信息传递时需要进行加密与解密,尤其是网银系统安全及Web Service系统安全相关内容时。

# MD5

message-digest algorithm 5 （信息-摘要算法）缩写

广泛用于加密和解密技术，常用于文件校验

# SHA

Secure Hash Algorithm，安全散列算法

数字签名等密码学应用中重要的工具，被广泛地应用于电子商务等信息安全领域

# HMAC

Hash Message Authentication Code，散列消息鉴别码

基于密钥的Hash算法的认证协议。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。