A）所有Client和Sever端都需要RSA信息

RSA信息初始化：通过调用RSA.rsa获取一个int rsa[ ]：

(公钥)pk=rsa[3],（私钥）sk=rsa[4], （参数）n=rsa[2];

通信时使用RSA加密：

发送信息加密调用方法 RSA.encode(String data, int pk_c, int n_c);

收到信息解密调用方法 RSA.decode(String data, int sk_s, int n_s);

B）会话密钥即$Client$的注册密码

C）报文调用函数参数以及返回值对照

*IPs：发送方IP

IPr：接收方IP（IP输入时均不带点，且不足位数不足要用0补齐，如“192168001001”）

所有的输入输出均为明文，二进制转换，报文的加密在方法内部完成

“m1”为报文包，输入对应参数就可生成报文，返回值为字符串

“m1_d”为对应报文的解码包，返回值为字符串数组，数组内内容均为已经写好格式的明文，如IP（192.168.1.1，已加点），可以直接查看，每个包内的内容排序如表格

m1(String ID_c, String ID_tgs, String Ts1,String IPs,String IPr) {//C->AS 发起请求

m1_d(String data)

info[0]= IDc
info[1]= IDtgs
info[2]= TS1

m2(String ID_tgs, String Ts2, String lifetime, String Kc_tgs, String TGT,String IDc,String IPs,String IPr) {//AS->C 回复

m2_d(String data,String IDc)

info[0]= IDtgs
info[1]= TS2
info[2]= LT1
info[3]= Kc_tgs
info[4]= TGT

TGT(String Kc_tgs,String ID_c,String AD_c,String ID_tgs, String Ts2,String LT1,int Pk_tgs,int n)

TGT_d(String data,int sk,int n){//RSA TGSPk 公钥加密

info[0]=data.substring(0,8);//Kc_tgs
info[1]= IDc
info[2]= ADc
info[3]= IDtgs
info[4]= TS2
info[5]= LT1

m3(String ID_v, String TGT, String ID_c, String AD_c, String TS_3,String Kc_tgs,String IPs,String IPr) {//C->TGS 发起请求

m3_d(String data,String Kc_tgs)

info[0]= IDv
info[1]= TGT
info[2]= IDc
info[3]= ADc
info[4]= TS3

m4(String Kc_v, String ID_v, String TS4,String ST,String Kc_tgs,String IPs,String IPr)
m4_d(String data,String Kc_tgs)

info[0]=data.substring(0,8);//Kc_v
info[1]= IDv
info[2]= TS4
info[3]= ST

ST(String Kc_v, String ID_c, String AD_c, String IDv, String TS4, String lifetime2)
ST_d(String data,String Kc_v)

info[0]= Kc_v
info[1]= Dc
info[2]= ADc
info[3]= IDv
info[4]= TS4
info[5]= LT2

m5(String ST, String IDc, String ADc,String TS5,String Kc_v,String IPs,String IPr) //C->S

发起请求

public String[] m5_d(String data,String Kc_v)

info[0]= ST
nfo[1]= IDc
info[2]= ADc
info[3]= TS5

m6 (String TS5,String Kc_v,String IPs,String IPr) //S->C 回复

m6_d(String data,String Kc_v)

info[0]= TS5

m7(String ID_c,String K_c,int pk,int n,String IPs,String IPr)//C->A 提交注册请求

m7_d(String data,int sk,int n)

info[0]= IDc
info[1]= Kc

m8(Boolean FB,int sk,int n,String IPs,String IPr)//AS 反馈

m8_d(String data,int k,int n)

info[0]= 反馈信息

m9(String Kc_v,String IPs,String IPr)//刷新目录

m9_d(String data,String Kc_v)

info[0]= Sys order

m10(String n,String name,String Kc_v,String IPs,String IPr)//S->C 返回文件目录数据

m10_d(String data,String Kc_v)

info[0]= num
info[1]= name 文件名间用星号隔开，需拆分至数组

m11(String name,String sum,String num,String file,String Kc_v,String IPs,String IPr)//C->S 上传文件

m11_d(String data,String Kc_v){

info[0]= name
info[1]= 文件总片数
info[2]= 当前序号
info[3]= 文件数据

m12(String order,String send,String k,String IPs,String IPr)//ack

m12_d(String data,String K)

info[0]=命令反馈
info[1]=发送反馈

m13(String filename,String Kc_v,String IPs,String IPr)//C->S 发送下载请求

m13_d(String data,String kc_v)

info[0]= file name

m14(String filename,String sum,String num,String file,String Kc_v,String IPs,String IPr)//S->C 发送指定文件

m14_d(String data,String Kc_v)

info[0]= file name
info[1]=文件总片数
info[2]=当前序号
info[3]=文件数据

m15(String IDc,String Kc,String lTS,int pk,int n,String IPs,String IPr)//AS->TGS 同步注册信息

m15_d(String data,int k,int n)

info[0]= IDc
info[1]= Kc
info[2]= LTS

m16(String IDc,String TS4,int pk,int n,String IPs,String IPr)//TGS->AS 同步时间戳

m16_d(String data,int k,int n)

info[0]= IDc
info[1]=TS4

m17(String sys_m,int pk,int n,String IPs,String IPr)//AS->C 错误信息反馈

m17_d(String data,int k,int n)

info[0]=错误信息

m18(String sys_m,int pk,int n,String IPs,String IPr)//TGS->C 错误信息

m18_d(String data,int k,int n)

info[0]=错误信息

m19(String sys_m,String Kc_v,String IPs,String IPr)//S->C 错误信息
m19_d(String data,String Kc_v){

info[0]=错误信息

m20(String filename,String Kc_v,String IPs,String IPr)//C->S 上传请求
m20_d(String data,String Kc_v)

info[0]= File name

m21(String filename,String Kc_v,String IPs,String IPr)//C->S 删除指定文件
m21_d(String data,String Kc_v)

info[0]= File name

m22(String order_fb,String delete_fb,String k,String IPs,String IPr)/S->C 返回删除结果

info[0]=命令反馈
info[1]=删除反馈（00：失败，11 成功）

m23a(String state,String IDc,int pk,int n,String IPs,String IPr)//C->AS 发送离线请求
m23a_d(String data,int sk,int n)

info[0]=status
info[1]=IDc

m23s(String state,String IDc,String Kc_v,String IPs,String IPr)//C->S 发送离线请求
m23s_d(String data,String Kc_v)

info[0]= status
info[1]= IDc

m24(String offl_fb,String Kc_v,String IPs,String IPr)//S->C 离线反馈
m24_d(String data,String Kc_v)

info[0]= sys_info