**1.**挑战应答方式是由验证方发送一个随机串给示证方，示证方用密钥加密后返回给验证方，验证方通过相同的密钥解密来验证身份，只涉及两方操作。

Needham-Schroeder则存在可信任的第三方，由第三方作为中介，通过分别与两方产生密钥建立联系，最终用第三方产生的密钥建立联系。

可以建立一个类似于Needham-Schroeder的方法：

①

②

③

④

⑤

**2.**

①首先由客户端向AS端发送自己的用户标识，要访问的TGS标识和时间戳。

AS接受到后用与客户端均有的对称密钥加密产生的用于客户端和TGS通信的密钥，以及其他的信息和用TGS特有的密钥加密的表明要通信的客服端C的信息。

②客户端得到AS发送的信息后解密，向TGS发送得到的、自己要访问的服务器端标识信息和用于验证时效性的信息。

TGS接收到后验证客户端的身份，并向客户端返回用加密后的用于客户端和服务器端通信的密钥，等信息，是用服务器的密钥加密客户端身份信息和要与客户端通信的密钥。

③客户端解密得到了与服务器通信用的密钥后，发送和用于验证时效性的信息。

服务器端用密钥解密验证身份信息并得到与客户端通信的密钥。服务器端用得到的密钥加密时间戳的信息给客户端向客户端表明身份。

**3.** 数字证书是一个经过权威的、可信赖的、公正的第三方机构（即CA认证中心，Certificate Authority）签名的包含拥有者信息及公开密钥的文件。

①A提交资料申请证书

②CA审核并颁发用CA的私钥签名的数字证书

③A向B发送用A的私钥签名的特定信息和数字证书

④B获取CA的公钥并对A发送的数字证书进行验证，验证通过则可获得A的公钥，得到A的公钥后即可对A用私钥签名的特定信息解密，从而确认A的身份及签名的信息。

**4.** PKI是一种遵循一定标准的密钥管理基础平台，为所有网络应用提供加密和数字签名等密码服务所必需的密钥和证书管理。

包含的功能有：

1.接收验证用户数字证书的申请；

2.确定是否接受用户数字证书的申请；

3.向申请者颁发（或拒绝颁发）数字证书；

4.接收、处理用户的数字证书更新请求；

5.接收用户数字证书的查询、撤销；

6.产生和发布证书的有效期；

7.数字证书的归档；

8.密钥归档；

9.历史数据归档。

PKI的认证机构完成数字证书的申请注册、证书签发和管理，在生成证书时会完成密钥的备份，当用户丢失密钥需要恢复时，可以通过备份恢复。当用户密钥泄露或其他原因需要撤销原来的证书时，可将原证书加入黑名单。证书库供公众查询颁发和撤销的证书，且提供专门的PKI应用接口供人使用。

**5.** 证书链是由一串数字证书链接而成的，证书链通过使用上层私钥对下层的证书进行数字签名构成。如**KRA《CAB》KRB《CAC》KRC《CAD》KRD《CAa》**即用A的私钥在B的证书上签名，用B的的私钥在C的证书上签名。

如上述例子，若用户需要得到a的公钥，则需要查看由D签名的A的数字证书。而得到D的公钥又需要查看D的数字证书得到，则需得到C的公钥以此类推，直到用户得到最顶层的公钥，逐层向下身份认证从而得到a的公钥。