通讯加密说明

# 安全性设计

网信客户端与网信服务器之间的关键数据传输，通过加密算法对数据进行加密。客户端与服务端之间的数据传输使用RSA和AES混合加密的方式进行数据加密。服务端与客户端通过相同的算法生成RSA公钥；客户端保有RSA公钥，服务端保有RSA公钥和私钥。数据传输交互过程中，如服务端发现客户端的RSA公钥失效或非法，则重新向客户端下发RSA公钥。

# 传输加密流程



1. 客户端登录时，客户端用RSA公钥加密AES密钥，且用AES密钥加密登录数据包；
2. 服务端收到客户端登录数据包，用RSA私钥解出AES密钥，用AES密钥解出AES加密的登录数据包；
3. 服务端用AES密钥加密登录应答包，并发给客户端；
4. 客户端收到登录应答包后使用AES密钥解密登录应答包，完成登录过程；
5. 客户端与服务端之间进行正常数据传输，使用AES密钥加密、解密传输数据。

# 加密算法简介

AES:密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院 （NIST）于2001年11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效的标准。2006年，高级加密标准已然成为对称密钥加密中最流行的算法之一。高级加密标准，是下一代的加密算法标准，速度快，安全级别高。

# 工具使用说明

利用encodersa源代码， 编译生成加密工具生成一对非对称RSA公钥， 客户端和服务器保存RSA公钥，用于登录时加密使用。

1. **encodersa 应用程序概要**
   1. encodersa.vcproj这是使用应用程序向导生成的 VC++ 项目的主项目文件，其中包含生成该文件的 Visual C++ 的版本信息，以及有关使用应用程序向导选择的平台、配置和项目功能的信息。
   2. encodersa.cpp 这是主应用程序源文件。
   3. 其他标准文件：StdAfx.h, StdAfx.cpp这些文件用于生成名为 encodersa.pch 的预编译头 (PCH) 文件和名为 StdAfx.obj 的预编译类型文件。
   4. 其他注释：应用程序向导使用“TODO:”注释来指示应添加或自定义的源代码部分。