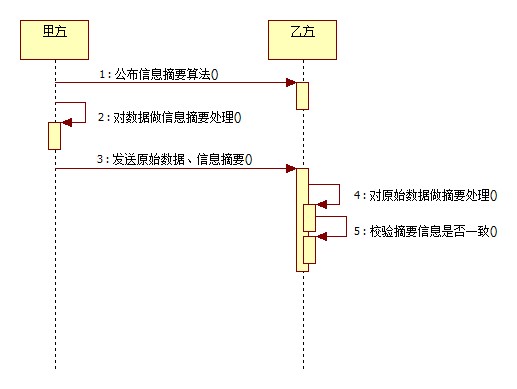
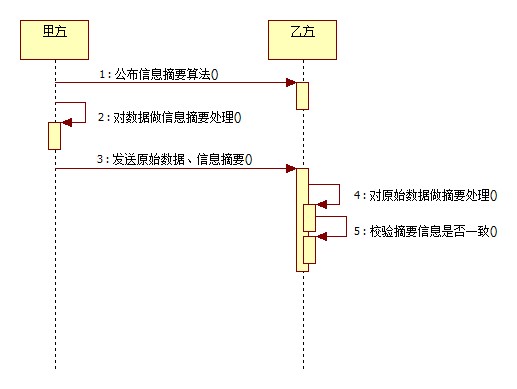
**MD5**

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。校验？不管文件多大，经过MD5后都能生成唯一的MD5值。现在的ISO校验，多是MD5校验。怎么用？当然是把ISO经过MD5后产生MD5的值。一般下载Linux-ISO的朋友都见过下载链接旁边放着MD5的串。就是用来验证文 件是否一致的。



**SHA**

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。虽然，SHA与MD5通过碰撞法都被破解了，但是SHA仍然是公认的安全加密算法，较之MD5更为安全。



**HMAC**

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。

