**用户认证加密解密解决方案**

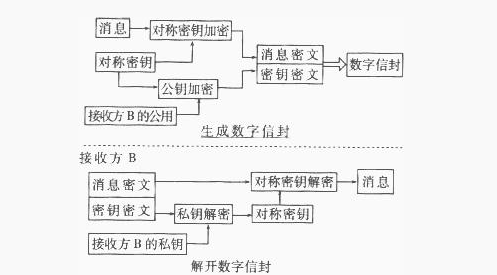
## 用户认证（数字信封）

数字信封是一种综合利用了对称加密技术和非对称加密技术两者的优点进行信息安全传输的一种技术。数字信封既发挥了对称加密算法速度快、安全性好的优点，又发挥了非对称加密算法密钥管理方便的优点。

## 应用

数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称数字信封）之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据(通信密钥)还原；数字信封拆解是使用私钥将加密过的数据解密的过程。



## 加密算法

对称加密（des）DES/ECB/NoPadding

非对称加密（rsa）RSA/ECB/PKCS1Padding

base64

md5

## 加密过程

### 客户端加密

1. 客户端唯一标识原文使用客户端随机生成8位秘钥des加密，密文base64后作为参数c
2. 客户端唯一标识原文md5截取16位拼接客户端随机生成8位秘钥 作为rsa加密原文
3. 使用rsa非对称加密算法公钥对步骤2拼接后的字符串进行加密，密文base64后作为参数k
4. 参数c与参数k作为接口必传参数

### 服务端解密

1. 服务端对k使用rsa算法，使用私钥对k进行解密，获取客户端随机8位秘钥与原文md5 16位拼接，截取获得客户端随机8位秘钥
2. 服务端使用步骤1获取的客户端随机8位秘钥对c进行des解密，获得客户端唯一标识

## java源码

