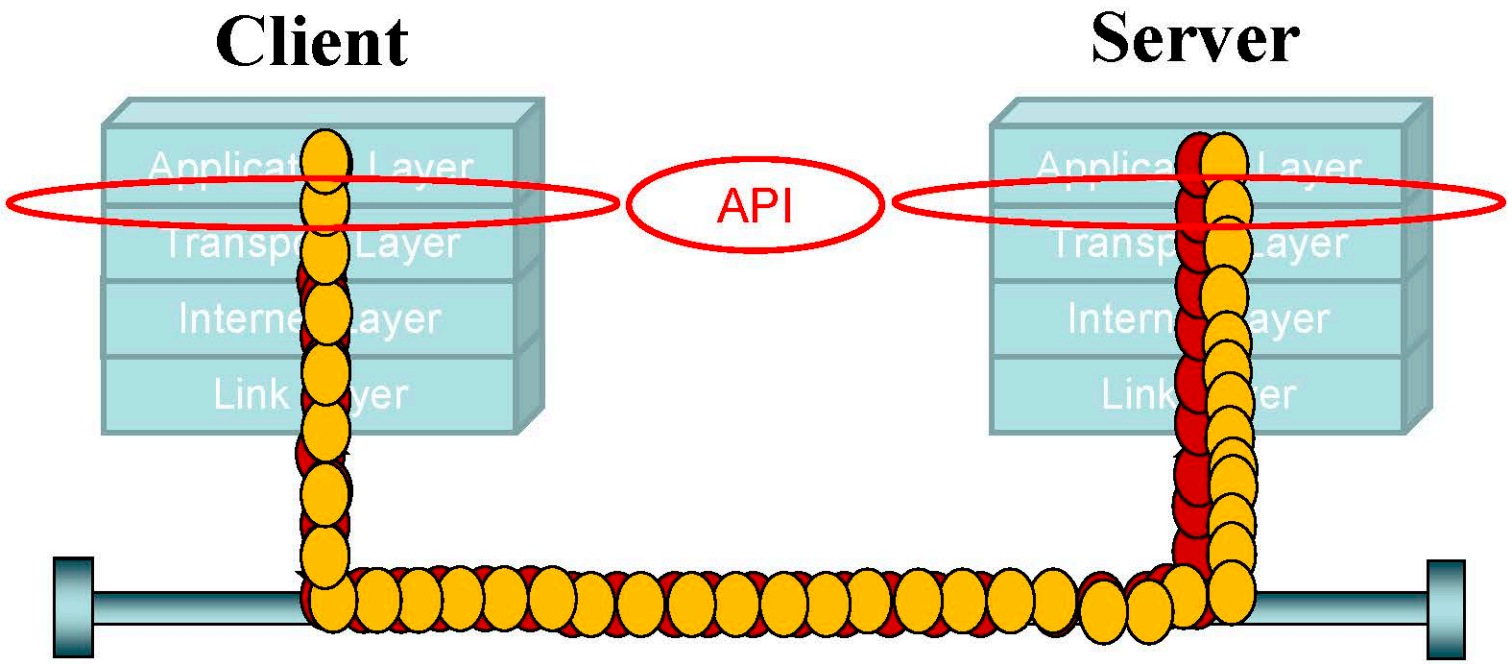
网络应用通信过程


应用层
运输层
网络层
链路层
FTP
客户
FTP协议
FTP
服务器
TCP
TCP协议
TCP
IP
IP协议
IP
以太网驱
动程序
以太网协议
以太网驱
动程序
以太网
用户进程
内核
处理应用
程序细节
处理通信细节

数据进入协议栈的封装过程



网络报文传输过程



Socket

- A socket is a communication mechanism between the client and server.

- Sockets is also used as a name for an application programming interface for the TCP/IP protocol stack

- Sockets constitute a mechanism for delivering incoming data packets to the appropriate application process or thread, based on a combination of local and remote IP addresses and port numbers.

Socket

- 套接字：通讯端点
- 70 年代,伯克利分校版本的 BSD UNIX

- Socket Family

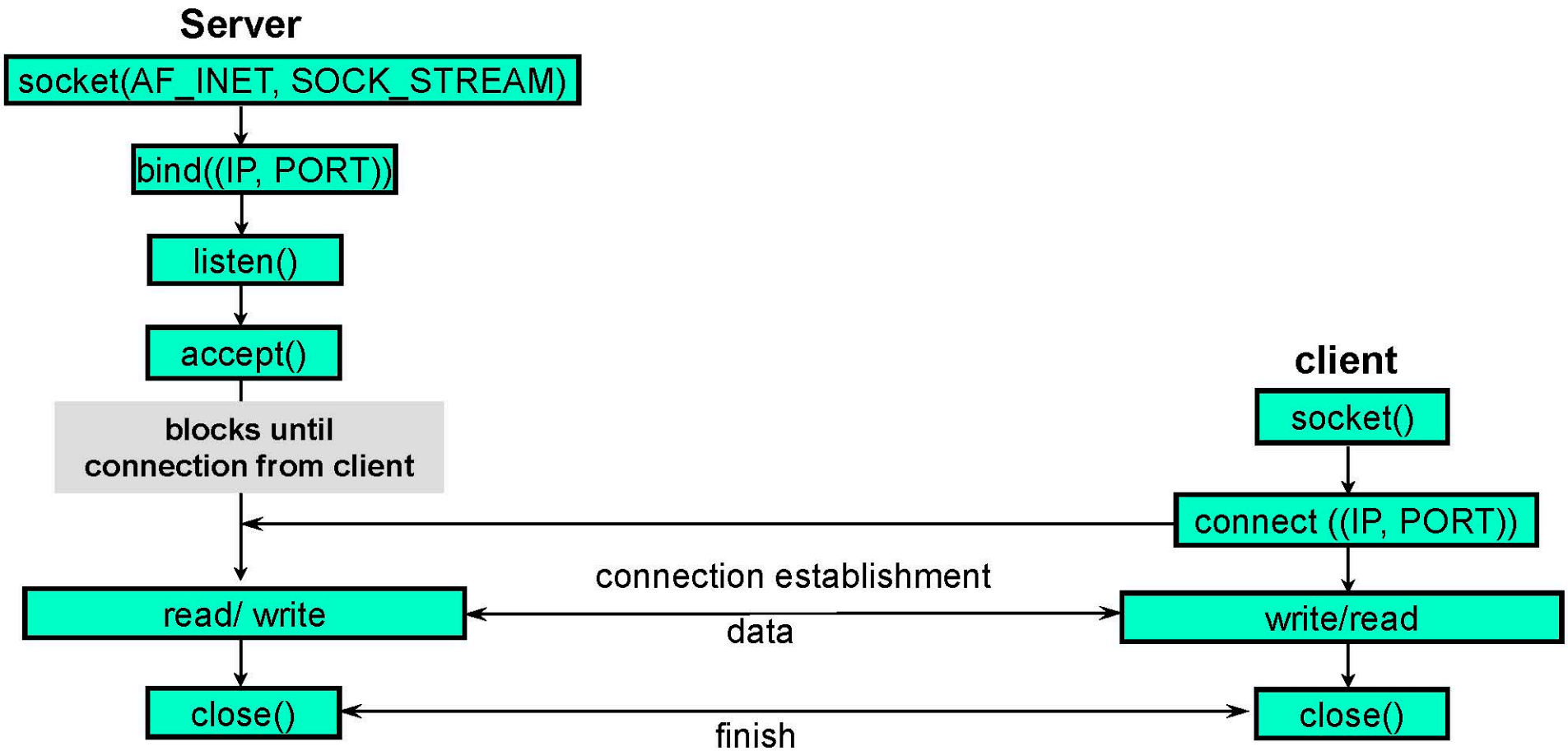
AF_INET、AF_UNIX、AF_NETLINK

- Socket Types

SOCK_STREAM、SOCK_DGRAM

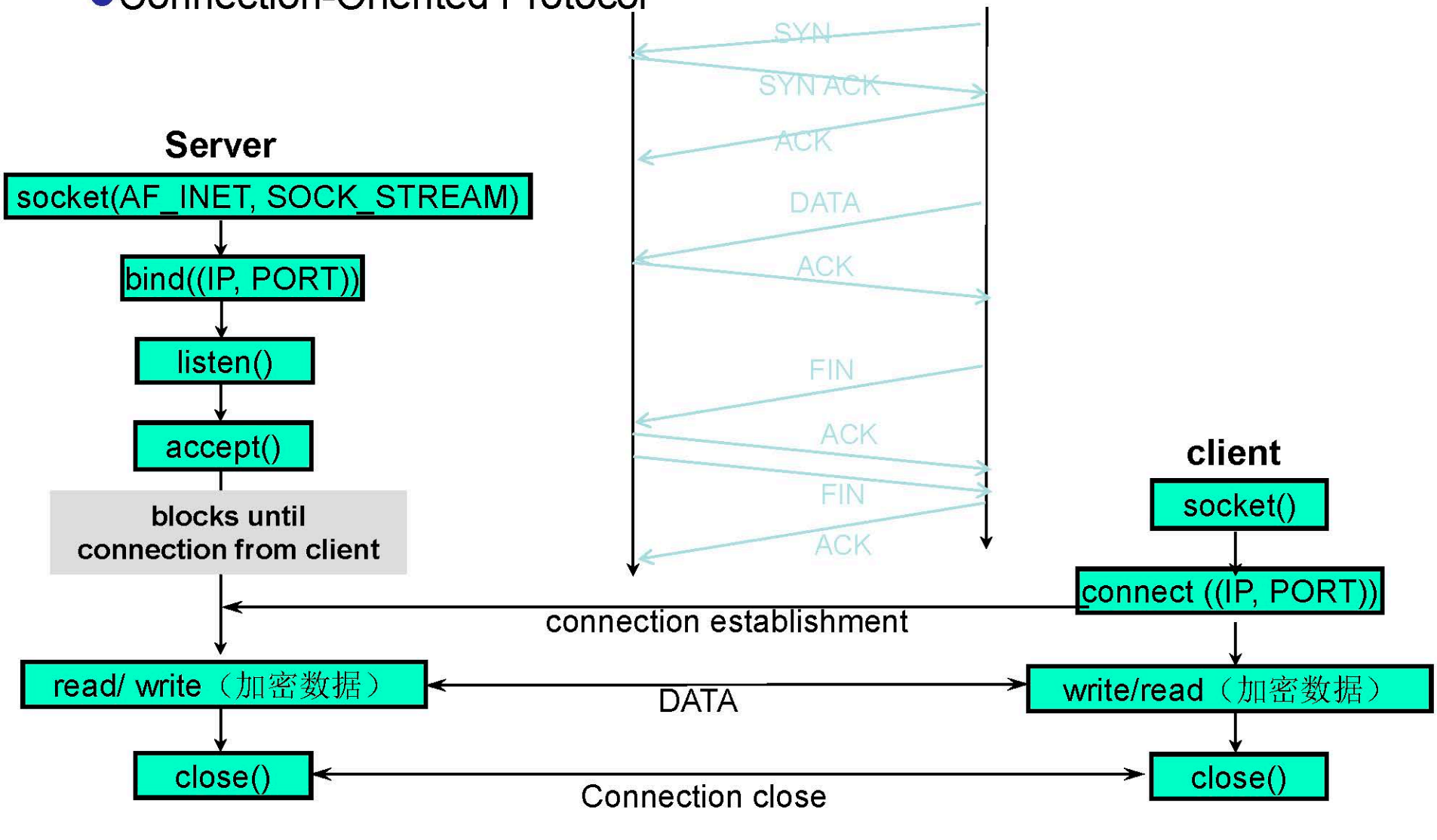
Network Programming

- Connection-Oriented Protocol



Network Programming

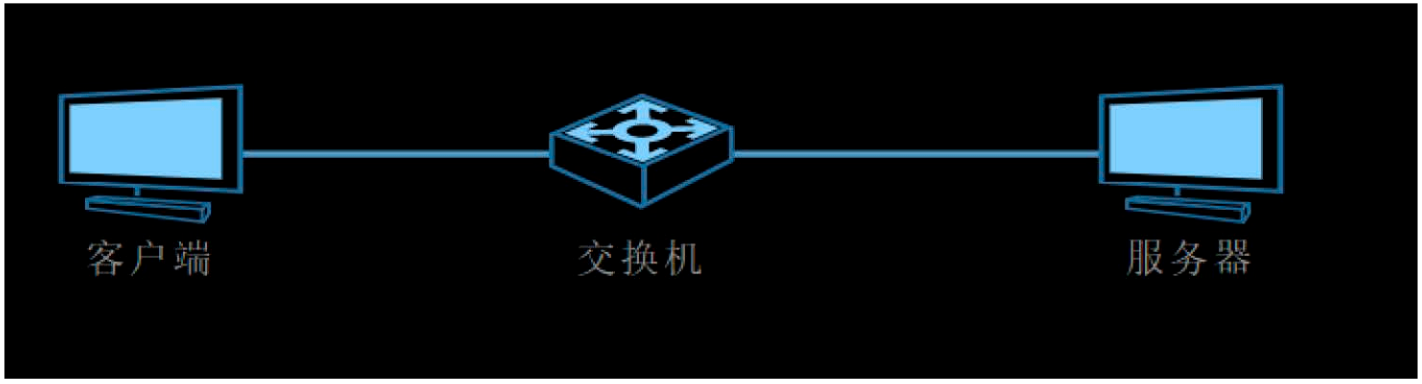
- Connection-Oriented Protocol



实验内容与要求

实验内容

- **学习**理解网络通信
- 学习数据加密和解密
- 开发网络通信的客户端程序、服务器端程序，实现客户端将传输的网络数据进行加密、服务器端将收到的加密数据进行解密，在客户端和服务器端间传输加密数据。需要对比发送的数据、接受的数据是否一致，验证网络传输的正确性；需要对比两端的明文数据、密文数据是否一致，验证加密、解密的正确性。



实验要求

- 完成加密通信实验内容。
- 提交实验报告，包括:加密通信环境设计、客户端程序和服务器端程序概要设计、加密算法介绍，以及实验中遇到的问题和原因等。
- 2024年5月22日（星期三）提交给各班学委

思考

- 采取的加密算法的加密强度如何？
- 服务器端接收并发的多客户的加密数据如何实现？
- 多个socket（套接字）如何管理？

谢 谢！