**23.** 加密算法

**23.1.1. AES**

高级加密标准(AES,Advanced Encryption Standard)为最常见的对称加密算法(微信小程序加密传输就是用这个加密算法的)。对称加密算法也就是加密和解密用相同的密钥，具体的加密流程如下图：



**23.1.2. RSA**

RSA加密算法是一种典型的非对称加密算法，它基于大数的因式分解数学难题，它也是应用最广泛的非对称加密算法。

非对称加密是通过两个密钥（公钥-私钥）来实现对数据的加密和解密的。公钥用于加密，私钥用于解密。 13/04/2018 Page 256 of 283





**23.1.3. CRC**

循环冗余校验(Cyclic Redundancy Check, CRC)是一种根据网络数据包或电脑文件等数据产生简短固定位数校验码的一种散列函数，主要用来检测或校验数据传输或者保存后可能出现的错误。它是利用除法及余数的原理来作错误侦测的。

**23.1.4. MD5**

MD5常常作为文件的签名出现，我们在下载文件的时候，常常会看到文件页面上附带一个扩展名为.MD5的文本或者一行字符，这行字符就是就是把整个文件当作原数据通过MD5计算后的值，我们下载文件后，可以用检查文件MD5信息的软件对下载到的文件在进行一次计算。两次结果对比就可以确保下载到文件的准确性。 另一种常见用途就是网站敏感信息加密，比如用户名密码，支付签名等等。随着https技术的普及，现在的网站广泛采用前台明文传输到后台，MD5加密（使用偏移量）的方式保护敏感数据保护站点和数据安全。

MD5Util.java

CryptoUtil.java

LicenseCoder.java

DESUtil

UrlUtils