4.6. 简述用杂凑函数来实现消息认证的三大类基本方式

答：1. 先对消息计算杂凑值，在对杂凑值进行对称加密，提供认证性和完整性服务，还分为带保密性和不带保密性两种方式。



2. 先对消息计算杂凑值，再前面签名再对称加密(也可以用收方公钥加密)，提供认证性、完整性和不可否认性，也分为带保密性和不带保密性两种方式



3. 连同秘密值一起对消息计算杂凑值，提供认证性和完整性，，也分为带保密性和不带保密性两种方式



6.2. 某用户A想要给用户B发送一个消息m，如果要对消息m的保密性与认证性进行保护，有四种方法，采用数据认证算法、先hash再加密、先签名再加密、HMAC

1. 请分别给出这几种方法下认证消息m的表达式。所需符号和算法自行定义和选取。
2. 其中安全性最强的和最弱的分别是哪一种方法，为什么

解：(1) 采用数据认证算法 m||*C*K(m)，C是初始向量为0的DES-CBC算法；先hash再加密 EK{m||H(m)}；先签名再加密:EK{m||Sigsk(H(m)}；HMAC：m||H(k||m)

（2）安全性最强的是先签名再加密方法，它同时能提供保密性、完整性、认证性和不可否认性；最弱的是数据认证算法和HMAC，它们只提供认证性和完整性。