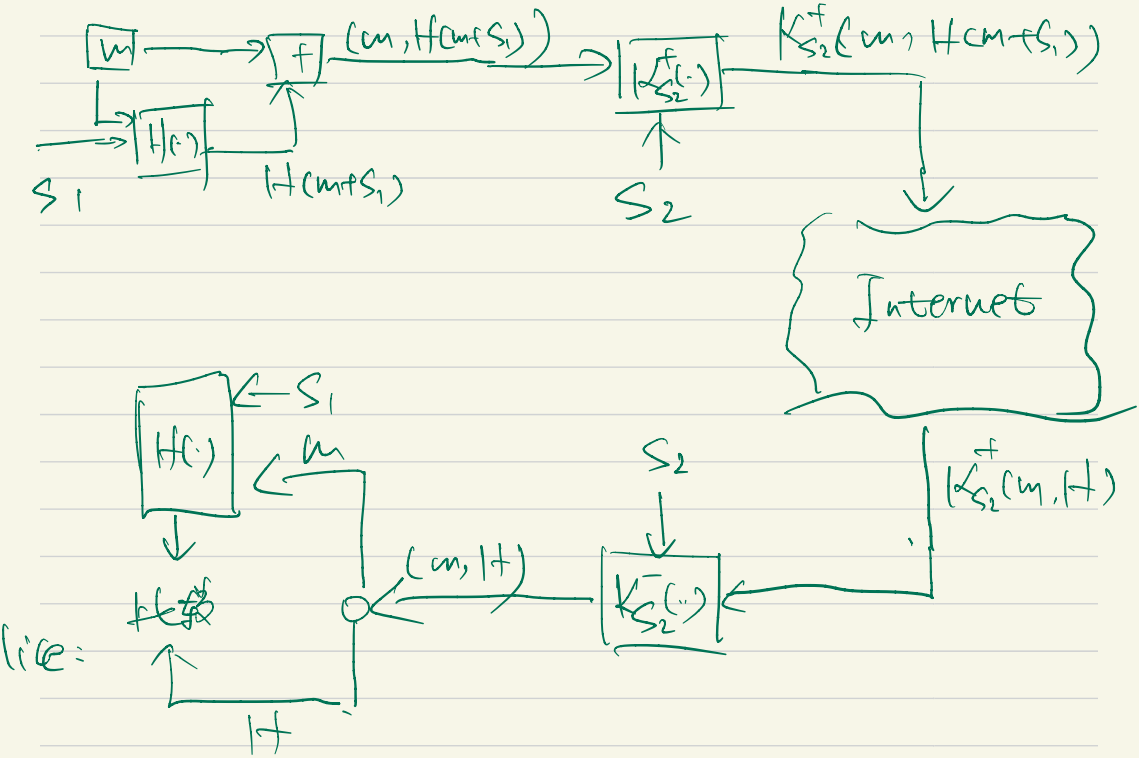
第八章作业 (2022-3-26)

P12

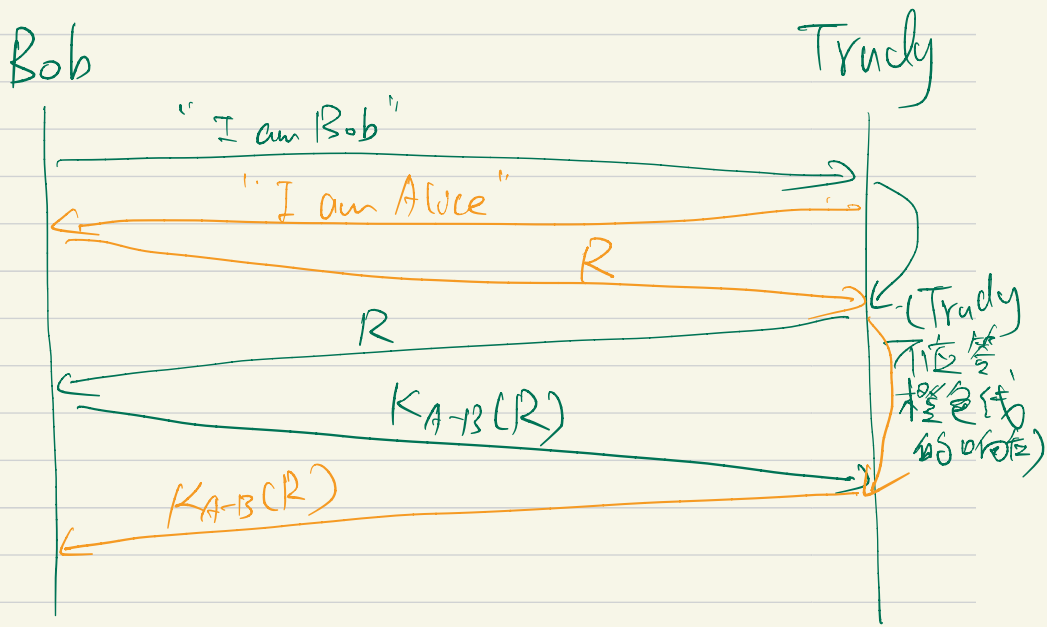
Bob:



☆ P14

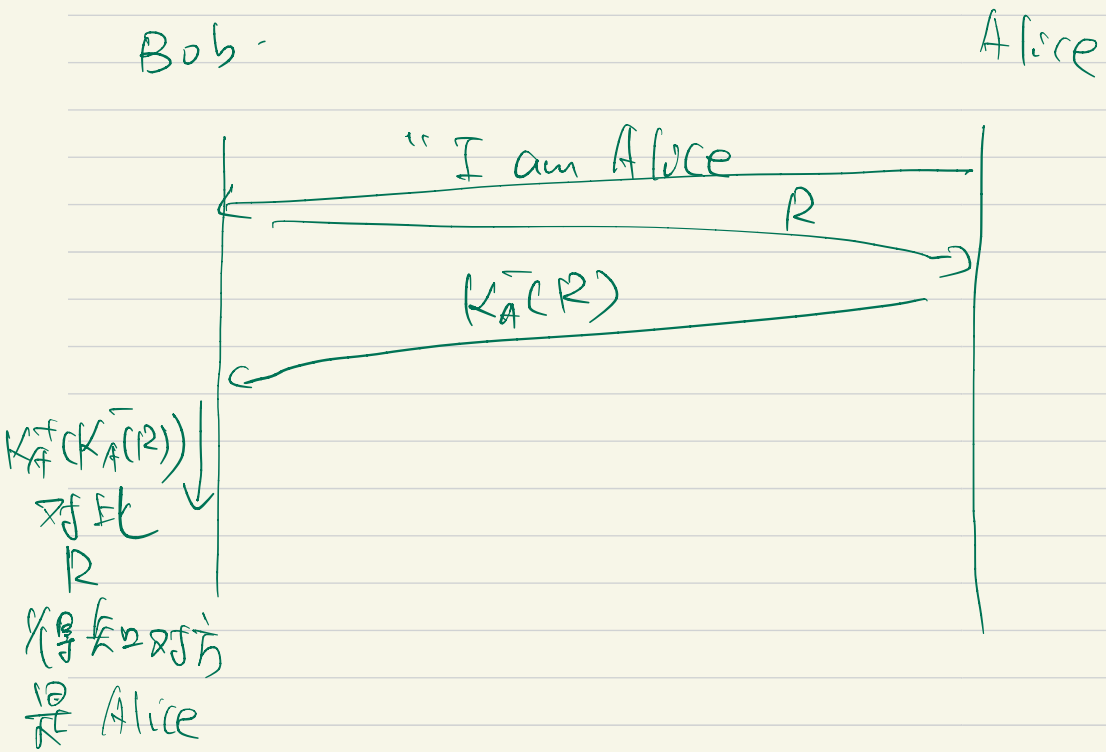
数字签名需要CA颁发的公钥，但对于OSPF，所有路由器都位于同一个域中，管理者可以很容易的分发对称钥匙给每个路由器，不需要公钥。

☆ P15



P16

a.)



b.) 当 Trudy 向 Bob 假装自己是 Alice，Bob 向 Trudy 发送 nonce 字段 R，Trudy 用自己的私钥加密 R 发送给 Bob，因为没有 CA 验证 Trudy 的公钥不是 Alice，所以

Bob 错把 Trudy 的公钥解密出 R，
于是错认了 Trudy 为 Alice.

☆ 20

Trudy 也是可以删掉其中的 TCP 段，她只要调整 Alice 发送给 Bob 的包中的 sequence number 和 Bob 发送给 Alice 的答复包中的 acknowledgement number 即可.

这可导致 Bob 丢失掉一些包

☆ 21

SSL 最终不包接收这个 bogus packet.
因为数据完整性校验不通过，Alice与Bob可通过共享密钥进行数据包的完整性校验

23

若Trudy插入一些数据在流中，R2可以通过数据完整性校验把这些数据删了。

若Trudy进行replay attack，R2可以通过检查ESP头部的sequence number，删掉有重复sequence number的包。