**Java加密算法**

一、基本的单项加密算法：

BASE64 ：双向加密，严格地说，属于编码格式，而非加密算法。加密场景：常见于邮件、http加密，截取http信息。

MD5(信息摘要算法)：单向加密，加密场景：广泛用于加密和解密技术，常用于文件校验。

SHA(安全散列算法)：单向加密，加密场景：广泛地应用于电子商务等信息安全领域。

HMAC(，散列消息鉴别码)：单向加密，加密场景：消息鉴别码实现鉴别的原理是，用公开函数和密钥产生一个固定长度的值作为认证标识，用这个 标识鉴别消息的完整性。使用一个密钥生成一个固定大小的小数据块，即MAC，并将其加入到消息中，然后传输。接收方利用与发送方共享的密钥进行鉴别认证等。

二、复杂的对称加密（DES、PBE）、非对称加密算法：

DES(数据加密算法)：这是一种简单的加密解密方式，只有一个密钥。

PBE(基于密码验证)：其特点在于口令由用户自己掌管，不借助任何物理媒体；采用随机数杂凑多重加密等方法保证数据的安全性。

RSA(Ron Rivest, AdiShamir 和Leonard Adleman)：第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，也很流行。

DH(密钥一致协议)：允许两名用 户在公开媒体上交换信息以生成"一致"的、可以共享的密钥。

DSA(数字签名)：一种更高级的验证方式，用作数字签名。不单单只有公钥、私钥，还有数字签名。私钥加密生成数字签名，公钥验证数据及签名。如果数据和签名不匹配则认为验证失败！数字签名的作用就是校验数据在传输过程中不被修改。数字签名，是单向加密的升级！

ECC(椭圆曲线密码编码学)：在软件注册保护方面起到很大的作用，一般的序列号通常由该算法产生。