|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 包 | 对（datacrc+protoID+dataSize）组成的byte[] 进行计算而得到 | 对（数据内容）进行crc计算而得到 | 协议号 | 数据内容的字节长度 | 数据内容 |
| 字段 | headcrc | datacrc | protoID | dataSize | data |
| 类型 | int | int | int | int | byte[] |
| 字节数 | 4 | 4 | 4 | 4 | dataSize |

1.crc校验

2.加密，解密

介绍：

不可逆加密：md5 ，sha1，加密后就不能解密，只能用于存储密码和校验文件变动，不能用网络通讯

可逆对称加密**：DES，3DES，AES**

可逆非对称加密**： RSA**

选定：对称加密：DES 非对称加密：RSA

.net有封装好的，DESCryptoServiceProvider, RSACryptoServiceProvider

流程：

**一般流程为：先用非对称加密去加密对称加密的密钥(对称加密的密钥比较短，可视为不怎么耗时) ，然后再用对称加密去加密数据。**

客户端用RSA生成公钥和私钥，发送公钥给服务器，服务器用收的公钥对3DES的key进行加密后，发还给客户端，客户端用私钥进行解密得到3DES的key，之后就可以用此key来进行加密解密。

3.数据内容形式：json, protobuf-net, protobuf-java, pbc, pb-lua-gen, sproto

选定:Client：pbc Server: protobuf-java