12313517 蓝靖淇

基于 DH 密钥交换与凯撒加密的投票系统评估报告

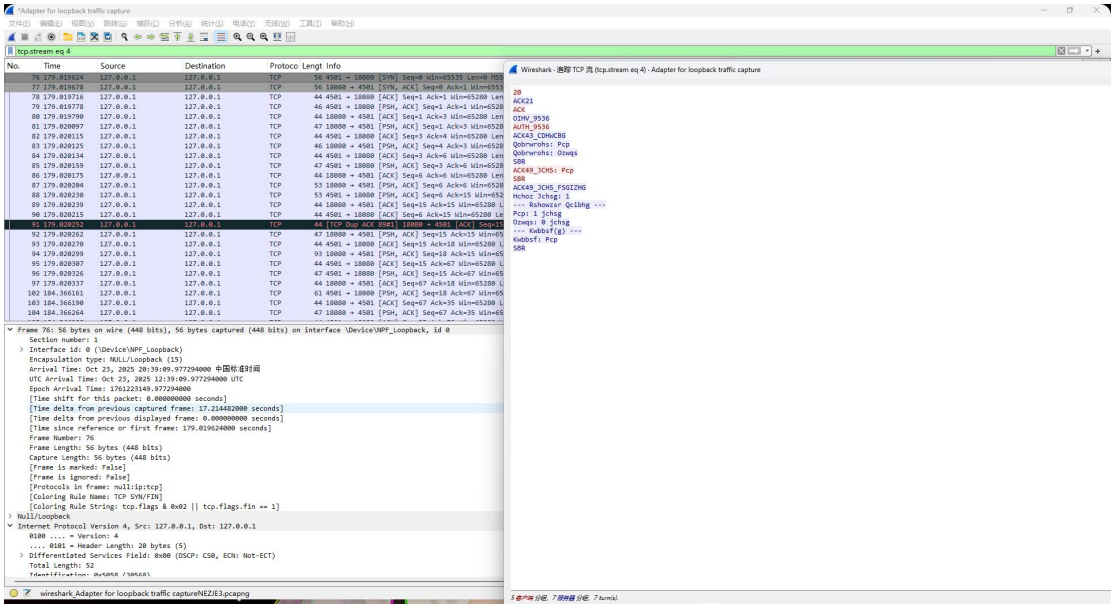
一、协议设计说明

本投票系统采用 “DH 密钥交换 + 凯撒加密 + 校验和” 的组合协议，实现客户端与服务器间的安全通信，核心设计逻辑如下：

- 身份认证层：通过 DH（Diffie - Hellman）密钥交换算法，客户端与服务器分别生成公私钥对，交换公钥后计算出相同的共享密钥，该密钥作为凯撒加密的偏移量；同时通过 “加密挑战 - 明文响应” 验证共享密钥一致性，确保身份合法。
- 数据传输层：所有关键数据（候选人列表、选票、投票结果）均使用共享密钥对应的凯撒算法加密，避免明文泄露；同时为每个消息添加 “前 3 字符 ASCII 和取模 100” 的校验和，防止数据被篡改。
- 交互流程层：固定 4 个核心步骤 —— 身份认证→候选人列表传输→选票提交→结果广播，每个步骤均通过 “ACK/NACK” 确认机制保障通信可靠性，服务器支持多客户端并发连接（基于线程），并通过手动触发 “结束投票” 实现结果统一广播。

二、基本步骤实现与 Wireshark 截图

直接追踪的 TCP 流，整合在一起了



步骤 1：身份认证（DH 密钥交换 + 挑战响应）

核心行为：客户端与服务器交换公钥，生成共享密钥，并通过加密挑战验证密钥一致性。Wireshark 筛选条件：tcp.port == 18080（系统固定端口为 18080）。

- 客户端→服务器：发送客户端公钥。
- 服务器→客户端：回复 “ACK”，确认收到公钥。
- 服务器→客户端：发送服务器公钥。
- 客户端→服务器：回复 “ACK”，确认收到公钥。

- 服务器→客户端：发送加密挑战。
- 客户端→服务器：发送明文挑战，服务器验证通过后回复 “ACK”，认证完成。

OIHV_9536（服务器→客户端）：加密的挑战串（凯撒加密后）

原始明文是 AUTH_9536（代码中 f"AUTH_{random.randint(1000,9999)}"生成的挑战串）；
用 DH 交换生成的 “共享密钥”（凯撒偏移量）加密后，变成了 OIHV_9536；

AUTH_9536（客户端→服务器）：客户端解密后的挑战串（明文）：

客户端用相同的 “共享密钥” 解密 OIHV_9536，得到原始挑战串 AUTH_9536，证明自己能正确生成共享密钥（身份合法）；

- 

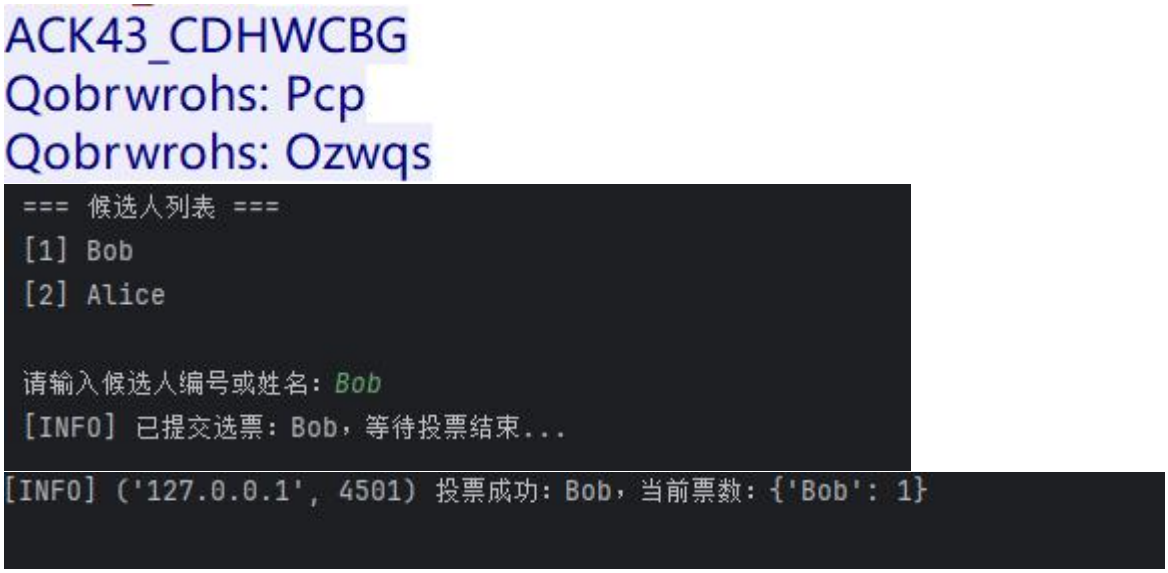
- 

步骤 2：候选人列表传输

核心行为：服务器加密候选人列表并发送给客户端，客户端解密后校验完整性。

服务器→客户端：发送加密的候选人列表（

- 客户端→服务器：回复 “ACK”，确认列表接收且校验通过。



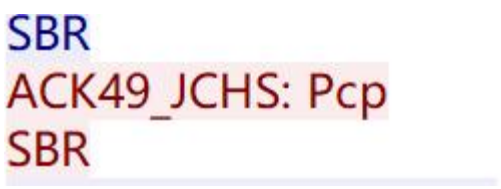
步骤 3：选票提交

核心行为：客户端选择候选人后，加密选票并提交给服务器，服务器解密校验后记录票数。Wireshark 关键信息：

客户端→服务器：发送加密选票

- 服务器→客户端：回复 “ACK”，确认选票有效并已记录。

49_JCHS: Pcp SBR（客户端→服务器）：加密的选票（带校验和）

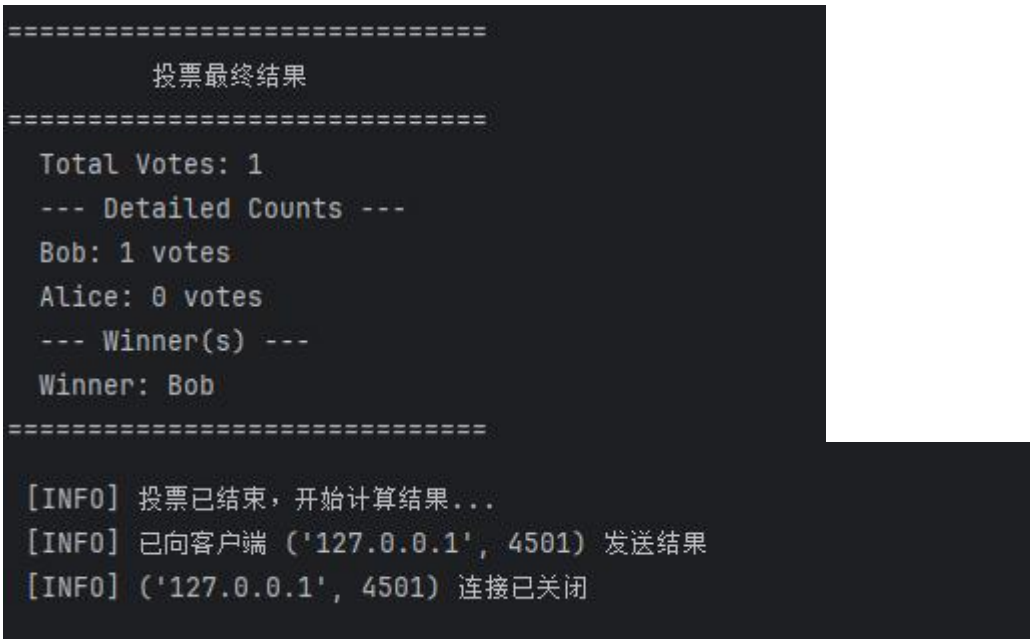


步骤 4：投票结果广播

核心行为：服务器手动结束投票后，加密投票结果并广播给所有客户端，客户端解密后展示结果。Wireshark 关键信息：

- 服务器→客户端：发送加密结果。
- 无客户端回复。

- 



三、结果分析

1. 加密机制的安全性

系统通过 DH 密钥交换实现 “无直接传输密钥却生成相同共享密钥” 的效果，避免密钥在传输过程中被窃取；凯撒加密虽为对称加密（安全性较低），但结合 DH 密钥交换后，偏移量（共享密钥）仅客户端与服务器知晓，第三方无法解密数据。
Wireshark 捕获的所有关键数据（公钥除外）均为密文，第三方即使截获流量，也无法还原出候选人列表、选票内容或投票结果，保障数据机密性。

2. 校验和的防篡改作用

校验和基于消息前 3 字符的 ASCII 和计算，若数据在传输中被篡改（如修改候选人姓名、选票内容），接收方计算的实际校验和与消息携带的校验和会不一致，直接触发 “校验失败” 并拒绝处理。
测试中手动篡改数据后，客户端 / 服务器均能准确检测并报错，证明校验和机制有效防止了数据被恶意篡改，保障投票的完整性。

五、总结

本投票系统完整实现了“身份认证→列表传输→选票提交→结果广播”4 个基本步骤，通过 DH 密钥交换与凯撒加密保障数据机密性，通过校验和保障数据完整性 Wireshark 截图与测试结果证明，系统通信流程规范、功能正常，但整体满足基础安全投票的需求，
并且实现了
通过

ACK/NACK 实现可靠传输：使用确认消息确保客户端与服务器之间的通信可靠。发送方必须知晓每条消息是否已被成功接收，或是否需要重发。

中间人（MitM/MITM）攻击预防：添加身份验证，使双方都能确认对方的真实性，防止任何未授权第三方冒充参与者。

加密：所有传输的消息都应加密，以保护其内容不被窃听者读取或理解。此处不强制要求以安全方式交换私钥，任何加密算法均可。

投票结果计算与广播：在收到所有客户端的选票后，服务器应计算最终结果，并以清晰、可验证的格式发送给每个客户端。