网络通信系统项目演讲稿

各位评委老师好，今天我将介绍我们团队开发的局域网安全通信系统。该系统基于DES加密算法实现，主要包含客户端和服务端两大模块，支持群组聊天、私聊和广播三种通信模式。

在连接建立方面，客户端通过socket API创建TCP连接。服务端采用多线程架构，每个新连接都会创建独立线程进行处理。我们在Windows环境下使用Winsock库实现网络通信，服务端默认监听5000端口，客户端通过127.0.0.1进行本地测试。

通信协议设计采用"TYPE|TARGET|CONTENT"的格式。消息类型包含登录、创建群组、群发消息等六种指令。数据加密前会进行PKCS#7填充确保8字节对齐，采用CBC加密模式增强安全性，并通过HMAC-SHA1进行完整性校验。

DES加密是本系统的核心模块。我们实现了完整的加密流程：64位明文经过初始置换后分割为32位左右半区，经过16轮Feistel网络处理，最后进行逆初始置换生成密文。密钥生成阶段通过56位置换和16次循环移位，产生16组48位子密钥。每轮加密使用扩展置换将32位数据扩展为48位，与子密钥异或后经S盒置换压缩回32位。

特别要说明的是Feistel网络的设计特点：每轮只处理一半数据，通过异或操作实现可逆加密。这种结构保证了加密解密的对称性，解密过程只需反向使用子密钥。我们还实现了CBC模式，通过初始化向量增强相同明文的密文随机性。

在多设备支持方面，服务端使用哈希表维护群组与成员的映射关系，每个客户端连接对应独立线程。客户端状态机记录用户加入的群组和创建的群组，实现权限分级管理。当用户发送群消息时，服务端会遍历群组成员列表进行消息路由。

测试环节我们构建了完整的验证流程：服务端编译后启动监听，多个客户端实例并行连接。通过发送创建群组、加入群组、发送消息等指令验证系统功能。加密测试模块使用标准测试向量验证DES实现的正确性，包括密钥已知情况下的密文比对。

实际演示时，可以观察到加密后的网络数据包内容完全不可读，而解密后能准确还原原始消息。系统支持同时20个客户端稳定连接，消息端到端延迟小于100ms。经过压力测试，单服务端可承载200个并发连接，满足中小型办公环境需求。

未来我们计划增加RSA密钥交换机制，实现更安全的混合加密方案。同时优化线程池管理，提升高并发场景下的性能表现。以上就是本项目的核心内容，欢迎各位老师提问指导。